

210-260

Number: 210-260
Passing Score: 800
Time Limit: 120 min
File Version: 1



VCE to PDF Converter : <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : https://twitter.com/VCE_Plus

Google+ : <https://plus.google.com/+Vcepluscom>

LinkedIn : <https://www.linkedin.com/company/vceplus>

210-260

VCE To PDF - Free Practice Exam

Implementing Cisco Network Security

Exam A**QUESTION 1**

Which two services define cloud networks? (Choose two.)

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

Correct Answer: AB

Section: (none)

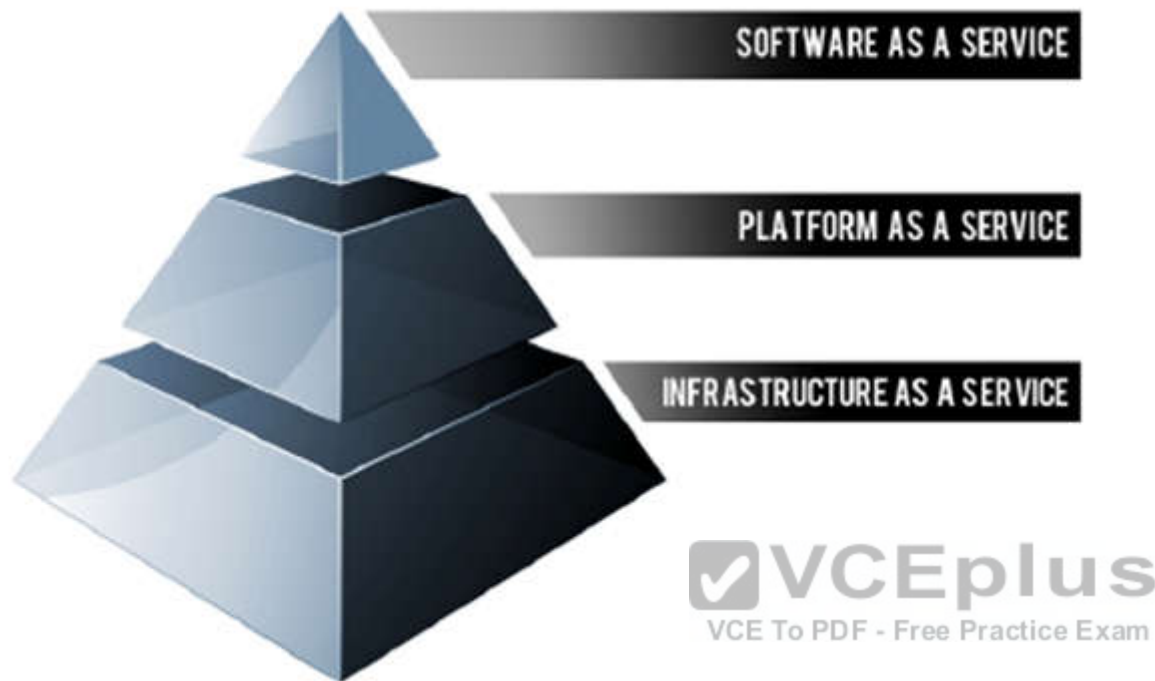
Explanation

Explanation/Reference:

Explanation:

The diagram below depicts the Cloud Computing stack – it shows three distinct categories within Cloud Computing: Software as a Service, Platform as a Service and Infrastructure as a Service.





A simplified way of differentiating these flavors of Cloud Computing is as follows;

- SaaS applications are designed for end-users, delivered over the web
- PaaS is the set of tools and services designed to make coding and deploying those applications quick and efficient
- IaaS is the hardware and software that powers it all – servers, storage, networks, operating systems

Reference: <https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas/>

QUESTION 2

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Out-of-band refers to an interface that allows only management protocol traffic to be forwarded or processed. An out-of-band management interface is defined by the network operator to specifically receive network management traffic. The advantage is that forwarding (or customer) traffic cannot interfere with the management of the router, which significantly reduces the possibility of denial-of-service attacks.

Out-of-band interfaces forward traffic only between out-of-band interfaces or terminate management packets that are destined to the router. In addition, the out-of-band interfaces can participate in dynamic routing protocols. The service provider connects to the router's out-of-band interfaces and builds an independent overlay management network, with all the routing and policy tools that the router can provide.

Reference: http://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-0/security/configuration/guide/b_sc40asr9kbook/b_sc40asr9kbook_chapter_0101.pdf

QUESTION 3

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

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

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

TACACS+ uses Transmission Control Protocol (TCP) port 49 to communicate between the TACACS+ client and the TACACS+ server. An example is a Cisco switch authenticating and authorizing administrative access to the switch's IOS CLI. The switch is the TACACS+ client, and Cisco Secure ACS is the server.

TACACS+ communication between the client and server uses different message types depending on the function. In other words, different messages may be used for authentication than are used for authorization and accounting. Another very interesting point to know is that TACACS+ communication will encrypt the entire packet.

Reference: <http://www.networkworld.com/article/2838882/radius-versus-tacacs.html>

QUESTION 4

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

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

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

ACL-DEFAULT allows DHCP, DNS, ICMP, and TFTP traffic and denies everything else.

Reference: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_Wired.html

QUESTION 5

Which two next-generation encryption algorithms does Cisco recommend? (Choose two.)

- A. AES
- B. 3DES
- C. DES
- D. MD5
- E. DH-1024
- F. SHA-384

Correct Answer: AF

Section: (none)

Explanation

Explanation/Reference:

Answer: A, F

Explanation:

The following table shows the relative security level provided by the recommended and NGE algorithms. The security level is the relative strength of an algorithm. An algorithm with a security level of x bits is stronger than one of y bits if $x > y$. If an algorithm has a security level of x bits, the relative effort it would take to "beat"

the algorithm is of the same magnitude of breaking a secure x-bit symmetric key algorithm (without reduction or other attacks). The 128-bit security level is for sensitive information and the 192-bit level is for information of higher importance.

| Algorithm | Security Level |
|--|----------------|
| AES-128 DH, DSA, RSA-3072 SHA-256 ECDH, ECDSA-256 | 128 bits |
| AES-192 SHA-384 ECDH, ECDSA-384 | 192 bits |
| AES-256 SHA-512 ECDH, ECDSA-521 | 256 bits |

Reference: <http://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html>

QUESTION 6

Which three ESP fields can be encrypted during transmission? (Choose three.)

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

Correct Answer: DEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The remaining four parts of the ESP are all encrypted during transmission across the network. Those parts are as follows:

- The *Payload Data* is the actual data that is carried by the packet.
- The *Padding*, from 0 to 255 bytes of data, allows certain types of encryption algorithms to require the data to be a multiple of a certain number of bytes. The padding also ensures that the text of a message terminates on a four-byte boundary (an architectural requirement within IP).
- The *Pad Length* field specifies how much of the payload is padding rather than data.
- The *Next Header* field, like a standard *IP Next Header* field, identifies the type of data carried and the protocol.

Reference: http://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/ip_security/provisioning/guide/IPsecPG1.html

QUESTION 7

What are two default Cisco IOS privilege levels? (Choose two.)

- A. 0
- B. 1
- C. 5
- D. 7
- E. 10
- F. 15



Correct Answer: BF

Section: (none)

Explanation

Explanation/Reference:

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.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfpass.html#wp1001016

QUESTION 8

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

- A. plaintext
- B. MD5
- C. HMAC

- D. AES 256
- E. SHA-1
- F. DES

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

These are the three different types of authentication supported by OSPF.

- **Null Authentication**—This is also called Type 0 and it means no authentication information is included in the packet header. It is the default.
- **Plain Text Authentication**—This is also called Type 1 and it uses simple clear-text passwords.
- **MD5 Authentication**—This is also called Type 2 and it uses MD5 cryptographic passwords.

Authentication does not need to be set. However, if it is set, all peer routers on the same segment must have the same password and authentication method. The examples in this document demonstrate configurations for both plain text and MD5 authentication.

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

QUESTION 9

Which two features do CoPP and CPPr use to protect the control plane? (Choose two.)

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

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

- A. They compare the 5-tuple of each incoming packet against configurable rules.

- B. They cannot track connections.
- C. They are designed to work most efficiently with stateless protocols such as HTTP or HTTPS.
- D. Cisco IOS cannot implement them because the platform is stateful by nature.
- E. The Cisco ASA is implicitly stateless because it blocks all traffic by default.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

However, since iptables and Netfilter were introduced and connection tracking in particular, this option was gotten rid of. The reason for this is that connection tracking can not work properly without defragmenting packets, and hence defragmenting has been incorporated into conntrack and is carried out automatically. It can not be turned off, except by turning off connection tracking. Defragmentation is always carried out if connection tracking is turned on.

Reference: <http://www.iptables.info/en/connection-state.html>

QUESTION 11

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.

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cisco Host based IPS can generate alerts based on behavior at desktop level. They can also be more restrictive in policies than network based IPS. And you can view encrypted files using Host-based IPS solution.

Reference: <http://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=3>

QUESTION 12

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

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

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The following actions require the device to be deployed in Inline mode and are in affect for a user- configurable default time of 3600 seconds (60 minutes).

Deny attacker inline: This action is the most severe and effectively blocks all communication from the attacking host that passes through the IPS for a specified period of time. Because this event action is severe, administrators are advised to use this only when the probability of false alarms or spoofing is minimal.

Deny attacker service pair inline: This action prevents communication between the attacker IP address and the protected network on the port in which the event was detected. However, the attacker would be able to communicate on another port that has hosts on the protected network. This event action works well for worms that attack many hosts on the same service port. If an attack occurred on the same host but on another port, this communication would be allowed. This event action is appropriate when the likelihood of a false alarm or spoofing is minimal.

Deny attacker victim pair inline: This action prevents the attacker from communicating with the victim on any port. However, the attacker could communicate with other hosts, making this action better suited for exploits that target a specific host. This event action is appropriate when the likelihood of a false alarm or spoofing is minimal.

Deny connection inline: This action prevents further communication for the specific TCP flow. This action is appropriate when there is the potential for a false alarm or spoofing and when an administrator wants to prevent the action but not deny further communication.

Deny packet inline: This action prevents the specific offending packet from reaching its intended destination. Other communication between the attacker and victim or victim network may still exist. This action is appropriate when there is the potential for a false alarm or spoofing. Note that for this action, the default time has no effect.

Modify packet inline: This action enables the IPS device to modify the offending part of the packet. However, it forwards the modified packet to the destination. This action is appropriate for packet normalization and other anomalies, such as TCP segmentation and IP fragmentation re-ordering.

Reference: <http://www.cisco.com/c/en/us/about/security-center/ips-mitigation.html>

QUESTION 13

When an IPS detects an attack, which action can the IPS take to prevent the attack from spreading?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

This action prevents the attacker from communicating with the victim on any port. However, the attacker could communicate with other hosts, making this action better suited for exploits that target a specific host. This event action is appropriate when the likelihood of a false alarm or spoofing is minimal.

Reference: <http://www.cisco.com/c/en/us/about/security-center/ips-mitigation.html>

QUESTION 14

What is an advantage of implementing a Trusted Platform Module for disk encryption?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A Trusted Platform Module (TPM) is a specialized chip on an endpoint device that stores RSA encryption keys specific to the host system for hardware authentication.

Each TPM chip contains an RSA key pair called the Endorsement Key (EK). The pair is maintained inside the chip and cannot be accessed by software. The Storage Root Key (SRK) is created when a user or administrator takes ownership of the system. This key pair is generated by the TPM based on the Endorsement Key and an owner-specified password.

Reference: <http://whatis.techtarget.com/definition/trusted-platform-module-TPM>

QUESTION 15

What is the purpose of the Integrity component of the CIA triad?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The I in CIA stands for Integrity — specifically, data integrity. The key to this component of the CIA Triad is protecting data from modification or deletion by unauthorized parties, and ensuring that when authorized people make changes that shouldn't have been made the damage can be undone.

Reference: <http://www.techrepublic.com/blog/it-security/the-cia-triad/>

QUESTION 16

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.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Addressing compliance is an integral part of security context. It implement rules to prevent vulnerability.

Reference: <http://www.cisco.com/security/>

QUESTION 17

Which type of secure connectivity does an extranet provide?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Extranet or external network provides secure connectivity to other company networks from your own company's network.

Reference: <http://searchenterprise.wan.techtarget.com/definition/extranet>

QUESTION 18

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Attackers build networks of infected computers, known as 'botnets', by spreading malicious software through emails, websites and social media. Once infected, these machines can be controlled remotely, without their owners' knowledge, and used like an army to launch an attack against any target. Some botnets are millions of machines strong.

Reference: <http://www.digitalattackmap.com/understanding-ddos/>

QUESTION 19

What type of security support is provided by the Open Web Application Security Project?

- A. Education about common Web site vulnerabilities.
- B. A Web site security framework.
- C. A security discussion forum for Web site developers.
- D. Scoring of common vulnerabilities and exposures.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

OWASP seeks to educate developers, designers, architects and business owners about the risks associated with the most common Web application security

vulnerabilities. OWASP, which supports both open source and commercial security products, has become known as a forum in which information technology professionals can network and build expertise. The organization publishes a popular Top Ten list that explains the most dangerous Web application security flaws and provides recommendations for dealing with those flaws.

Reference: <http://searchsoftwarequality.techtarget.com/definition/OWASP>

QUESTION 20

What type of attack was the Stuxnet virus?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Stuxnet virus is part of cyber warfare unleashed by governments to hinder their opponents computer systems and steal vital information.

Reference: <https://en.wikipedia.org/wiki/Stuxnet>

QUESTION 21

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Symmetric encryption (or pre-shared key encryption) uses a single key to both encrypt and decrypt data. Both the sender and the receiver need the same key to communicate.

Reference: <https://www.digicert.com/ssl-cryptography.htm>

QUESTION 22

Refer to the exhibit.

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

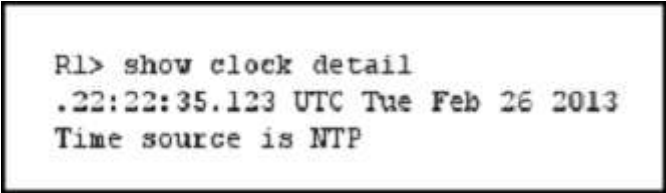
Explanation:

The read-only string attempted a write operation nine times as seen in the exhibit. It says, 9 illegal operations to community name supplied which means the read-only string attempted 9 write operations.

Reference: <http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

QUESTION 23

Refer to the exhibit.



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

Which statement about the device time is true?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The read-only string attempted a write operation nine times as seen in the exhibit. It says, 9 illegal operations to community name supplied which means the read-only string attempted 9 write operations.

Reference: <http://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

QUESTION 24

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.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When user LDAP authentication for VPN access has succeeded, the ASA queries the LDAP server, which returns LDAP attributes. These attributes generally include authorization data that applies to the VPN session. Thus, using LDAP accomplishes authentication and authorization in a single step.

Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/access_aaa.html

QUESTION 25

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.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The ACS console server provides the scalability, reliability and security a company requires to control and manage servers and other networked devices.

Reference: <http://www.uk.insight.com/content/dam/insight/EMEA/uk/shop/emerson/advanced-console-server.pdf> (page 2)

QUESTION 26

Refer to the exhibit.

```
authentication event fail action next-method
authentication event no-response action authorize vlan 101
authentication order mab dot1x webauth
authentication priority dot1x mab
authentication port-control auto
dot1x pae authenticator
```

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

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

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

Explanation:

Incorrect credentials supplied will result in failure to advance beyond webauth method. The authentication needs correct credentials as seen in the exhibit.

QUESTION 27

Which EAP method uses Protected Access Credentials?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

EAP-FAST is an EAP method that enables secure communication between a client and an authentication server by using Transport Layer Security (TLS) to establish a mutually authenticated tunnel. Within the tunnel, data in the form of type, length, and value (TLV) objects are used to send further authentication-related data between the client and the authentication server.

EAP-FAST supports the TLS extension as defined in RFC 4507 to support the fast re-establishment of the secure tunnel without having to maintain per-session state on the server. EAP-FAST-based mechanisms are defined to provision the credentials for the TLS extension. These credentials are called Protected Access Credentials (PACs).

Reference: http://www.cisco.com/c/en/us/td/docs/wireless/wlan_adapter/cb21ag/user/vista/1-0/configuration/guide/cb21ag10vistaconfigguide/eap_types.html

QUESTION 28

What is one requirement for locking a wired or wireless device from ISE?

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

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

Explanation:

To lock a wired or wireless device from ISE, you need to install ISE agent on that device first. The agent will assist in locking the device promptly.

QUESTION 29

What VPN feature allows traffic to exit the security appliance through the same interface it entered?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

This feature is useful for VPN traffic that enters an interface, but is then routed out of that same interface. For example, if you have a hub-and-spoke VPN network where the security appliance is the hub and the remote VPN networks are spokes, in order for one spoke to communicate with another spoke traffic must go to the security appliance and then out again to the other spoke.

Enter the same-security-traffic command in order to allow traffic to enter and exit the same interface.

ciscoasa(config)#same-security-traffic permit intra-interface

Reference: <http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html>

QUESTION 30

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When split tunneling is enabled, Internet traffic goes directly from your computer to the Internet and back without involving the VPN at all. Split tunneling also allows you to access other systems on your local network which is impossible if all traffic has to go to the corporate network first, although this can be mitigated in some configurations.

Reference: <http://www.tripwire.com/state-of-security/security-data-protection/36th-article-vpn-split-tunneling/>

QUESTION 31

Refer to the exhibit.


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

What is the effect of the given command sequence?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To create an IKE policy, enter the **crypto ikev1 | ikev2 policy** command from global configuration mode. The prompt displays IKE policy configuration mode. For example:

```
hostname(config)# crypto ikev1 policy 1
```

```
hostname(config-ikev1-policy)#
```

After creating the policy, you can specify the settings for the policy.

Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/vpn_ike.html

QUESTION 32

Refer to the exhibit.

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

What is the effect of the given command sequence?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Crypto map entry "mymap 30" references the dynamic crypto map set "mydynamicmap," which can be used to process inbound security association negotiation requests that do not match "mymap" entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in "mydynamicmap," for a flow "permitted" by the access list 103, IPSec will accept the request and set up security associations with the remote peer without previously knowing about the remote peer. If accepted, the resulting security associations (and temporary crypto map entry) are established according to the settings specified by the remote peer.

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

QUESTION 33

Refer to the exhibit.

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Phase 1 of IPsec is used to establish a secure channel between the two peers that will be used for further data transmission. The ASAs will exchange secret keys, they authenticate each other and will negotiate about the IKE security policies. This is what happens in phase 1:

- Authenticate and protect the identities of the IPsec peers.
- Negotiate a matching IKE policy between IPsec peers to protect the IKE exchange.
- Perform an authenticated Diffie-Hellman exchange to have matching shared secret keys.
- Setup a secure tunnel for IKE phase 2.

Reference: <https://networklessons.com/security/cisco-asa-site-site-ikev1-ipsec-vpn/>

QUESTION 34

Refer to the exhibit.

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Once the secure tunnel from phase 1 has been established, we will start phase 2. In this phase the two firewalls will negotiate about the IPsec security parameters that will be used to protect the traffic within the tunnel. In short, this is what happens in phase 2:

- Negotiate IPsec security parameters through the secure tunnel from phase 1.
- Establish IPsec security associations.
- Periodically renegotiates IPsec security associations for security.

Reference: <https://networklessons.com/security/cisco-asa-site-site-ikev1-ipsec-vpn/>

QUESTION 35

Refer to the exhibit.

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The autocommand causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and contain embedded spaces, commands using the autocommand keyword must be the last option on the line.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/fsecr_r/srfpass.html#wp1030793

QUESTION 36

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Secured files will not appear on the output of a dir command issued from an executive shell because the IFS prevents secure files in a directory from being listed. ROM monitor (ROMMON) mode does not have any such restriction and can be used to list and boot secured files.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/15-mt/sec-usr-cfg-15-mt-book/sec-resil-config.html

QUESTION 37

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

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

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

Send-lifetime infinite command configures the device to begin transmitting the authentication key to other devices at 23:59:00 local time on December 31, 2013 and continue using the key indefinitely

QUESTION 38

What type of packet creates and performs network operations on a network device?

- A. control plane packets
- B. data plane packets
- C. management plane packets
- D. services plane packets

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

Under normal network operating conditions, the vast majority of packets handled by network devices are data plane packets. These packets are handled in the fast path. Network devices are optimized to handle these fast path packets efficiently. Typically, considerably fewer control and management plane packets are required to create and operate IP networks. Thus, the punt path and route processor are significantly less capable of handling the kinds of packets rates experienced in the fast path since they are never directly involved in the forwarding of data plane packets

Reference: <http://www.cisco.com/c/en/us/about/security-center/copp-best-practices.html>

QUESTION 39

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

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

Correct Answer: B

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

The BPDU guard feature is designed to allow network designers to keep the active network topology predictable. BPDU guard is used to protect the switched network from the problems that may be caused by the receipt of BPDUs on ports that should not be receiving them. The receipt of unexpected BPDUs may be accidental or may be part of an unauthorized attempt to add a switch to the network. BPDU guard is best deployed toward user-facing ports to prevent rogue switch network extensions by an attacker.

QUESTION 40

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

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

Correct Answer: D

Section: (none)

Explanation**Explanation/Reference:****Explanation:**

If your original MAC address is revealed, an hacker can use it to impersonate you! On many networks (wired or wireless) access is restricted based on MAC address to avoid access to unauthorized devices on the network. So, when you go offline, someone can use your machine's MAC address and access the network as 'you'.

Reference: <http://blog.technitium.com/2011/06/why-you-need-to-change-mac-address.html>

QUESTION 41

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To retain the bindings across reloads, you must use the DHCP snooping database agent. Without this agent, the bindings established by DHCP snooping are lost upon reload, and connectivity is lost as well.

The database agent stores the bindings in a file at a configured location. Upon reload, the switch reads the file to build the database for the bindings. The switch keeps the file current by writing to the file as the database changes.

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html#wp1090624>

QUESTION 42

If a switch receives a superior BPDU and goes directly into a blocked state, what mechanism must be in use?

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

Correct Answer: A

Section: (none)

Explanation

**Explanation/Reference:**

Explanation:

The root guard feature protects the network against such issues.

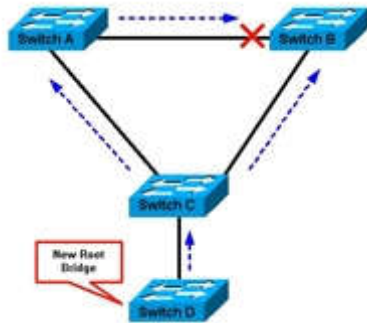
The configuration of root guard is on a per-port basis. Root guard does not allow the port to become an STP root port, so the port is always STP-designated. If a better BPDU arrives on this port, root guard does not take the BPDU into account and elect a new STP root. Instead, root guard puts the port into the root-inconsistent STP state. You must enable root guard on all ports where the root bridge should not appear. In a way, you can configure a perimeter around the part of the network where the STP root is able to be located.

In the following figure, enable root guard on the Switch C port that connects to Switch D.

Switch C in figure below blocks the port that connects to Switch D, after the switch receives a superior BPDU. Root guard puts the port in the root-inconsistent STP state. No traffic passes through the port in this state. After device D ceases to send superior BPDUs, the port is unblocked again. Via STP, the port goes from the listening state to the learning state, and eventually transitions to the forwarding state. Recovery is automatic; no human intervention is necessary.

This message appears after root guard blocks a port:

%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77.
Moved to root-inconsistent state



Reference: <http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html>

QUESTION 43

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

A promiscuous port can communicate with all interfaces, including the isolated and community ports within a PVLAN.

Reference: <http://www.cisco.com/c/en/us/tech/lan-switching/private-vlans-pvlans-promiscuous-isolated-community/index.html>

QUESTION 44

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The key feature of a double tagging attack is exploiting the native VLAN. Since VLAN 1 is the default VLAN for access ports and the default native VLAN on trunks, it's an easy target. The first countermeasure is to remove access ports from the default VLAN 1 since the attacker's port must match that of the switch's native VLAN.

Reference: <https://www.nlogic.co/understanding-vlan-hopping-attacks/>

QUESTION 45

What is a reason for an organization to deploy a personal firewall?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The sole purpose of firewall is to protect endpoints (workstations, and other devices) from malicious activity and network connections with nefarious purposes.

Reference: <http://searchmidmarketsecurity.techtarget.com/definition/personal-firewall>

QUESTION 46

Which statement about personal firewalls is true?

- A. They can protect a system by denying probing requests.
- B. They are resilient against kernel attacks.
- C. They can protect email messages and private documents in a similar way to a VPN.
- D. They can protect the network against attacks.

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

Drop or ignore any probing requests sent to certain service ports on your system. This can mask the presence of the computer from the attacker who is fooled into thinking that no machine is there.

Reference: <https://www.polyu.edu.hk/~ags/itsnews0604/security.html>

QUESTION 47

Refer to the exhibit.

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

What type of firewall would use the given configuration line?

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



Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:**

Explanation: stateful firewalls, a type of firewall that attempts to track the state of network connections when filtering packets. The stateful firewall's capabilities are somewhat of a cross between the functions of a packet filter and the additional application-level protocol intelligence of a proxy.

Reference: <http://www.informit.com/articles/article.aspx?p=373120>

QUESTION 48

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

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

- C. Stateful inspection for multicast traffic is supported only between the self-zone and the internal zone.
- D. Stateful inspection of multicast traffic is supported only for the internal zone.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: stateful inspection support for multicast traffic is not supported between any zones, including the self zone. Use Control Plane Policing for the protection of the control plane against multicast traffic.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/sec-zone-pol-fw.html

QUESTION 49

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: By default, the traffic between interfaces in the same zone is not subject to any policy and passes freely. Firewall zones are used for security features.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/sec-zone-pol-fw.html

QUESTION 50

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.

Correct Answer: AE

Section: (none)

Explanation**Explanation/Reference:**

Explanation: If SSH is not enabled, the Java applet uses Telnet. But as soon as the SSH service is enabled on the switch, the Java applet will stop using Telnet and use SSH instead.

Reference: https://www.alliedtelesis.com/sites/default/files/alliedwareplus-best-practice-guide_reva.pdf

QUESTION 51

Which statement about communication over failover interfaces is true?

- A. All information that is sent over the failover and stateful failover interfaces is sent as clear text by default.
- B. All information that is sent over the failover interface is sent as clear text, but the stateful failover link is encrypted by default.
- C. All information that is sent over the failover and stateful failover interfaces is encrypted by default.
- D. User names, passwords, and preshared keys are encrypted by default when they are sent over the failover and stateful failover interfaces, but other information is sent as clear text.

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:**

Explanation:

All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the security appliance is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the security appliance to terminate VPN tunnels.

Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa80/configuration/guide/conf_gd/failover.html

QUESTION 52

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.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: 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.

Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/mpf_service_policy.html

QUESTION 53

For what reason would you configure multiple security contexts on the ASA firewall?

- A. To separate different departments and business units.
- B. To enable the use of VRFs on routers that are adjacently connected.
- C. To provide redundancy and high availability within the organization.
- D. To enable the use of multicast routing and QoS through the firewall.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: You administer a large enterprise with different departmental groups, and each department wants to implement its own security policies.

Reference: <http://www.ciscopress.com/articles/article.asp?p=426641>

QUESTION 54

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Your IPS will generally be placed at an edge of the network, such as immediately inside an Internet firewall, or in front of a server farm. Position the IPS where it will see the bare minimum of traffic it needs to, in order to keep performance issues under tight control.

Reference: http://www.pcworld.com/article/144634/guide_network_intrusion_prevention_systems.html

QUESTION 55

What is the FirePOWER impact flag used for?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

QUESTION 56

Which FirePOWER preprocessor engine is used to prevent SYN attacks?

- A. Rate-Based Prevention
- B. Portscan Detection
- C. IP Defragmentation
- D. Inline Normalization



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The detection_filter keyword and the thresholding and suppression features provide other ways to filter either the traffic itself or the events that the system generates. You can use rate-based attack prevention alone or in any combination with thresholding, suppression, or the detection_filter keyword to prevent SYN attacks.

Reference: <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#10682>

QUESTION 57

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

- A. Enable logging at the end of the session.

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When the system detects a connection, in most cases you can log it at its beginning or its end.

However, because blocked traffic is immediately denied without further inspection, in most cases you can log only beginning-of-connection events for blocked or blacklisted traffic; there is no unique end of connection to log. An exception occurs when you block encrypted traffic. When you enable connection logging in an SSL policy, the system logs end-of-connection rather than beginning-of-connection events. This is because the system cannot determine if a connection is encrypted using the first packet in the session, and thus cannot immediately block encrypted sessions.

Reference: <http://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/AC-Connection-Logging.html#pgflid-1604681>

QUESTION 58

What can the SMTP preprocessor in FirePOWER normalize?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Transport and network layer preprocessors detect attacks that exploit IP fragmentation, checksum validation, and TCP and UDP session preprocessing. Before packets are sent to preprocessors, the packet decoder converts packet headers and payloads into a format that can be easily used by the preprocessors and the intrusion rules engine and detects various anomalous behaviors in packet headers. After packet decoding and before sending packets to other preprocessors, the inline normalization preprocessor normalizes traffic for inline deployments.

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

QUESTION 59

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

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

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To restrain servers to collect IP addresses of individual users, you have to configure a proxy server to hide users' local IP addresses and configure a firewall to use port address translation or PAT.

QUESTION 60

You have implemented a Sourcefire IPS and configured it to block certain addresses utilizing Security Intelligence IP Address Reputation. A user calls and is not able to access a certain IP address. What action can you take to allow the user access to the IP address?

- A. Create a whitelist and add the appropriate IP address to allow the traffic.
- B. Create a custom blacklist to allow the traffic.
- C. Create a user based access control rule to allow the traffic.
- D. Create a network based access control rule to allow the traffic.
- E. Create a rule to bypass inspection to allow the traffic.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

When a blacklist is too broad in scope, or incorrectly blocks traffic that you want to allow (for example, to vital resources), you can override a blacklist with a custom whitelist.

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

QUESTION 61

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

URL filtering window displays the global settings for URL filtering on the router. You can maintain the local URL list and the URL filter server list in the Additional Tasks screens or in the Application Security windows. The Global settings for URL filtering can only be maintained from this Additional Tasks window. Use the Edit Global Settings button to change these values.

Reference: http://www.cisco.com/c/en/us/td/docs/routers/access/cisco_router_and_security_device_manager/24/software/user/guide/URLftr.html

QUESTION 62

When is the best time to perform an anti-virus signature update?

- A. Every time a new update is available.
- B. When the local scanner has detected a new virus.
- C. When a new virus is discovered in the wild.
- D. When the system detects a browser hook.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can automatically check for Anti-Virus signature updates from Cisco's signature server every 24 hours or to manually check for Anti-Virus signature updates at any time by clicking Update. When a newer signature file is available on the server, the new signature file will be downloaded to your device.

Reference: https://www.cisco.com/assets/sol/sb/isa500_emulator/help/guide/af1321261.html

QUESTION 63

Which statement about application blocking is true?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Application filters allow you to quickly create application conditions for access control rules. They simplify policy creation and administration, and grant you assurance that the system will control web traffic as expected. For example, you could create an access control rule that identifies and blocks all high risk, low business relevance applications. If a user attempts to use one of those applications, the session is blocked.

Reference: <http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/AC-Rules-App-URL-Reputation.html#pgfId-1576835>

QUESTION 64

Scenario

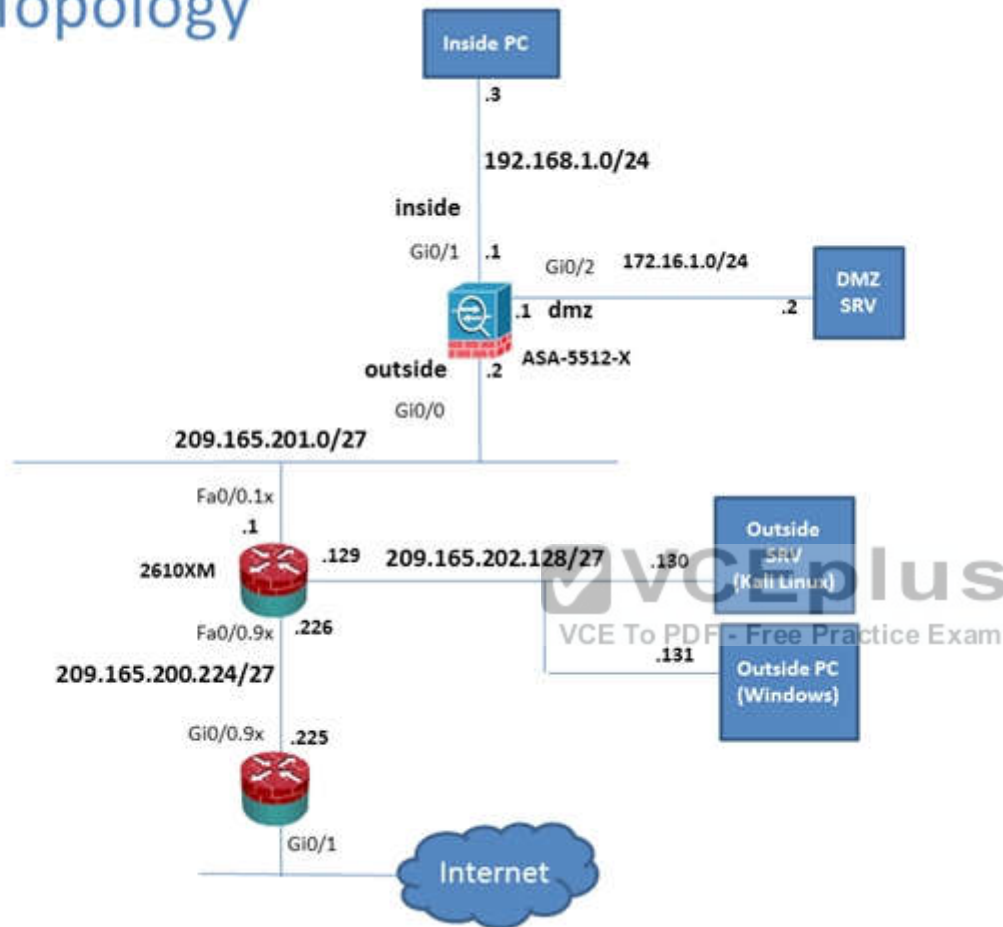
In this simulation, you have access to ASDM only. Review the various ASA configurations using ASDM then answer the five multiple choice questions about the ASA SSLVPN configurations.

To access ASDM, click the ASA icon in the topology diagram.

Note: Not all ASDM functionalities are enabled in this simulation.

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

Lab Topology



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Home Device Dashboard Firewall Dashboard ASA FirePOWER Status

Device Information

General License

Host Name: **P17-ASAsecure-x.local**
 ASA Version: **100.14(6)13**
 ASDM Version: **7.5(1)1**
 Firewall Mode: **Routed**
 Environment Status: **OK**

Device Uptime: **11d 21h 42m 47s**
 Device Type: **ASA 5512**
 Context Mode: **Single**
 Total Flash: **4096 MB**

Interface Status

| Interface | IP Address/Mask | Line | Link | Kbps |
|-----------|------------------|------|------|------|
| dmz | 172.16.1.1/24 | UP | UP | 0 |
| inside | 192.168.1.1/24 | UP | UP | 4 |
| mgmt | 10.10.10.1/24 | UP | UP | 0 |
| outside | 209.165.201.1/24 | UP | UP | 0 |

Select an interface to view input and output Kbps

VPN Sessions

IPsec: 0 Clientless SSL VPN: AnyConnect Clients: 0 [Details](#)

System Resources Status

Total Memory Usage Total CPU Usage Core Usage [Details](#)

Memory Usage (MB)

1500MB

1000MB

500MB

0

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

Traffic Status

Connections Per Second Usage

1500

1000

500

0

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

UDP: 0 TCP: 0 Total: 0

Input Kbps: 0 Output Kbps: 0

Latest ASDM Syslog Messages

| Severity | Date | Time | Syslog ID | Source IP | Source | Destination IP | Destination | Description |
|----------|-------------|----------|-----------|---------------|--------|----------------|-------------|---|
| 6 | May 13 2015 | 12:35:09 | 302016 | 10.81.254.202 | 223 | 209.165.201.2 | 65535 | Tear-down UDP connection 15136525 for outside:10.81.254.202/123 to identity:209.165.201.2/65535(any) duration 0:02:01 bytes 96 |
| 6 | May 13 2015 | 12:35:08 | 106015 | 192.168.1.3 | 443 | 192.168.1.1 | 443 | Deny TCP (no connection) from 192.168.1.3/14676 to 192.168.1.1/443 flags FIN ACK on interface inside |
| 6 | May 13 2015 | 12:35:08 | 302014 | 192.168.1.3 | 443 | 192.168.1.1 | 443 | Tear-down TCP connection 15136528 for inside:192.168.1.3/14676 to identity:192.168.1.1/443 duration 0:00:00 bytes 296 TCP Reset-O |

student 23 7/13/15 12:35:08 PM pst

Cisco ASDM 7.5 for ASA - 10216811

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

| Interface | IP Address | MAC Address | Proxy Arp |
|-----------|---------------|----------------|-----------|
| outside | 209.165.201.1 | 000c.3014.3820 | No |
| inside | 192.168.1.4 | 0050.5633.3033 | No |
| inside | 192.168.1.2 | 0050.5611.1111 | No |
| inside | 192.168.1.2 | 0050.5632.2222 | No |
| inside | 192.168.1.56 | 0050.5692.5c8b | No |
| inside | 192.168.1.55 | 0006.95e6.98f3 | No |
| dmz | 172.16.1.2 | 0050.5644.4444 | No |
| night | 10.10.10.1 | 000c.3014.3820 | No |

Clear Dynamic ARP Entries

Refresh

Data Refreshed Successfully.

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

Student 15 3/19/15 9:32:37 AM pac

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

VPN

VPN Statistics

- Overview
- VPN Cluster Loads
- Crypto Statistics
- Compression Statistics
- Encryption Statistics
- Global IKE/SPsec Statistics
- Protocol Statistics
- VLAN Mapping Sessions
- NEM Proxy Statistics
- NEM Proxy Sessions
- Clientless SSL VPN
- VPN Connection Graphs
- IPSA Sessions

VPN

Monitoring > VPN > VPN Statistics > Sessions

| Type | Active | Cumulative | Peak Concurrent | Inactive |
|----------------|--------|------------|-----------------|----------|
| Clientless VPN | 0 | 0 | 1 | 0 |
| Browser | 0 | 1 | 1 | 1 |

Filter By: Clientless SSL VPN All Sessions Filter

| Username IP Address | Group Policy Connection Profile | Protocol Encryption | Login Time Duration | Bytes Tx Bytes Rx |
|----------------------------|------------------------------------|----------------------------------|--|----------------------|
| student 209.165.202.111 | Sales Clientless | Clientless Clientless (IPsec) | 08:05:46:205 Thu May 21 2015 08:05:46:205 Thu May 21 2015 | 316779 41633 |

Details Logout Ping

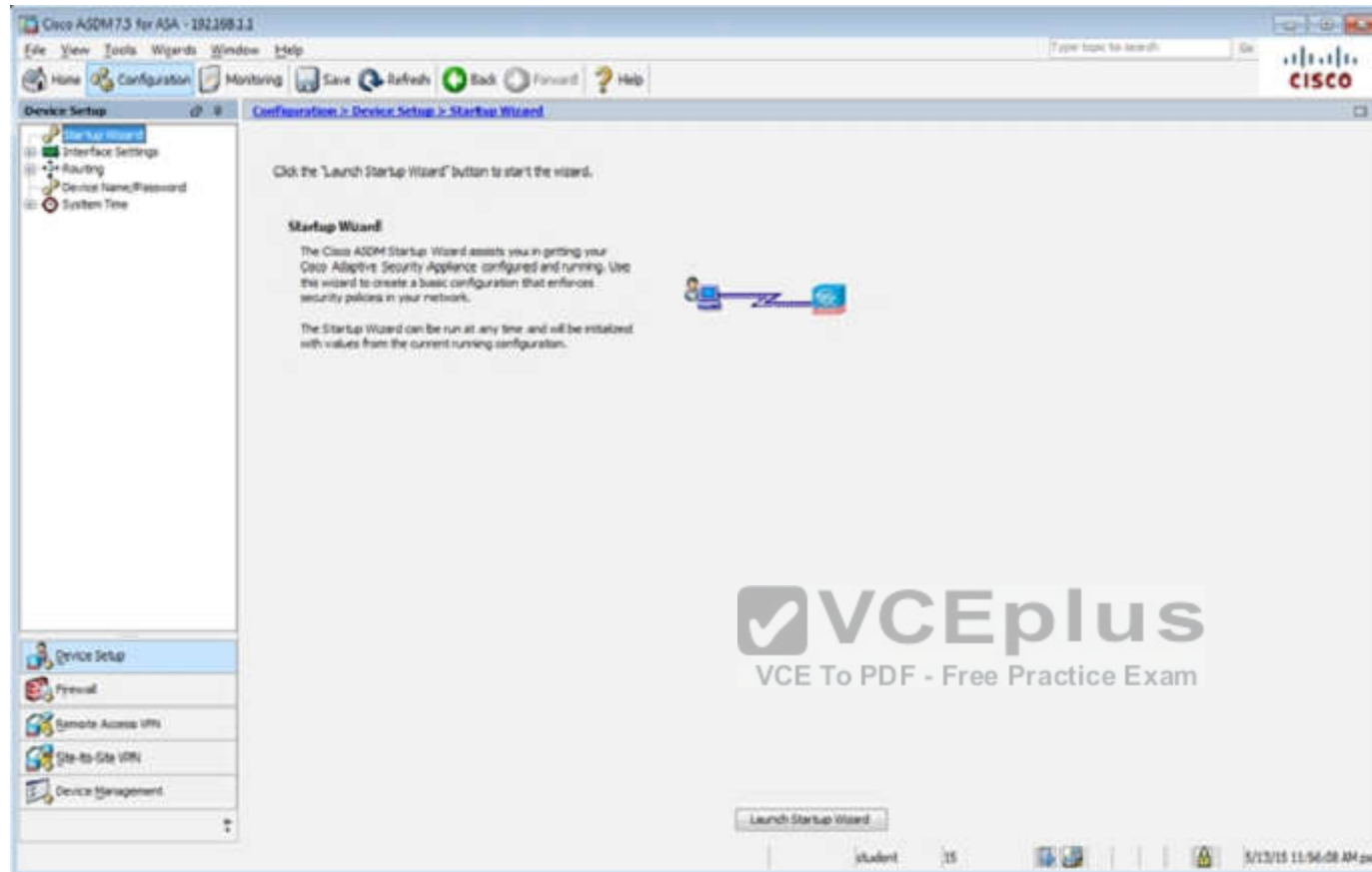
Refresh

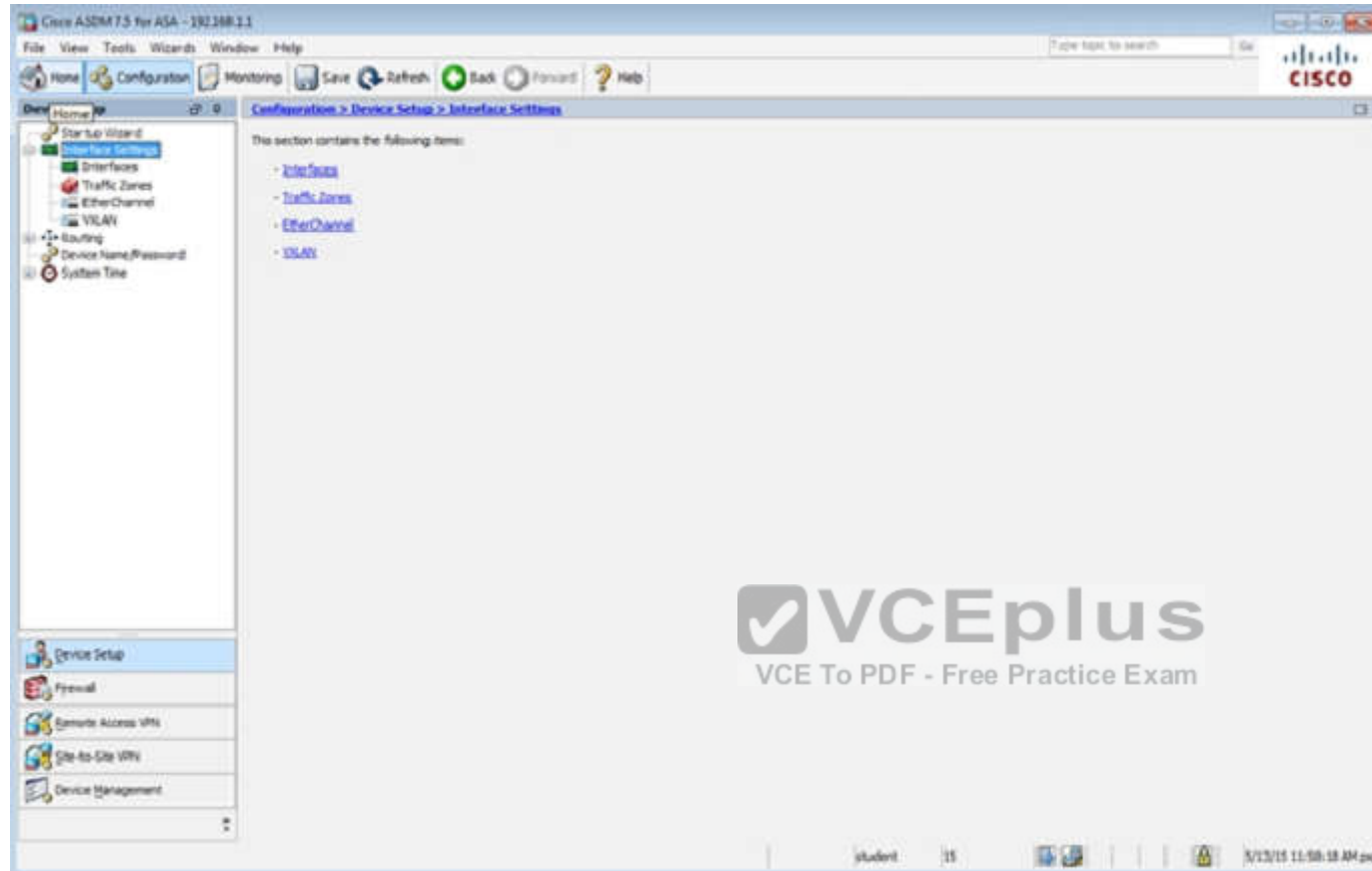
Last updated: 5/19/15 9:33:12 AM

student 25

5/19/15 9:33:37 AM PST

Data Refreshed Successfully.





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup Configuration > Device Setup > Interface Settings > Interfaces

Interface Name Zone Route Map State Security Level IP Address Subnet Mask Prefix Length Group Type

| Interface | Name | Zone | Route Map | State | Security Level | IP Address | Subnet Mask Prefix Length | Group | Type |
|------------------|---------|------|-----------|---------|----------------|-------------|---------------------------|-------|----------|
| GigabitEthernet0 | Outside | | | Enabled | 0/0/0 | 192.168.1.2 | 255.255.255.0 | | Hardware |
| GigabitEthernet1 | inside | | | Enabled | 100 | 192.168.1.1 | 255.255.255.0 | | Hardware |
| GigabitEthernet2 | dmz | | | Enabled | 170 | 16.1.1 | 255.255.255.0 | | Hardware |
| GigabitEthernet3 | | | | Enabled | | | | | Hardware |
| GigabitEthernet4 | | | | Enabled | | | | | Hardware |
| GigabitEthernet5 | mgmt | | | Enabled | 100 | 10.10.10.2 | 255.255.255.0 | | Hardware |
| Management0 | | | | Enabled | | | | | Hardware |

ASD EDIT Delete

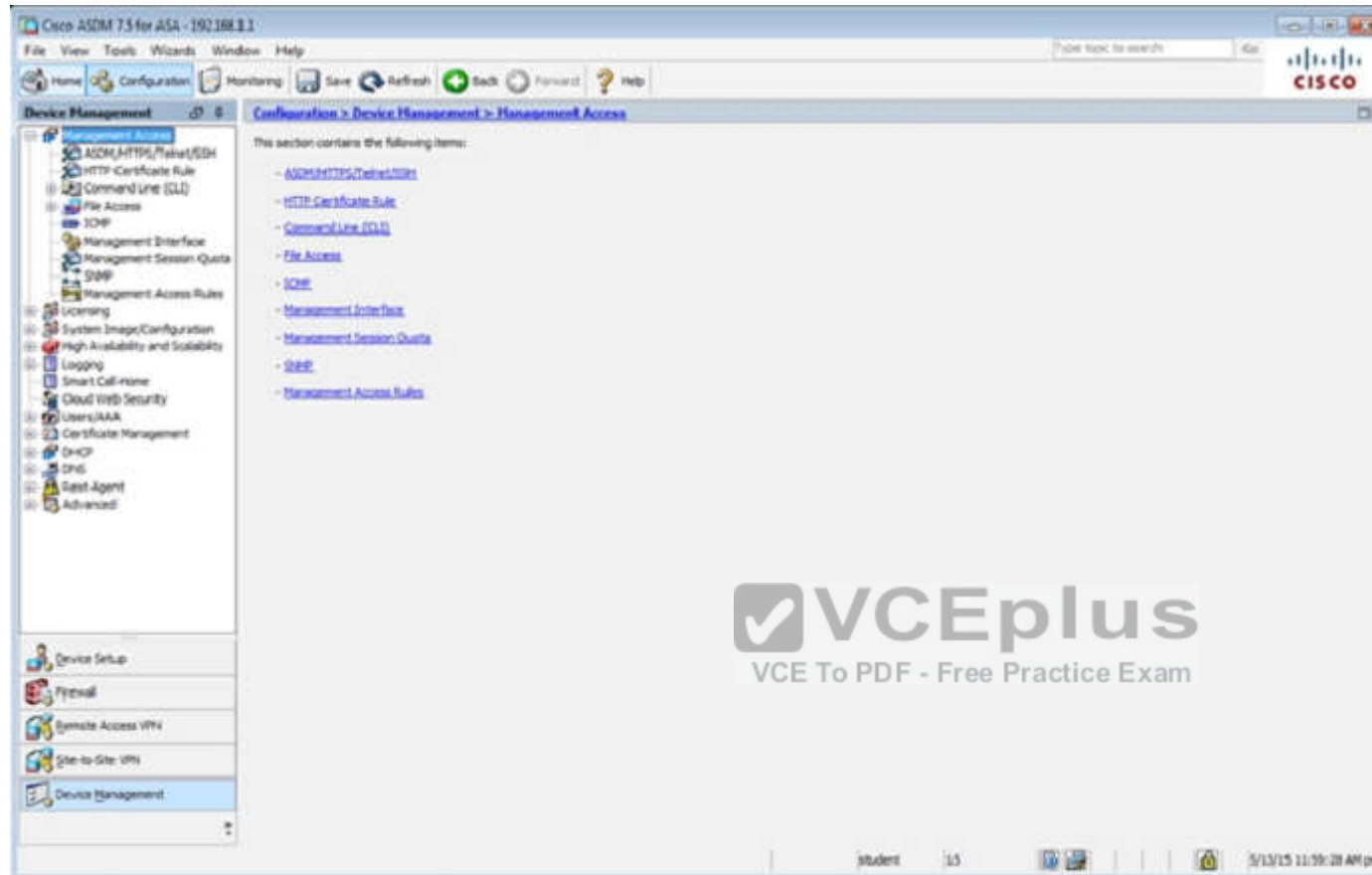
Enable traffic between two or more interfaces which are configured with same security levels

Enable traffic between two or more hosts connected to the same interface

Enable jumbo frame reservation

Apply Reset

Student 15 3/13/15 12:42:48 PM EDT



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

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

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

Buttons: Add, Edit, Delete

HTTP Settings

☒ Enable HTTP Server

Port Number: 443

Idle Timeout: 20 minutes

☐ Session Timeout: minutes

Require client certificate to access ASDM on the following interfaces

Interfaces:

Telnet Settings

Telnet Timeout: 5 minutes

SSH Settings

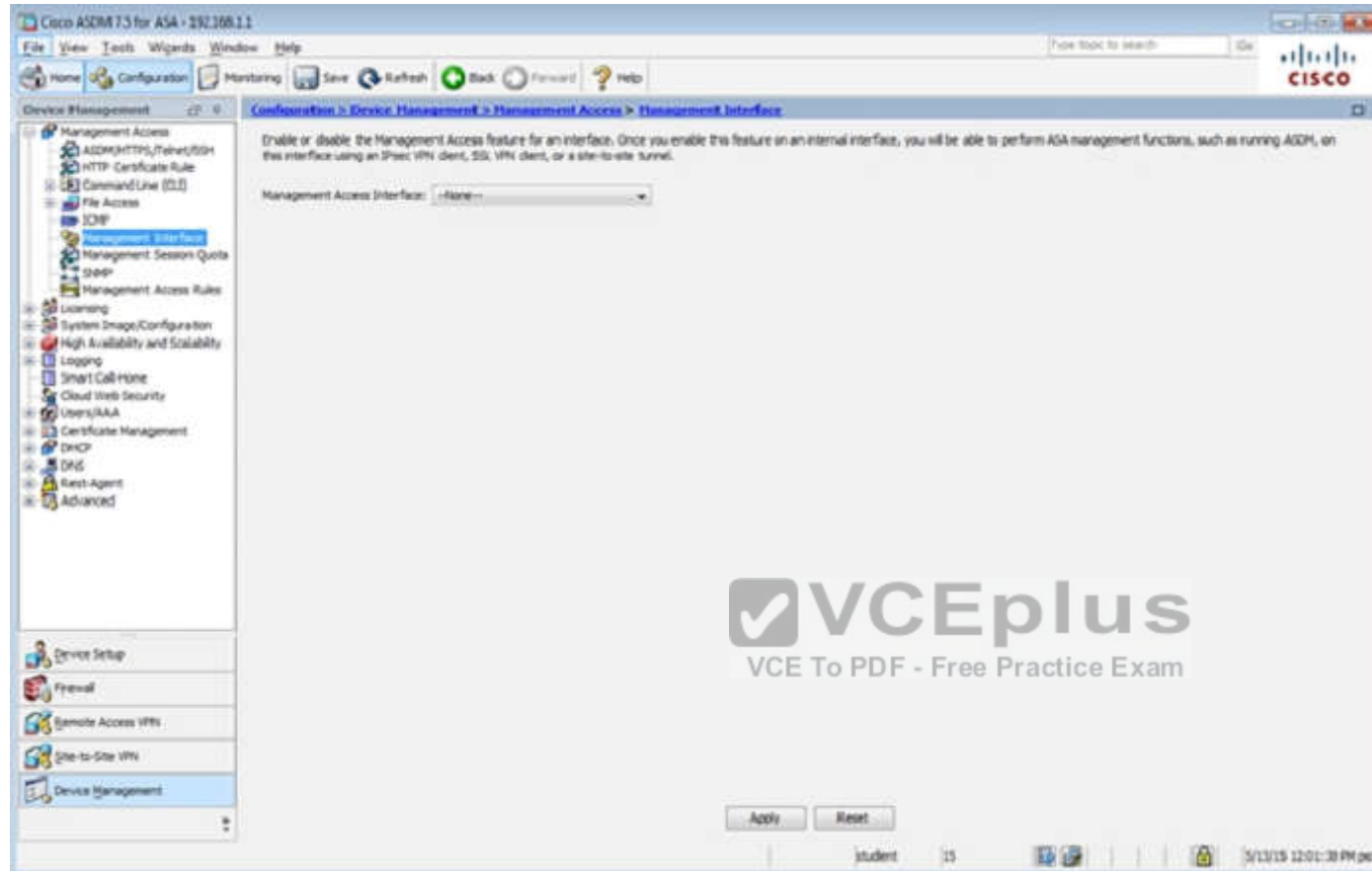
Allowed SSH Version(s): 1.9.2

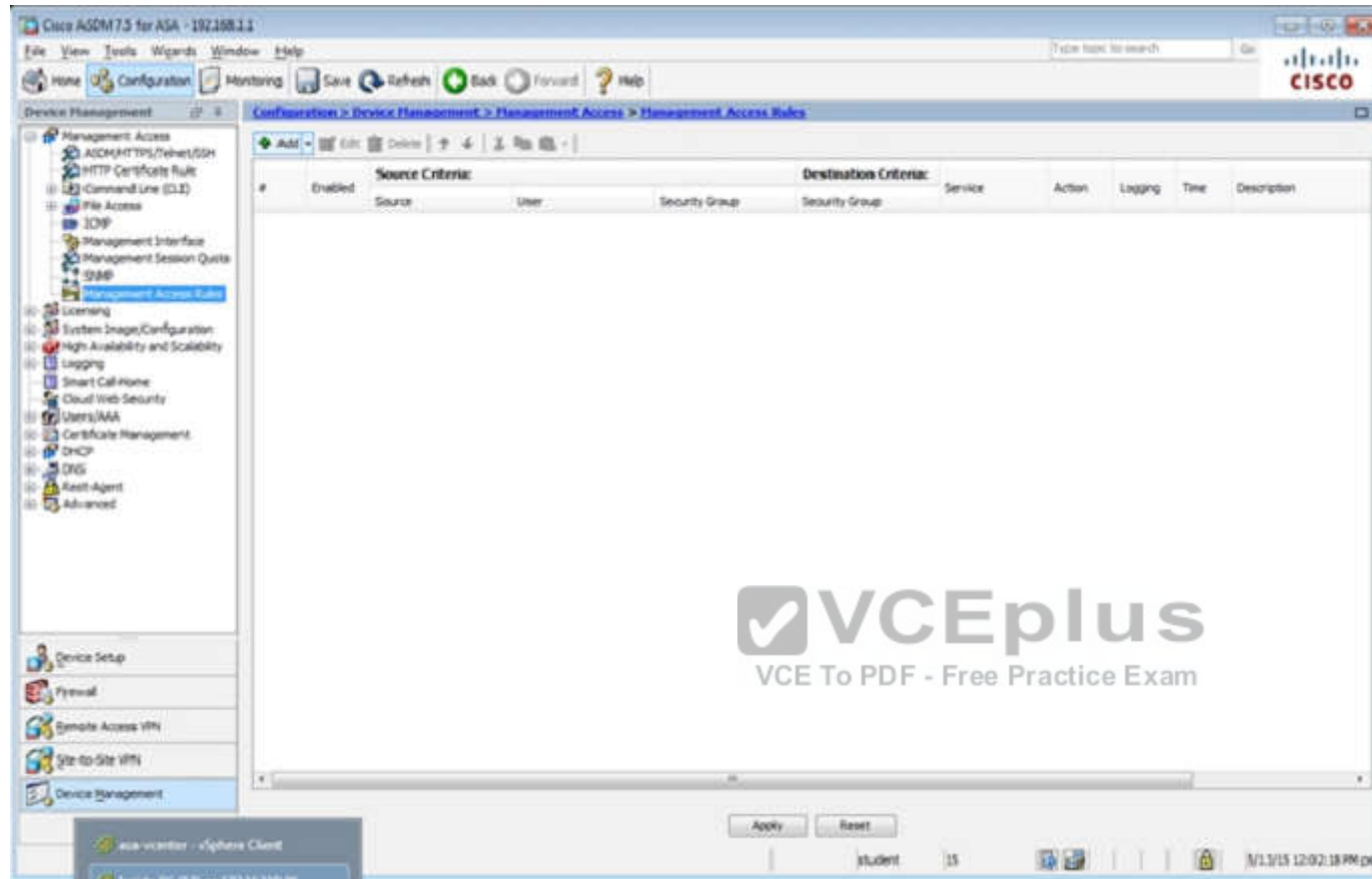
SSH Timeout: 5 minutes

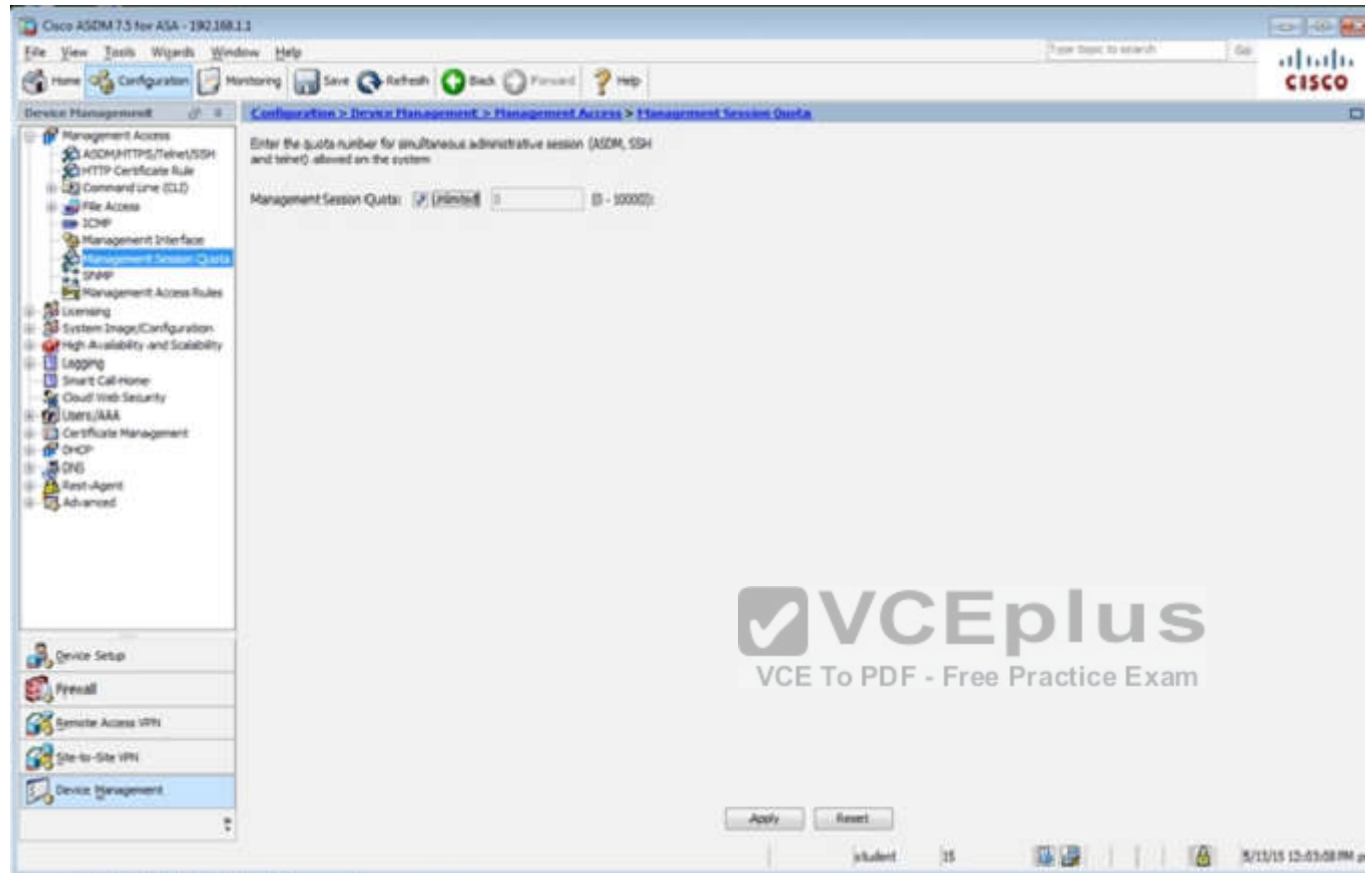
Diffie-Hellman: ☒ Group 1 ☐ Group 14

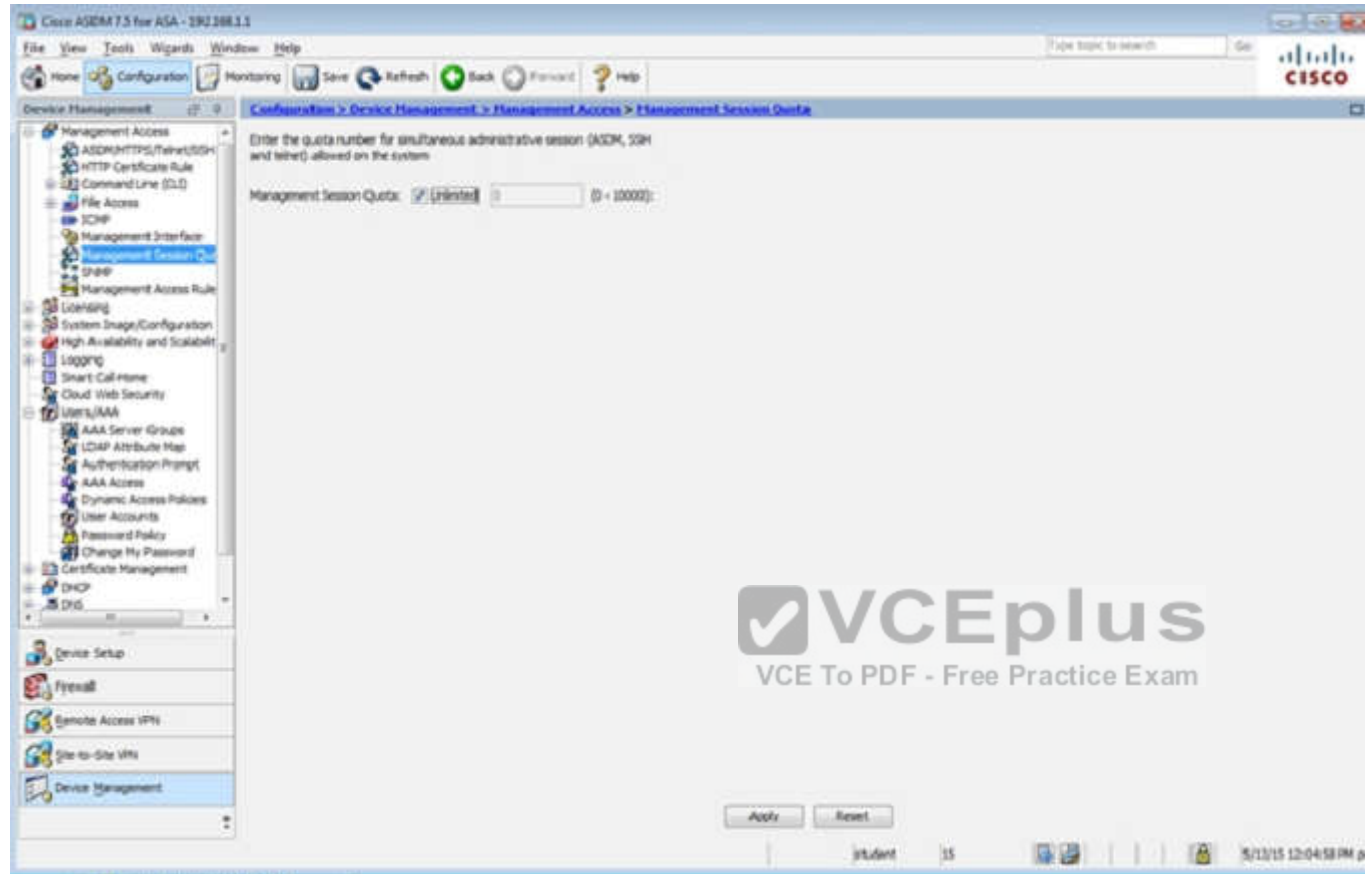
Buttons: Apply, Reset

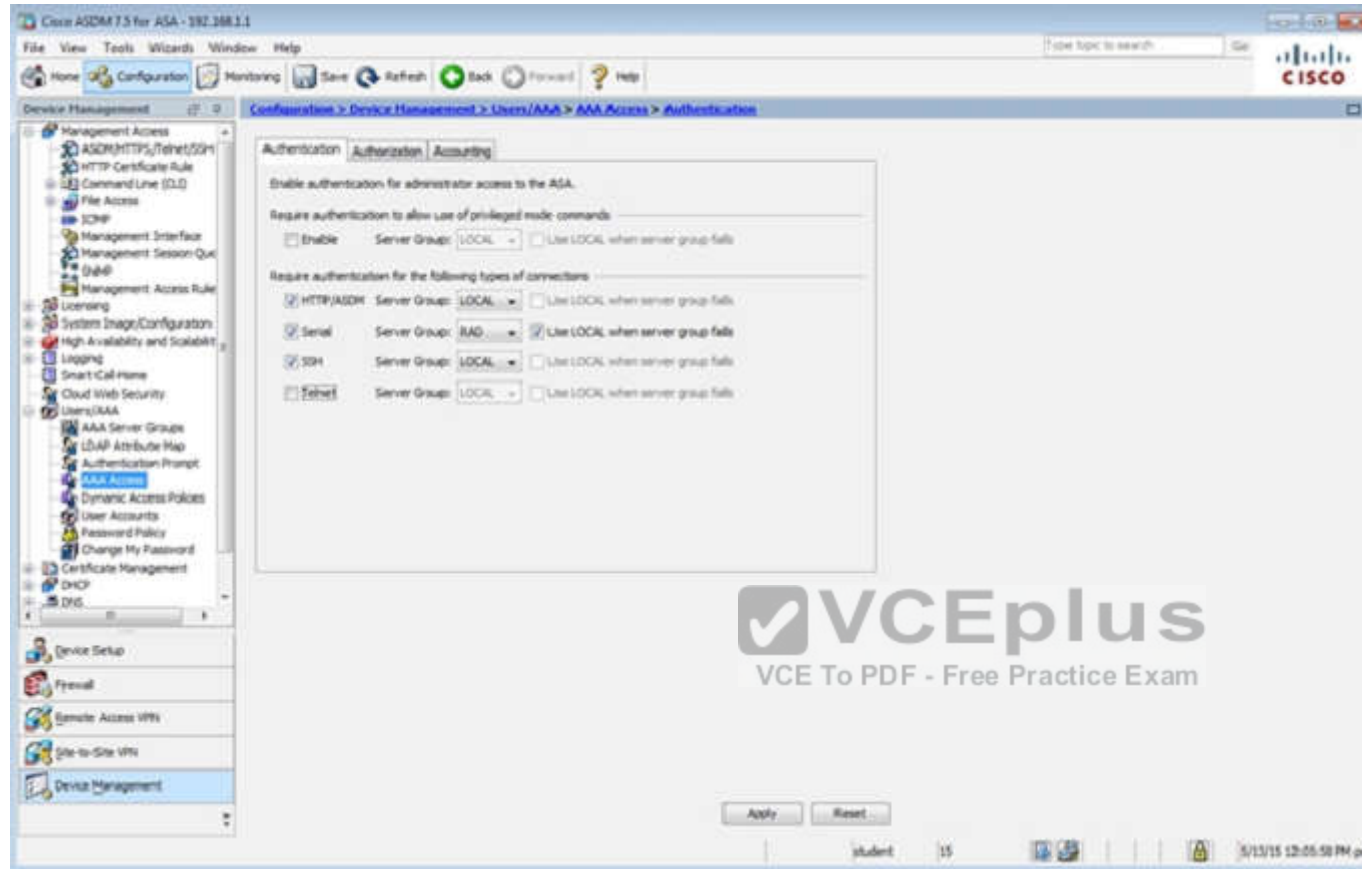
student 13 5/13/15 12:00:38 PM ppt

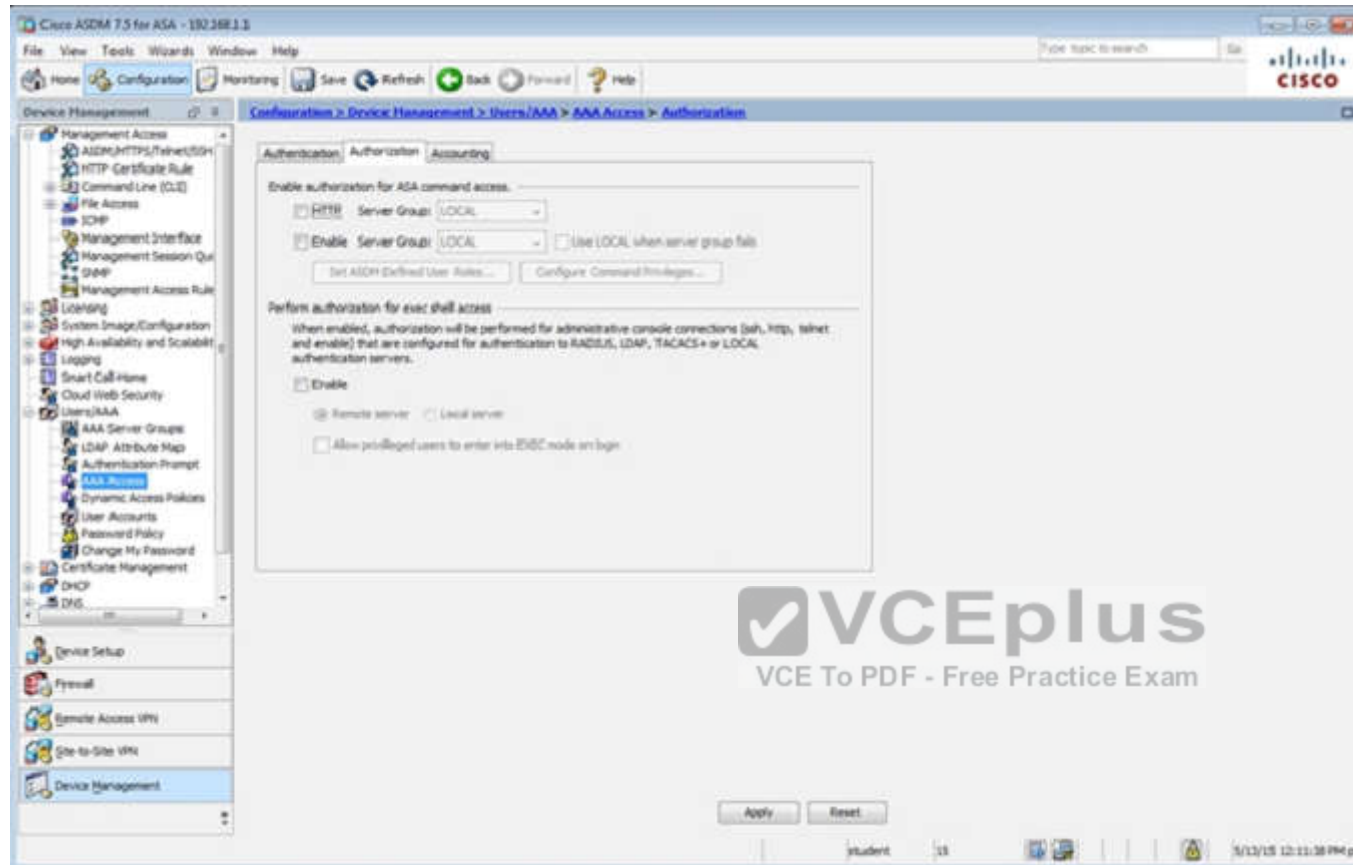


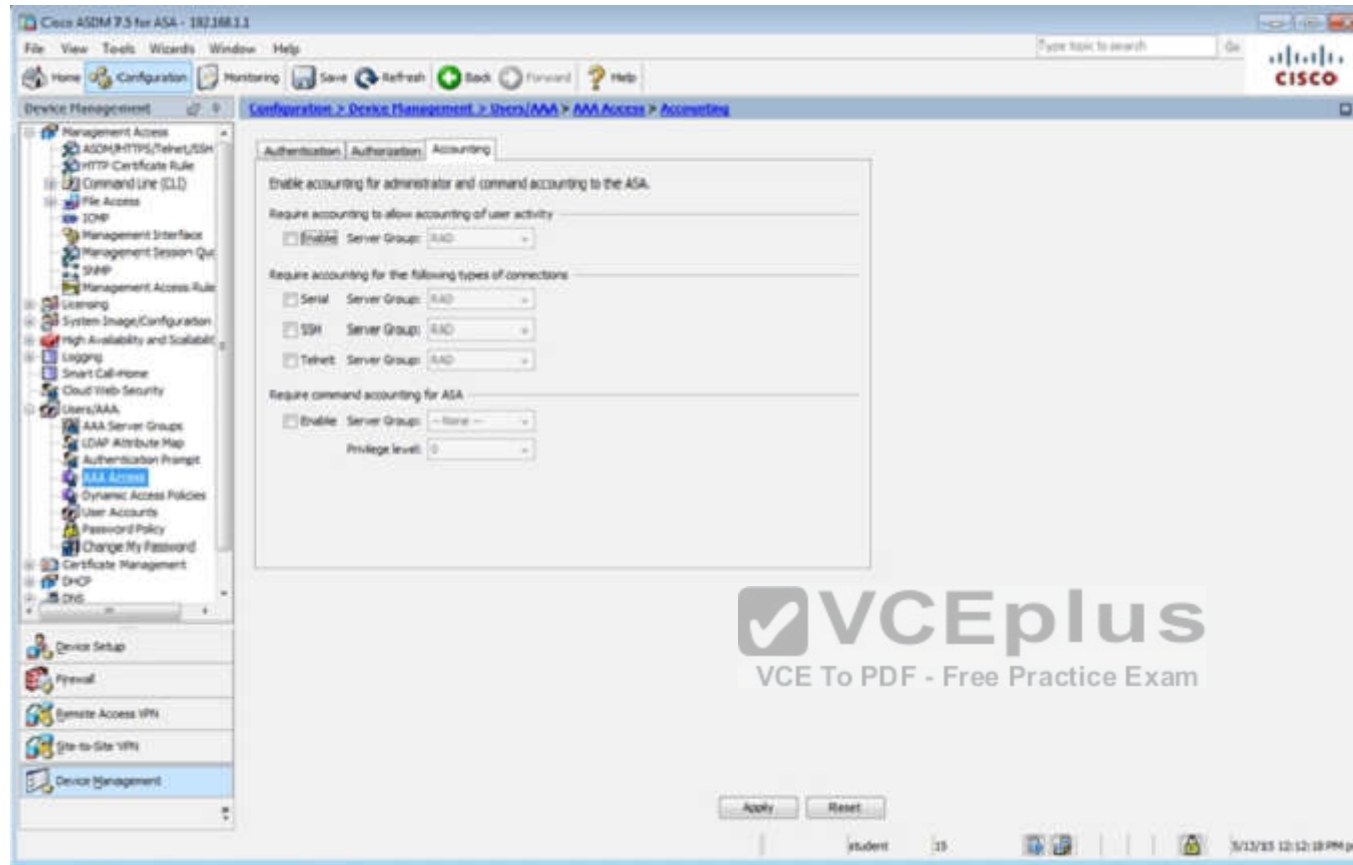


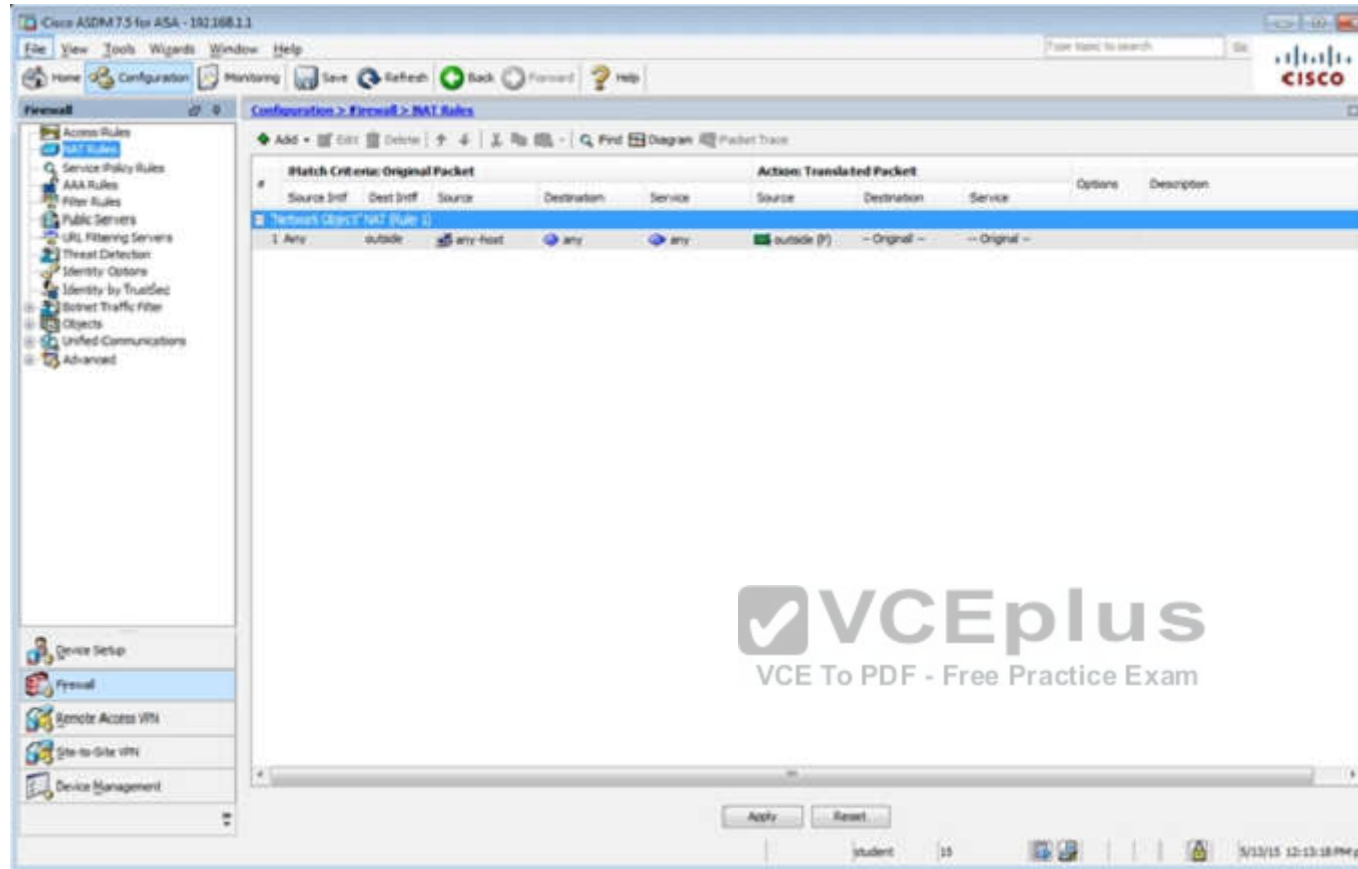


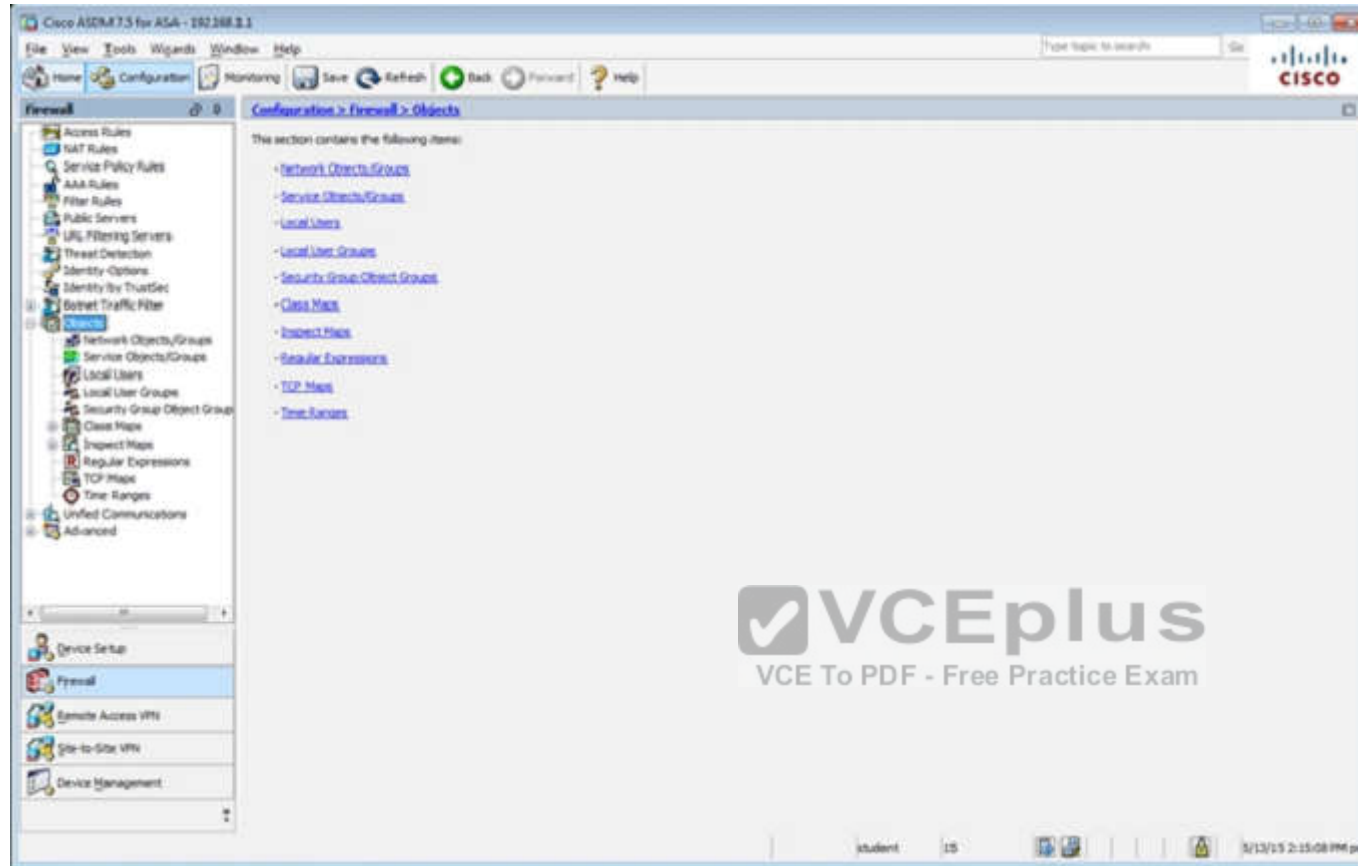












Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall

Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

Command authorization must be enabled in order for the user account privileges to be enforced. To enable command authorization, go to [Configuration > Firewall > Objects > Local Users](#).

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

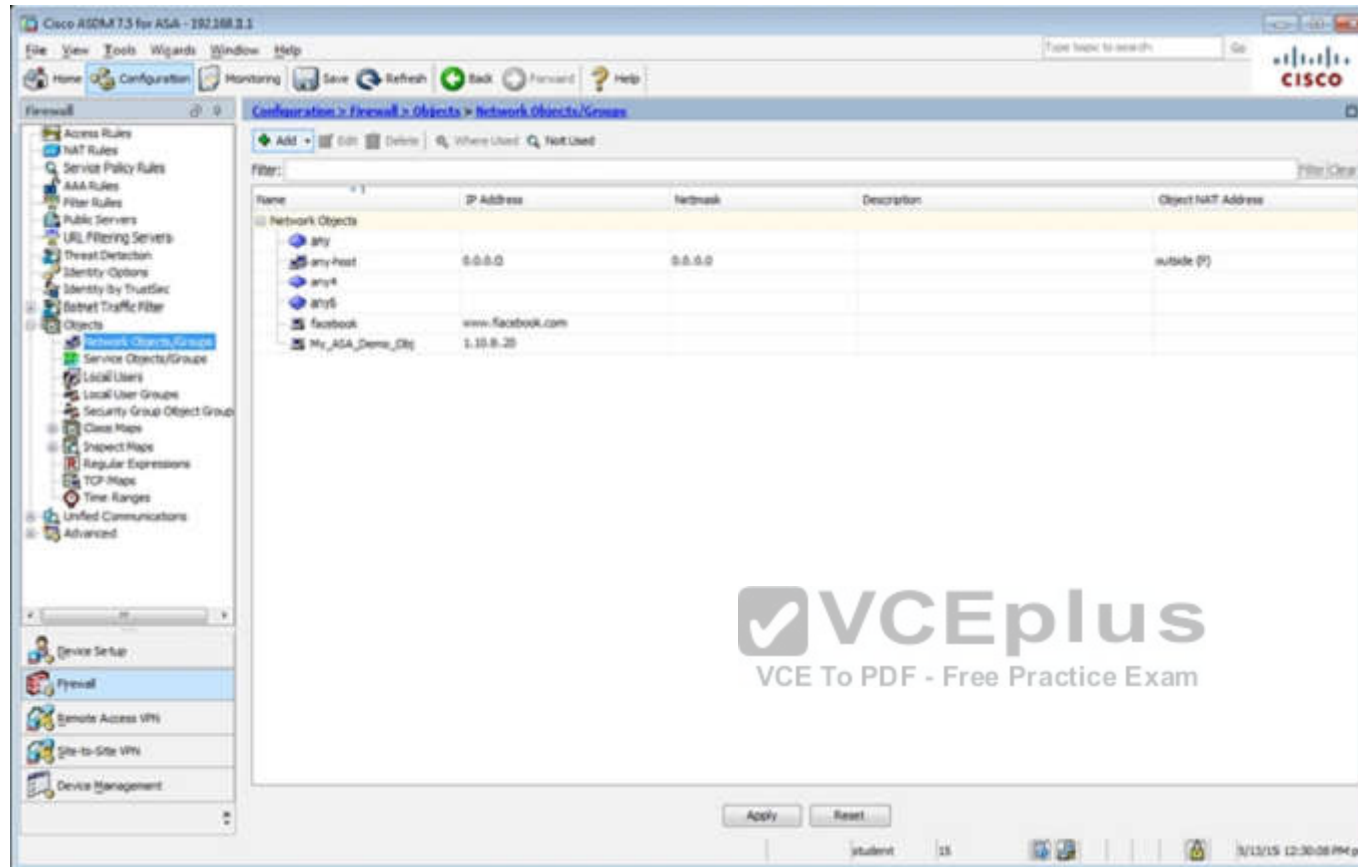
| Username | Privilege Level (Rule) | Access Restrictions | VPN Group Policy | VPN Group Link |
|-----------|------------------------|---------------------|----------------------------|----------------------------|
| student | 15 | Full | -- Inherit Group Policy -- | -- Inherit Group Policy -- |
| enable_15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

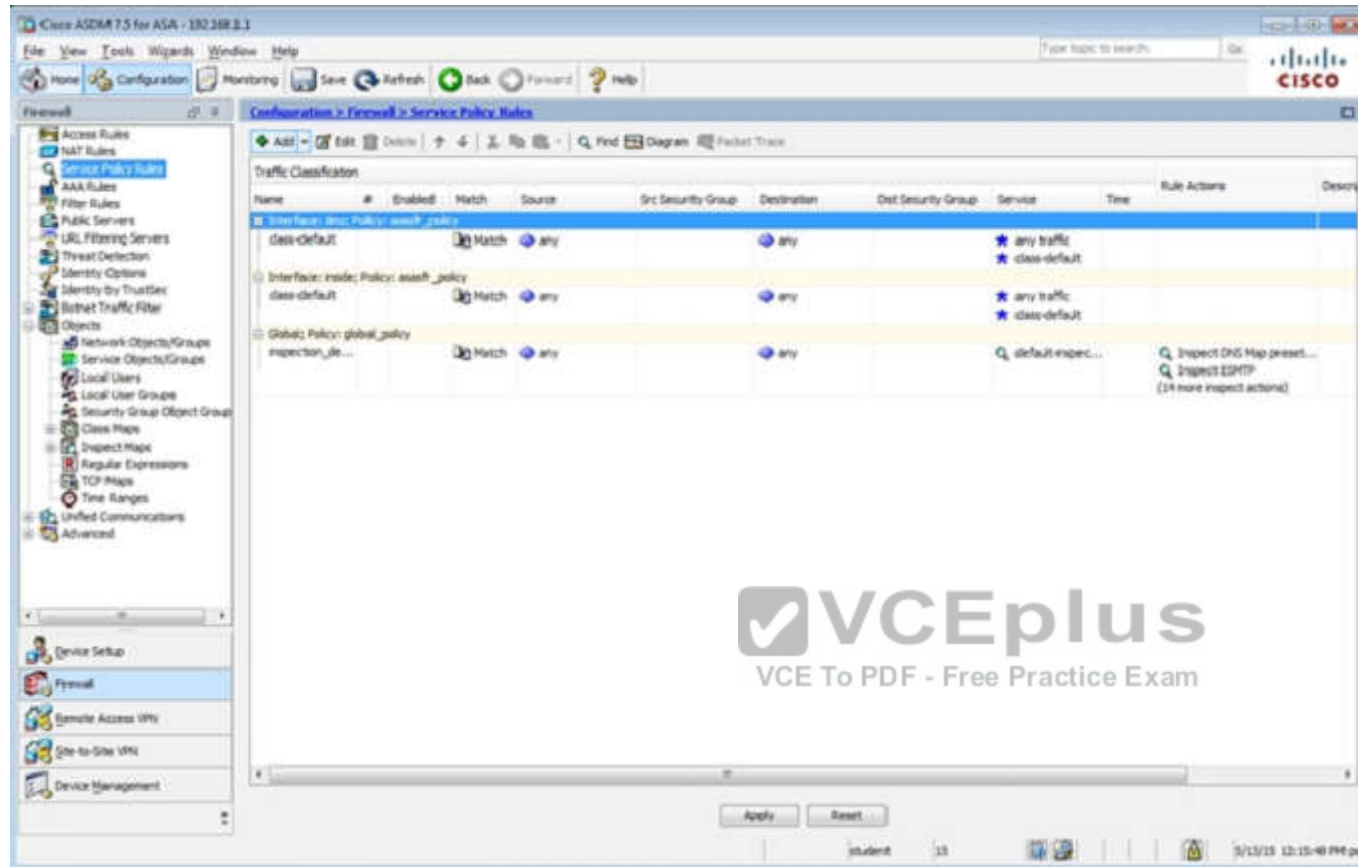
Add Edit Delete

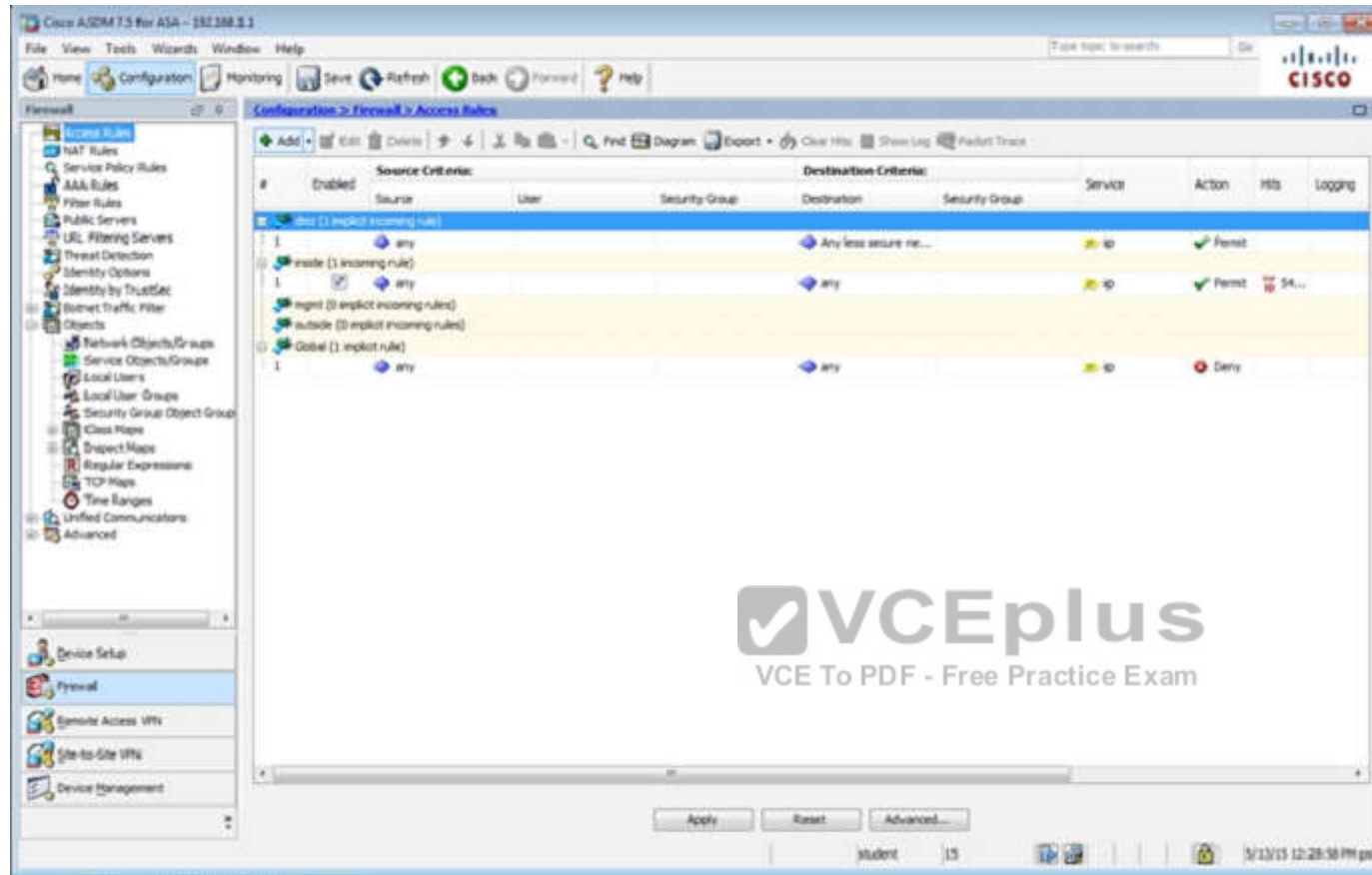
Find: Match Case

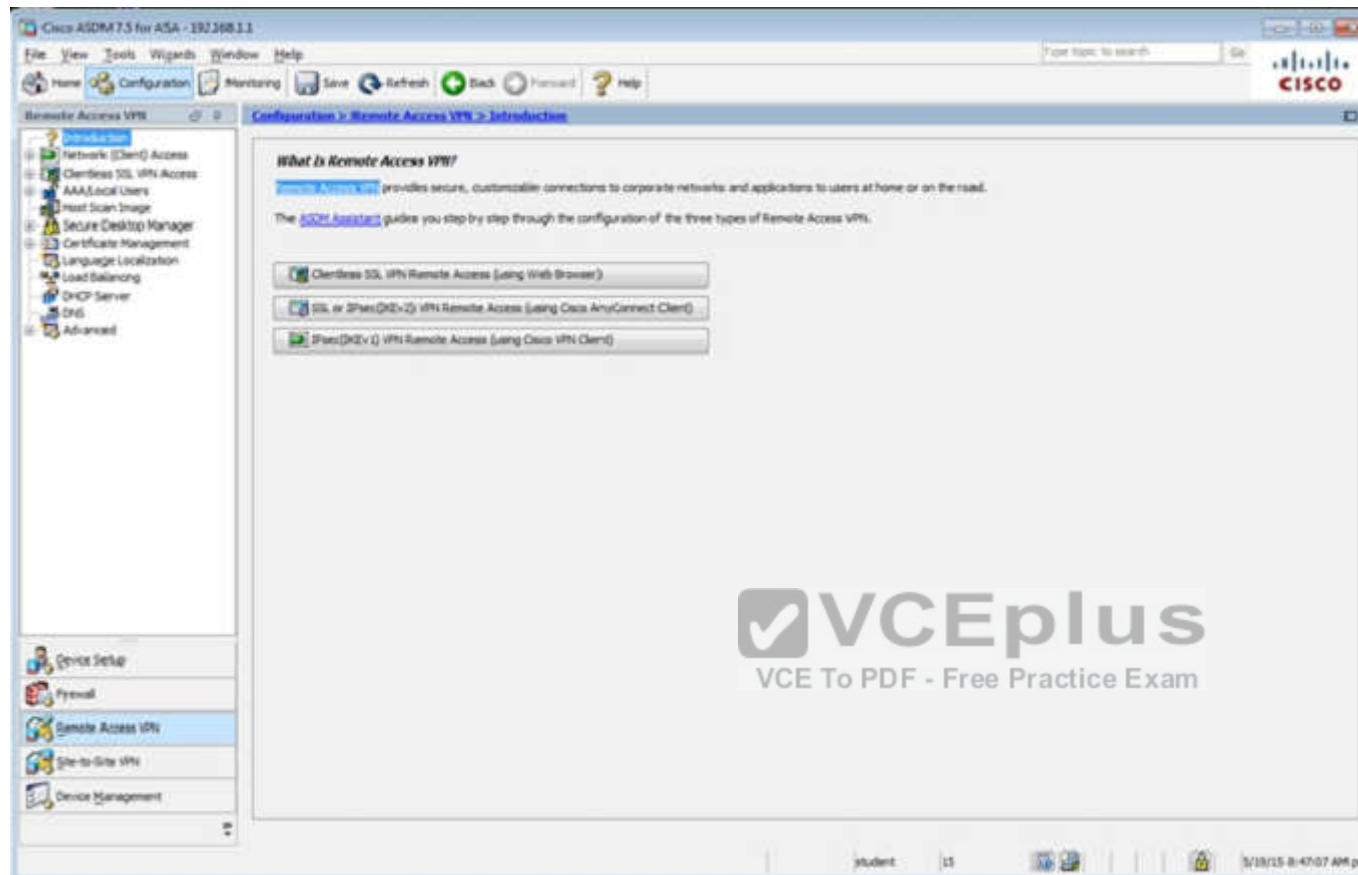
Apply Reset

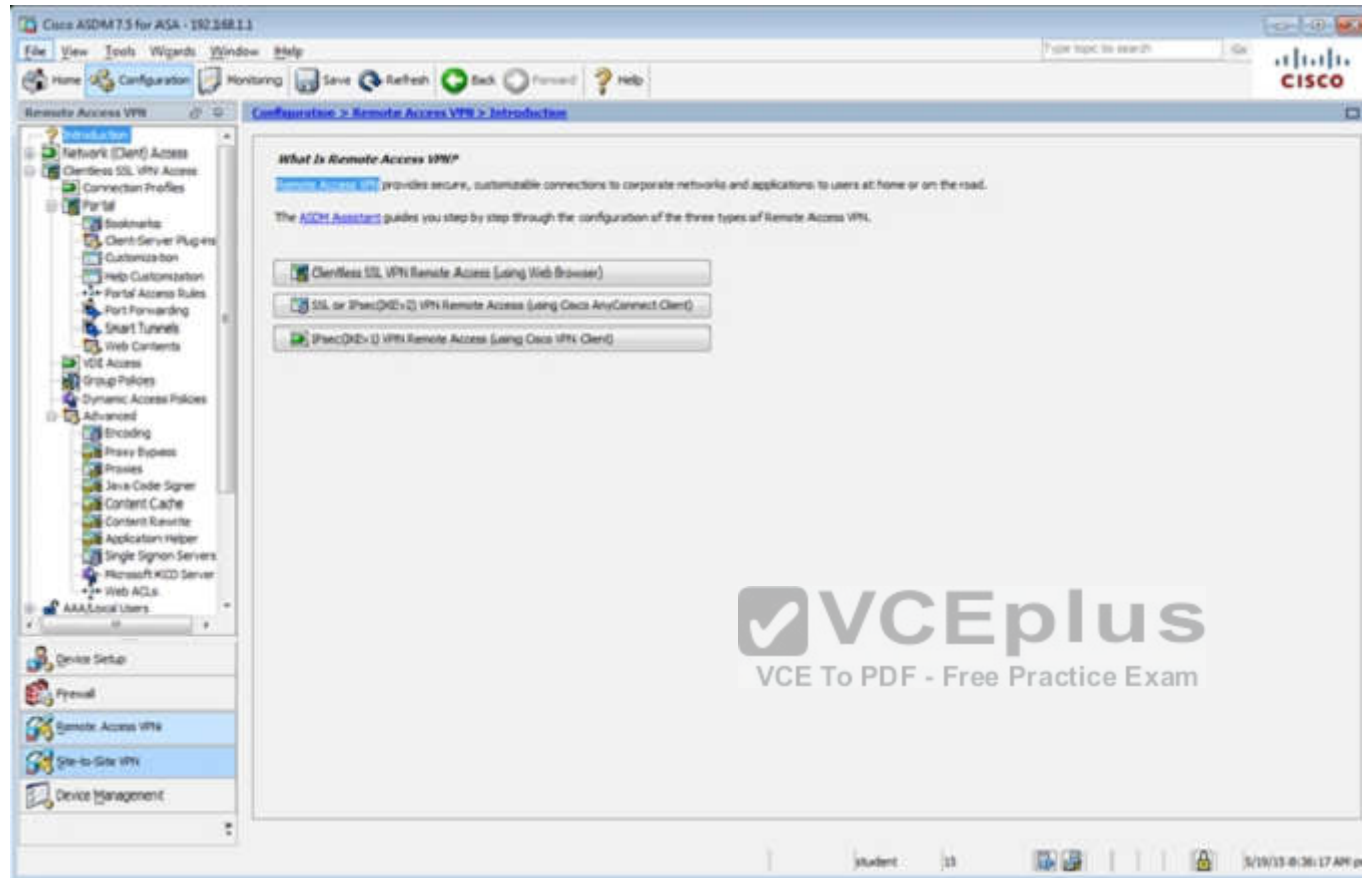
student 15 5/13/15 12:14:18 PM pst











Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction
Network (Client) Access
Clientless SSL VPN Access
Connection Profiles
Partial
Bookmarks
Client Server Plug-ins
Customization
Help Customization
Portal Access Rules
Port Forwarding
Smart Tunnels
Web Contents
VCC Access
Group Policies
Dynamic Access Policies
Advanced
Encoding
Proxy Bypass
Proxies
Java Code Signer
Content Cache
Content Resource
Application Helper
Single Signon Servers
Microsoft KDC Server
Web ACLs
AAA Local Users

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

Access Interfaces
Enable interfaces for clientless SSL VPN access.

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

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

Login Page Setting

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

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

Find:

| Name | Enabled | Aliases | Authentication Method | Group Policy |
|--------------------|-------------------------------------|---------|-----------------------|---------------|
| DefaultRAGroup | <input checked="" type="checkbox"/> | | AAA/Local | DefaultPolicy |
| DefaultWEBVpnGroup | <input checked="" type="checkbox"/> | | AAA/Local | DefaultPolicy |
| Clientless | <input checked="" type="checkbox"/> | Test | AAA/Local | DefaultPolicy |

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

student 15 5/15/15 8:38:47 AM pet

Edit Clientless SSL VPN Connection Profile: clientless

Basic
Advanced

Name: clientless
Aliases: test

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

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

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

Find: ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

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

Login and Logout Page Customization: DfltCustomization Manage...

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

☐ Enable the display of SecurId messages on the login screen

Connection Aliases

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

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

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

Group URLs

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

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

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

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

☒ Always run CSD

☐ Disable CSD for both AnyConnect and Clientless SSL VPN

☐ Disable CSD for AnyConnect only

Find: Next Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

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

Interface-Specific Authentication Server Groups

+ Add Edit Delete

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

Username Mapping from Certificate

☐ Pre-fill Username from Certificate

☐ Hide username from end user

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

☐ Use the entire DN as the username

☐ Use script to select username

-- None -- + Add Edit Delete

Find: Next Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

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

Secondary Authentication Server Group

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

☐ Use LOCAL if Server Group fails

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

Attributes Server: ☒ Primary ☐ Secondary

Session Username Server: ☒ Primary ☐ Secondary

Interface-Specific Secondary Authentication Server Groups

+ Add Edit Delete

| Interface | Server Group | Fallback to LOCAL | Use primary username |
|-----------|--------------|-------------------|----------------------|
|-----------|--------------|-------------------|----------------------|

Username Mapping from Certificate

☐ Pre-fill username from certificate

☐ Hide username from end user

☐ Fallback when a certificate is unavailable

Password: ☒ Prompt ☐ Use primary ☐ Use

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

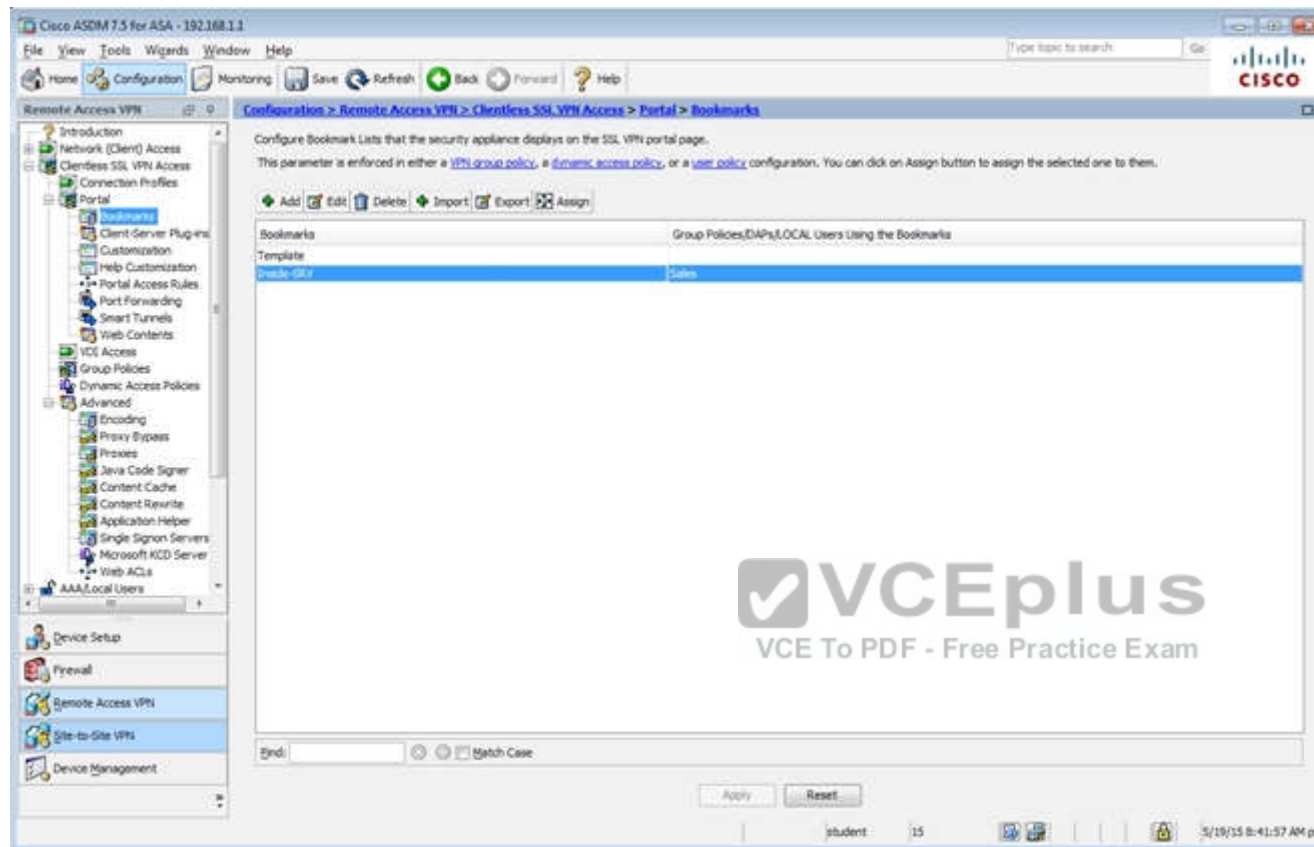
☐ Use the entire DN as the username

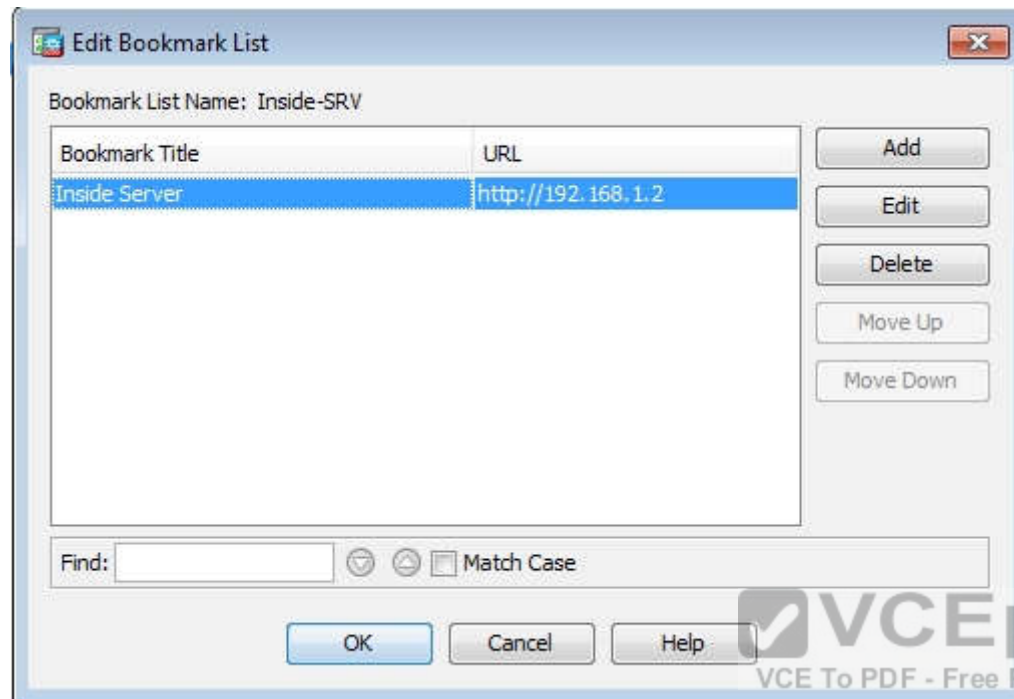
☐ Use script to select username

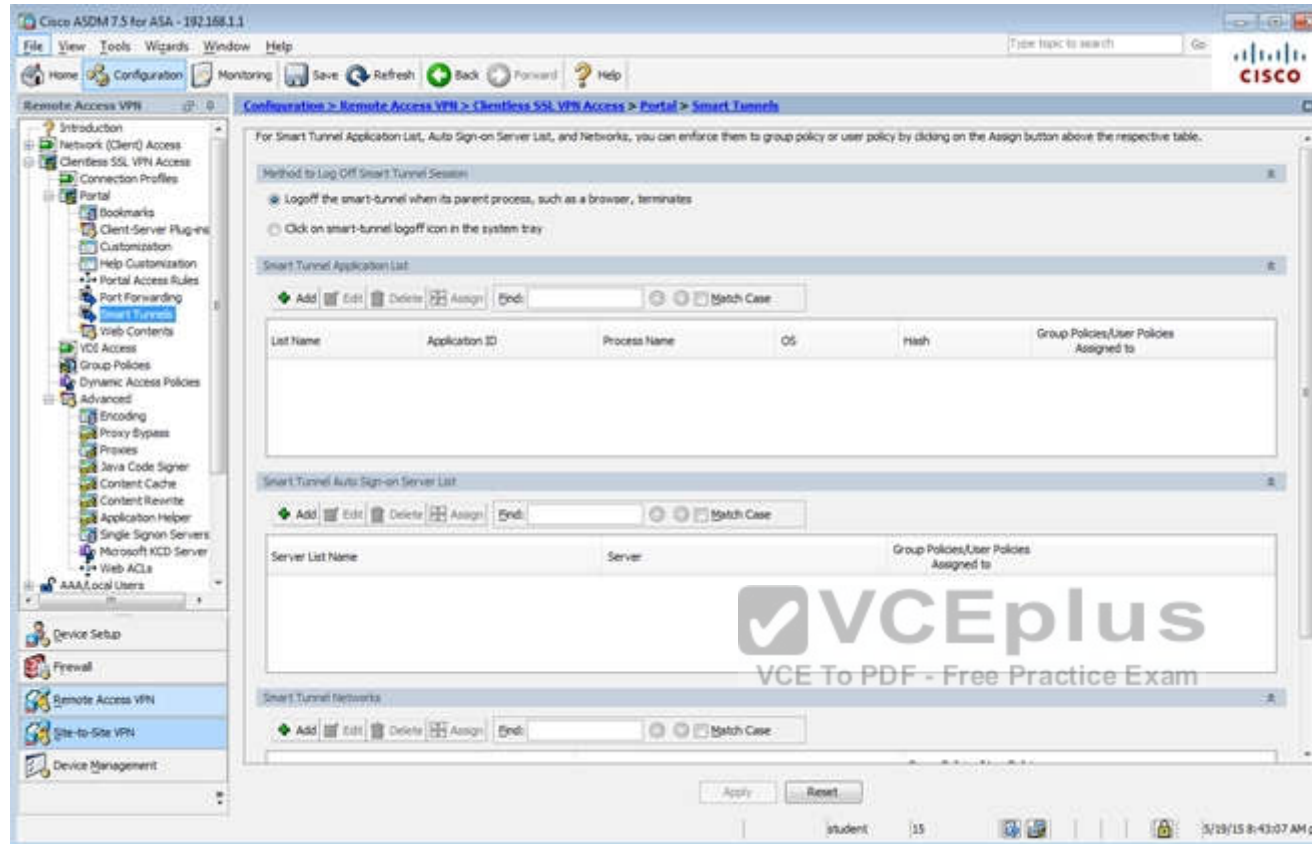
-- None -- + Add Edit Delete

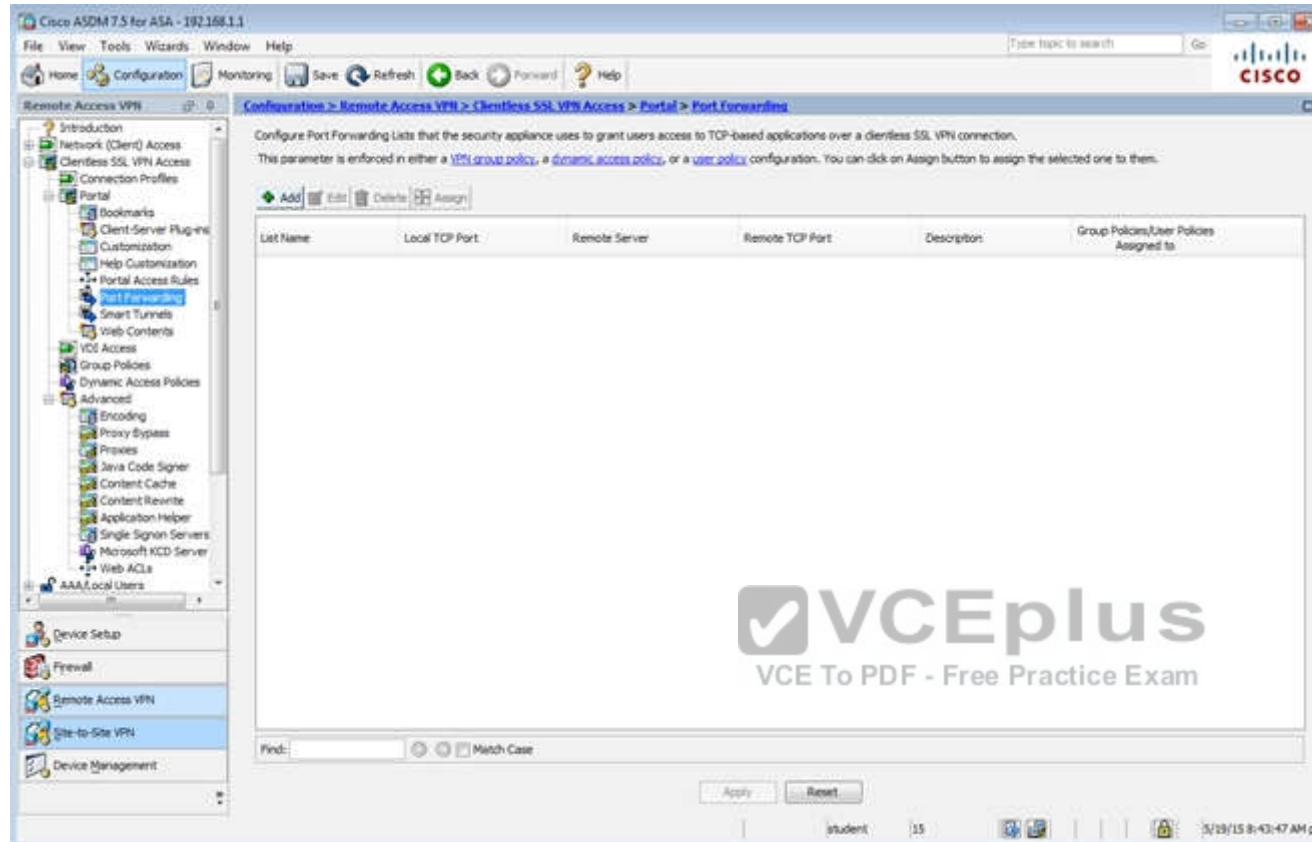
Find: Next Previous

OK Cancel Help









Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Clientless SSL VPN Access > 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 |
|--------------------------------|----------|------------------------------------|--|
| Swan | External | swan-clientless | Clientless |
| DefaultPolicy (System Default) | Internal | key1:key2:ssl-clientless/2tp-ipsec | DefaultRAGroup/DefaultL3Group/DefaultADMG/Def... |

End: Match Case

Apply Reset

student 15 3/19/15 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 ☐ LZTP/IPsec

Web ACL: ☒ Inherit Manage...

Access Hours: ☒ Inherit Manage...

Simultaneous Logins: ☒ Inherit

Restrict access to VLAN: ☒ Inherit

Connection Profile (Tunnel Group) Lock: ☒ Inherit

Maximum Connect Time: ☒ Inherit ☐ Unlimited minutes

Idle Timeout: ☒ Inherit ☐ Use Global Default minutes

Timeout Alerts

Session Alert Interval: ☒ Inherit ☐ Default minutes

Idle Alert Interval: ☒ Inherit ☐ Default minutes

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

Find: ☒ Next ☐ Previous

OK Cancel Help

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

- IPsec/SSL Connection
- Secure Mobility Solution
- Address Assignment
- Advanced
- Clientless SSL VPN Access
- Connection Profiles
- Portal
- Bookmarks
- Client-Server Plug-ins
- Customization
- Help Customization
- Portal Access Rules
- Port Forwarding
- Smart Tunnels
- Web Contents
- Voice Access
- Group Policies**
- Dynamic Access Policies
- Advanced
- AAA/Local Users
- AAA Server Groups
- LDAP Attribute Map
- Local Users
- Host Scan Image
- Secure Desktop Manager

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

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

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

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

| Name | Type | Tunneling Protocol | Connection Profiles/Users Assigned To |
|--------------------------------|----------|--------------------------------|---------------------------------------|
| Default | Internal | ssl-clientless | Default |
| DefaultPolicy (System Default) | Internal | ikev2/ssl-clientless/2to-ipsec | DefaultPolicy |

Find:

student 15 10/15/14 9:15:40 AM pet

Edit Internal Group Policy: Sales

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

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

URL Entry: ☒ Inherit ☐ Enable ☐ Disable

File Access Control

File Server Entry: ☒ Inherit ☐ Enable ☐ Disable

File Server Browsing: ☒ Inherit ☐ Enable ☐ Disable

Hidden Share Access: ☒ Inherit ☐ Enable ☐ Disable

Port Forwarding Control

Port Forwarding List: ☒ Inherit Manage...
☐ Auto Applet Download

Applet Name: ☒ Inherit

Smart Tunnel

Smart Tunnel Policy: ☒ Inherit Networks: Manage...
Tunnel Option: -- None --

Smart Tunnel Application: ☒ Inherit Manage...
☐ Smart Tunnel all Applications (This feature only works with Windows platform.)
☐ Auto Start

Auto Sign-on Server: ☒ Inherit Manage...
Windows Domain Name (optional):
Auto sign-on works only with Internet Explorer on Windows client or in Firefox on any platform.

ActiveX Relay

ActiveX Relay: ☒ Inherit ☐ Enable ☐ Disable

More Options

Find: Next Previous

OK Cancel Help

Edit Internal Group Policy: DfHGrpPolicy

Advanced

Name: DfHGrpPolicy

Banner:

SOCP forwarding URL:

Address Pools: Select...

IPv6 Address Pools: Select...

None Options

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

Filter: -- None -- Manage...

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

Simultaneous Logins: 3


Restrict access to VLANs: -- Unrestricted --

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

Maximum Connect Time: ☒ Unlimited ☐ 180/000

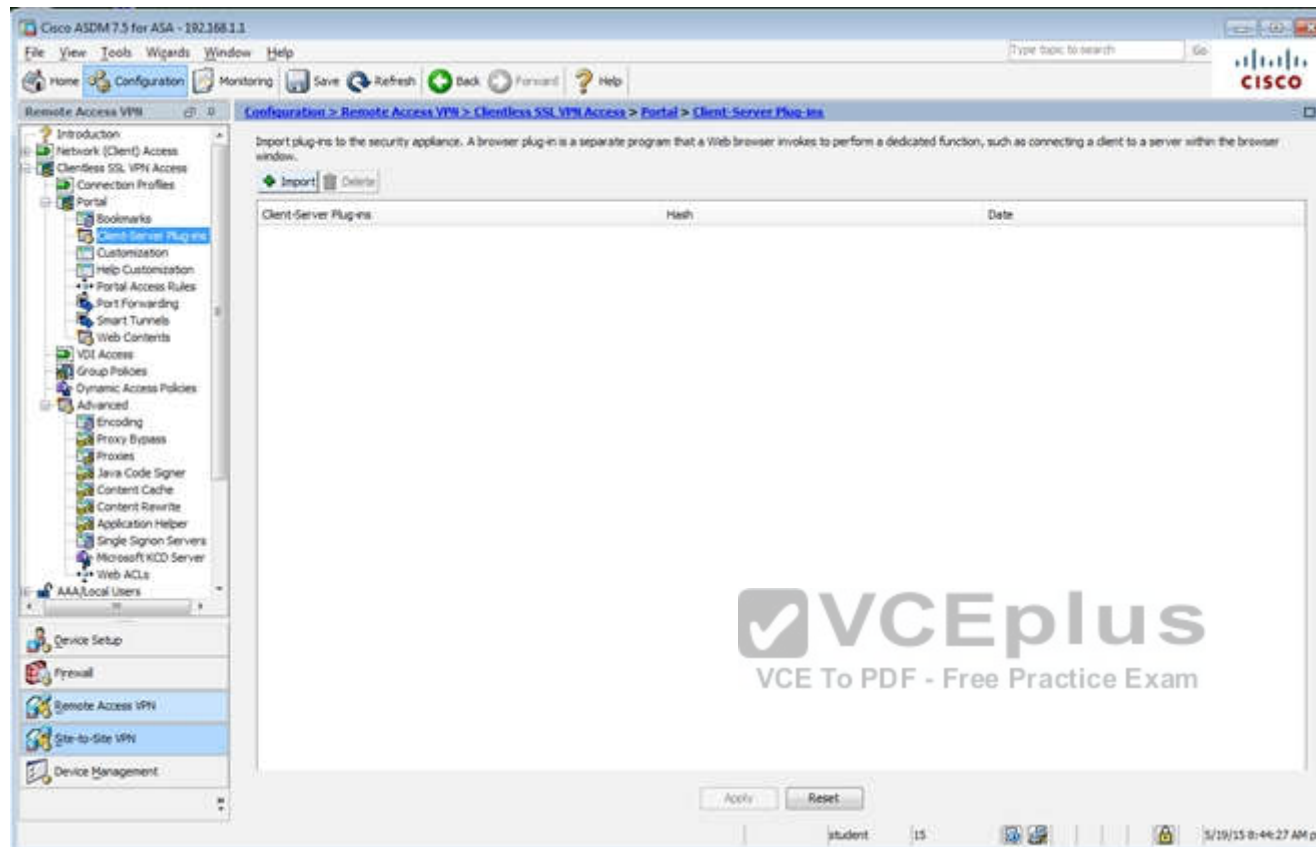
Idle Timeout: ☐ None 30 minutes

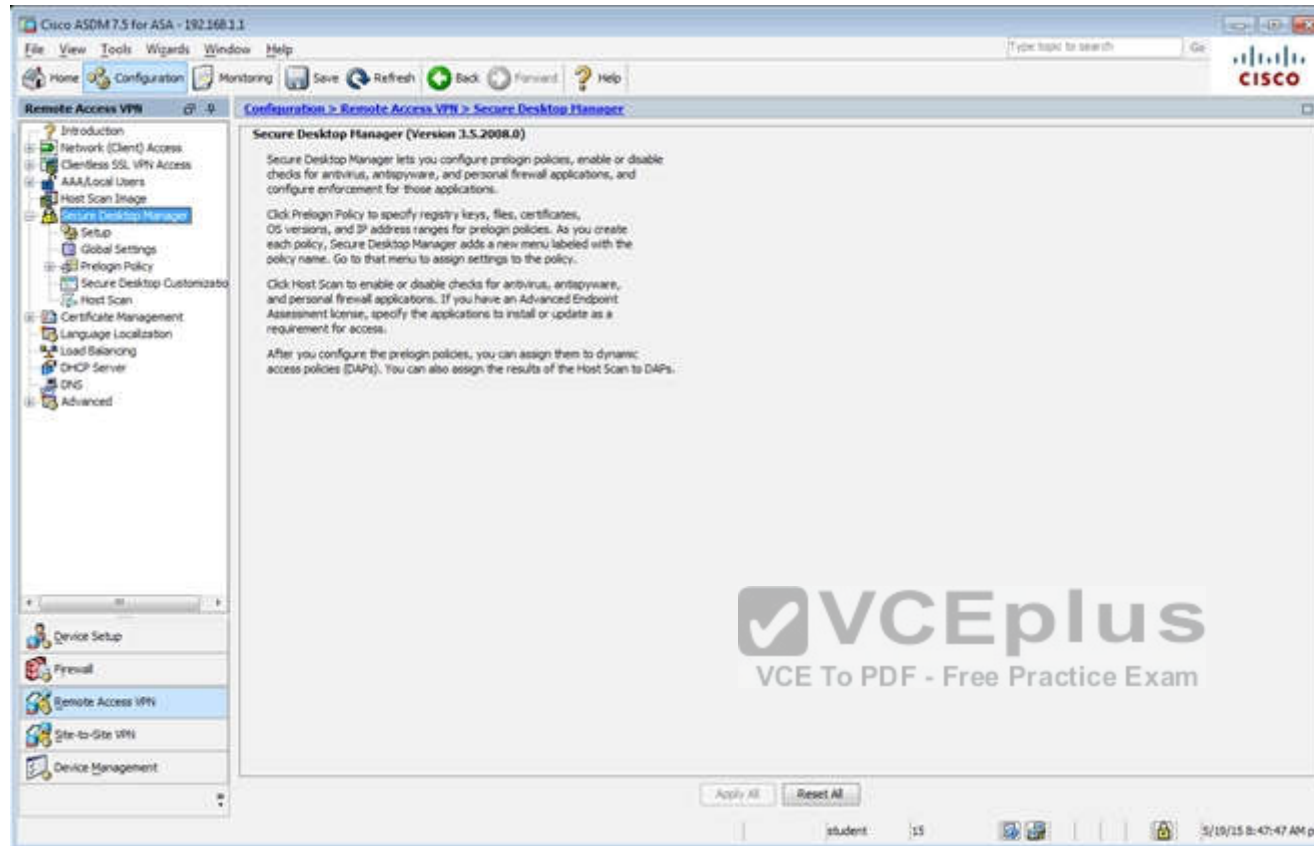
On smart card removal: ☒ Disconnect ☐ Keep the connection

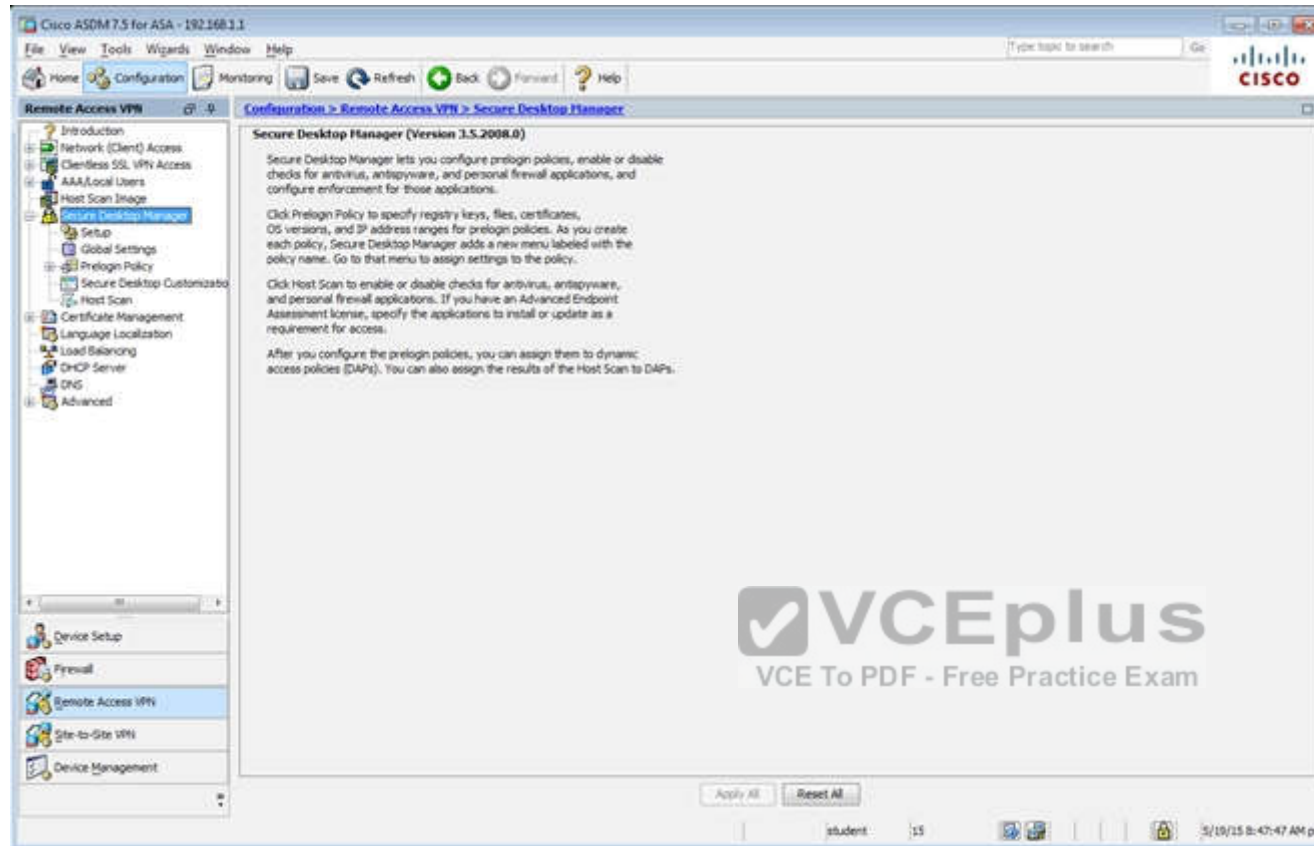
 **VCEplus**
VCE To PDF - Free Practice Exam

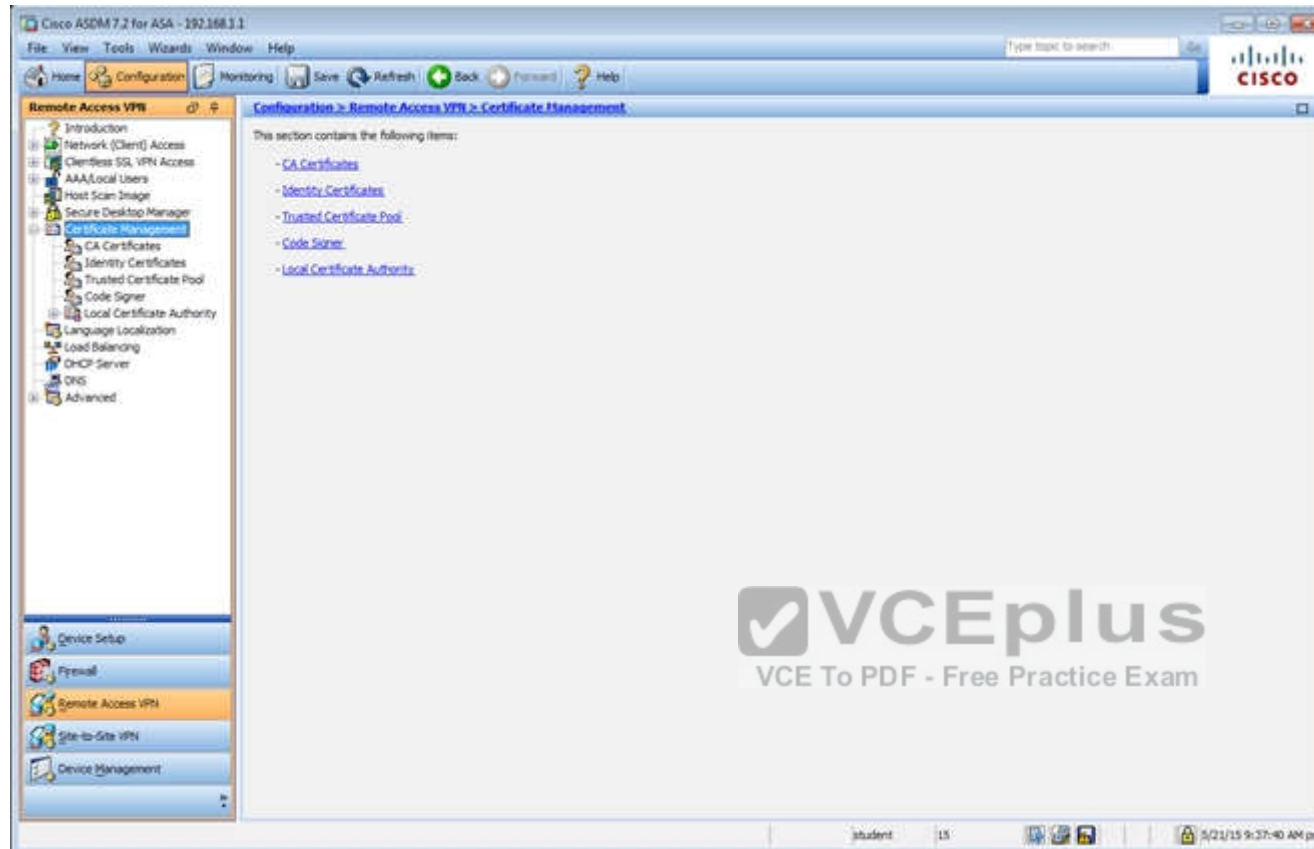
Find: Next Previous

OK Cancel Help

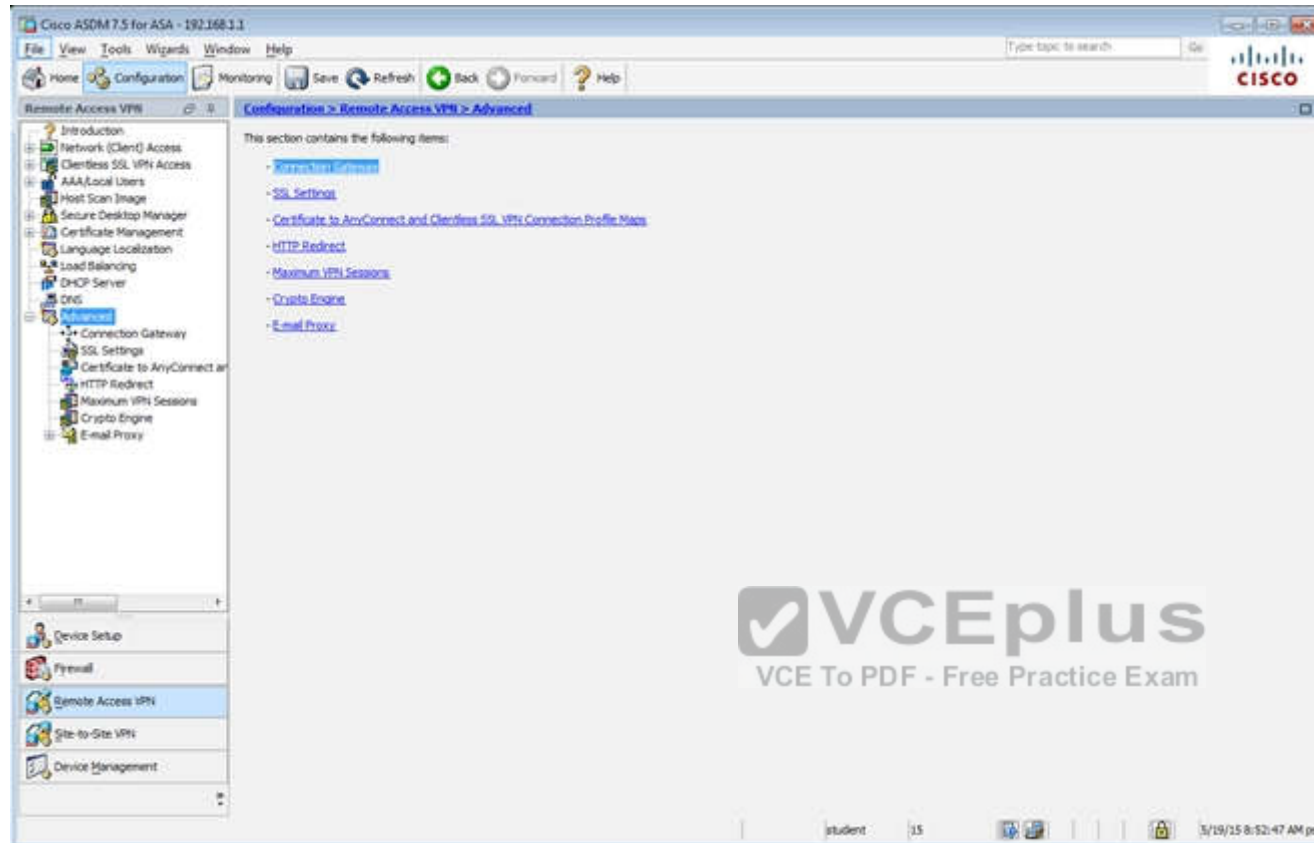


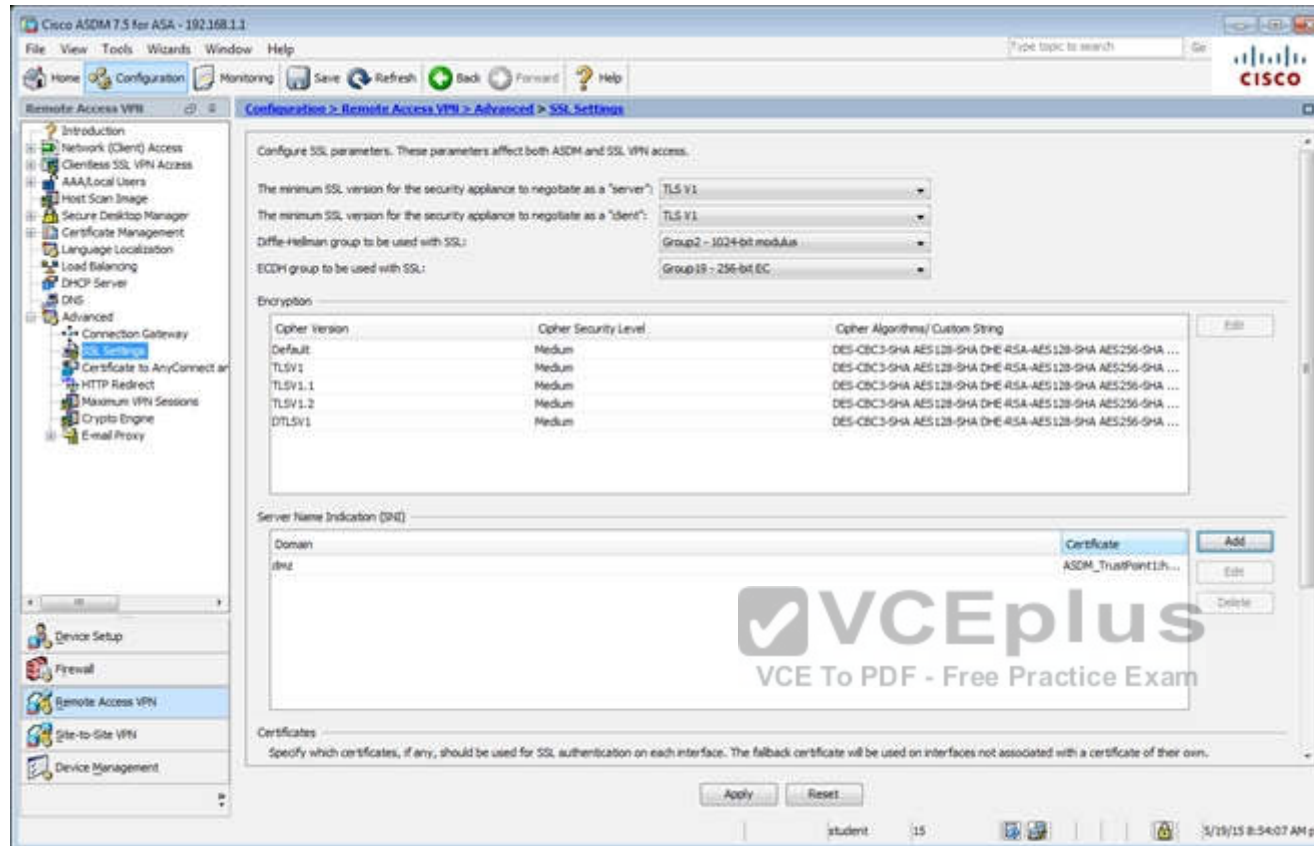


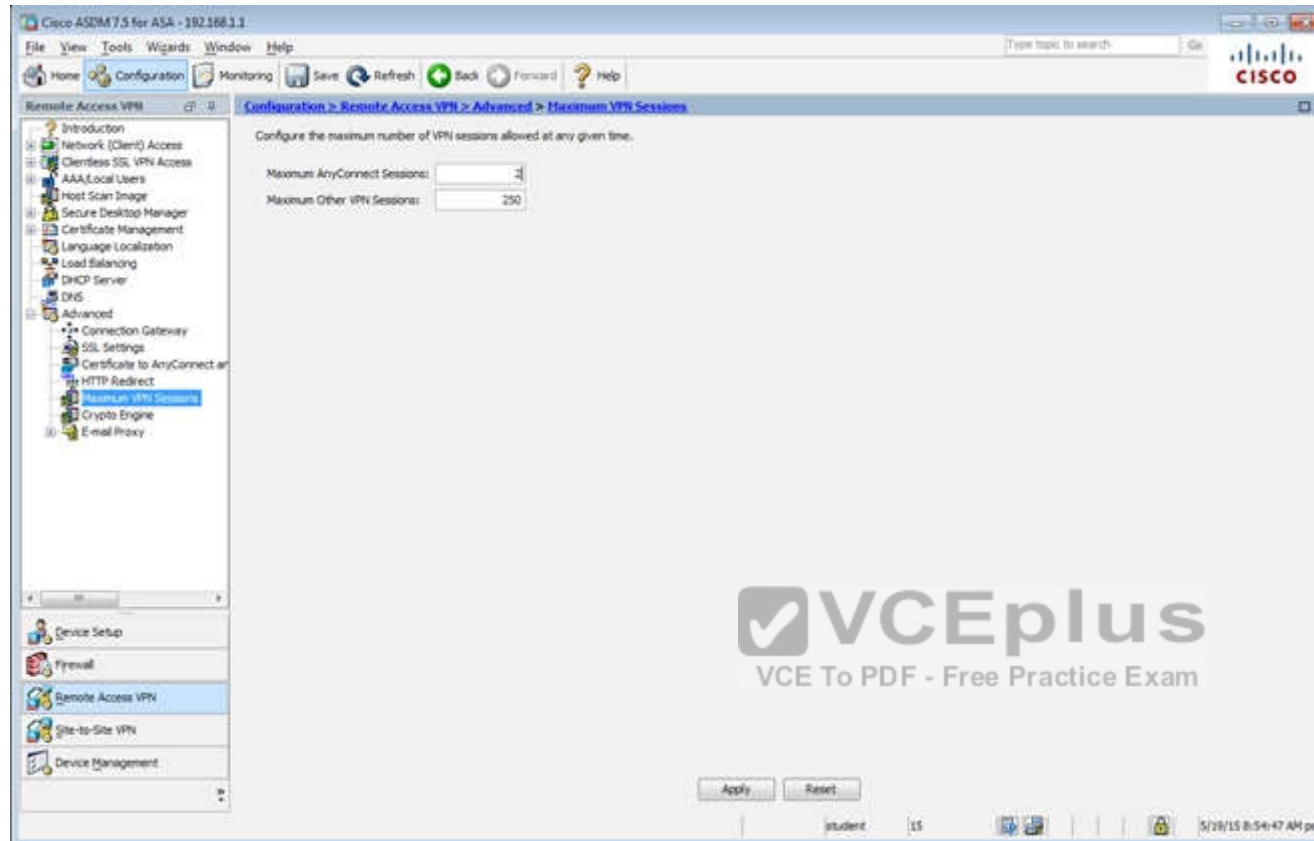


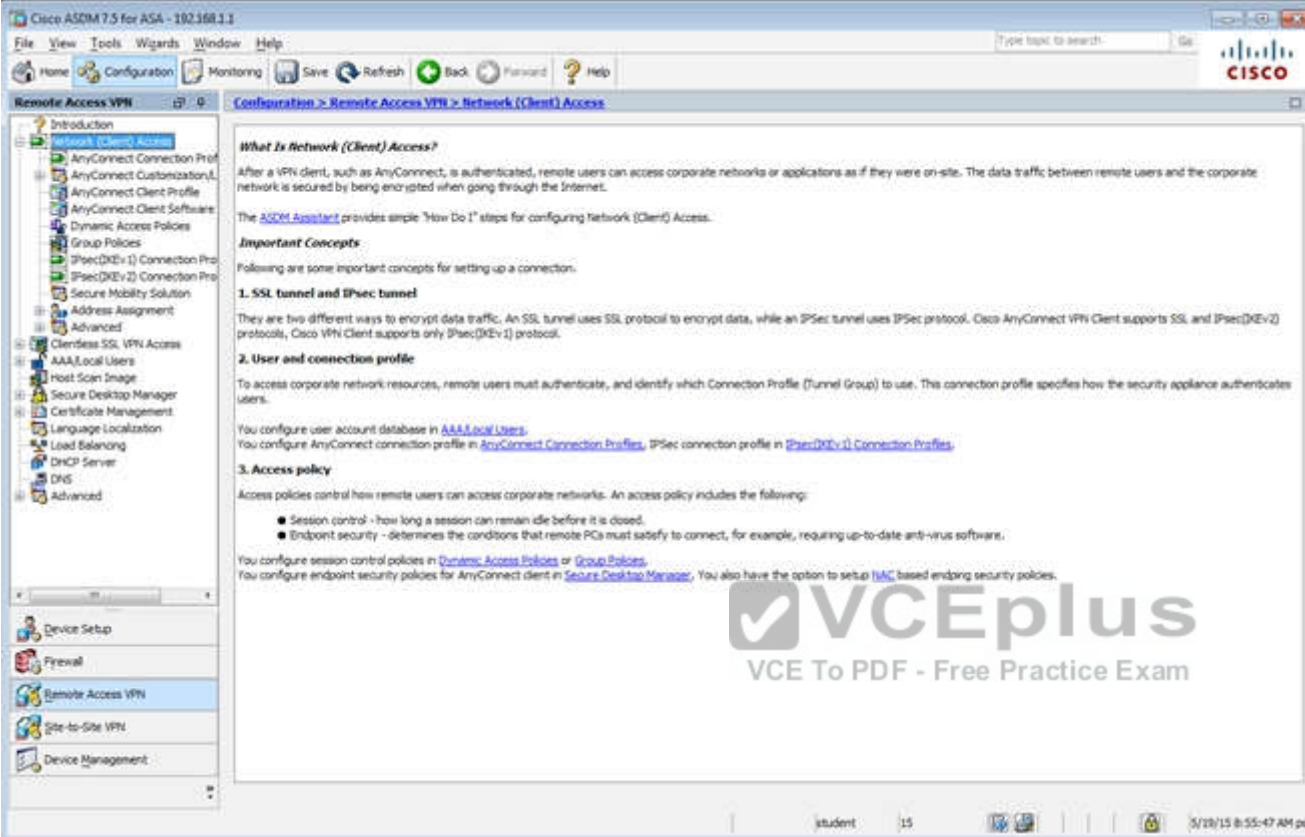


The screenshot shows the Cisco ASDM 7.3 for ASA - 192.168.1.1 interface. The left sidebar contains a tree view with categories like Remote Access VPN, Configuration, Monitoring, and Advanced. The main pane is titled 'Configuration > Remote Access VPN > Certificate Management > Identity Certificates'. It features a table with columns: Issued To, Issued By, Expiry Date, Associated Trustpoints, Usage, and Public Key Type. A single entry is visible: 'hostname-4P (17-ASA-sec...' issued by 'hostname-4P (17-ASA-sec...' with an expiry date of '11:00:33 pet 1 Dec 20 2024'. Below the table are buttons for Add, Show Details, Delete, Export, and Install. Further down, there are sections for 'Certificate Expiration Alerts' with input fields for 'Send the first alert before' (60 days) and 'Repeat Alert Interval' (7 days), and a 'Public CA Enrollment' section with a button 'Enroll ASA SSL certificate with Enroll...'. At the bottom, there is an 'ASDM Identity Certificate Wizard' section with a button 'Launch ASDM Identity Certificate Wizard...'. The status bar at the bottom indicates 'student' and '15'.









Cisco ASDM 7.5 for ASA - 102.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

What Is Network (Client) Access?

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

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

Important Concepts

Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel

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

2. User and connection profile

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

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

3. Access policy

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

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

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

student 15 5/29/15 8:55:47 AM pct

The screenshot shows the Cisco ASDM 7.2 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Remote Access VPN' expanded, showing 'Network (Client) Access' and 'Group Policies'. The main pane shows the 'Group Policies' configuration page. It includes a description of VPN group policies and a table of existing policies.

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

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

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

Buttons: Add, Edit, Delete, Assign

| Name | Type | Tunneling Protocol | Connection Profiles/Users Assigned To |
|----------------------------------|----------|--|---|
| Sales | Internal | ssl-clientless | clientless |
| TestGroupPolicy (System Default) | Internal | l2l3-clientless/ssl-clientless/zip-gwsec | [Default]RAGroupDefault & GroupDefaultWebVPNGroup |

Find: Match Case

Buttons: Apply, Reset

Taskbar: student 15 3/21/15 10:17:10 AM pet

Edit Internal Group Policy: DfGpPolicy

Advanced

Servers

Advanced

- Split Tunneling
- Browser Proxy
- AnyConnect Client
- Spec(DfGp) Client

Name: DfGpPolicy

Server:

SCP forwarding URL:

Address Pool:

IPv6 Address Pool:

Select...

Select...

More Options

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

Filter: --None-- Manage...

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

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

Simultaneous Logins: 3

Restrict access to VLAN: --Unrestricted--

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

Maximum Connect Time: ☒ Unlimited ☐ minutes

Idle Timeout: ☐ None ☐ 30 minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

VCEplus
VCE To PDF - Free Practice Exam

Find: Next Previous

OK Cancel Help

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction
Network (Client) Access
AnyConnect Connection Profile
AnyConnect Customization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec (IKEv1) Connection Profile
IPsec (IKEv2) Connection Profile
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced

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

Access Interfaces
Enable interfaces for IPsec access.

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

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

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

+ Add Edit Delete

| Name | IPsec Enabled | L2TP/IPsec Enabled | Authentication Server Group | Group Policy |
|--------------------|-------------------------------------|-------------------------------------|-----------------------------|---------------|
| DefaultRAGroup | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD | DiffGrpPolicy |
| DefaultWEBVPNGroup | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD | DiffGrpPolicy |
| Services | <input type="checkbox"/> | <input type="checkbox"/> | LOCAL | Local |

End: Match Case

Apply Reset

student 15 5/18/15 8:56:47 AM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec (IKEv2) 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

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

Access Interfaces

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

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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

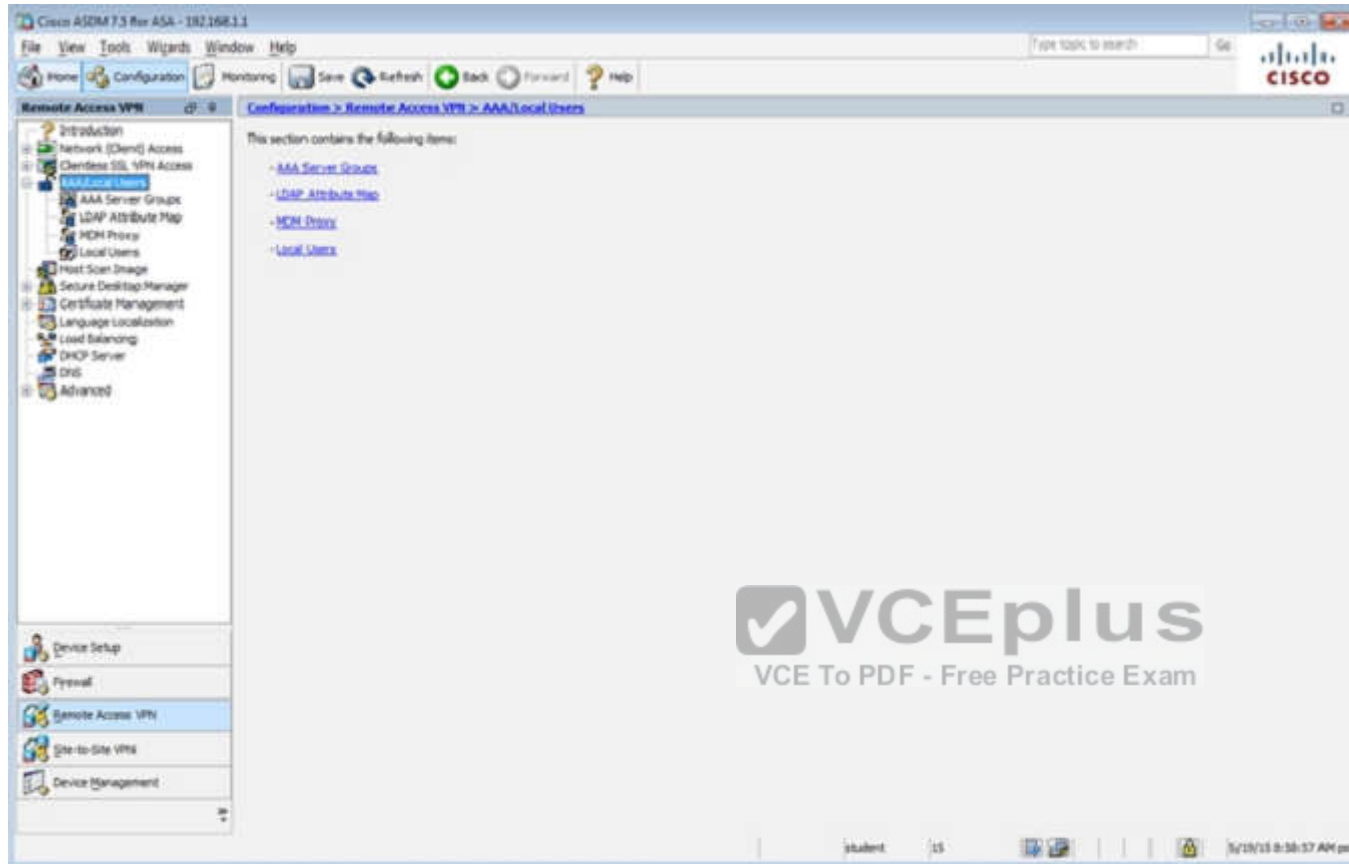
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Find:

| Name | SSL Enabled | IPsec Enabled | Authentication Method | Group Policy |
|--------------------|-------------------------------------|-------------------------------------|-----------------------|--------------------|
| DefaultRAGroup | <input type="checkbox"/> | <input type="checkbox"/> | AAA(RADIUS) | DefaultGroupPolicy |
| DefaultTNSVPNGroup | <input type="checkbox"/> | <input checked="" type="checkbox"/> | AAA(RADIUS) | DefaultGroupPolicy |
| Clientless | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | AAA(LOCAL) | DefaultGroupPolicy |

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

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > AAA Local Users > 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 [Authentication](#).

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

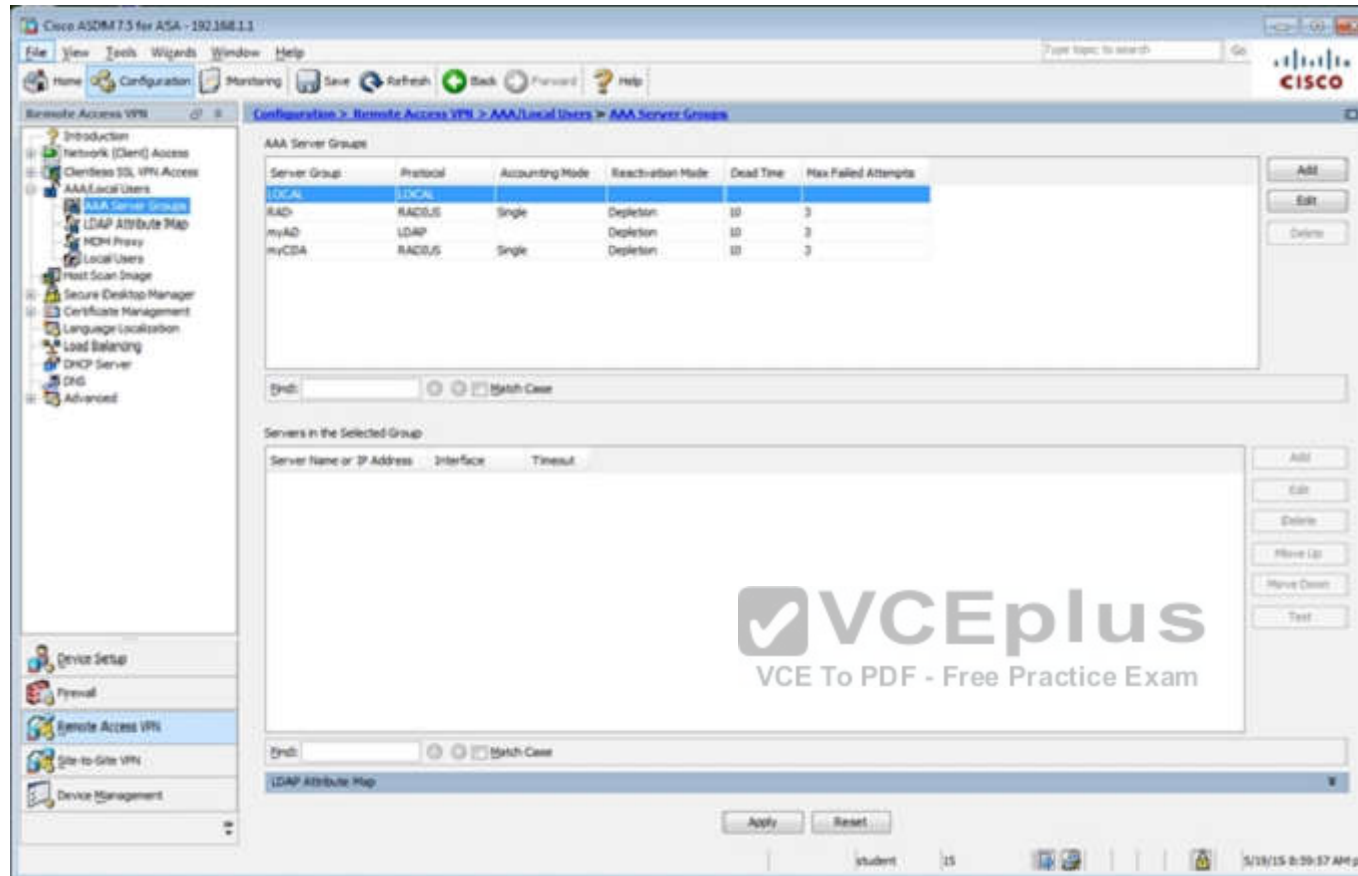
| Username | Privilege Level (Role) | Access Restrictions | VPN Group Policy | VPN Group Lock |
|-----------|------------------------|---------------------|----------------------------|----------------------------|
| student | 15 | Full | -- Inherit Group Policy -- | -- Inherit Group Policy -- |
| enable_15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

Buttons: Add, Edit, Delete

End: [] [] [] Switch Case

Buttons: Apply, Reset

student 15 5/19/13 8:59:27 AM pct



Which four 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

Correct Answer: ADEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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



Virtual Terminal

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

- Introduction
- Network (Client) Access
- Clientless SSL VPN Access
 - Connection Profiles
 - Portal
 - Bookmarks
 - Client-Server Plug-ins
 - Customization
 - Help Customization
 - Portal Access Rules
 - Port Forwarding
 - Smart Tunnels
 - Web Contents
 - VDI Access
 - Group Policies**
 - Dynamic Access Policies
 - Advanced
 - Encoding
 - Proxy Bypass
 - Proxies
 - Java Code Signer
 - Content Cache
 - Content Rewrite
 - Application Helper
 - Single Signon Servers
 - Microsoft KCD Server
 - Web ACLs
- AAA/Local Users

Manage VPN group policies. A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally. 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 |
|--------------------------------|----------|---------------------------------------|
| Sales | Internal | ssl-clientless |
| DfltGrpPolicy (System Default) | Internal | ikev1;ikev2;ssl-clientless;l2tp-ipsec |

VCEplus
VCE To PDF - Free Practice Exam

Device Setup

QUESTION 65**Scenario**

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

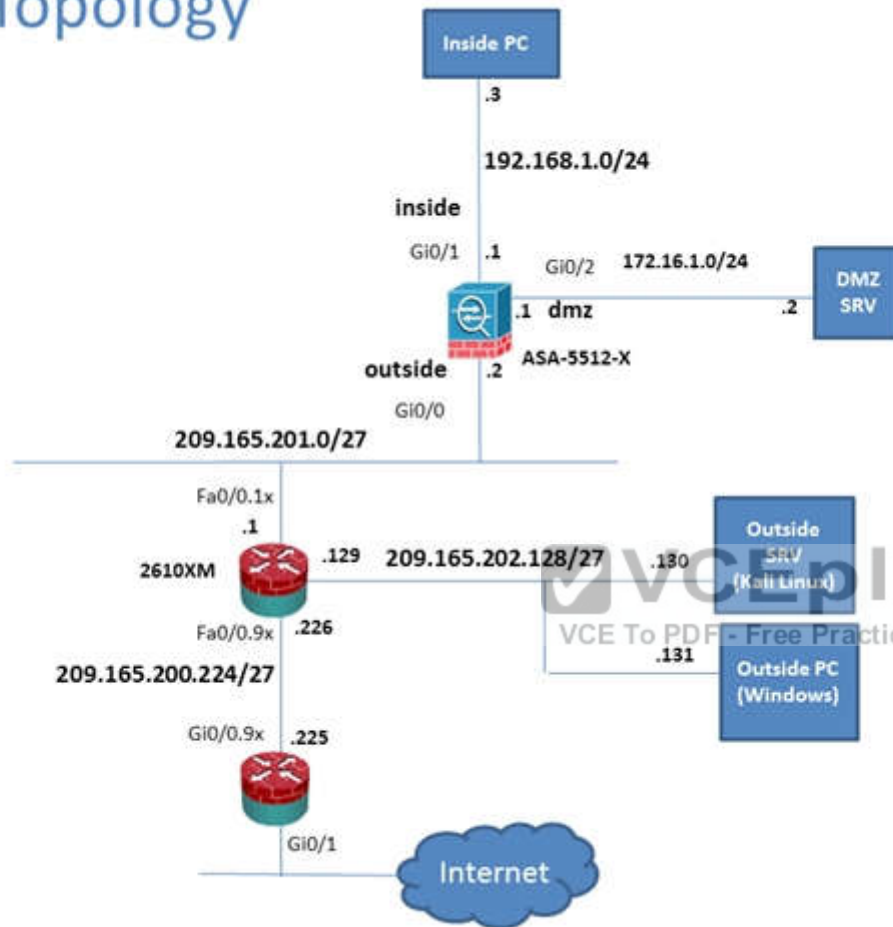
To access ASDM, click the ASA icon in the topology diagram.

Note: Not all ASDM functionalities are enabled in this simulation.

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



Lab Topology



Cisco ASDM 7.5 for ASA - 100.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Home: Device Dashboard Firewall Dashboard ASA Firewall Status

Device Information

General License

Host Name: **P17-ASA-secure-x-local**
 ASA Version: **100.14(6)13**
 ASDM Version: **7.5(131)**
 Firewall Mode: **Routed**
 Environment Status: **OK**

Device Uptime: **11d 23h 42m 47s**
 Device Type: **ASA 5512**
 Context Mode: **Single**
 Total Flash: **4096 MB**

Interface Status

| Interface | IP Address/Mask | Line | Link | Up | Down | Kbps |
|-----------|------------------|------|------|----|------|------|
| Gig0/0 | 172.16.1.1/24 | 0 | Up | 0 | 0 | 0 |
| inside | 192.168.1.1/24 | 0 | Up | 0 | 0 | 4 |
| mgmt | 10.10.10.1/24 | 0 | Up | 0 | 0 | 0 |
| outside | 209.165.201.2/24 | 0 | Up | 0 | 0 | 0 |

Select an interface to view input and output Kbps

VPN Sessions

IPsec: 0 Clientless SSL VPN: AnyConnect Client: 0 [Details](#)

System Resources Status

Total Memory Usage Total CPU Usage Core Usage [Details](#)

Memory Usage (MB)

Traffic Status

Connections Per Second Usage

Legend: UDP: 0 TCP: 0 Total: 0

Outside Interface Traffic Usage (Kbps)

Legend: Input Kbps: 0 Output Kbps: 0

Latest ASDM Syslog Messages

| Severity | Date | Time | Syslog ID | Source IP | Source | Destination IP | Destination Description |
|----------|-------------|----------|-----------|---------------|--------|----------------|---|
| 6 | May 13 2015 | 12:35:09 | 302016 | 20.81.254.202 | 123 | 209.165.201.2 | 65535 Teardown UDP connection 15136525 for outside:20.81.254.202/223 to identity:209.165.201.2/65535[any] duration 0:02:01 bytes 96 |
| 6 | May 13 2015 | 12:35:08 | 109015 | 192.168.1.1 | 84676 | 192.168.1.1 | 443 Deny TCP (no connection) from 192.168.1.1/4476 to 192.168.1.1/443 flags PSH ACK on interface inside |
| 6 | May 13 2015 | 12:35:08 | 302014 | 192.168.1.1 | 84676 | 192.168.1.1 | 443 Teardown TCP connection 15136528 for inside:192.168.1.1/4476 to identity:192.168.1.1/443 duration 0:00:00 bytes 200 TCP Reset O |

Student 15 3/13/15 12:35:18 PM PST

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

| Interface | IP Address | MAC Address | Proxy ARP |
|-----------|--------------|----------------|-----------|
| outside | 192.168.1.1 | 000c.3014.3030 | No |
| inside | 192.168.1.4 | 0050.5635.3333 | No |
| inside | 192.168.1.3 | 0050.5631.1111 | No |
| inside | 192.168.1.2 | 0050.5623.2222 | No |
| inside | 192.168.1.56 | 0050.5692.5c7b | No |
| inside | 192.168.1.55 | 0006.8e65.9ef3 | No |
| dmz | 172.16.1.2 | 0050.5644.4444 | No |
| right | 10.10.10.1 | 000c.3014.3030 | No |

Clear Dynamic ARP Entries

Refresh

Data Refreshed Successfully.

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

student 15 3/19/15 9:32:27 AM pet

Cisco ASDM 7.3 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

VPN

Monitoring > VPN > VPN Statistics > Sessions

VPN Statistics

- Sessions
- VPN Cluster Loads
- Crypto Statistics
- Compression Statistics
- Encryption Statistics
- Global IKE/Peer Statistics
- Protocol Statistics
- LAN Mapping Sessions
- MDM Proxy Statistics
- MDM Proxy Sessions
- Clientless SSL VPN
- VPN Connection Graphs
- WSA Sessions

Interfaces

VPN

Outbound Traffic Filter

Routing

Properties

Logging

Data Refreshed Successfully.

Type Active Cumulative Peak Concurrent Inactive

| | | | | |
|----------------|--|---|---|---|
| Clientless VPN | | 1 | 1 | 1 |
| Broadband | | 1 | 1 | 1 |

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

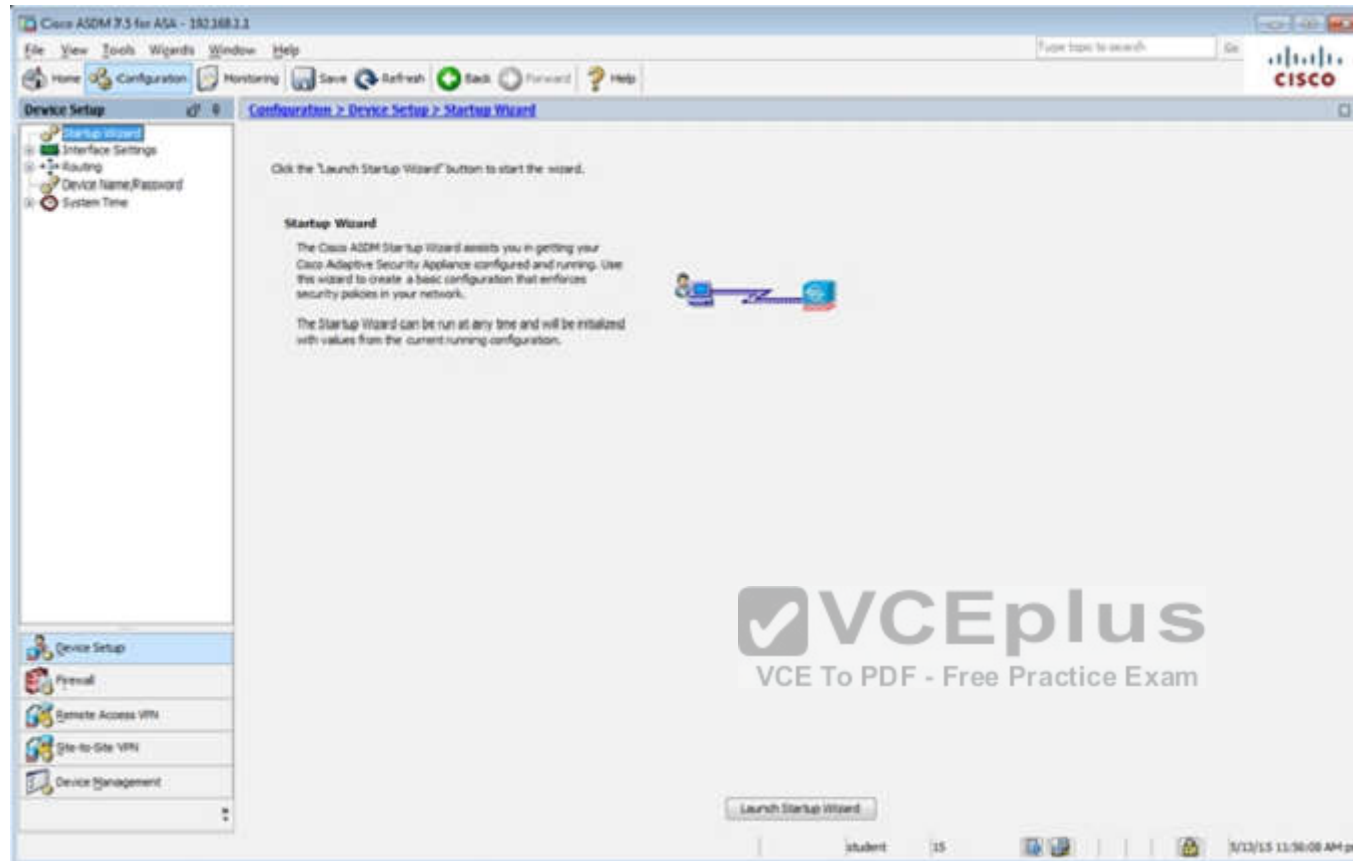
| Username IP Address | Group Policy Connection Profile | Protocol Encryption | Login Time Duration | Bytes Tx Bytes Rx |
|------------------------|------------------------------------|------------------------|------------------------------|----------------------|
| student | Default | Clientless | 08-05-16 per Thu May 21 2015 | 216724 |
| 192.168.1.1 | Clientless | Clientless (IKEv2) | 08-05-16 | 14615 |

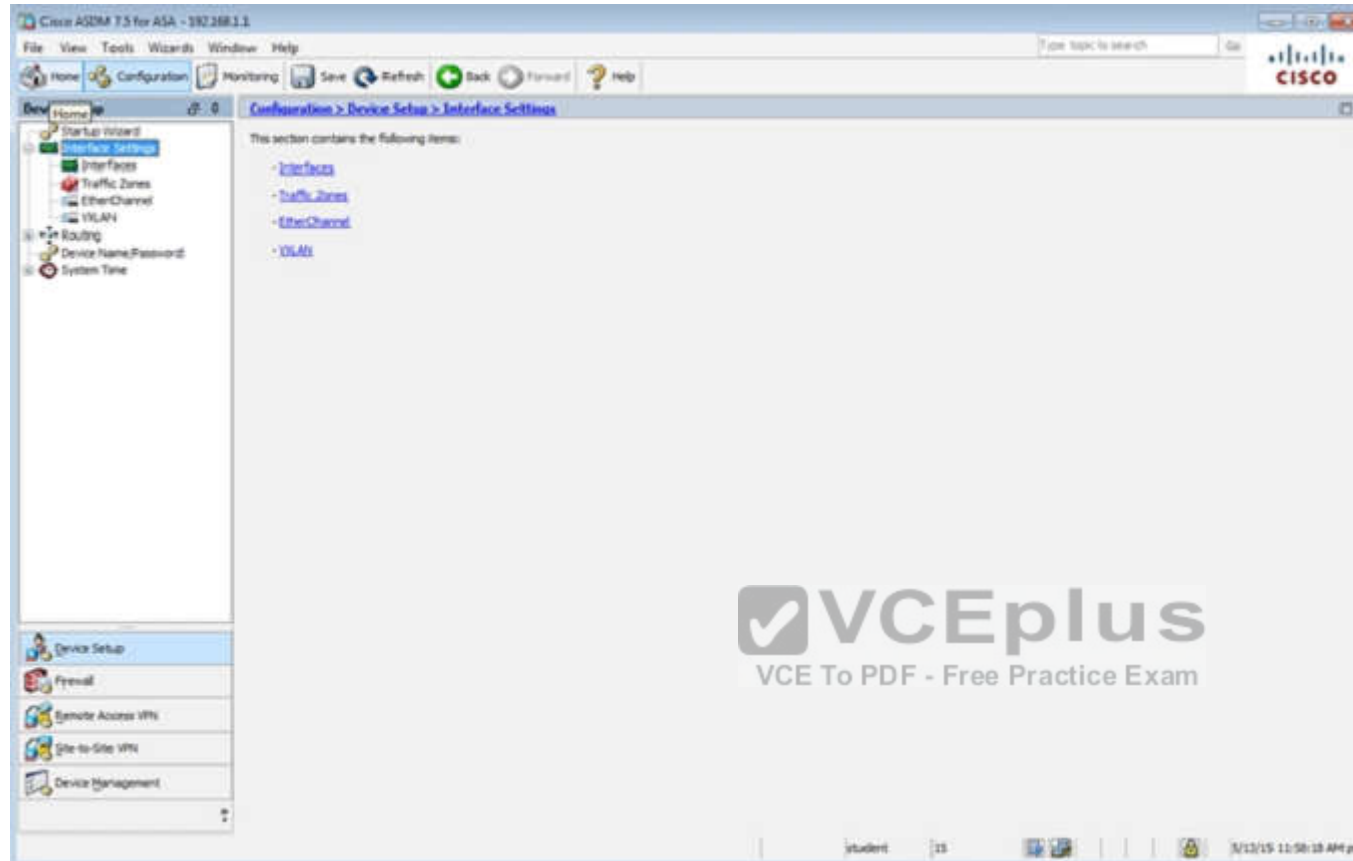
Details Logout Ping

Refresh

Last Updated: 5/16/15 9:33:12 AM

student 15 5/16/15 9:33:17 AM per





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup Configuration > Device Setup > Interface Settings > Interfaces

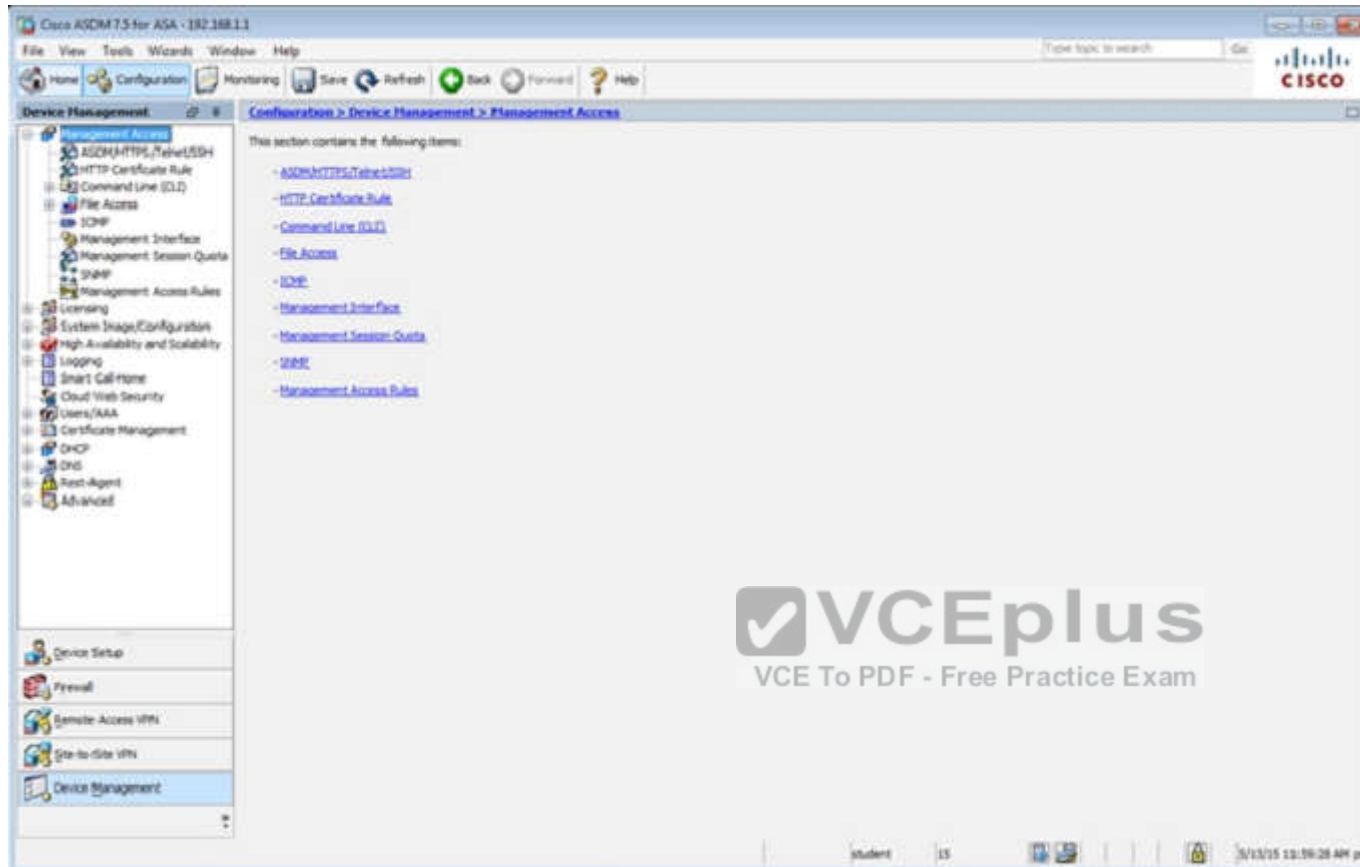
Startup Wizard
Interface Settings
Traffic Zones
EtherChannel
VLANs
Routing
Device Name/Password
System Time

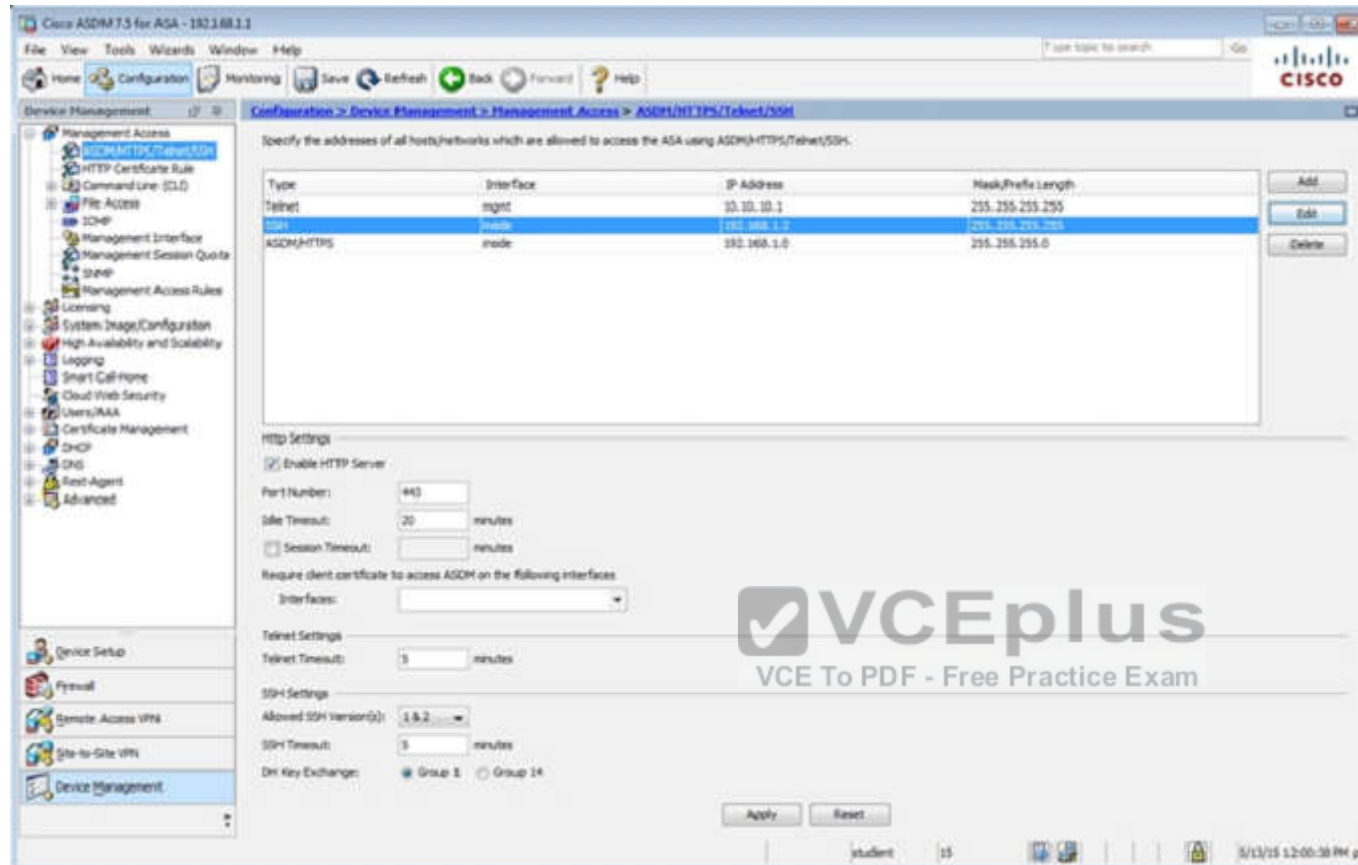
Device Setup
Firewall
Remote Access VPNs
Site-to-Site VPNs
Device Management

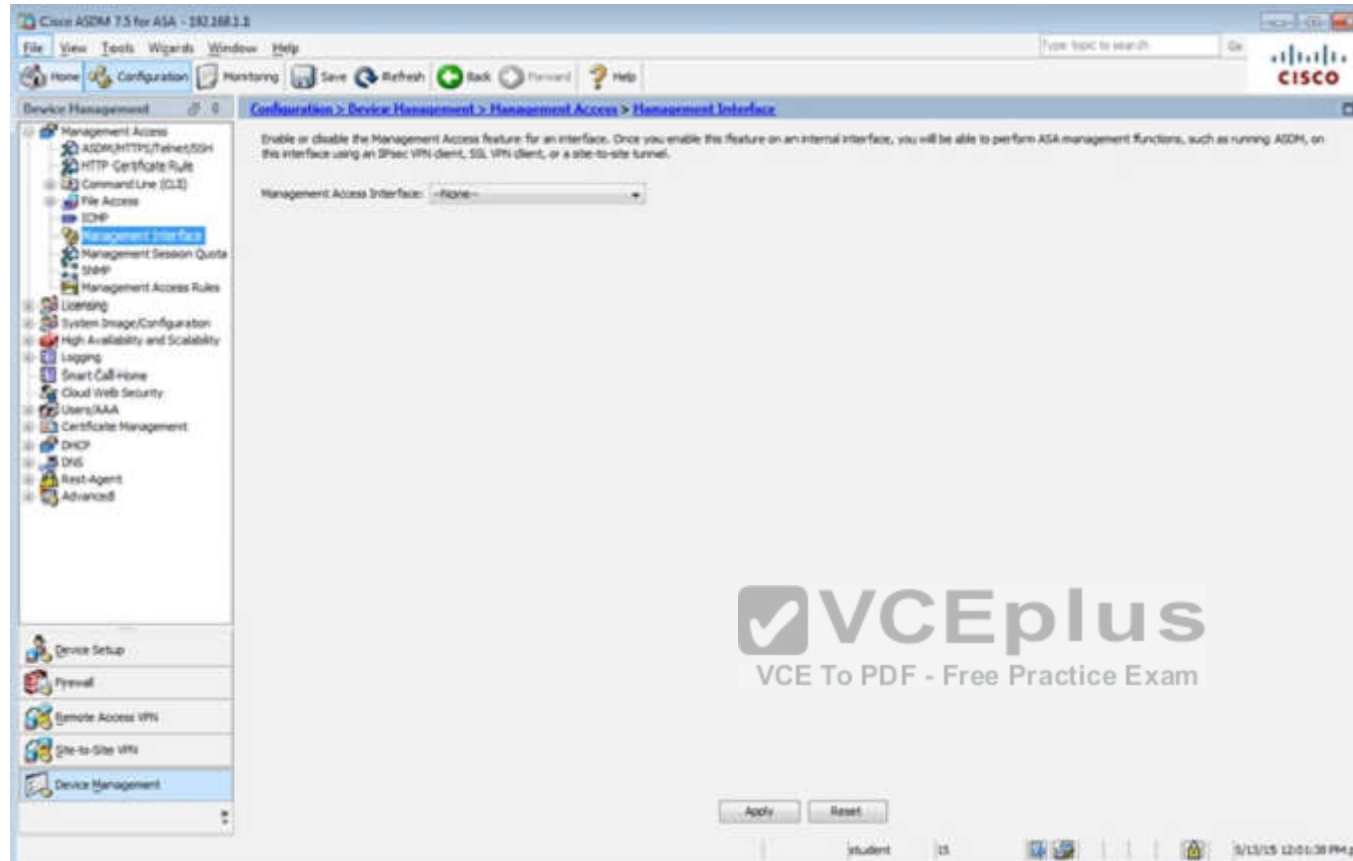
| Interface | Name | Zone | Route Map | State | Security Level | IP Address | Subnet Mask Prefix Length | Group | Type |
|--------------------|---------|------|-----------|---------|----------------|-------------|------------------------------|-------|----------|
| GigabitEthernet0/0 | outside | | |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

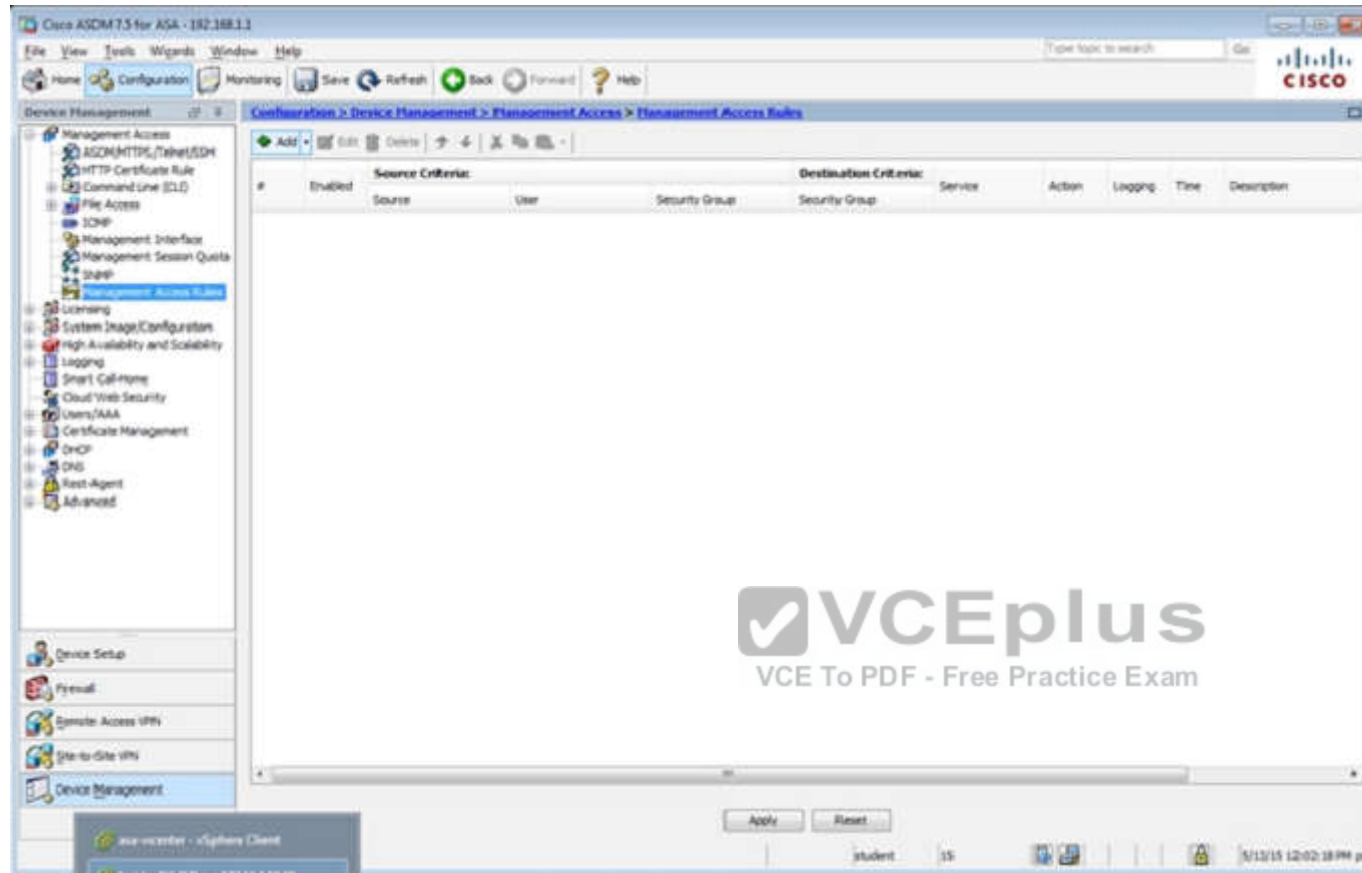
☐ Enable traffic between two or more interfaces which are configured with same security levels
☐ Enable traffic between two or more hosts connected to the same interface
☐ Enable jumbo-frame reservation

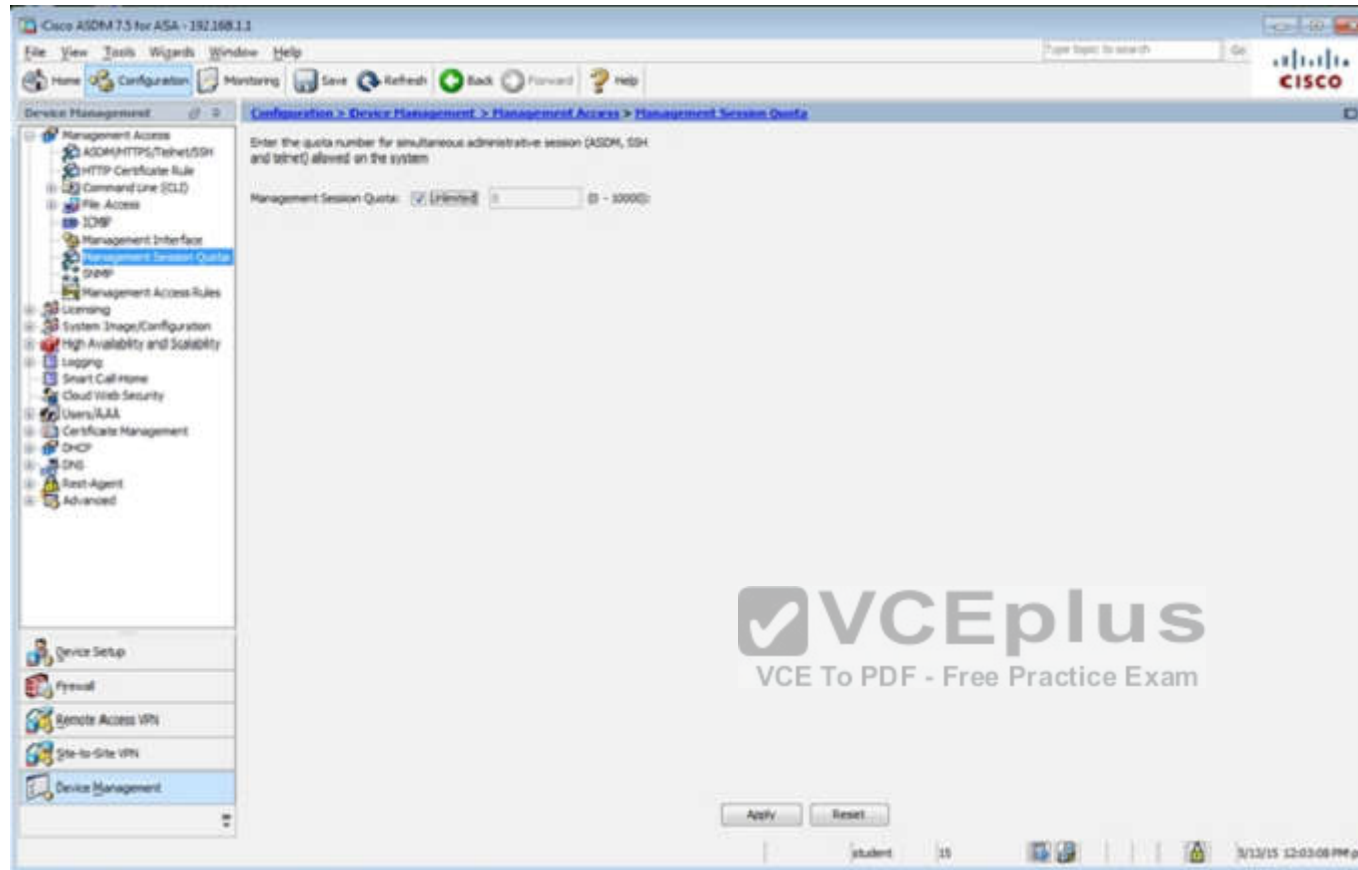
student 15 5/13/15 12:42:48 PM pet

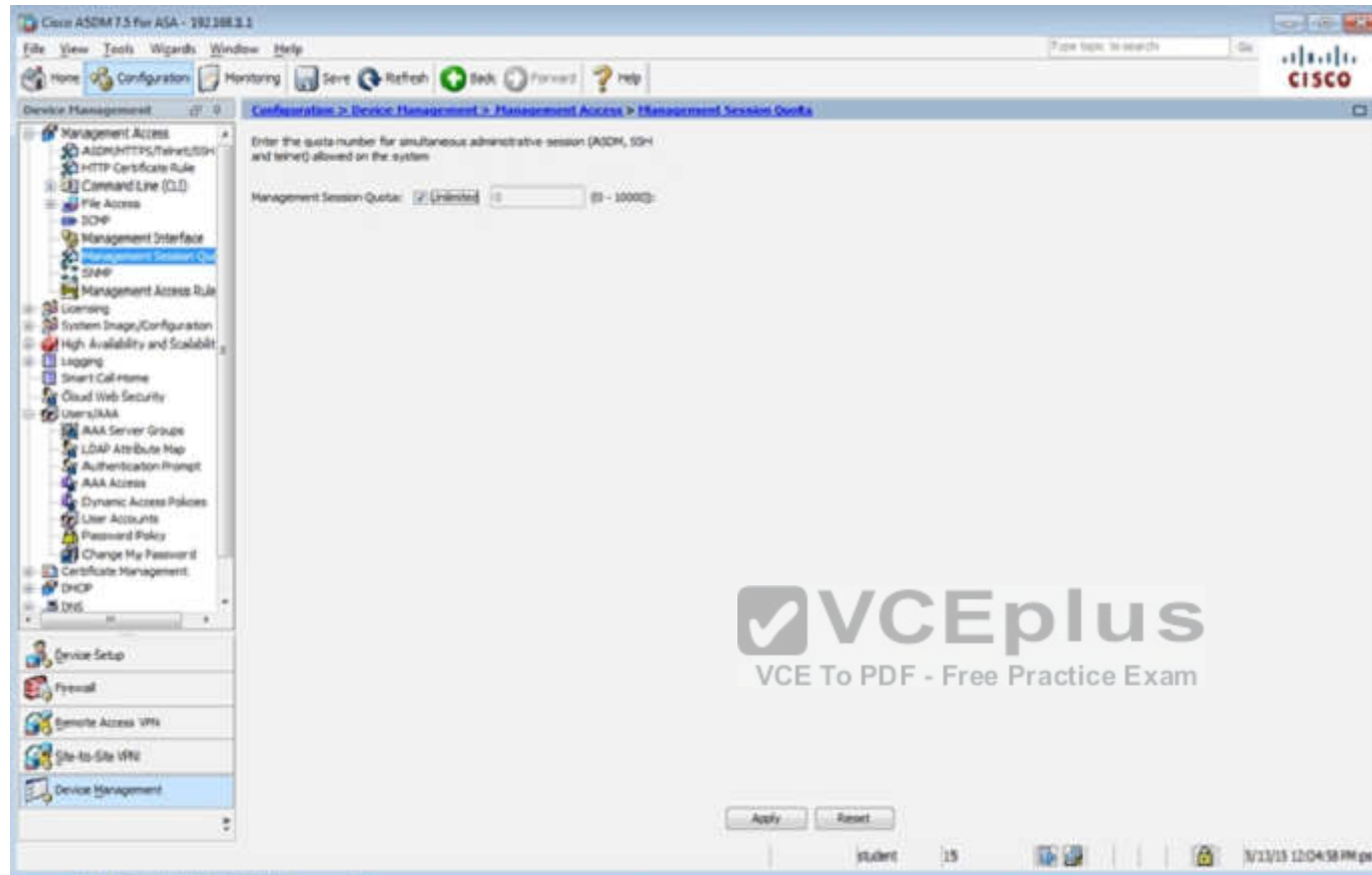


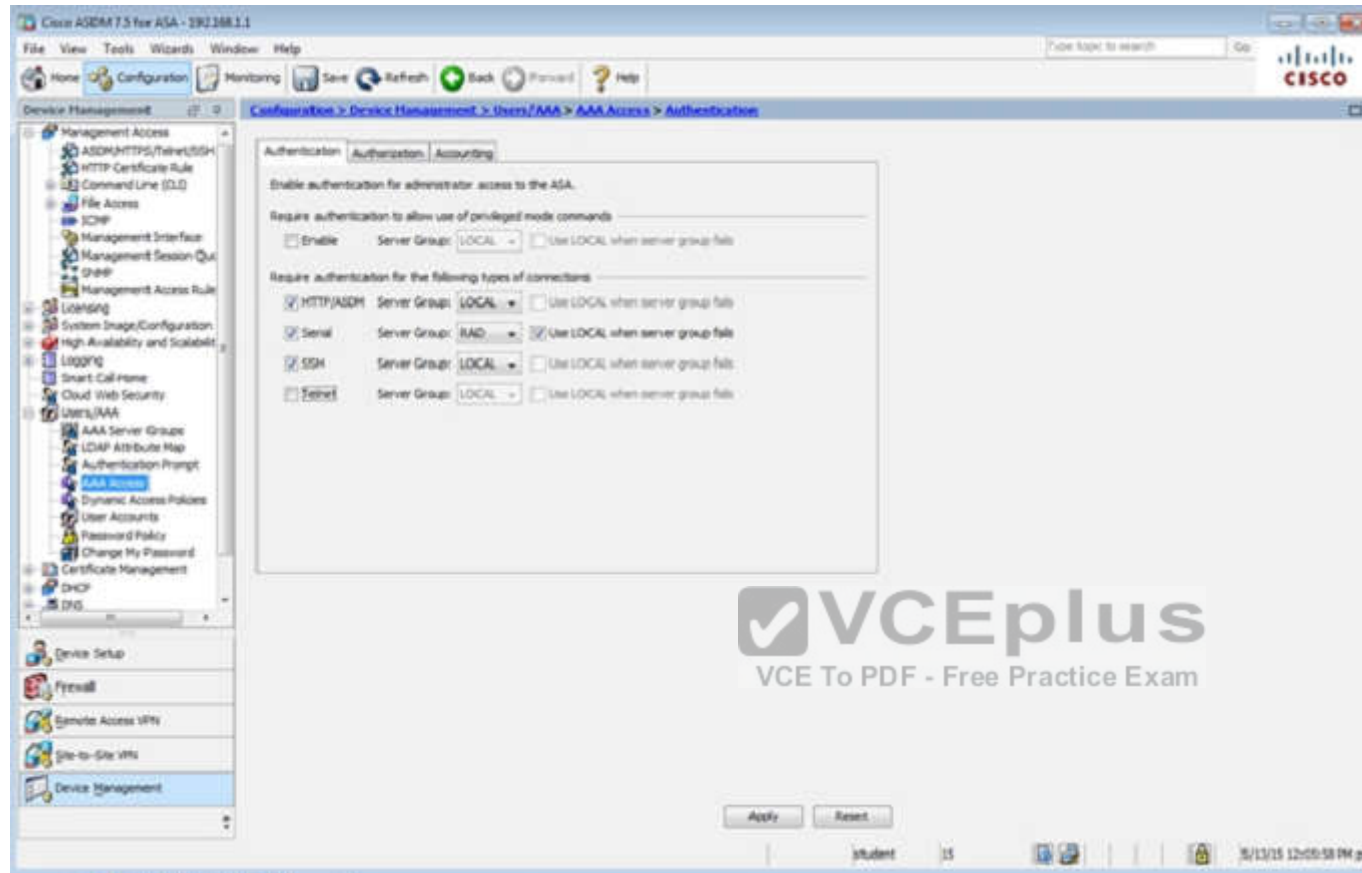


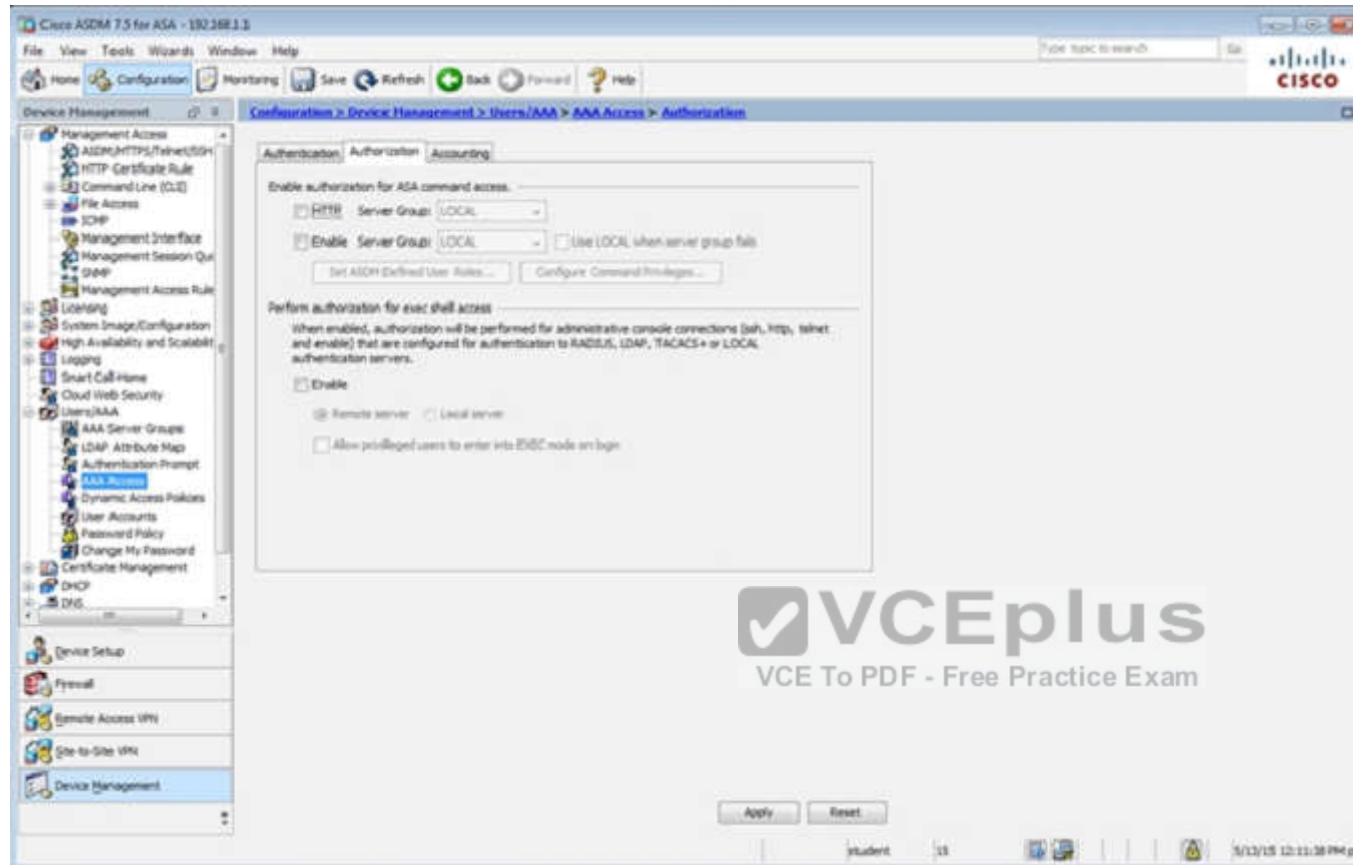


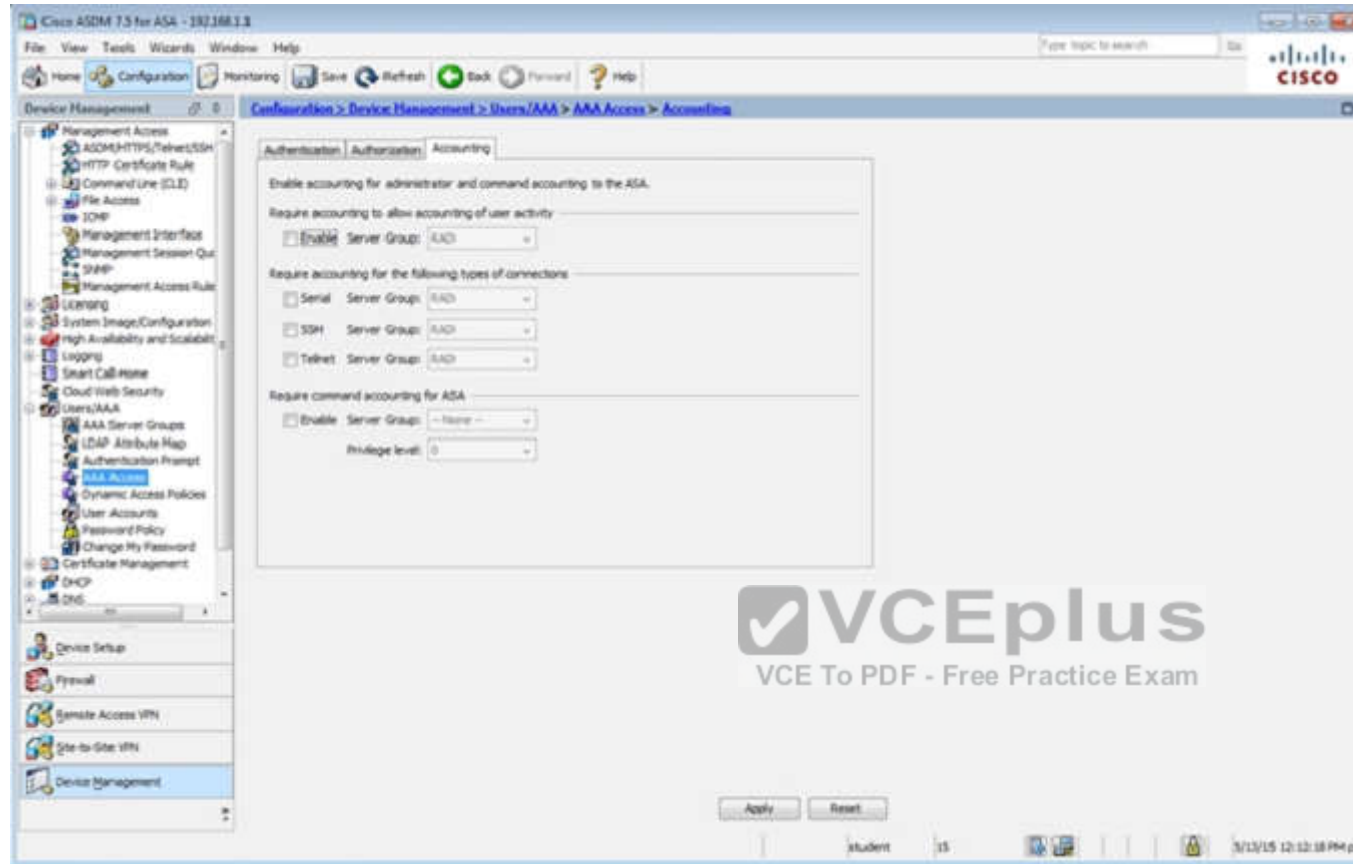


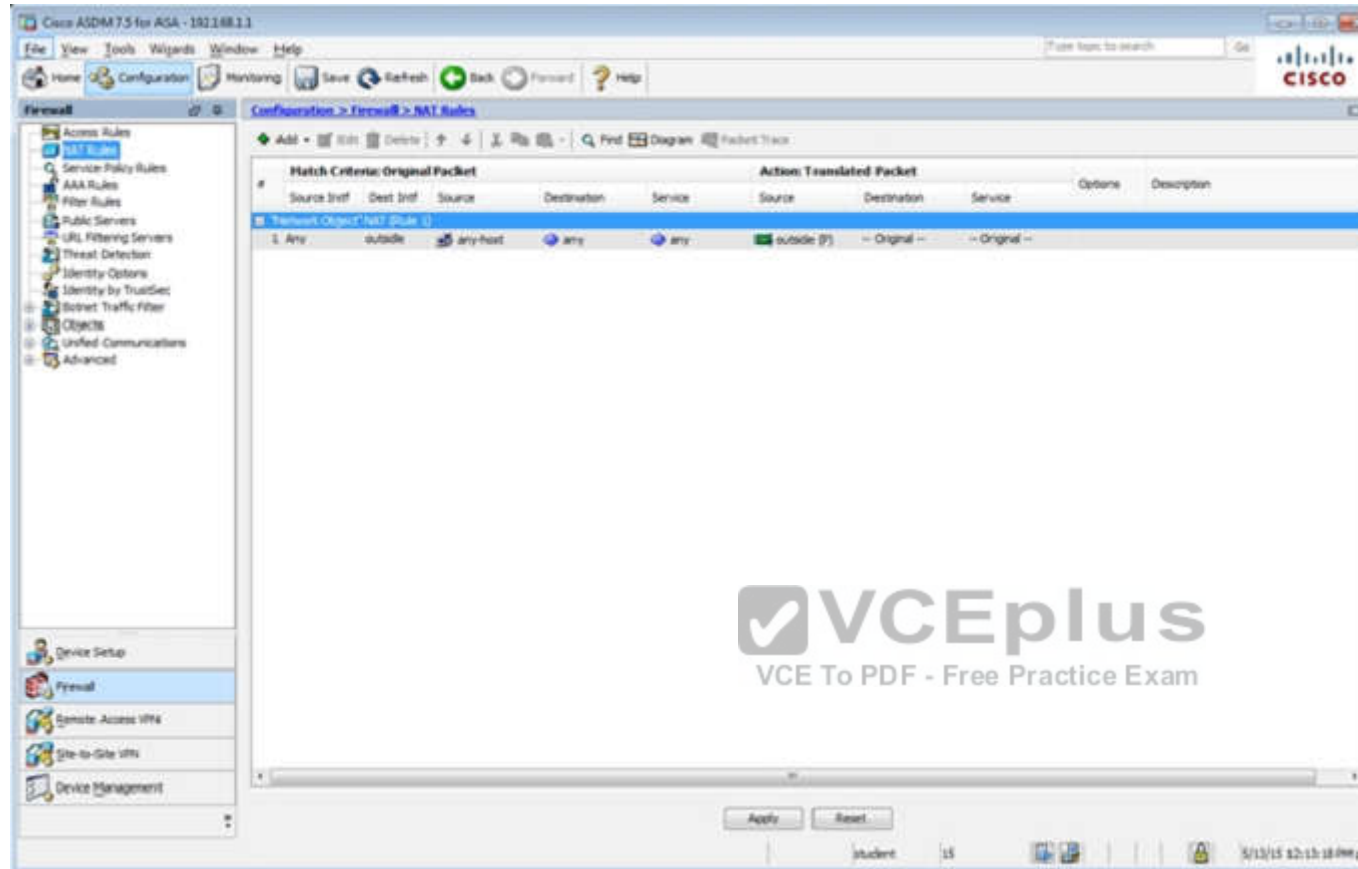


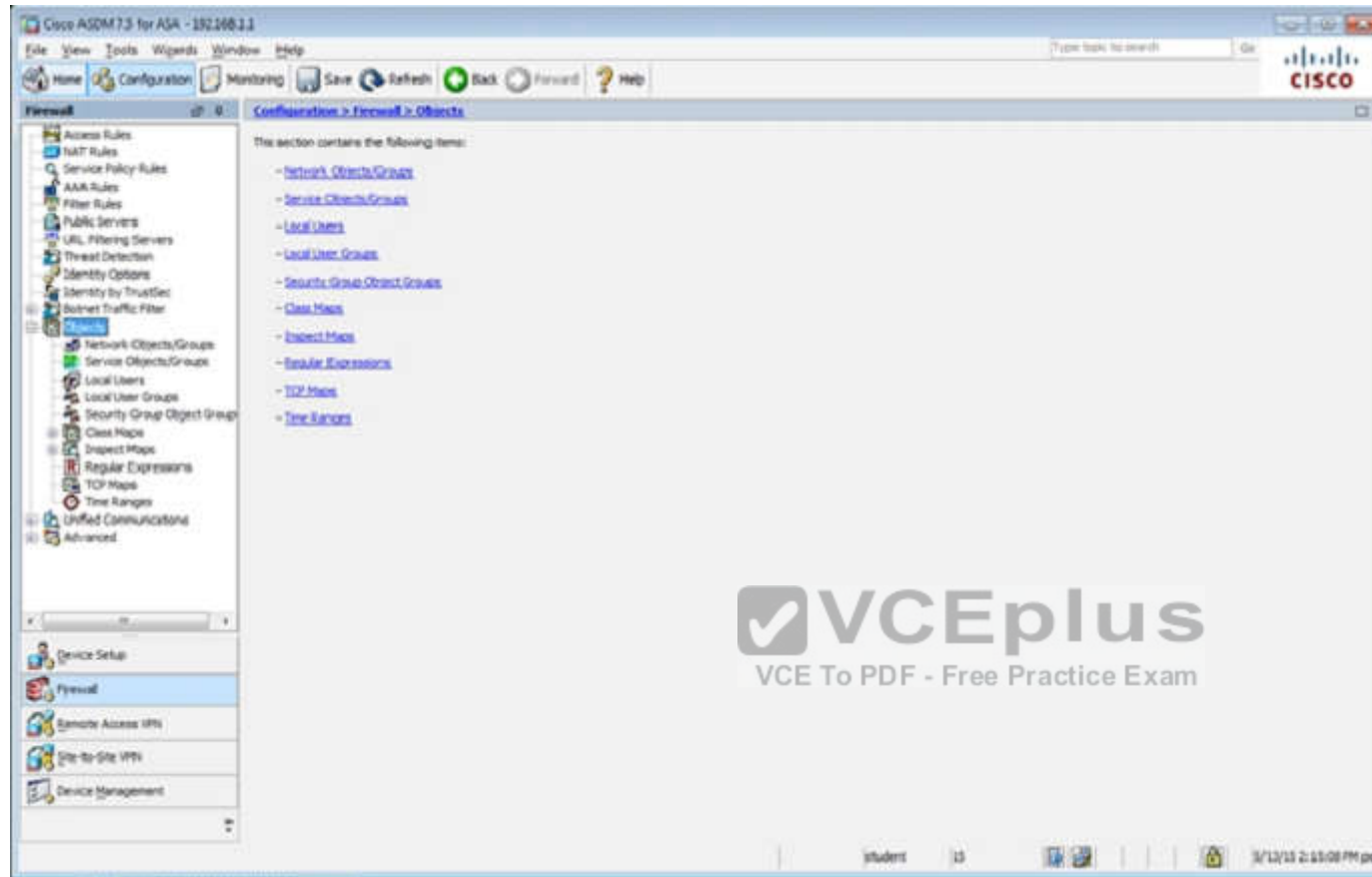




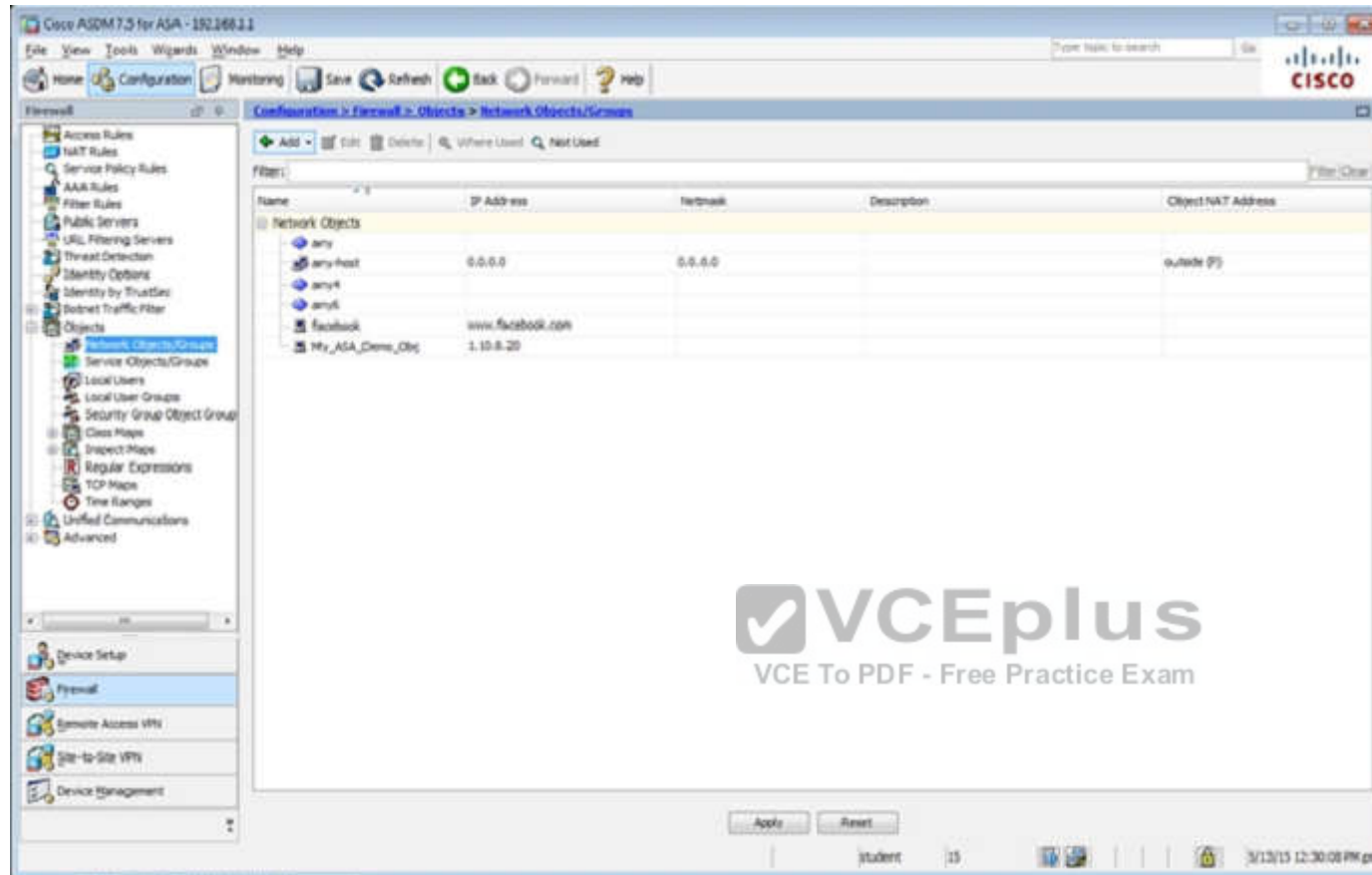












Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

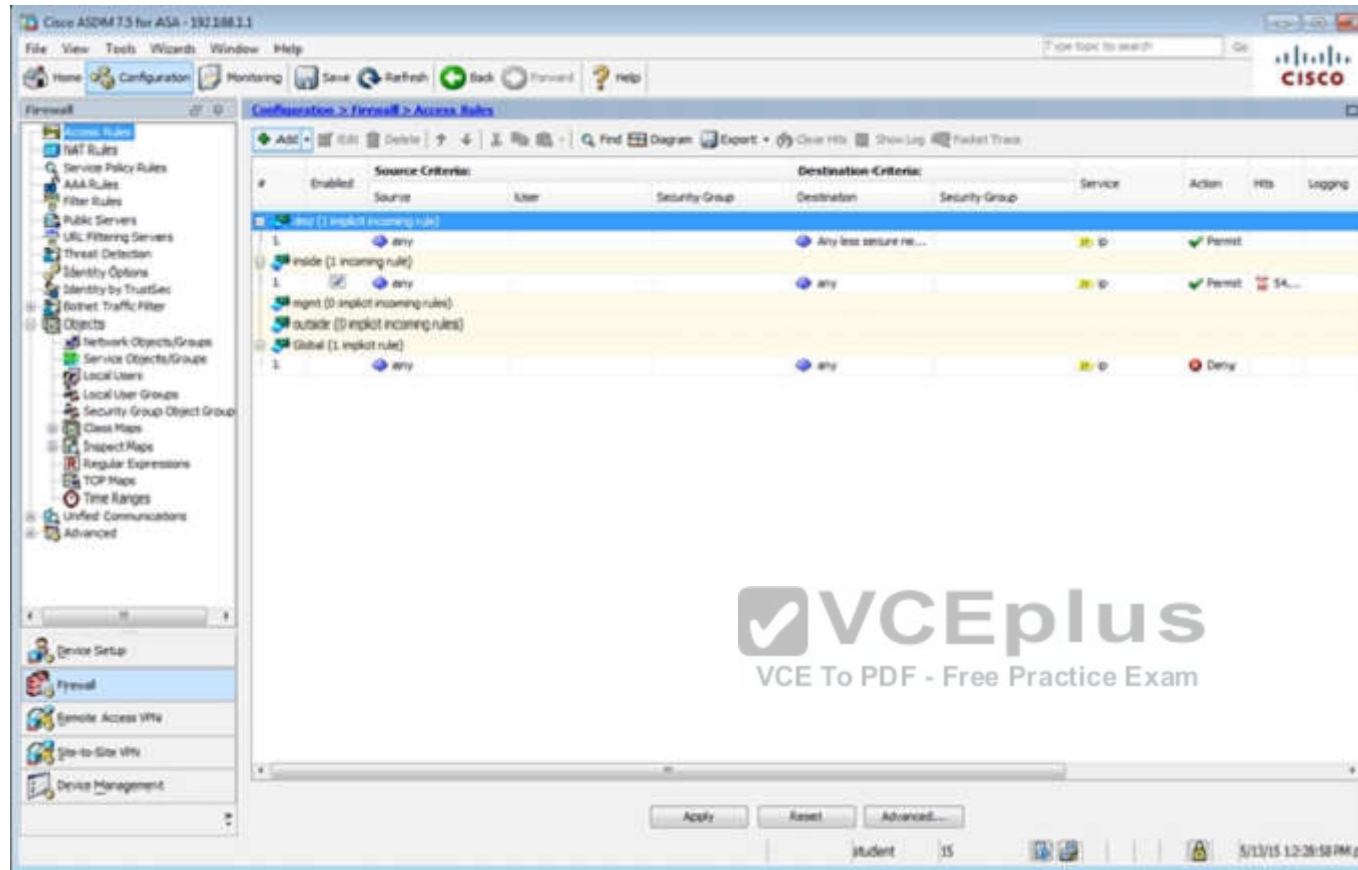
Configuration > Firewall > Service Policy Rules

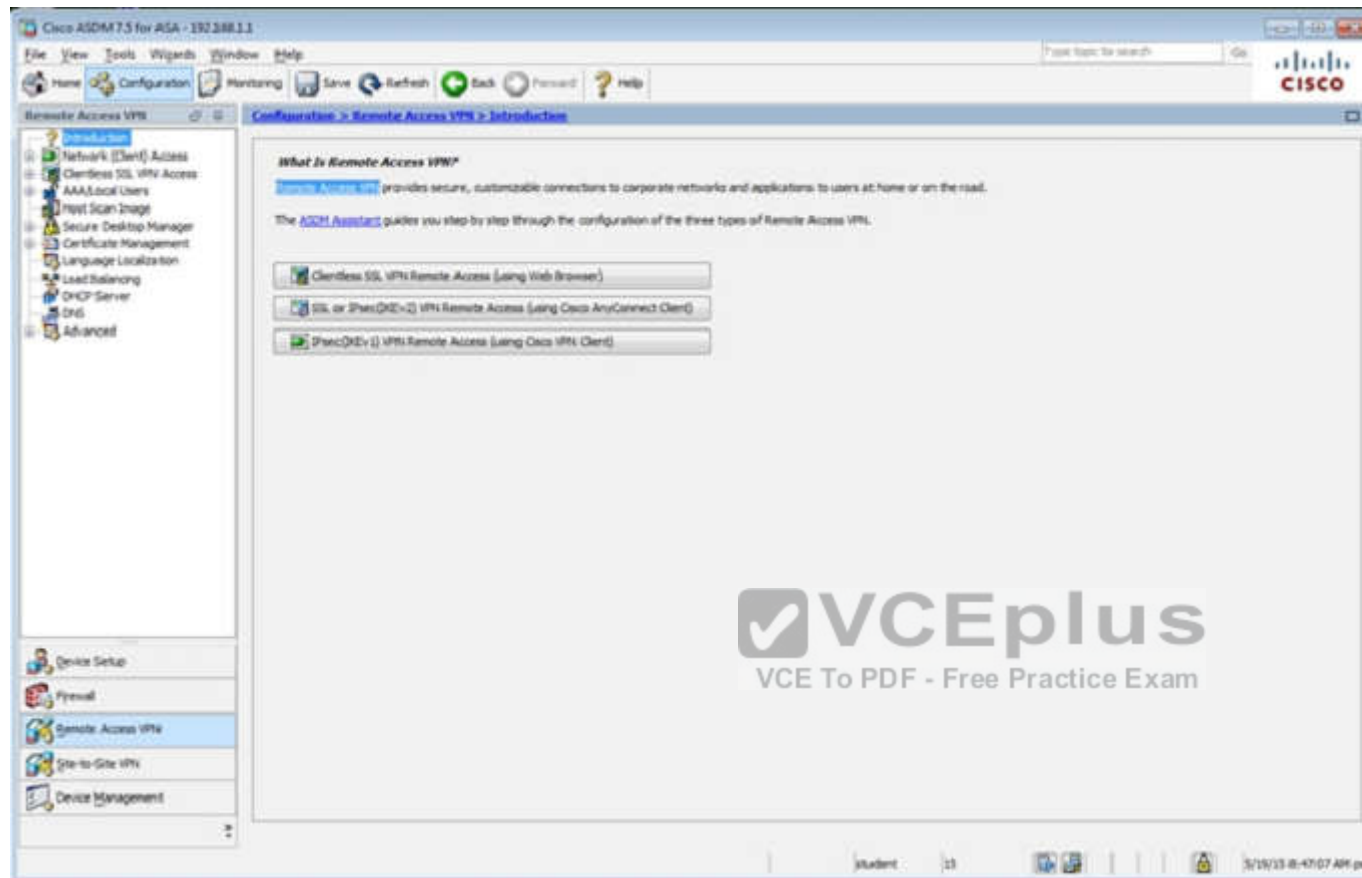
Add Edit Delete Find Diagram Packet Trace

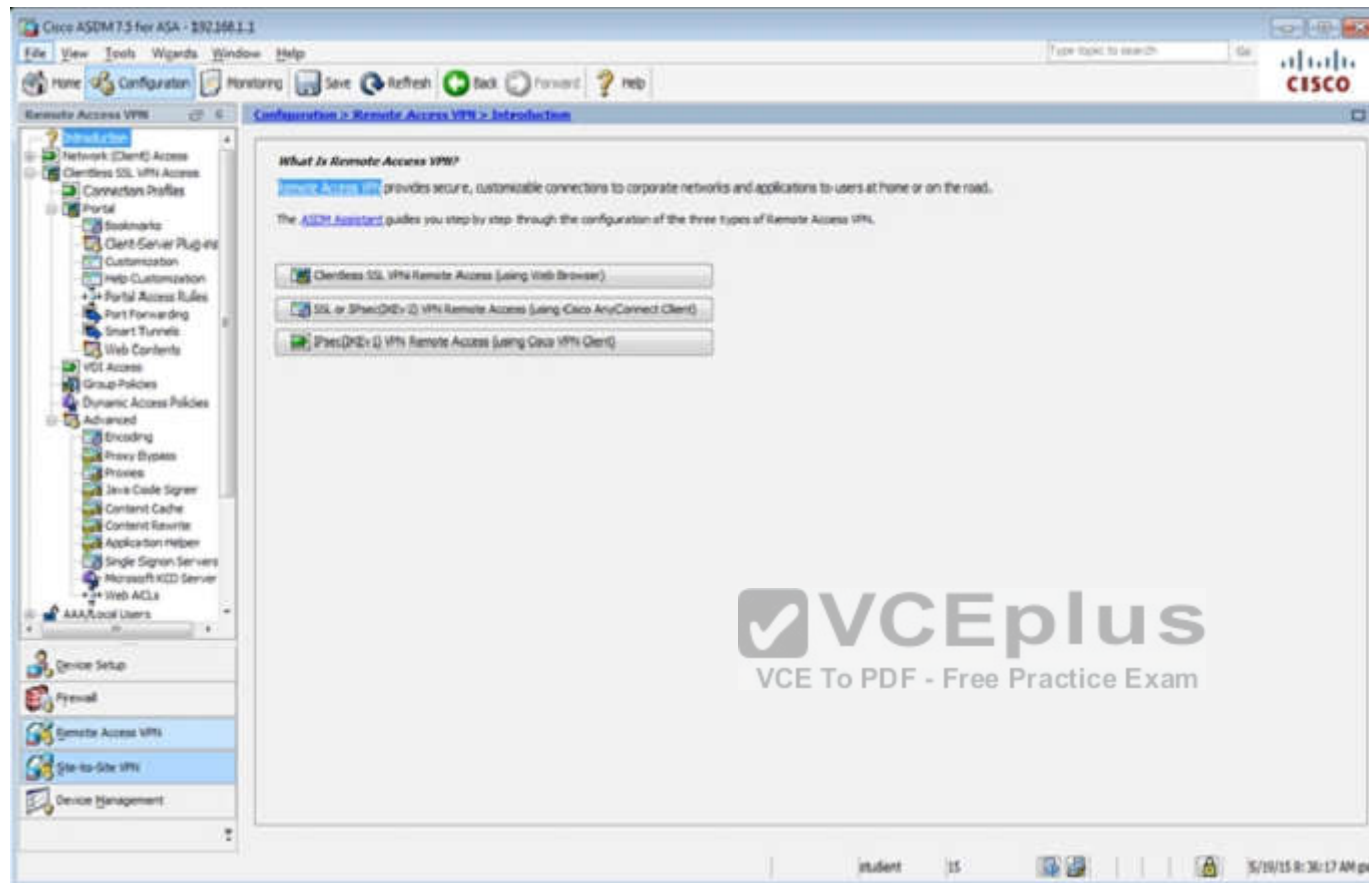
| Name | # | Enabled | Match | Source | Src Security Group | Destination | Dst Security Group | Service | Time | Rule Actions | Details |
|---|---|---------|-------|--------|--------------------|-------------|--------------------|--------------------|------|--|---------|
| Interface: dmz; Policy: dmz_policy | | | | | | | | | | | |
| class-default | | | Match | any | | any | | any traffic | | class-default | |
| Interface: inside; Policy: inside_policy | | | | | | | | | | | |
| class-default | | | Match | any | | any | | any traffic | | class-default | |
| Global; Policy: global_policy | | | | | | | | | | | |
| inspection_policy... | | | Match | any | | any | | default inspect... | | Inspect DNS Map present... Inspect ESMTP (14 more inspect actions) | |

Apply Reset

student 13 5/13/15 12:15:48 PM PST







Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

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

☐ Shutdown portal login page.

Connection Profiles

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

Add Edit Delete Find: Match Case

| Name | Enabled | Aliases | Authentication Method | Group Policy |
|--------------------|-------------------------------------|---------|-----------------------|--------------|
| DefaultRAGroup | <input checked="" type="checkbox"/> | | AAA(RADIUS) | Default |
| DefaultWEBVPNGroup | <input checked="" type="checkbox"/> | | AAA(RADIUS) | Default |
| Clientless | <input checked="" type="checkbox"/> | Test | AAA(RADIUS) | Default |

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

Apply Reset

student 10 3/10/15 9:30:17 AM pet

Edit Clientless SSL VPN Connection Profile: clientless

Basic
Advanced

Name: clientless
Aliases: test

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

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

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

Find: ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

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

Login and Logout Page Customization: DfltCustomization Manage...

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

☐ Enable the display of SecurId messages on the login screen

Connection Aliases

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

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

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

Group URLs

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

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

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

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

☒ Always run CSD

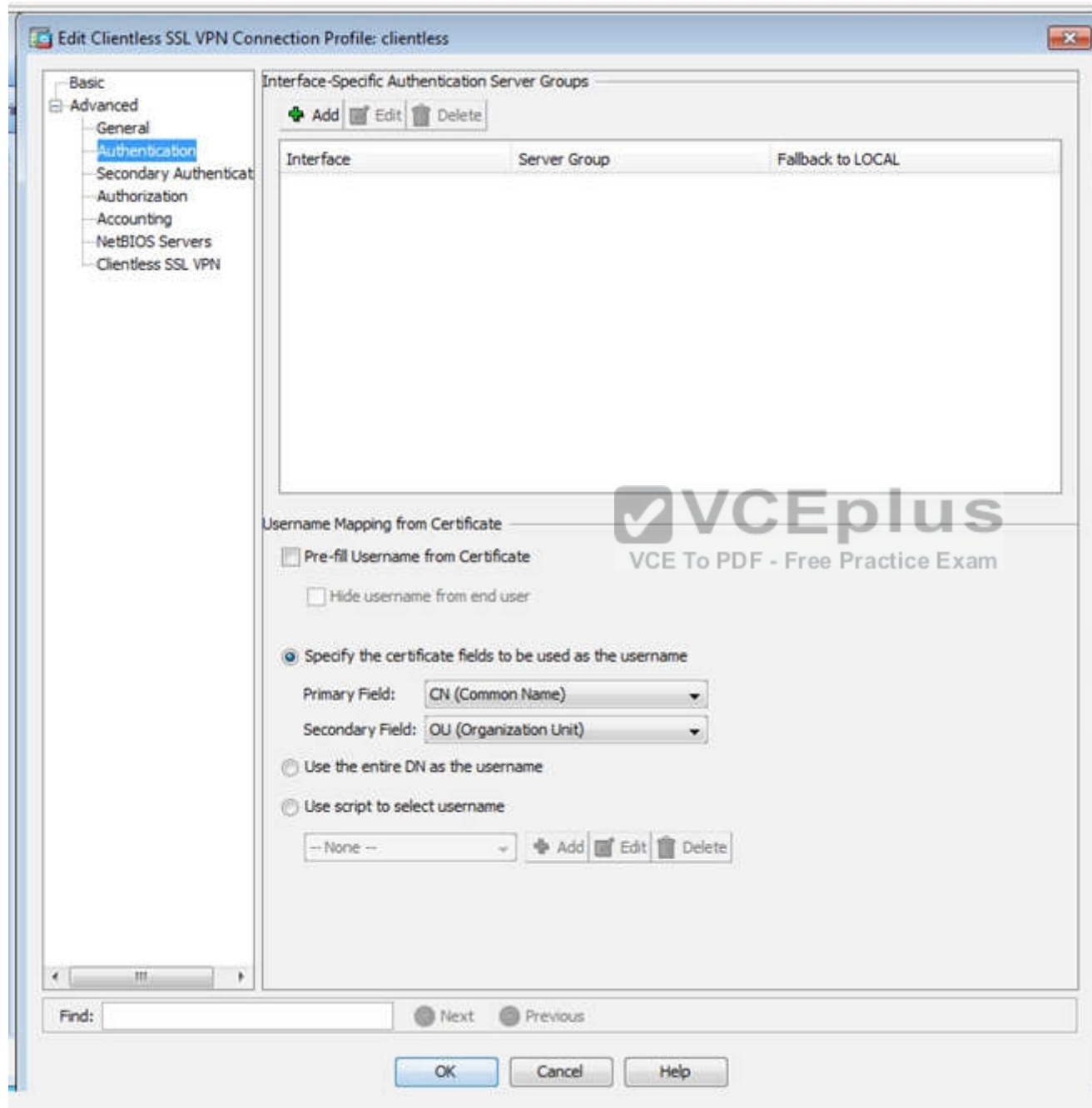
☐ Disable CSD for both AnyConnect and Clientless SSL VPN

☐ Disable CSD for AnyConnect only

Find: Next Previous

OK Cancel Help







Edit Clientless SSL VPN Connection Profile: clientless

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

Secondary Authentication Server Group

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

☐ Use LOCAL if Server Group fails

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

Attributes Server: ☒ Primary ☐ Secondary

Session Username Server: ☒ Primary ☐ Secondary

Interface-Specific Secondary Authentication Server Groups

+ Add Edit Delete

| Interface | Server Group | Fallback to LOCAL | Use primary username |
|-----------|--------------|-------------------|----------------------|
|-----------|--------------|-------------------|----------------------|

Username Mapping from Certificate

☐ Pre-fill username from certificate

☐ Hide username from end user

☐ Fallback when a certificate is unavailable

Password: ☒ Prompt ☐ Use primary ☐ Use

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

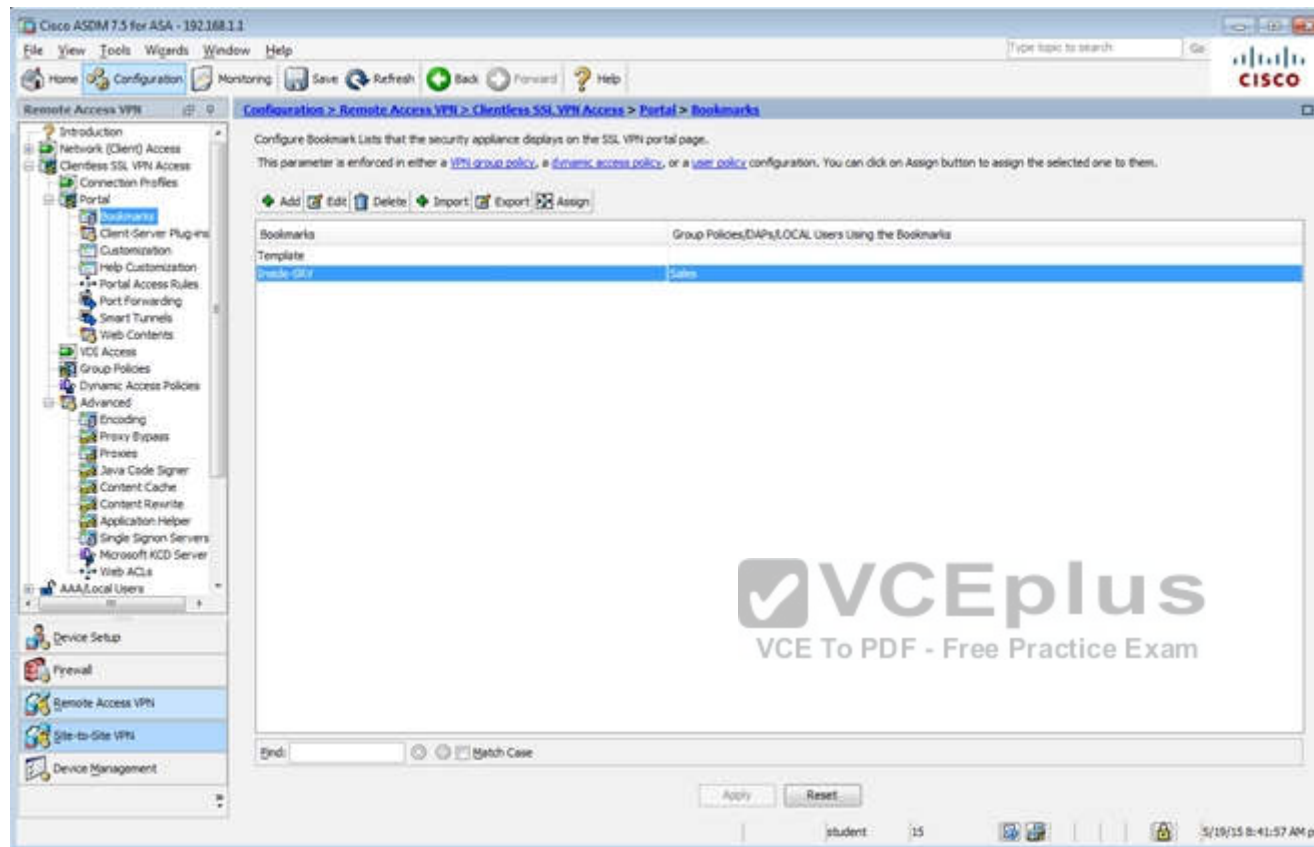
☐ Use the entire DN as the username

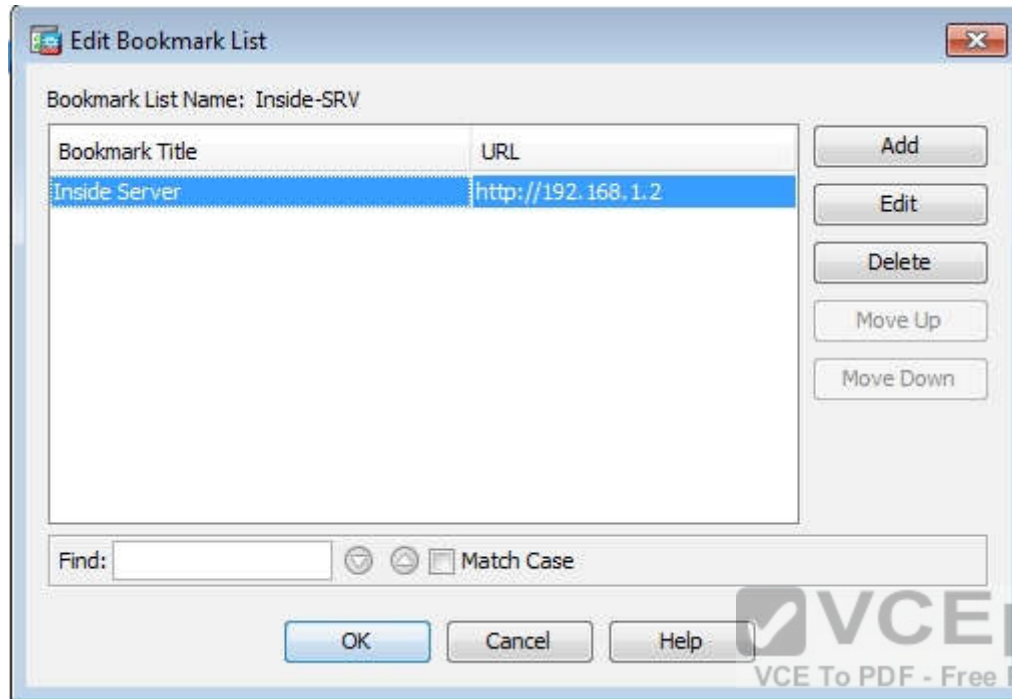
☐ Use script to select username

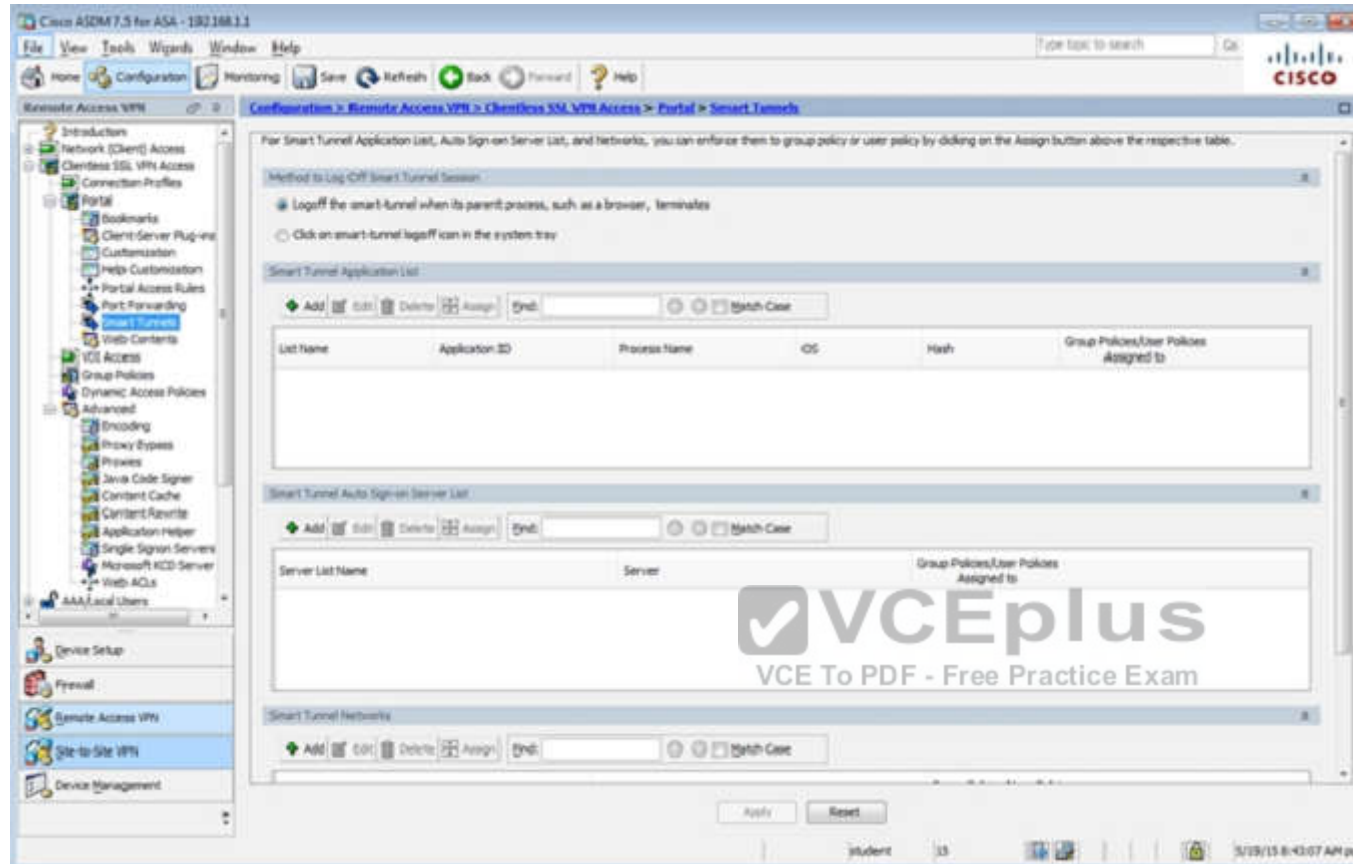
-- None -- + Add Edit Delete

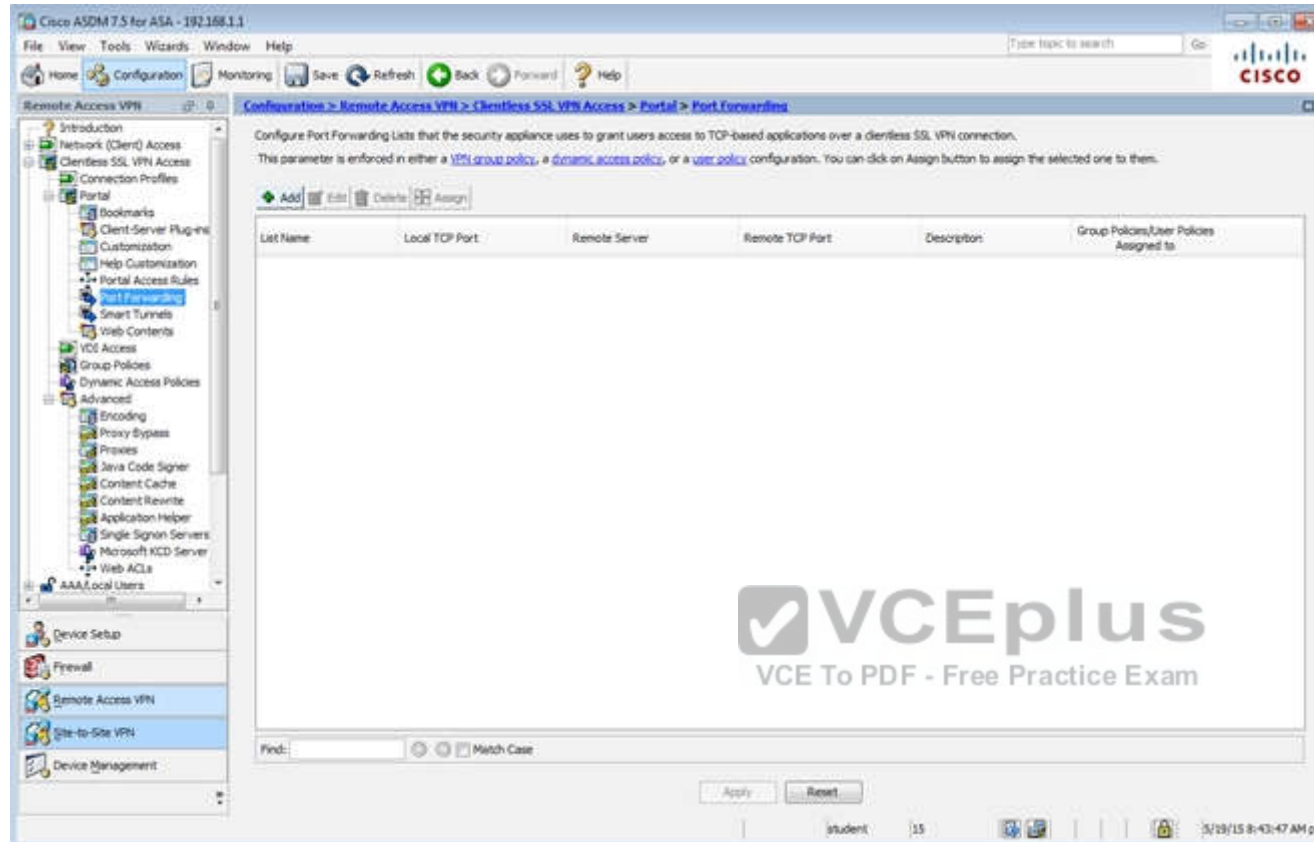
Find: ☐ Next ☐ Previous

OK Cancel Help









Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Clientless SSL VPN Access > 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 |
|--------------------------------|----------|------------------------------------|--|
| System | System | SSL-Clientless | Clientless |
| DefaultPolicy (System Default) | Internal | key1:key2:ssl-clientless/2tp-ipsec | DefaultRAGroup/DefaultL3Group/DefaultADMG/Def... |

End: Match Case

Apply Reset

student 15 3/19/15 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 ☐ LZTP/IPsec

Web ACL: ☒ Inherit Manage...

Access Hours: ☒ Inherit Manage...

Simultaneous Logins: ☒ Inherit

Restrict access to VLAN: ☒ Inherit

Connection Profile (Tunnel Group) Lock: ☒ Inherit

Maximum Connect Time: ☒ Inherit ☐ Unlimited minutes

Idle Timeout: ☒ Inherit ☐ Use Global Default minutes

Timeout Alerts

Session Alert Interval: ☒ Inherit ☐ Default minutes

Idle Alert Interval: ☒ Inherit ☐ Default minutes

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

Find: ☒ Next ☐ Previous

OK Cancel Help

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

- IPsec/SSL Connection
- Secure Mobility Solution
- Address Assignment
- Advanced
- Clientless SSL VPN Access
- Connection Profiles
- Portal
- Bookmarks
- Client-Server Plug-ins
- Customization
- Help Customization
- Portal Access Rules
- Port Forwarding
- Smart Tunnels
- Web Contents
- Voice Access
- Group Policies**
- Dynamic Access Policies
- Advanced
- AAA/Local Users
- AAA Server Groups
- LDAP Attribute Map
- Local Users
- Host Scan Image
- Secure Desktop Manager

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

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

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

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

| Name | Type | Tunneling Protocol | Connection Profiles/Users Assigned To |
|--------------------------------|----------|---|---------------------------------------|
| Default | Internal | ssl-clientless | Default |
| DfltGrpPolicy (System Default) | Internal | Rev 1.0 Rev 2.0 ssl-clientless/2to-ipssec | DfltGrpPolicy |

Find:

student 15 10/15/14 9:15:40 AM pet

Edit Internal Group Policy: Sales

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

Bookmark List: ☐ Inherit Manage...

URL Entry: ☒ Inherit ☐ Enable ☐ Disable

File Access Control

File Server Entry: ☒ Inherit ☐ Enable ☐ Disable

File Server Browsing: ☒ Inherit ☐ Enable ☐ Disable

Hidden Share Access: ☒ Inherit ☐ Enable ☐ Disable

Port Forwarding Control

Port Forwarding List: ☒ Inherit Manage...

☐ Auto Applet Download

Applet Name: ☒ Inherit

Smart Tunnel

Smart Tunnel Policy: ☒ Inherit Manage...

Tunnel Option: Manage...

Smart Tunnel Application: ☒ Inherit Manage...

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

☐ Auto Start

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

Windows Domain Name (optional):

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

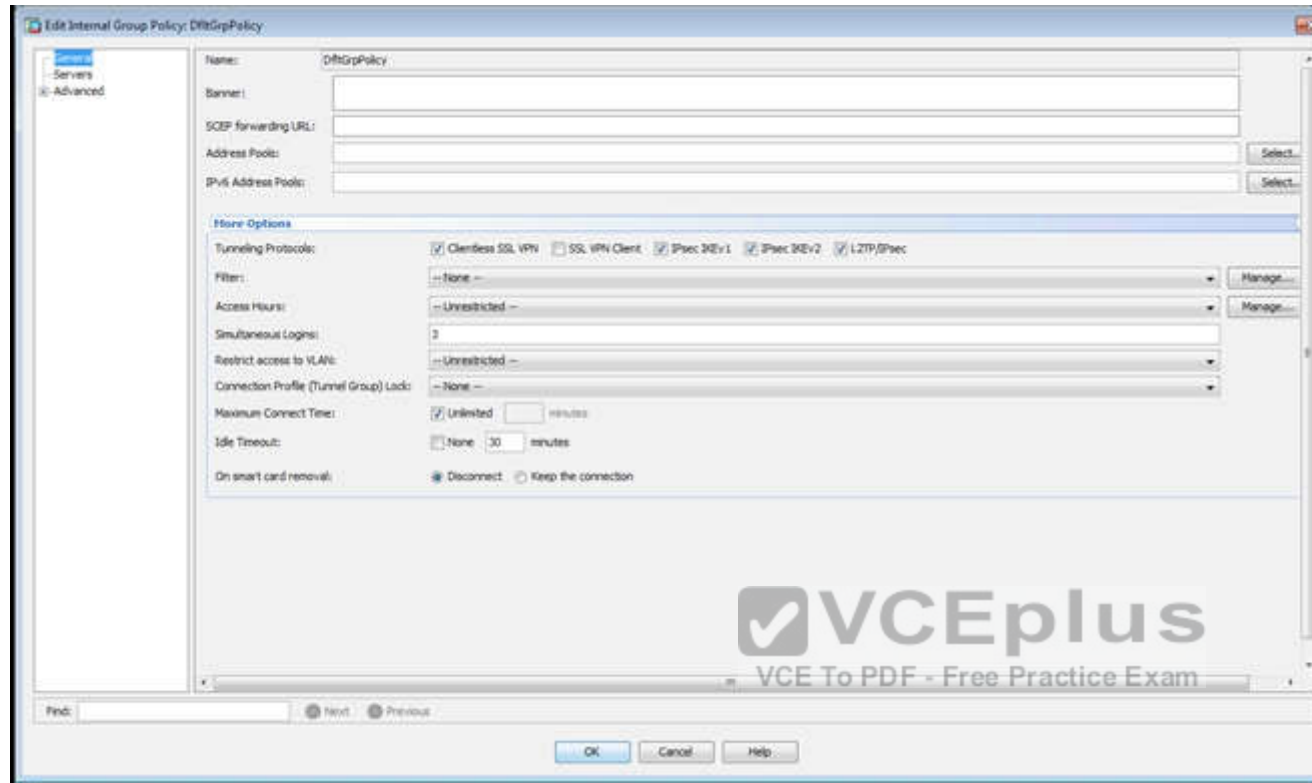
ActiveX Relay

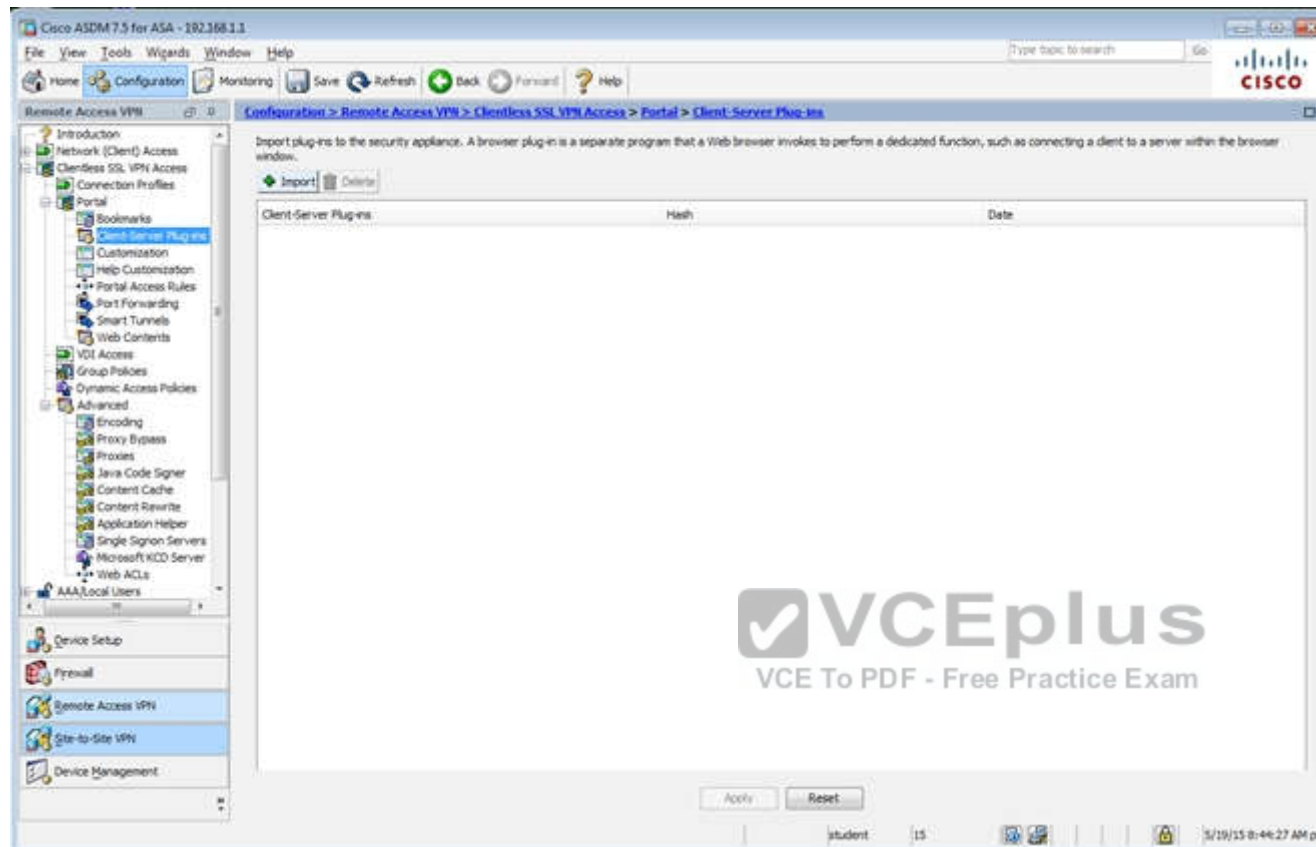
ActiveX Relay: ☒ Inherit ☐ Enable ☐ Disable

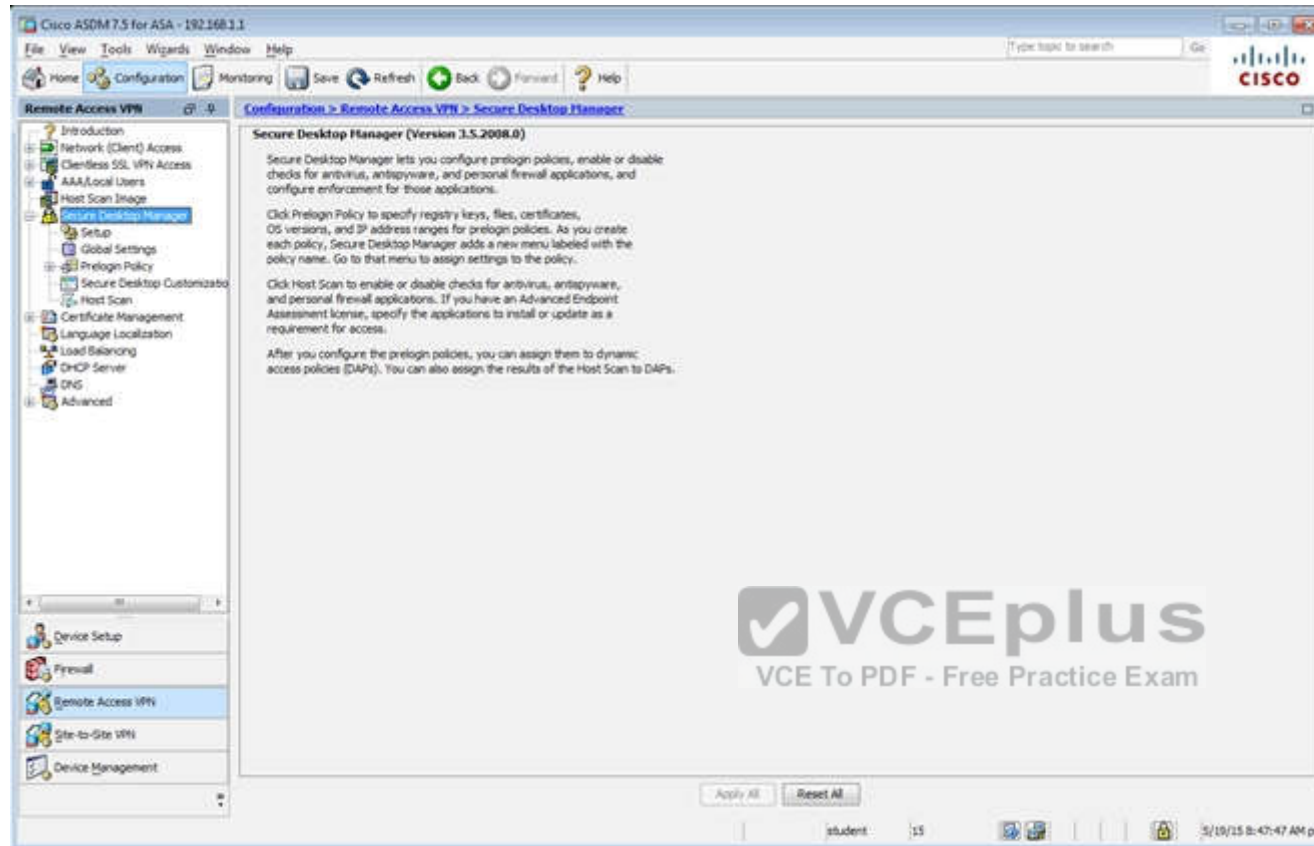
More Options

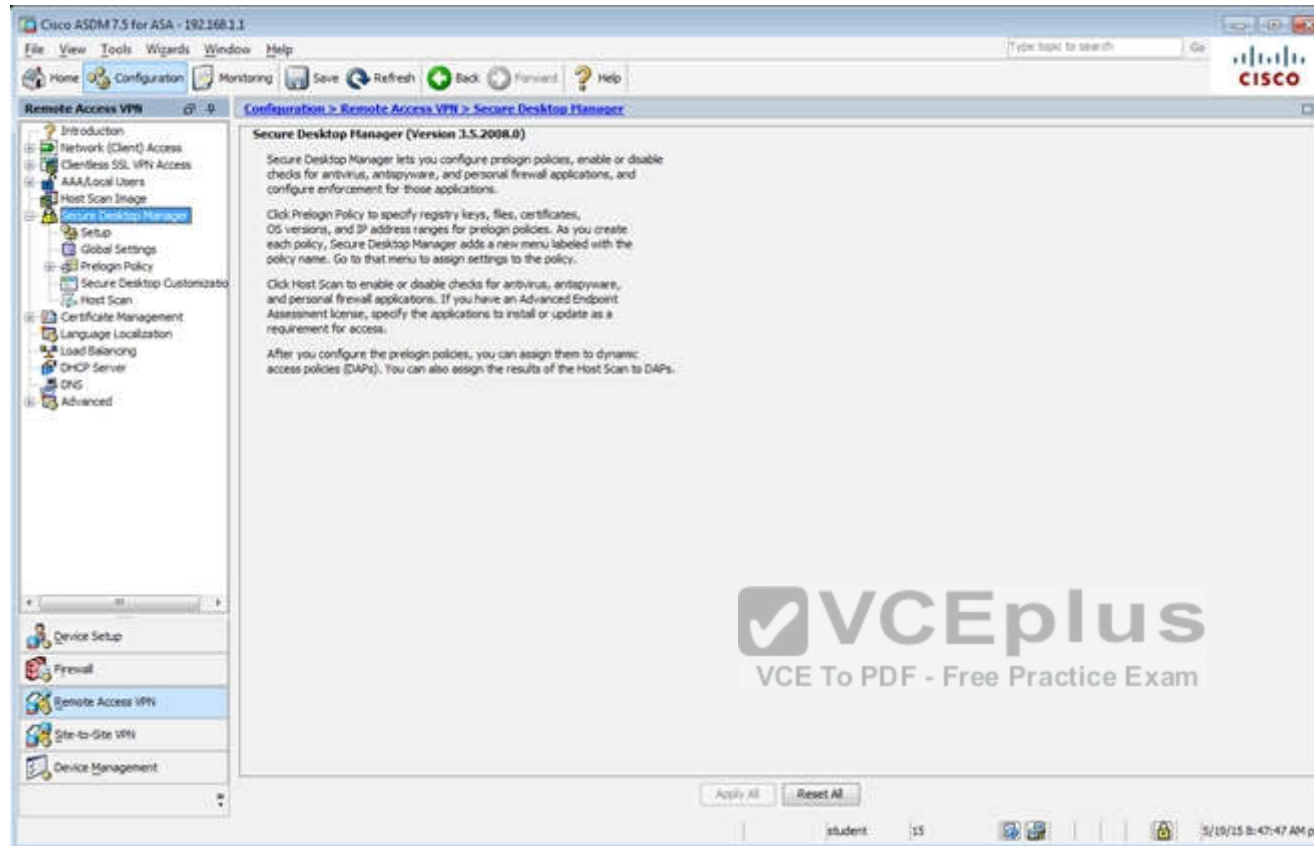
Find: ☐ Next ☐ Previous

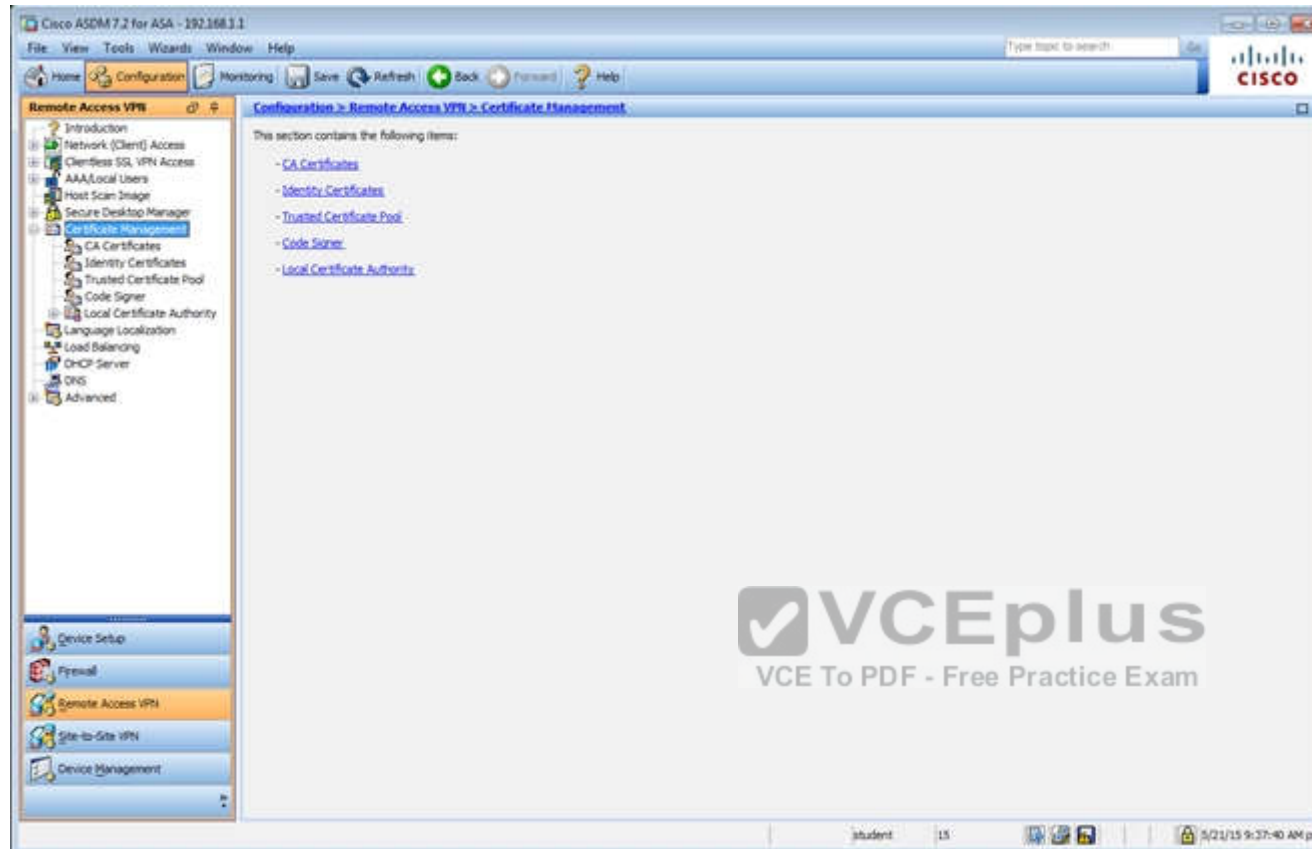
OK Cancel Help











Cisco ASDM 7.3 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Configuration > Remote Access VPN > Certificate Management > Identity Certificates

| Issued To | Issued By | Expiry Date | Associated Trustpoints | Usage | Public Key Type |
|----------------------------|----------------------------|----------------------------|------------------------|-----------------|-----------------|
| hostname-4P (17-ASA-sec... | hostname-4P (17-ASA-sec... | 11:59:33 pet 1 Dec 20 2024 | ASDM - Trustpoints | General Purpose | RSA 2048 bits |

Buttons: Add, Show Details, Delete, Export, Install

End: Match Case

Certificate Expiration Alerts

Send the first alert before: (days)

Repeat Alert Interval: (days)

Public CA Enrollment

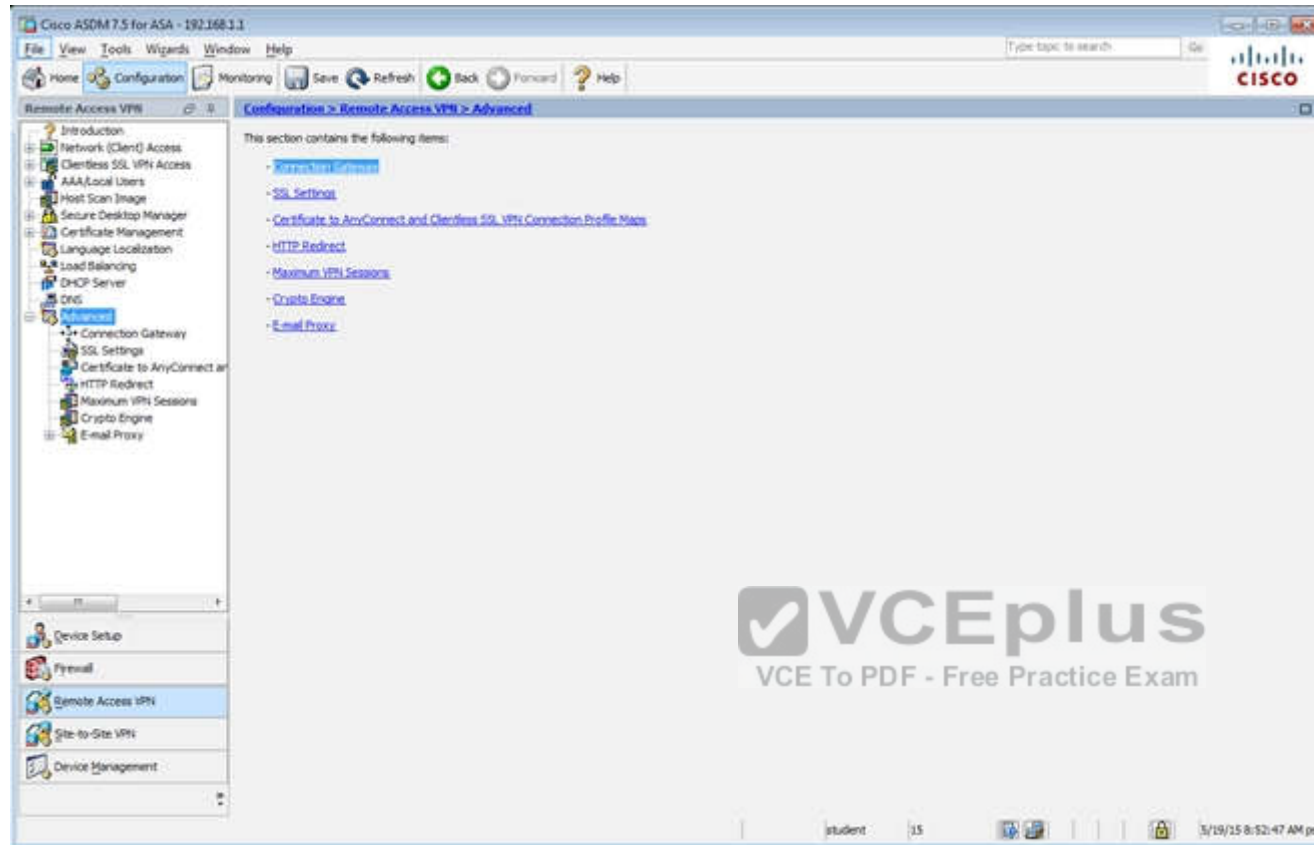
Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers Cisco customers a special promotional price for certificates and trial certificates for testing.

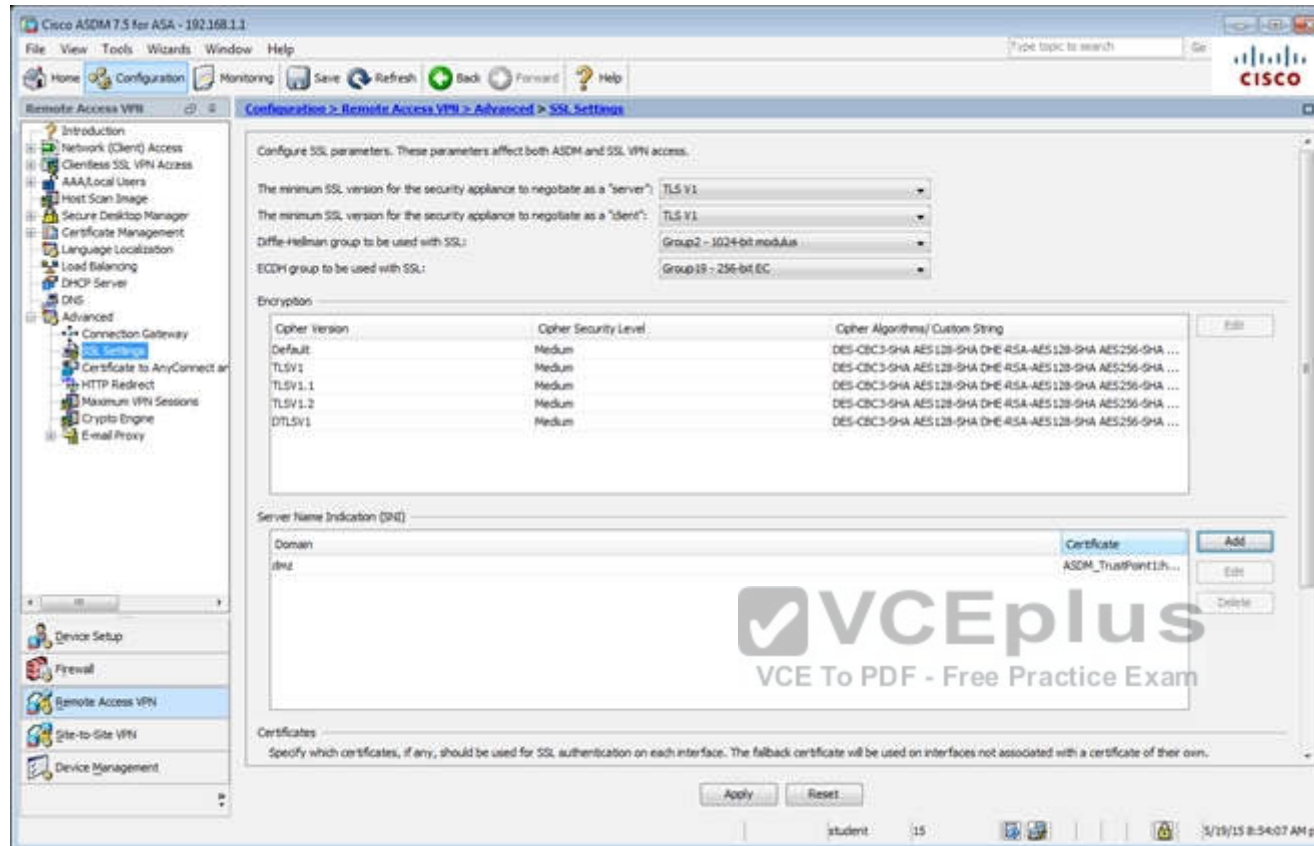
Using a previously saved certificate signing request, [enroll with Entrust](#).

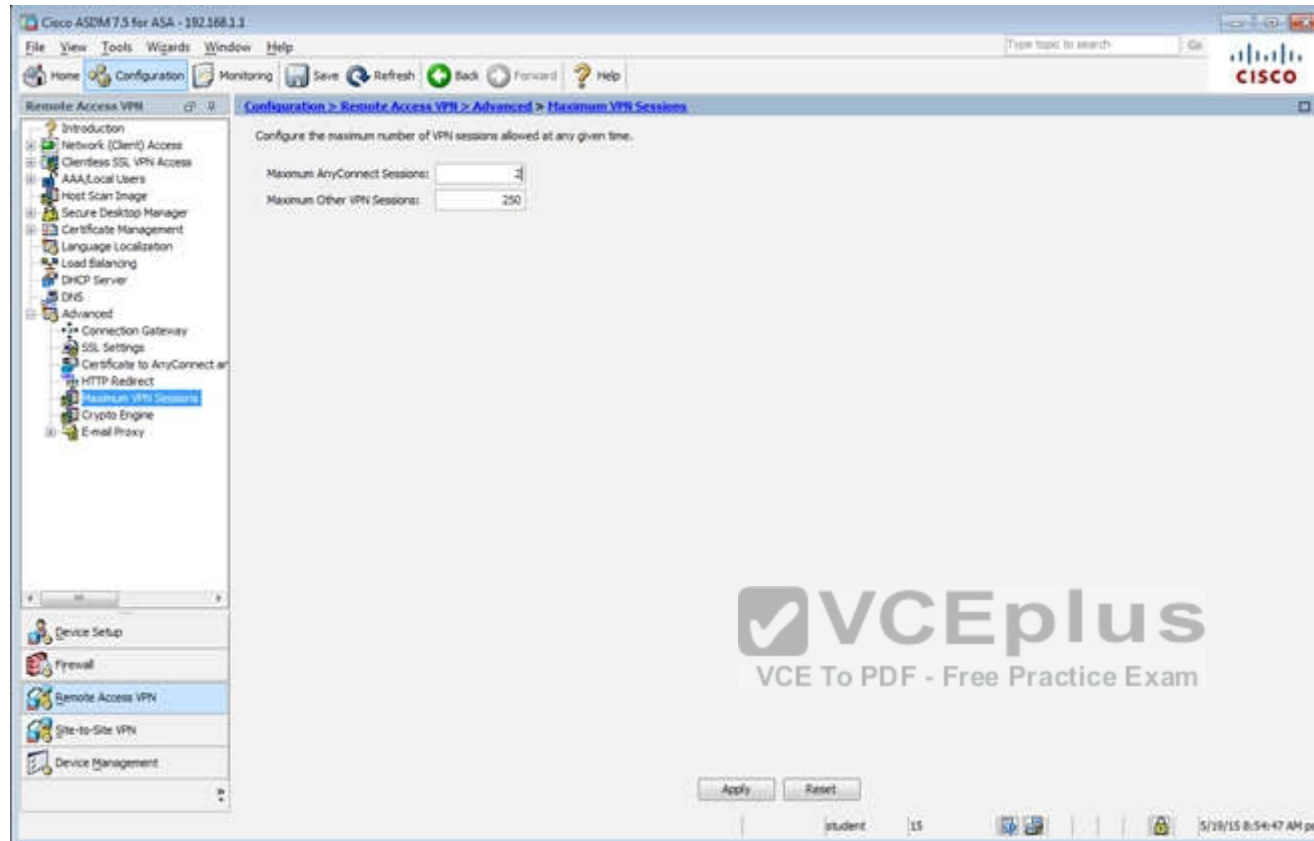
ASDM Identity Certificate Wizard

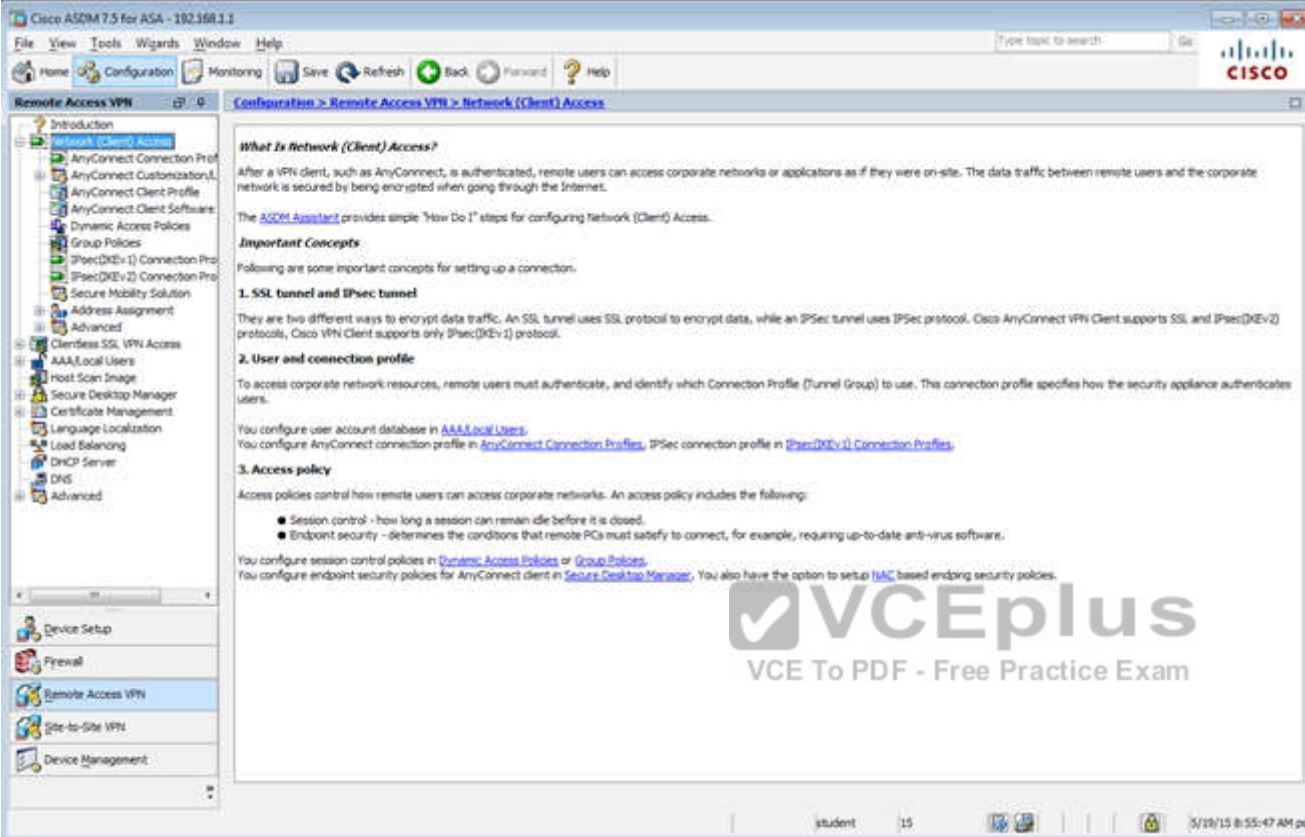
The Cisco ASDM Identity Certificate Wizard assists you in creating a self-signed certificate that is required for launching ASDM through launcher.

student 15 3/19/15 8:51:47 AM pet









Cisco ASDM 7.5 for ASA - 102.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

What Is Network (Client) Access?

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

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

Important Concepts

Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel

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

2. User and connection profile

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

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

3. Access policy

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

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

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

student 15 5/29/15 8:55:47 AM pct

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

- Introduction
- Network (Client) Access
 - AnyConnect Connection Profile
 - AnyConnect Customization
 - AnyConnect Client Profile
 - AnyConnect Client Software
 - Dynamic Access Policies
 - Group Policies**
 - IPsec (IKEv1) Connection Profile
 - 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

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

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

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

Add Edit Delete Assign

| Name | Type | Tunneling Protocol | Connection Profiles/Users Assigned To |
|-----------------------------|----------|--|--|
| Sales | Internal | ssl-clientless | clientless |
| GroupPolicy: System Default | Internal | l2l3-clientless/ssl-clientless/zip-gwsec | DefaultGroupDefault, GroupDefaultWebVPNGroup |

Find: Match Case

Apply Reset

student 15 3/21/15 10:17:10 AM pet

Edit Internal Group Policy: DiffGrpPolicy

Settings

- Servers
- Advanced
 - Split Tunneling
 - Browser Proxy
 - AnyConnect Client
 - IPsec (IKEv1) Client

Name: DiffGrpPolicy

Banner:

SCDP forwarding URL:

Address Pools: Select...

IPv6 Address Pools: Select...

Home Options

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

Filter: -- None -- Manage...

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

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

Simultaneous Logins: 3

Restrict access to VLAN: -- Unrestricted --

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

Maximum Connect Time: ☒ Unlimited ☐ minutes

Idle Timeout: ☐ None ☐ 30 minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

VCEplus
VCE To PDF - Free Practice Exam

Find: Next Previous

OK Cancel Help

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction
Network (Client) Access
AnyConnect Connection Profile
AnyConnect Customization
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

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

Access Interfaces
Enable interfaces for IPsec access.

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

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

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

+ Add Edit Delete

| Name | IPsec Enabled | L2TP/IPsec Enabled | Authentication Server Group | Group Policy |
|--------------------|-------------------------------------|-------------------------------------|-----------------------------|---------------|
| DefaultRAGroup | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD | DiffGrpPolicy |
| DefaultWEBVPNGroup | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD | DiffGrpPolicy |
| Services | <input type="checkbox"/> | <input type="checkbox"/> | LOCAL | Local |

End: Match Case

Apply Reset

student 15 5/18/15 8:56:47 AM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

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

Access Interfaces

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

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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

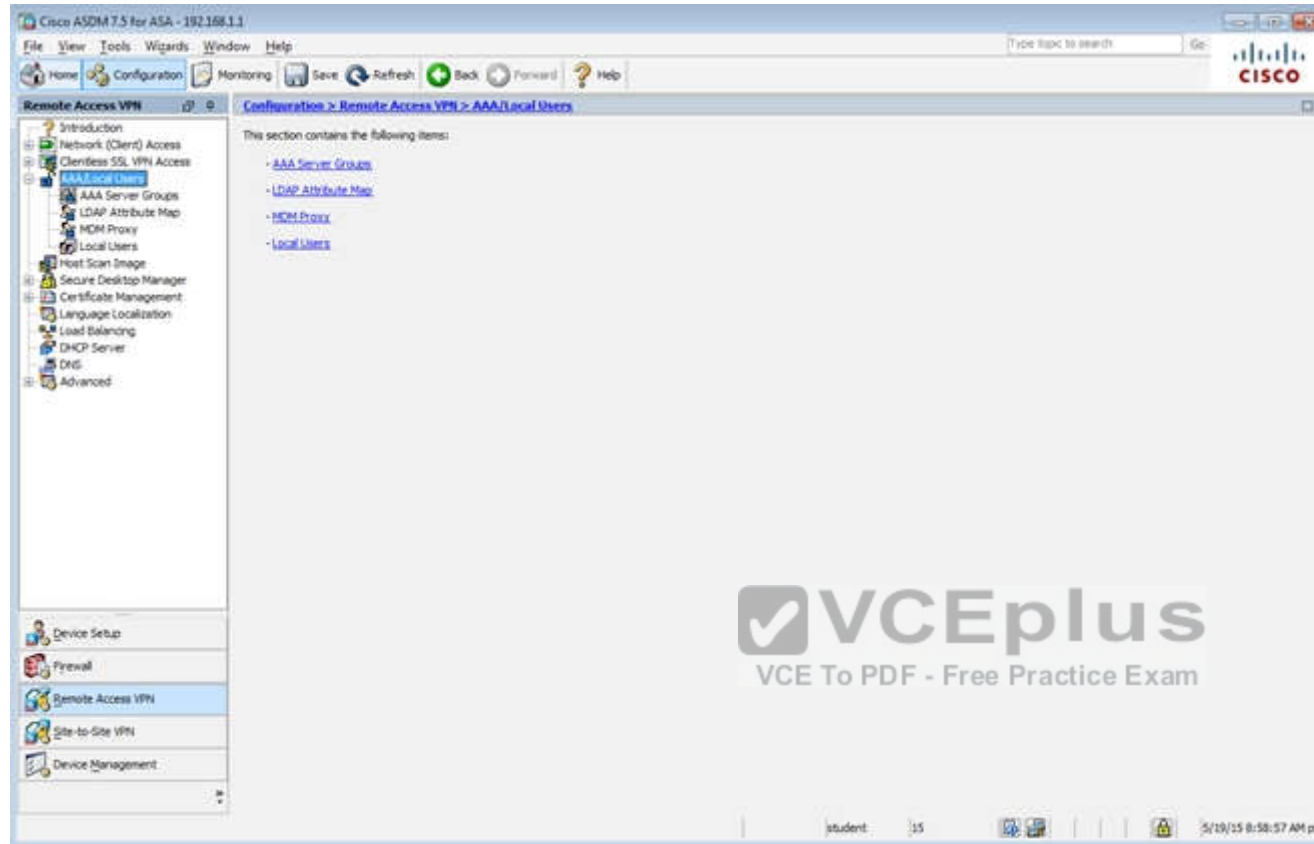
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Find:

| Name | SSL Enabled | IPsec Enabled | Authentication Method | Group Policy |
|-------------------|-------------------------------------|-------------------------------------|-----------------------|-----------------------|
| DefaultRAGroup | <input type="checkbox"/> | <input type="checkbox"/> | AAA(RADIUS) | DefaultGroupPolicy |
| DefaultTIVPNGroup | <input type="checkbox"/> | <input checked="" type="checkbox"/> | AAA(RADIUS) | DefaultGroupPolicy |
| AnyConnect | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | AAA(RADIUS) | AnyConnectGroupPolicy |

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

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
MDM Proxy
Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DnCP Server
DNS
Advanced

Create entries in the ASA local user database.

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

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

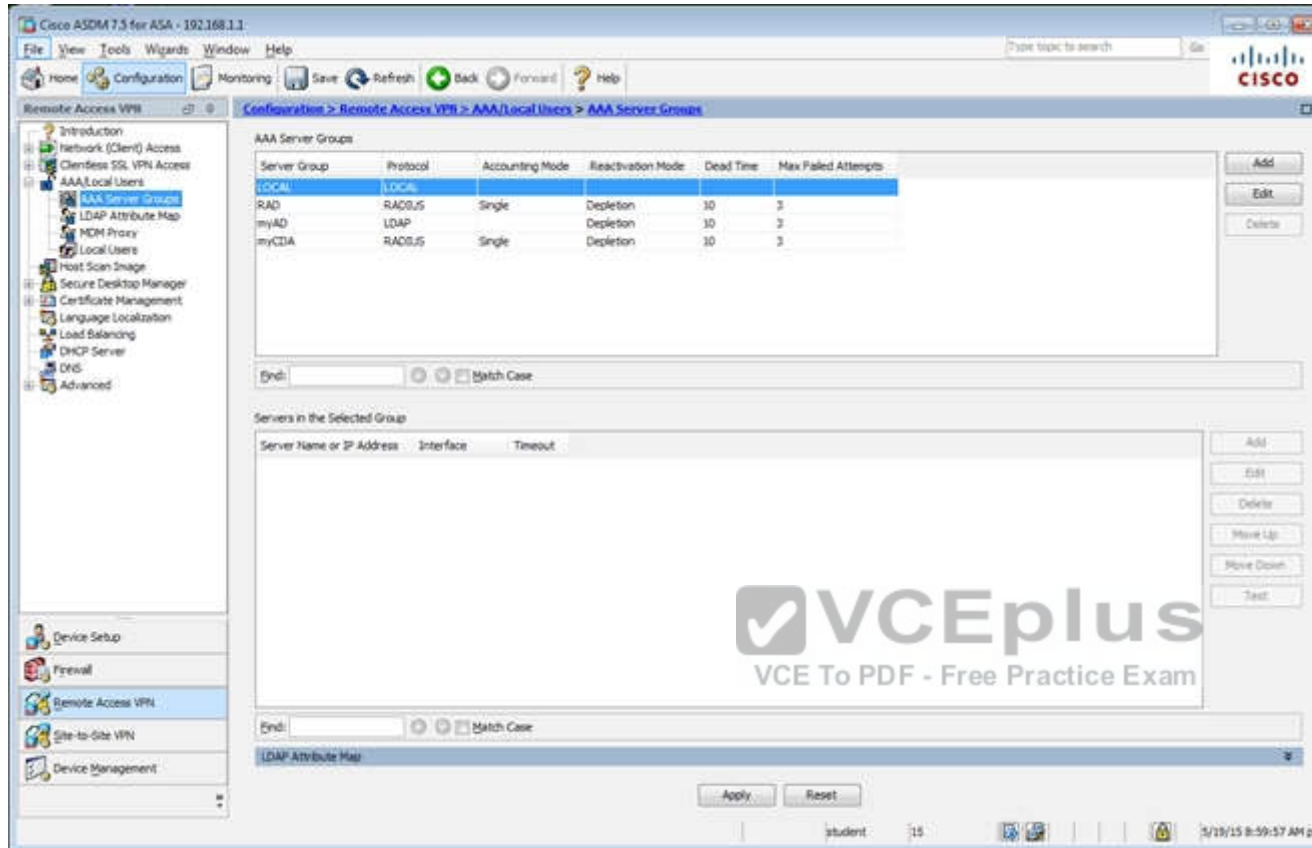
| Username | Privilege Level (Role) | Access Restrictions | VPN Group Policy | VPN Group Lock |
|-----------|------------------------|---------------------|----------------------------|----------------------------|
| student | 15 | Full | -- Inherit Group Policy -- | -- Inherit Group Policy -- |
| enable_15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

Add Edit Delete

End: Match Case

Apply Reset

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



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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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



Virtual Terminal

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

- 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

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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

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

Device Certificate ...

Port Setting ...

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

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

☐ Shutdown portal login page.

Connection Profiles

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

Add Edit Delete Find: ☐ Match Case

| Name | Enabled | Aliases | Authentication Me |
|--------------------|-------------------------------------|---------|-------------------|
| DefaultRAGroup | <input checked="" type="checkbox"/> | | AAA(RAD) |
| DefaultWEBVPNGroup | <input checked="" type="checkbox"/> | | AAA(RAD) |
| clientless | <input checked="" type="checkbox"/> | test | AAA(LOCAL) |

Device Setup

QUESTION 66**Scenario**

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

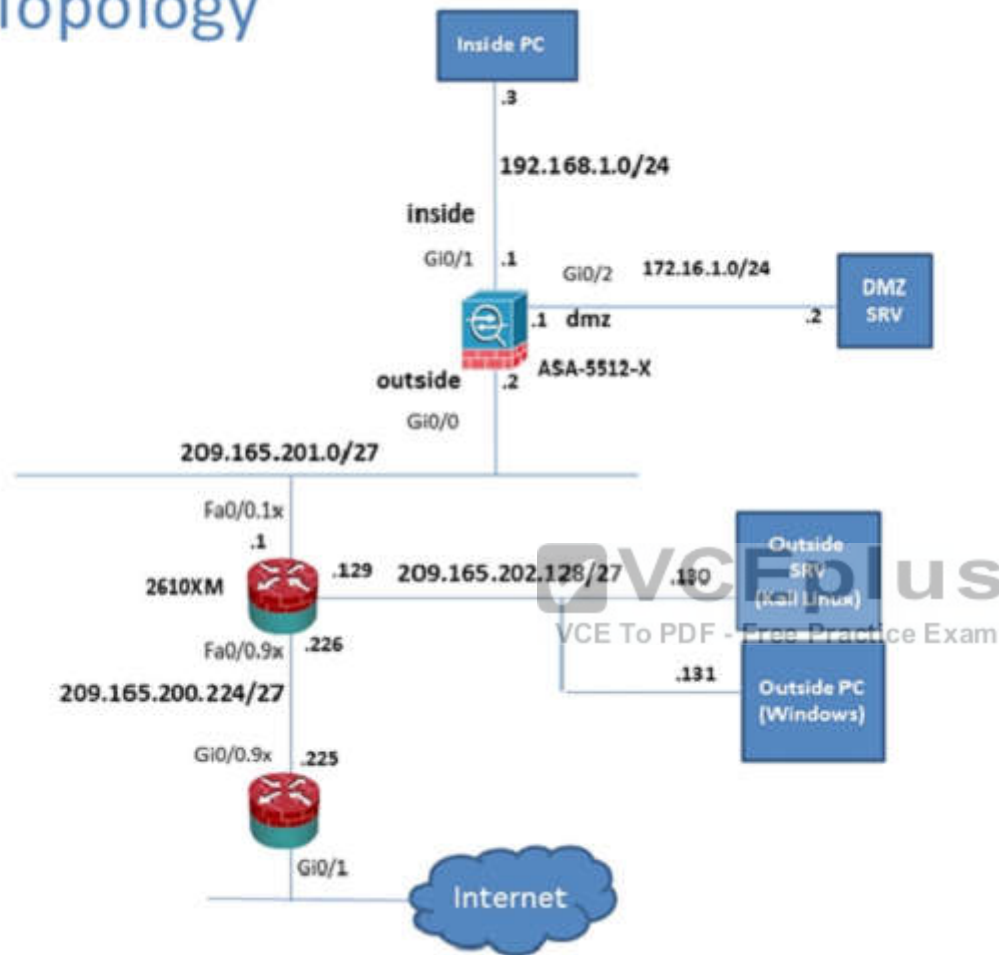
To access ASDM, click the ASA icon in the topology diagram.

Note: Not all ASDM functionalities are enabled in this simulation.

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



Lab Topology



Cisco ASDM 7.3 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Home

Device Dashboard Firewall Dashboard ASA FastPath Status

Device Information

General License

Host Name: **P17-ASA-secure-x-local**
 ASA Version: **100.14(6)13**
 ASDM Version: **7.5(13)**
 Firewall Mode: **Routed**
 Environment Status: **OK**

Device Uptime: **11d 21h 42m 47s**
 Device Type: **ASA 5512**
 Context Mode: **Single**
 Total Flash: **4096 MB**

Interface Status

| Interface | IP Address/Mask | Line | Link | Flt |
|-----------|------------------|------|------|-----|
| dmz | 172.16.1.1/24 | 0 | UP | 0 |
| inside | 192.168.1.1/24 | 0 | UP | 0 |
| mgmt | 10.10.10.1/24 | 0 | UP | 0 |
| outside | 209.165.201.2/24 | 0 | UP | 0 |

Select an interface to view input and output flaps

VPN Sessions

IPsec: 0 Clientless SSL VPN: AnyConnect Client: 0 [Details](#)

Failover Status

Failover not configured. Click the link to configure it. [Configure](#)

System Resources Status

Total Memory Usage Total CPU Usage Core Usage [Details](#)

Memory Usage (MB)

Traffic Status

Connections Per Second Usage

Input Kbps: 0 Output Kbps: 0

Latest ASDM Syslog Messages

| Severity | Date | Time | Syslog ID | Source IP | Source Destination IP | Destination Description |
|----------|-------------|----------|-----------|-------------|-----------------------|--|
| 6 | May 13 2015 | 12:15:09 | 302014 | 10.10.1.254 | 209.165.201.2 | Teardown UDP connection 25136525 for outside:10.10.1.254:202 to identity:209.165.201.2/191310(any) duration:0:02:01 bytes 96 |
| 6 | May 13 2015 | 12:15:08 | 100015 | 192.168.1.3 | 192.168.1.1 | Deny TCP (no connection) from 192.168.1.3/14676 to 192.168.1.1/443 flags FIN ACK on interface inside |
| 6 | May 13 2015 | 12:15:08 | 302014 | 192.168.1.3 | 192.168.1.1 | Teardown TCP connection 15136528 for inside:192.168.1.3/14676 to identity:192.168.1.1/443 duration:0:00:00 bytes 299 TCP Reset-O |

Student 15 3/13/15 12:15:18 PM.pdf

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces

Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

| Interface | IP Address | MAC Address | Proxy ARP |
|-----------|--------------|----------------|-----------|
| outside | 209.56.10.1 | 000c.3014.3830 | No |
| inside | 192.168.1.4 | 0090.5633.3333 | No |
| inside | 192.168.1.3 | 0090.5611.1111 | No |
| inside | 192.168.1.2 | 0090.5622.2222 | No |
| inside | 192.168.1.56 | 0090.5692.5c7b | No |
| inside | 192.168.1.55 | 0006.75e5.98f9 | No |
| Serial | 172.16.1.2 | 0050.5644.4444 | No |
| mgmt | 10.10.10.1 | 000c.3014.3830 | No |

Clear Dynamic ARP Entries

Refresh

Interfaces

IPs

Botnet Traffic Filter

Routing

Properties

Logging

Data Refreshed Successfully.

Last Updated: 5/19/15 9:32:52 AM

5/19/15 9:32:27 AM pac

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

VPN

VPN Statistics

- VPN Cluster Loads
- Crypto Statistics
- Compression Statistics
- Encryption Statistics
- Global IKE/DPsec Statistics
- Protocol Statistics
- VLAN Mapping Sessions
- MDM Proxy Statistics
- MDM Proxy Sessions
- Clientless SSL VPN
- VPN Connection Graphs
- WPA Sessions

Interfaces

VPN

Brinet Traffic Filter

Routing

Properties

Logging

Monitoring > VPN > VPN Statistics > Sessions

| Type | Active | Cumulative | Peak Concurrent | Inactive |
|-----------------|--------|------------|-----------------|----------|
| Clientless VPNs | 1 | 1 | 1 | 1 |
| Browser | 1 | 1 | 1 | 1 |

Filter By: Clientless SSL VPN - All Sessions - Filter

| Username IP Address | Group Policy Connection Profile | Protocol Encryption | Login Time Duration | Bytes Tx Bytes Rx |
|----------------------------|------------------------------------|---------------------------------|--|----------------------|
| student 192.168.202.131 | Clientless Secure | Clientless Clientless (CBC4) | 10:23:46 pm Thu May 21, 2015 00:00:00 | 216774 41820 |

Details

Logout

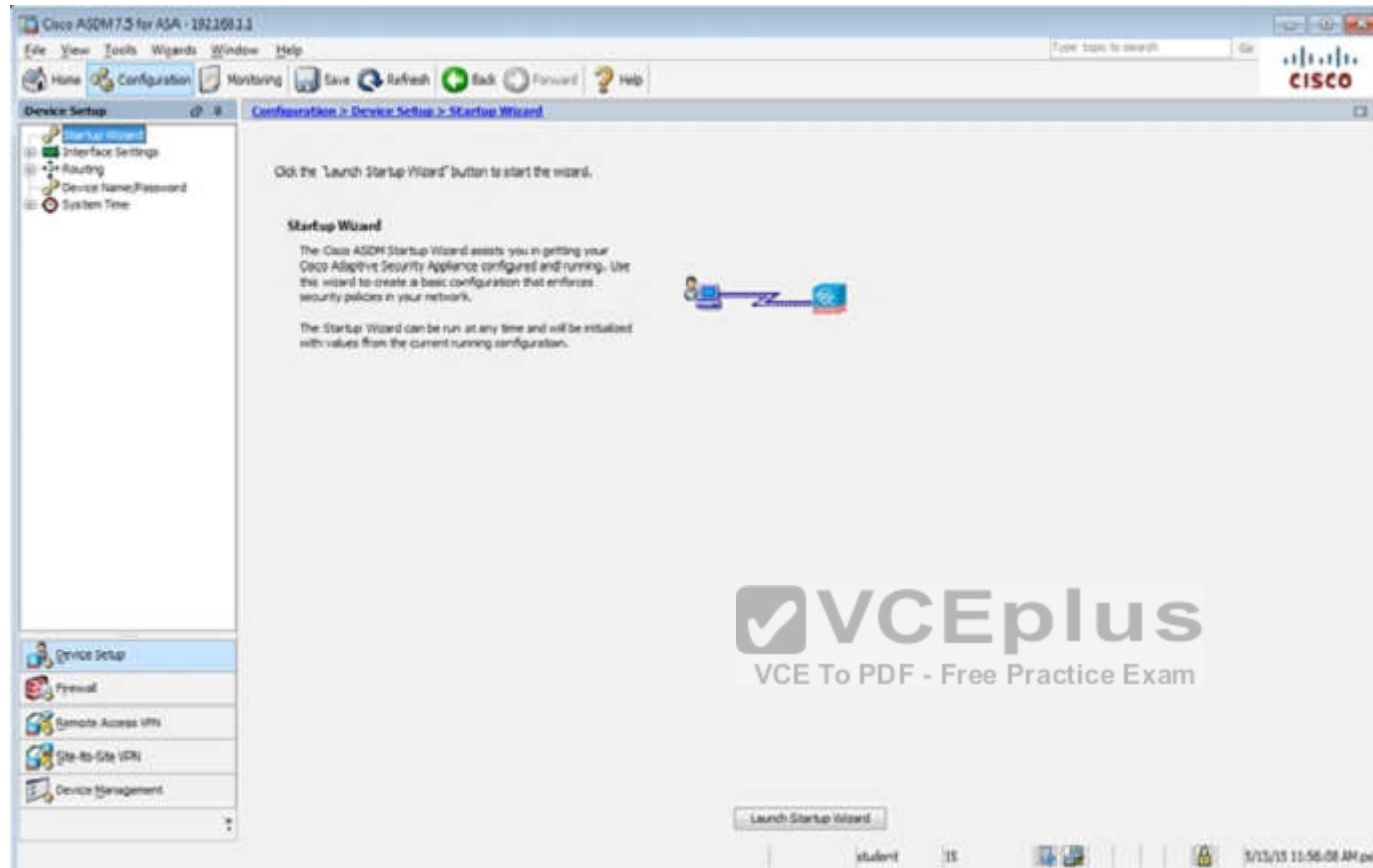
Ping

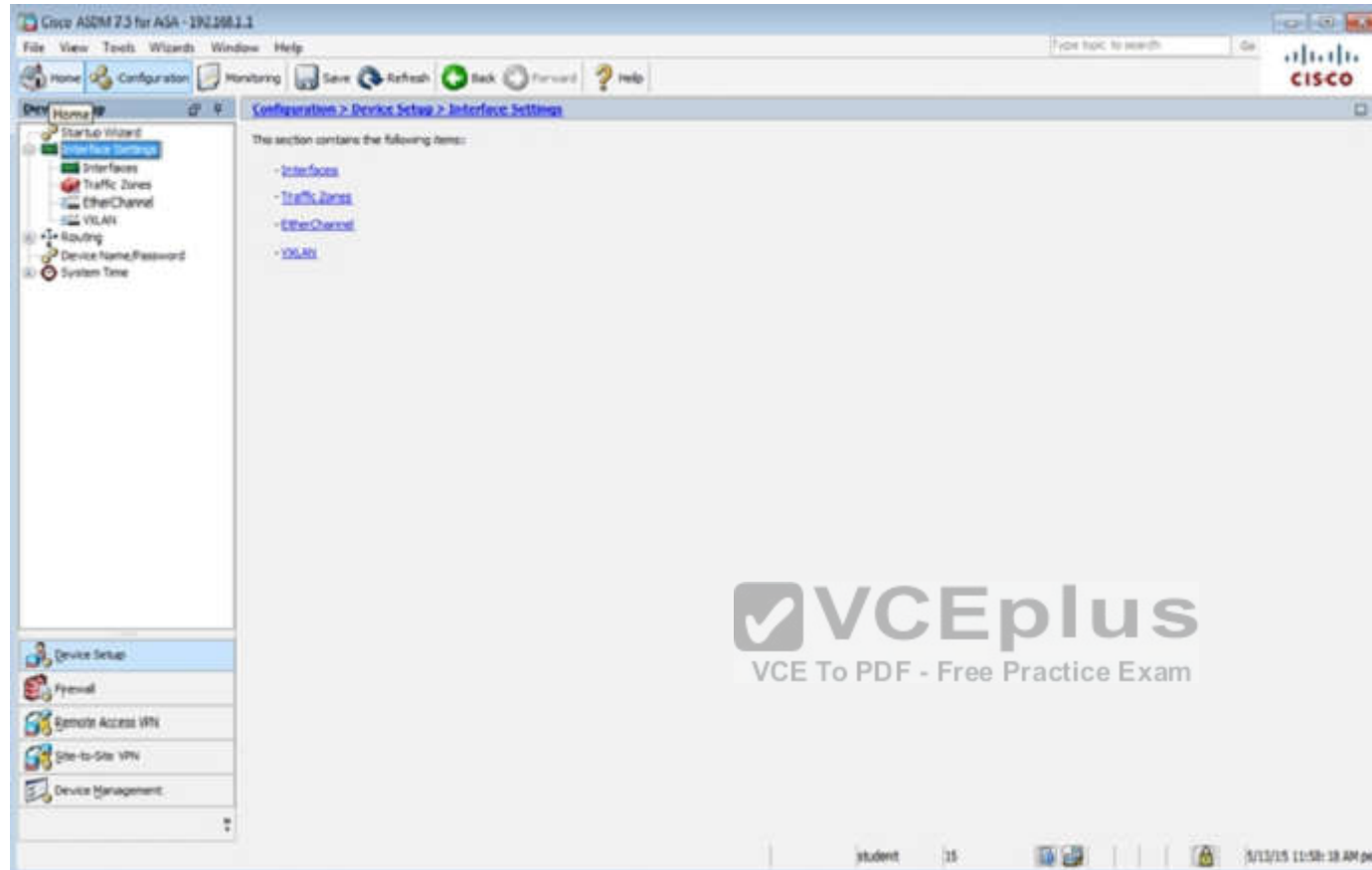
Refresh

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

Data Refreshed Successfully.

student 15 5/19/15 9:33:37 AM





Cisco ASDM 7.5 For ASA - 192.168.1.1

File View Tools Wizards Window Help

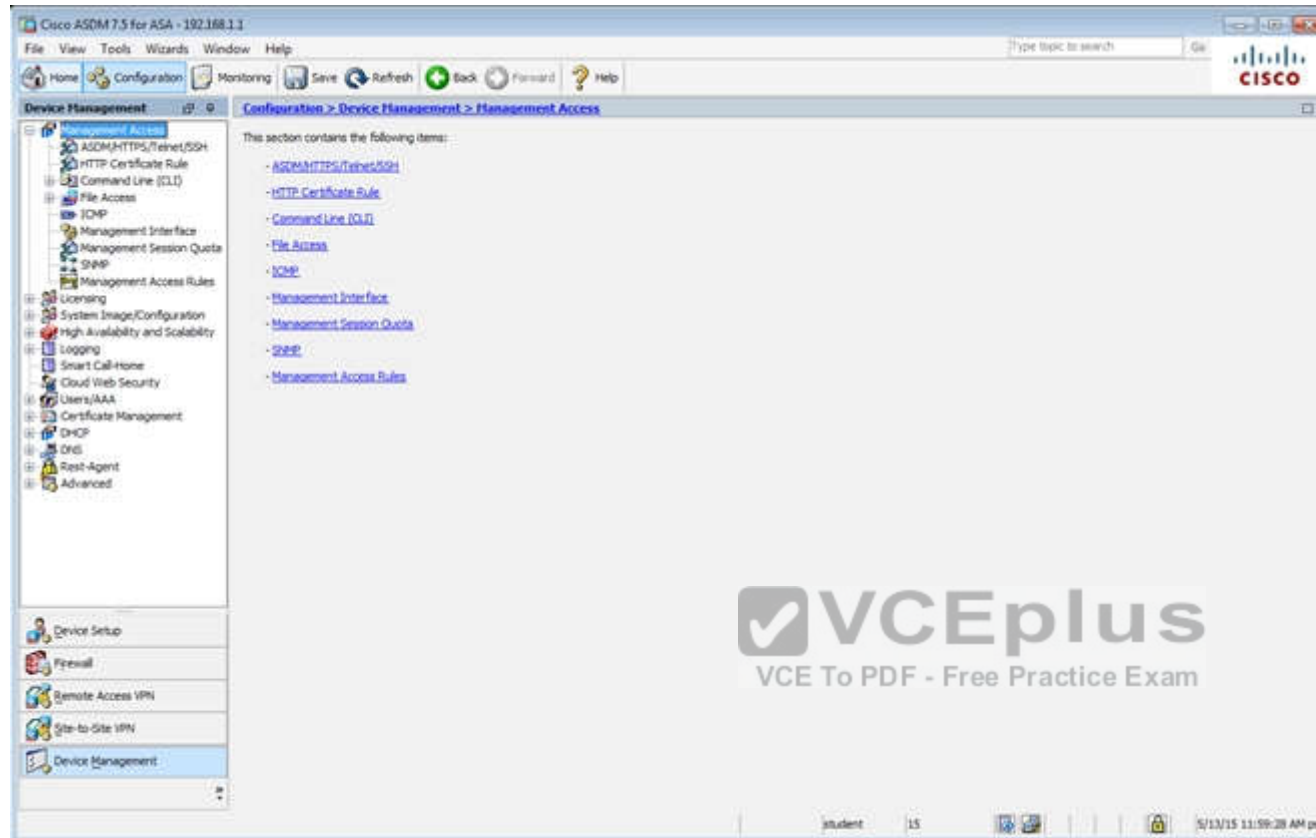
Home Configuration Monitoring Save Refresh Back Forward Help

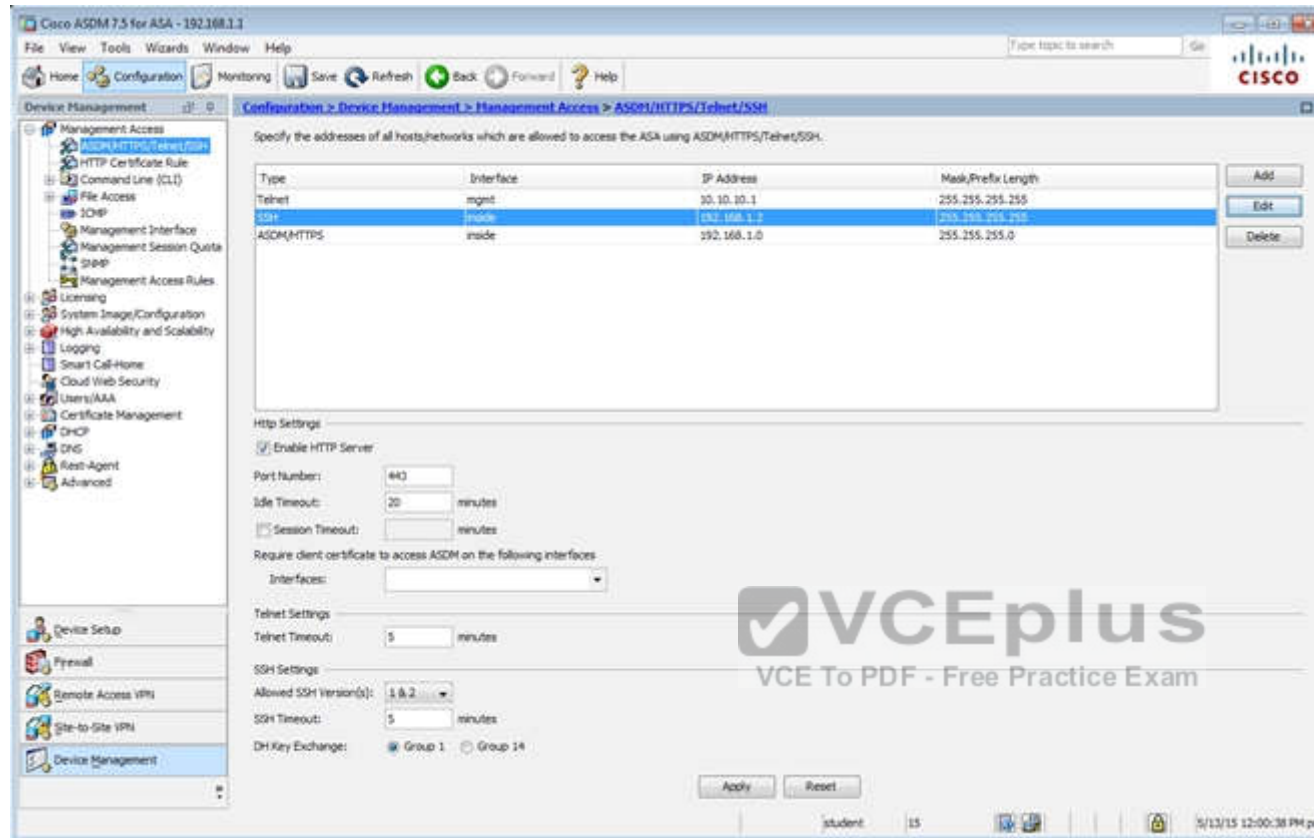
Configuration > Device Setup > Interface Settings > Interfaces

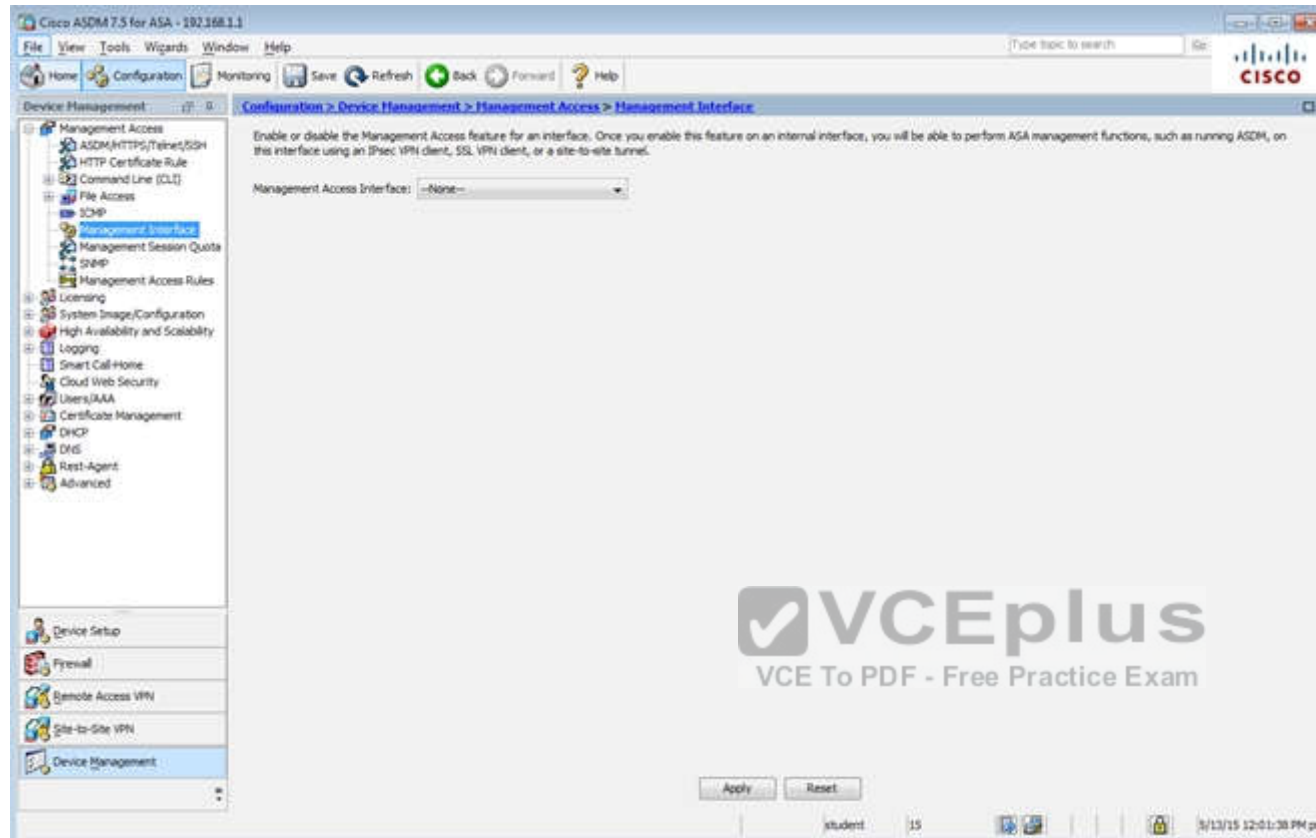
| Interface | Name | Zone | Route Map | Status | Security Level | IP Address | Subnet Mask | Prefix Length | Group | Type |
|---------------------|---------|------|-----------|---------|----------------|-------------------|---------------|---------------|-------|----------|
| GigabitEthernet0/20 | outside | | | Enabled | | 0/0/0 192.168.1.1 | 255.255.255.0 | | | Hardware |
| GigabitEthernet0/1 | inside | | | Enabled | | 100 192.168.1.1 | 255.255.255.0 | | | Hardware |
| GigabitEthernet0/2 | dmz | | | Enabled | | 172.16.1.1 | 255.255.255.0 | | | Hardware |
| GigabitEthernet0/3 | | | | Enabled | | | | | | Hardware |
| GigabitEthernet0/4 | | | | Enabled | | | | | | Hardware |
| GigabitEthernet0/5 | ngmt | | | Enabled | | 100 10.10.10.2 | 255.255.255.0 | | | Hardware |
| Management0/0 | | | | Enabled | | | | | | Hardware |

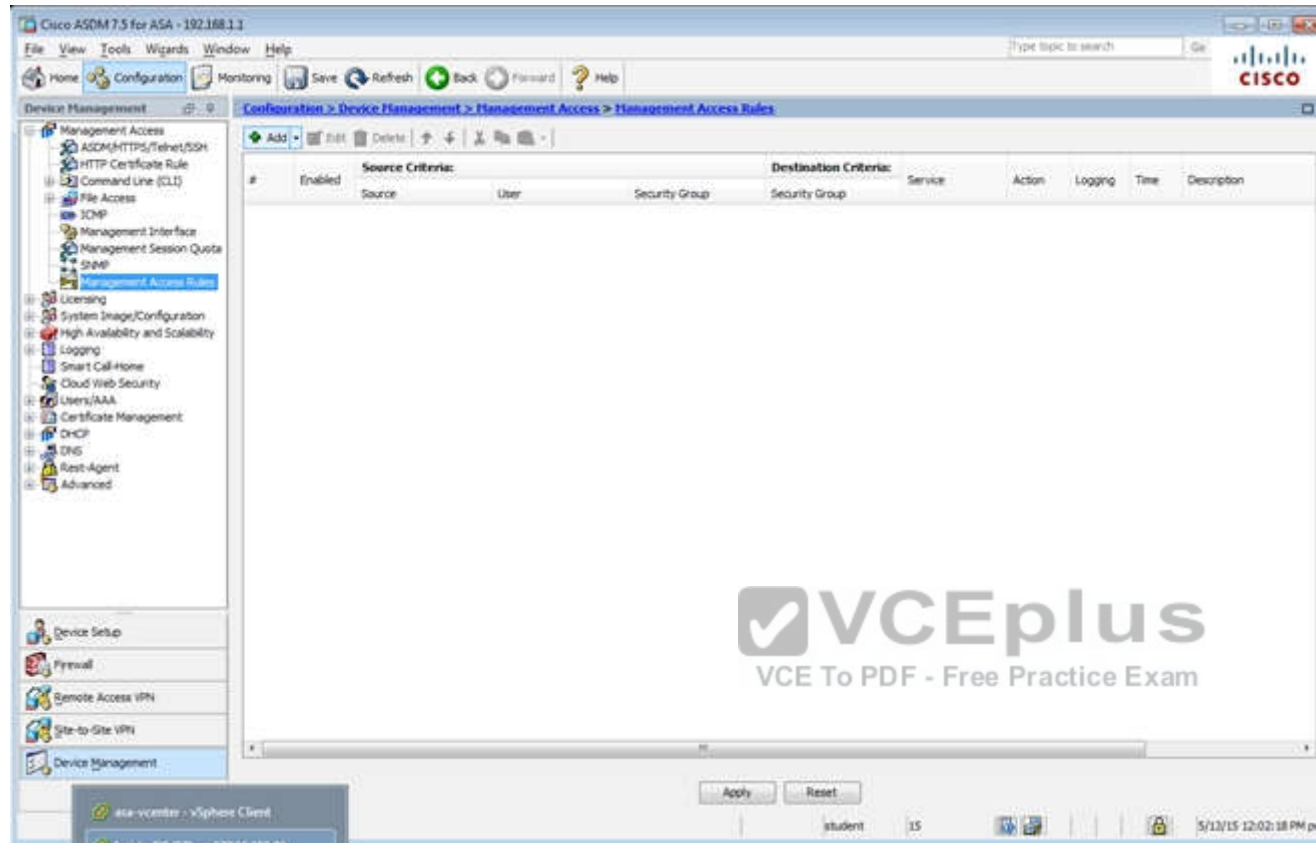
☐ Enable traffic between two or more interfaces which are configured with same security levels
☐ Enable traffic between two or more hosts connected to the same interface
☐ Enable jumbo frame reservation

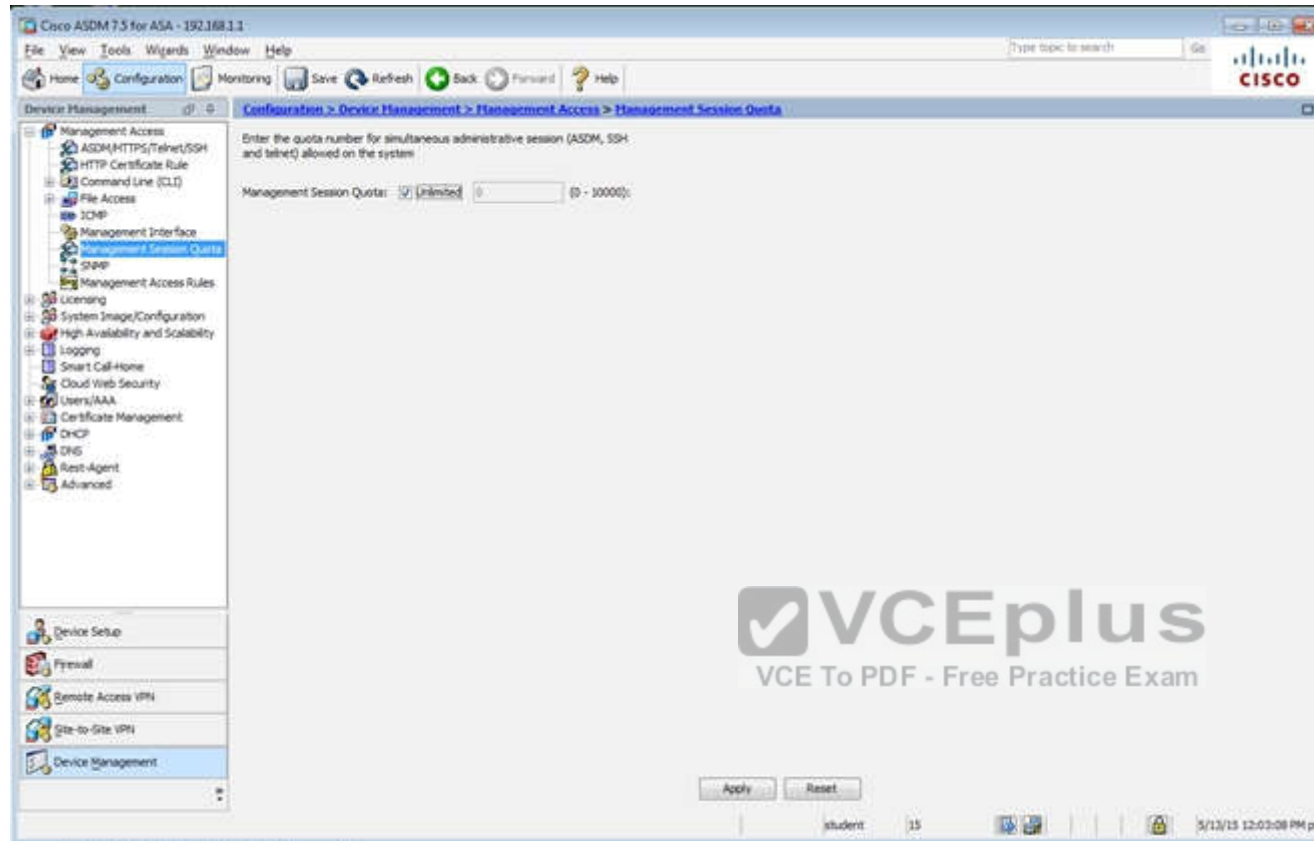
Student 15 3/13/15 12:42:48 PM pst

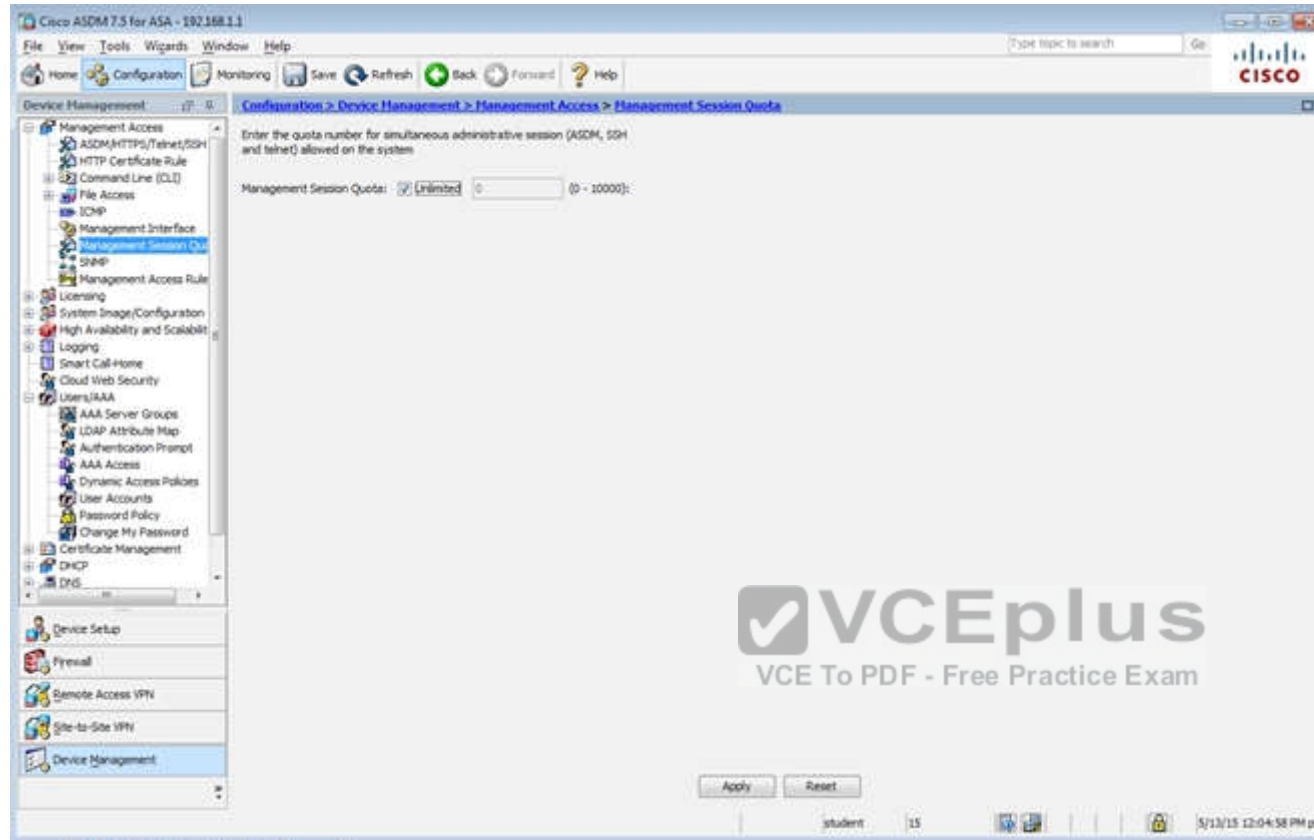


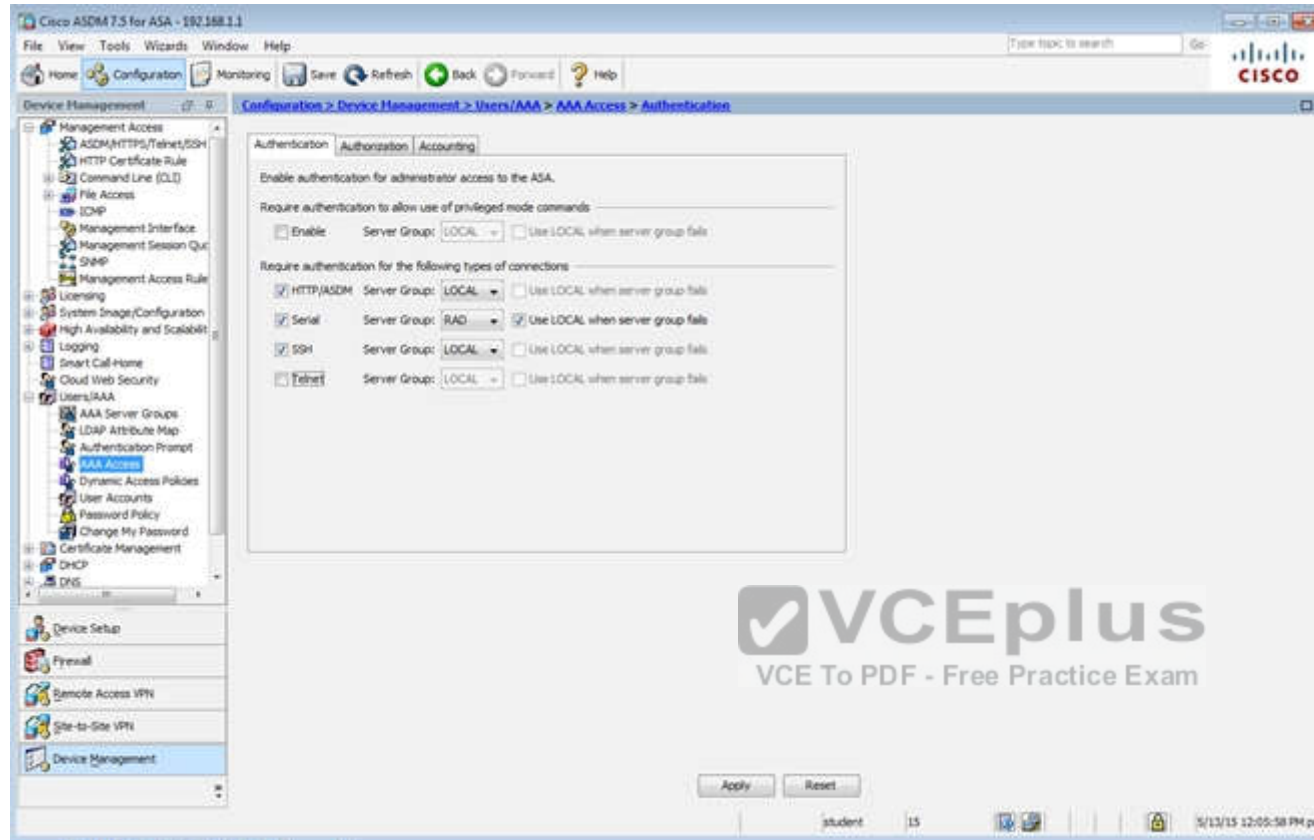


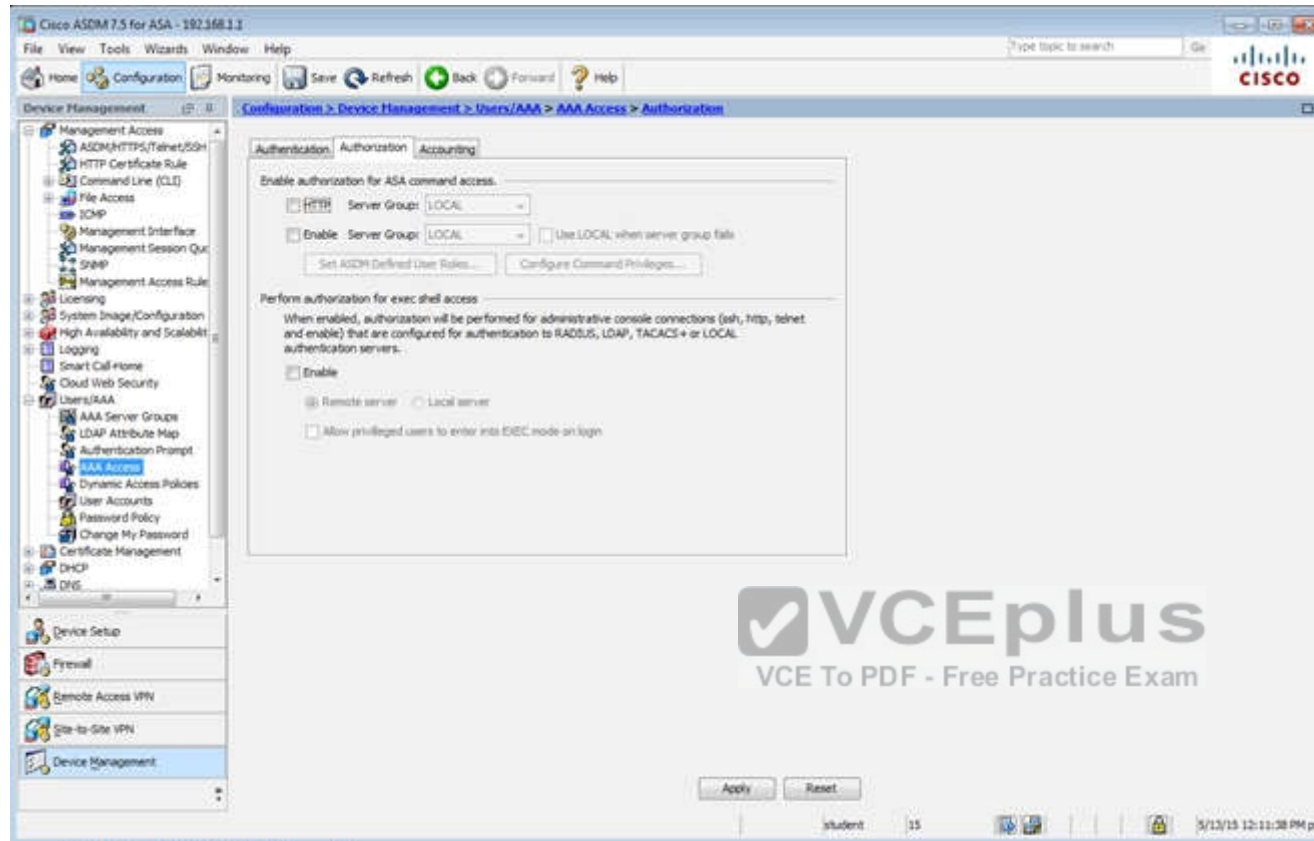


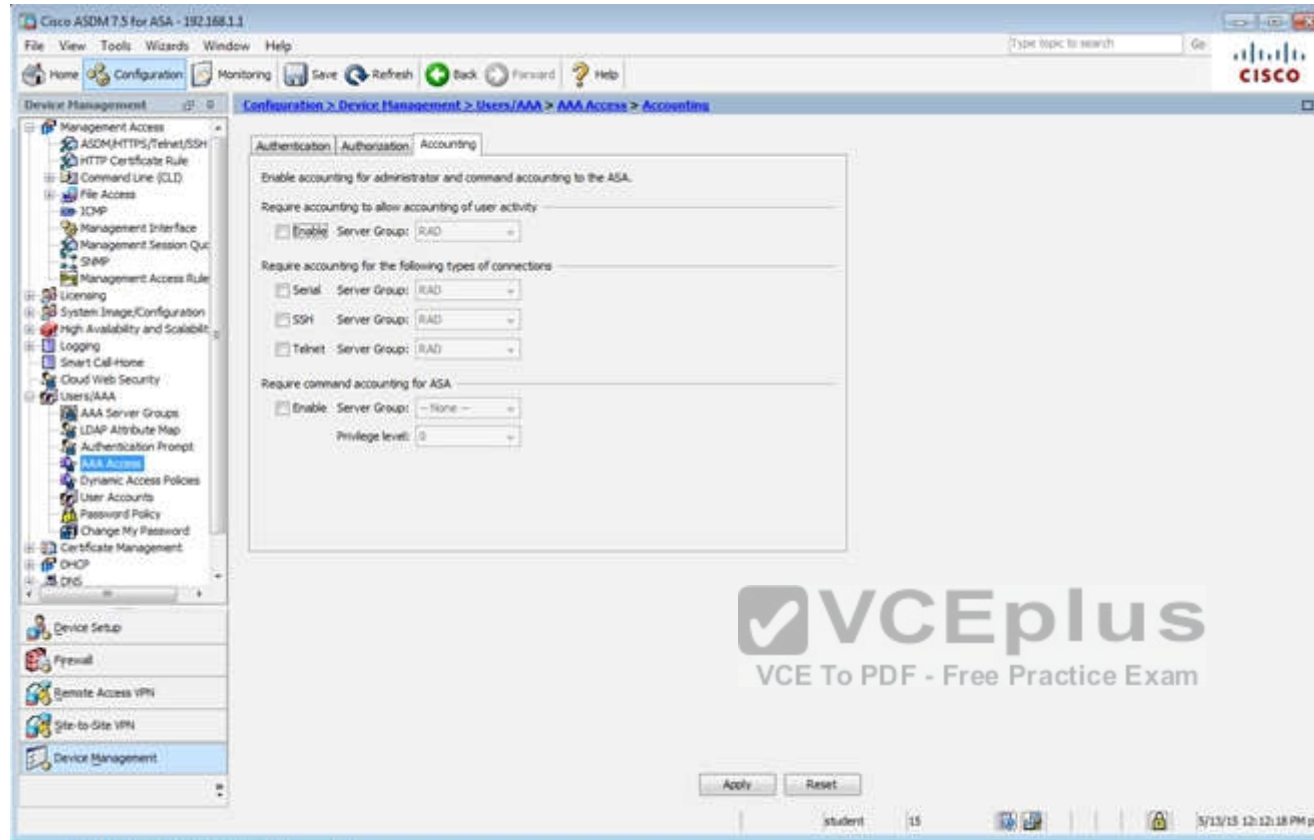


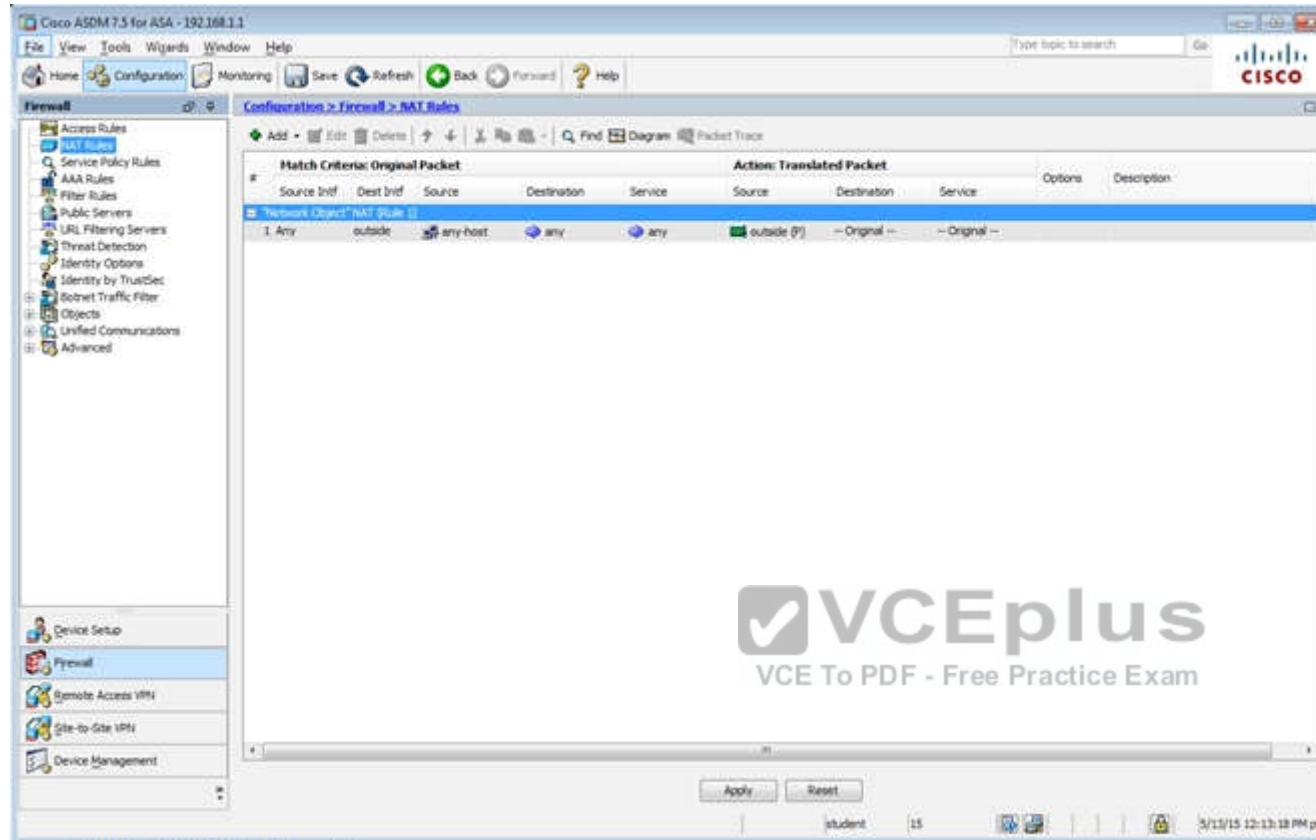


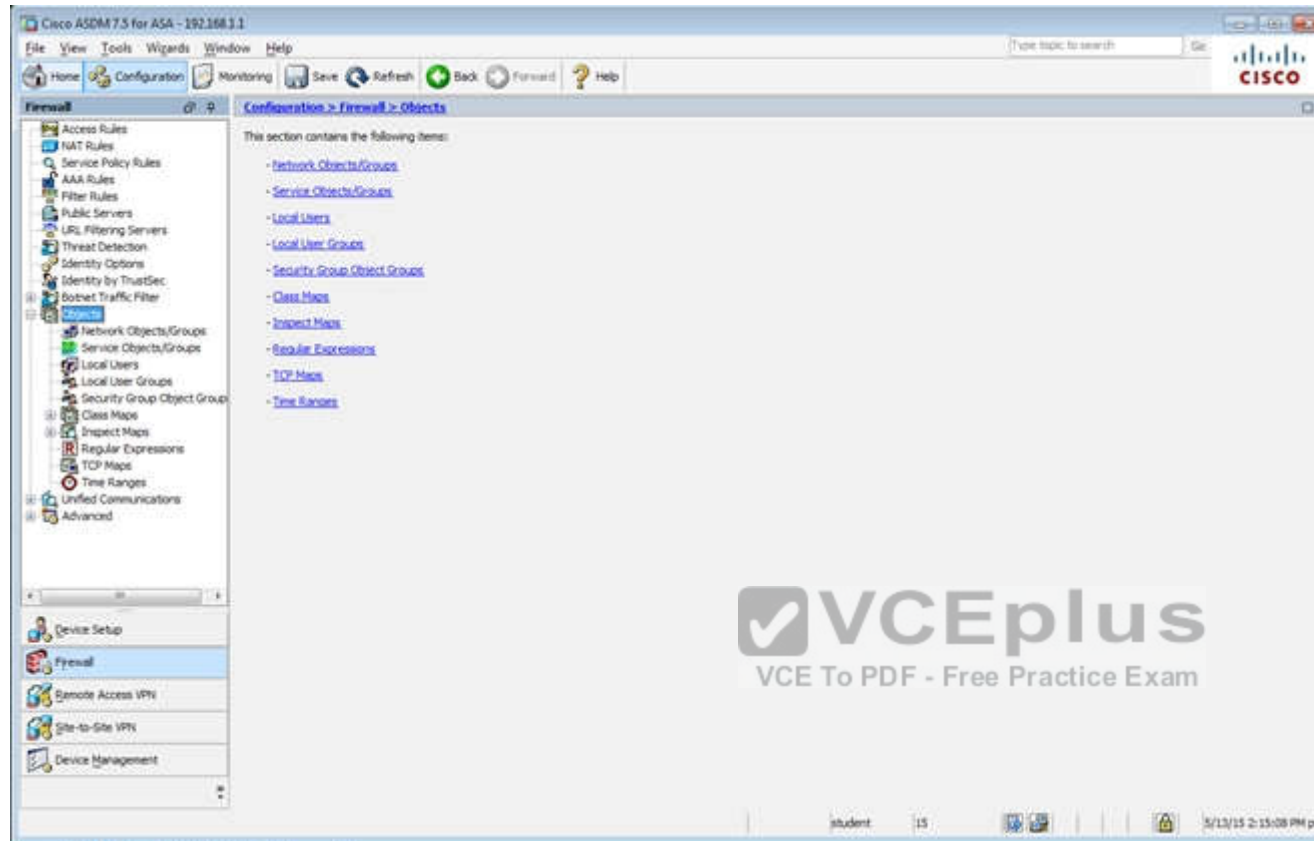












Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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 [Authentication](#).

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

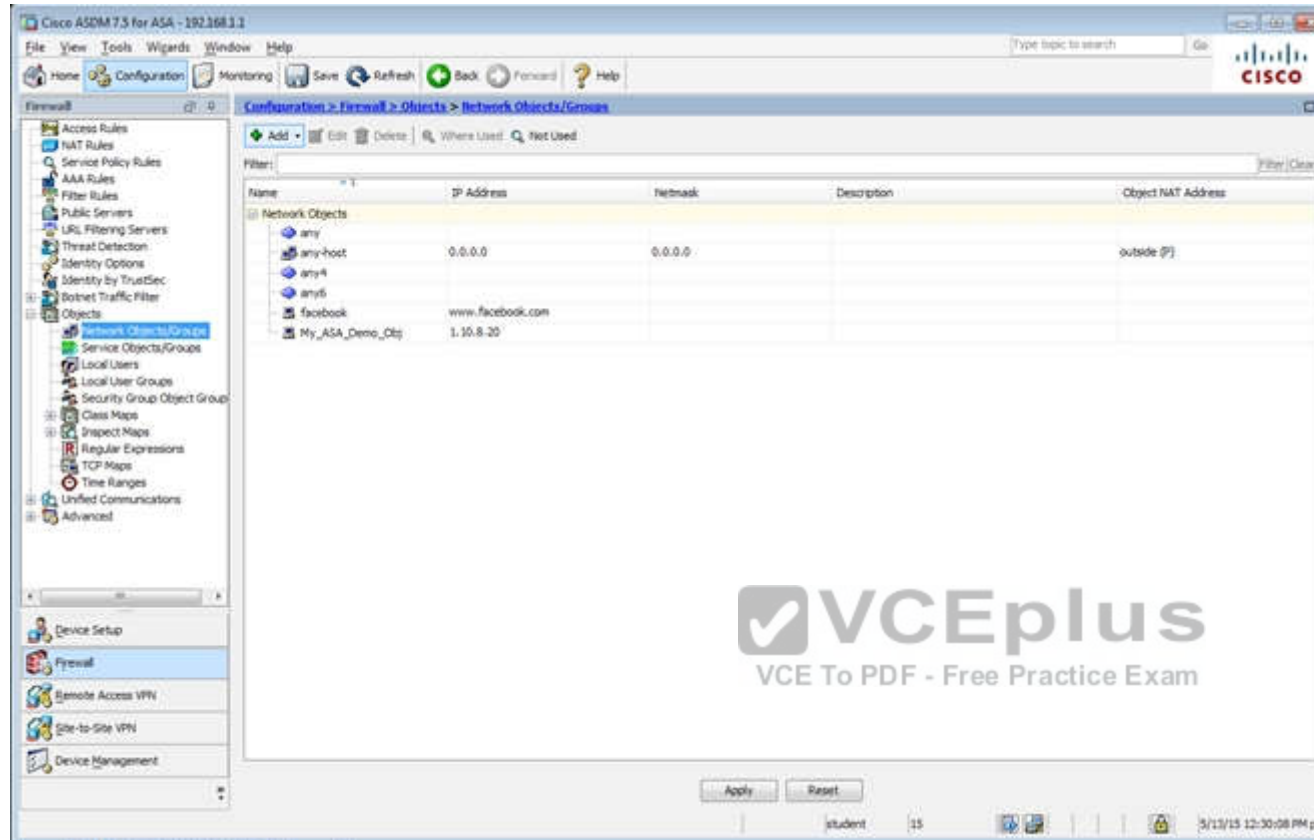
| Username | Privilege Level (Role) | Access Restrictions | VPN Group Policy | VPN Group Lock |
|-----------|------------------------|---------------------|----------------------------|----------------------------|
| student | 15 | Full | -- Inherit Group Policy -- | -- Inherit Group Policy -- |
| enable_15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

Add Edit Delete

Ends: Match Case

Apply Reset

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall Configuration > Firewall > 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 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

Configuration > Firewall > Service Policy Rules

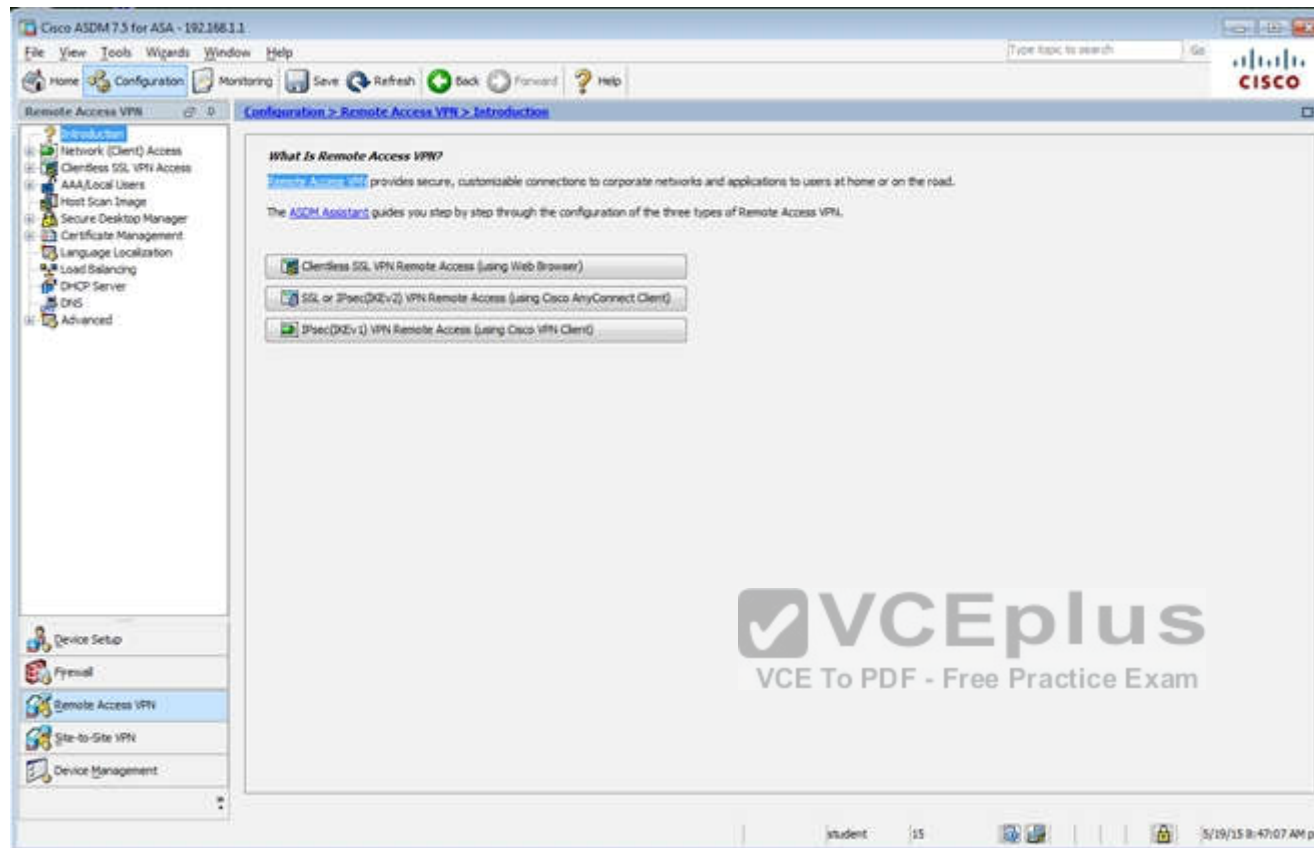
Add Edit Delete Find Diagram Packet Trace

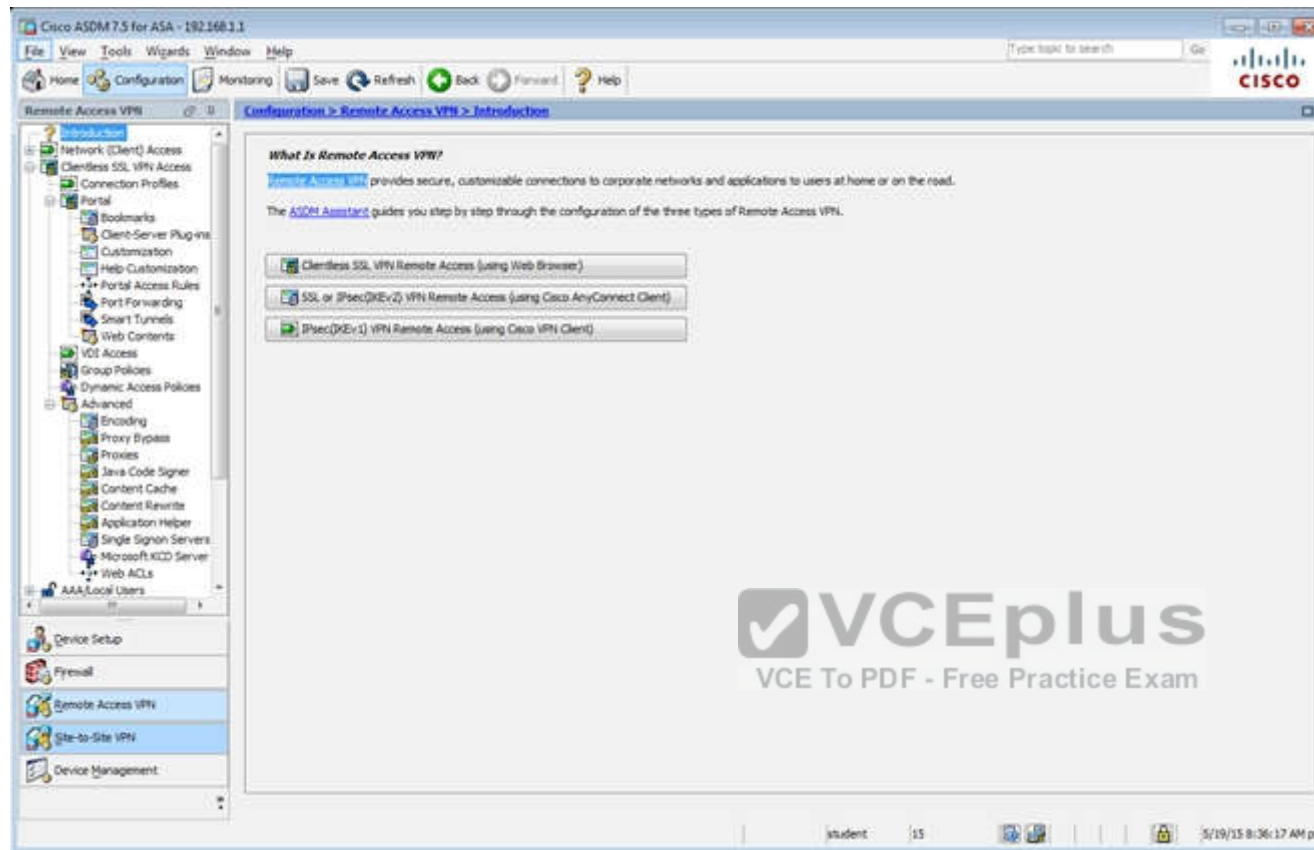
| Name | # | Enabled | Match | Source | Src Security Group | Destination | Dest Security Group | Service | Time | Rule Actions | Description |
|--|---|---------|-------|--------|--------------------|-------------|---------------------|-------------------|------|--------------|--|
| Interface: dmz; Policy: asastf_policy | | | | | | | | | | | |
| class-default | | | Match | any | | any | | any traffic | | | |
| | | | | | | | | class-default | | | |
| Interface: inside; Policy: asastf_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 SMTP (14 more inspect actions) |

Apply Reset

student 15 5/13/15 12:15:48 PM pst







Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

| Interface | Allow Access |
|-----------|-------------------------------------|
| outside | <input checked="" type="checkbox"/> |
| dns | <input type="checkbox"/> |
| inside | <input type="checkbox"/> |

Device Certificate ...
Port Setting ...

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

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

☐ Shutdown portal login page.

Connection Profiles

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

Add Edit Delete Find: Match Case

| Name | Enabled | Aliases | Authentication Method | Group Policy |
|--------------------|-------------------------------------|---------|-----------------------|---------------|
| DefaultRAGroup | <input checked="" type="checkbox"/> | | AAA(RADIUS) | DefaultPolicy |
| DefaultWEBVpnGroup | <input checked="" type="checkbox"/> | | AAA(RADIUS) | DefaultPolicy |
| Clientless | <input checked="" type="checkbox"/> | test | AAA(RADIUS) | DefaultPolicy |

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

Apply Reset

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

Edit Clientless SSL VPN Connection Profile: clientless

Basic
Advanced

Name: clientless
Aliases: test

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

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

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

Find: ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

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

Login and Logout Page Customization: DfltCustomization Manage...

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

☐ Enable the display of SecurId messages on the login screen

Connection Aliases

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

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

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

Group URLs

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

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

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

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

☒ Always run CSD

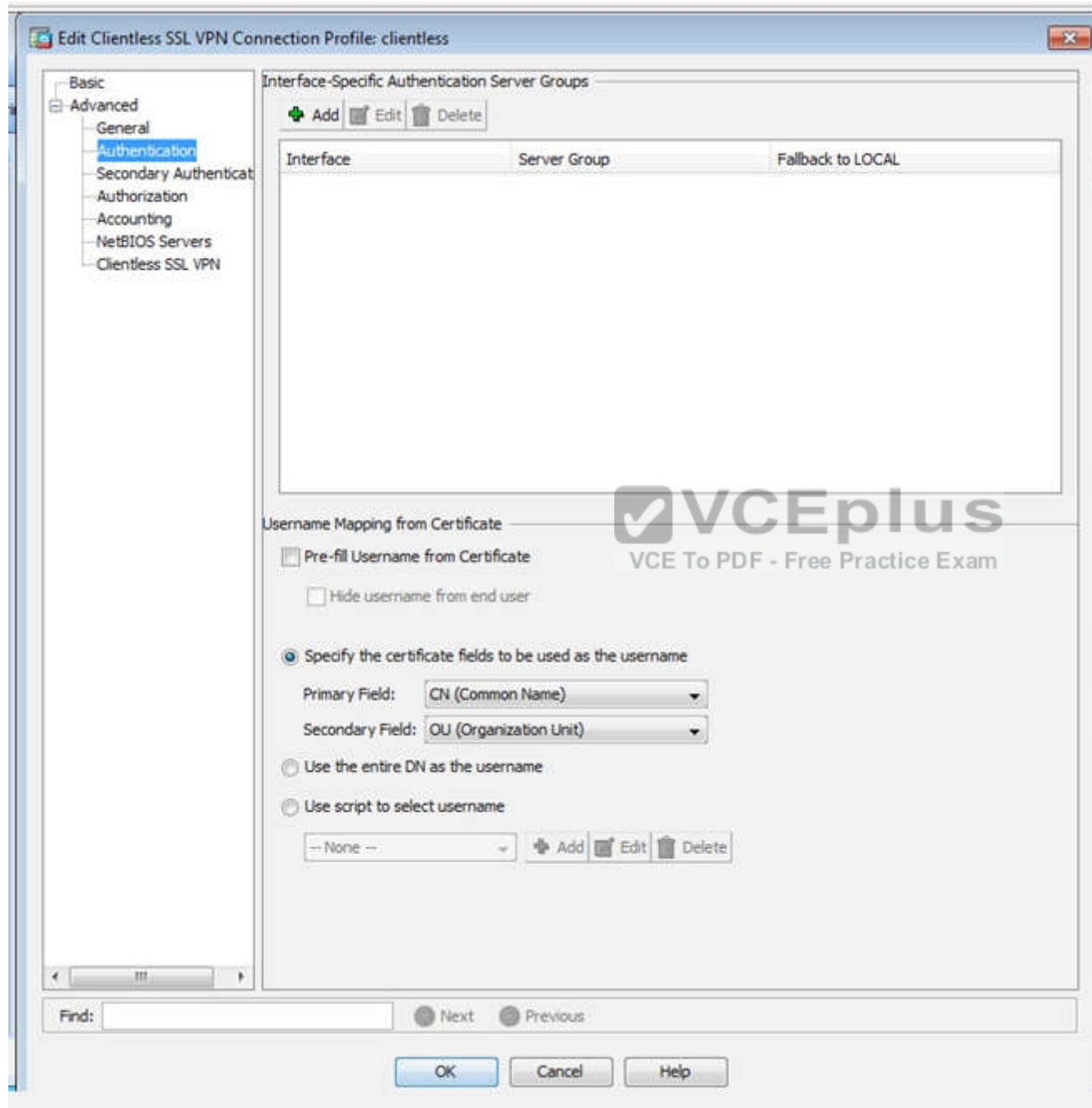
☐ Disable CSD for both AnyConnect and Clientless SSL VPN

☐ Disable CSD for AnyConnect only

Find: Next Previous

OK Cancel Help







Edit Clientless SSL VPN Connection Profile: clientless

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

Secondary Authentication Server Group

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

☐ Use LOCAL if Server Group fails

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

Attributes Server: ☒ Primary ☐ Secondary

Session Username Server: ☒ Primary ☐ Secondary

Interface-Specific Secondary Authentication Server Groups

+ Add Edit Delete

| Interface | Server Group | Fallback to LOCAL | Use primary username |
|-----------|--------------|-------------------|----------------------|
|-----------|--------------|-------------------|----------------------|

Username Mapping from Certificate

☐ Pre-fill username from certificate

☐ Hide username from end user

☐ Fallback when a certificate is unavailable

Password: ☒ Prompt ☐ Use primary ☐ Use

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

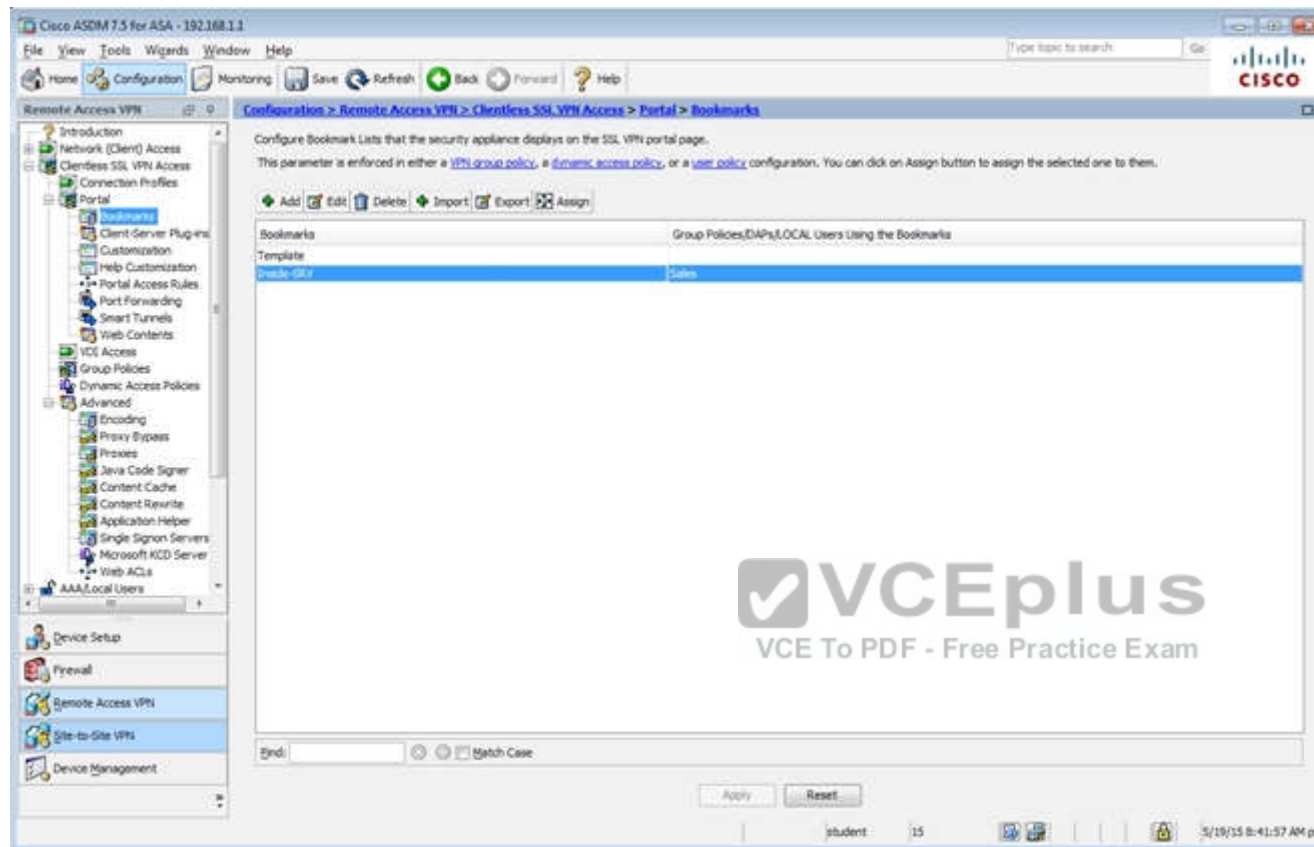
☐ Use the entire DN as the username

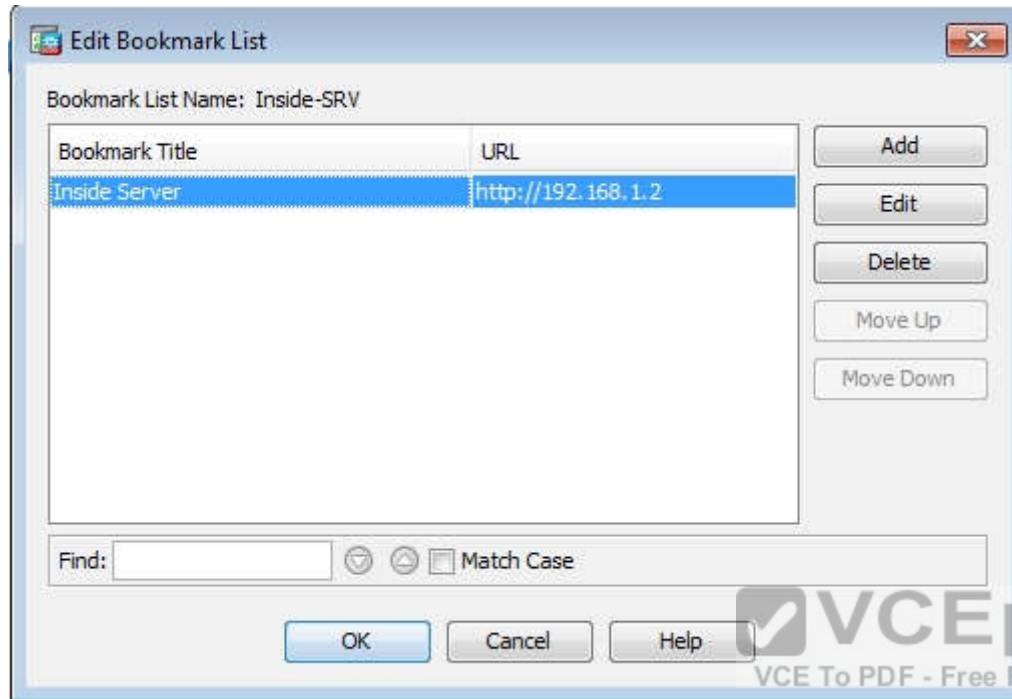
☐ Use script to select username

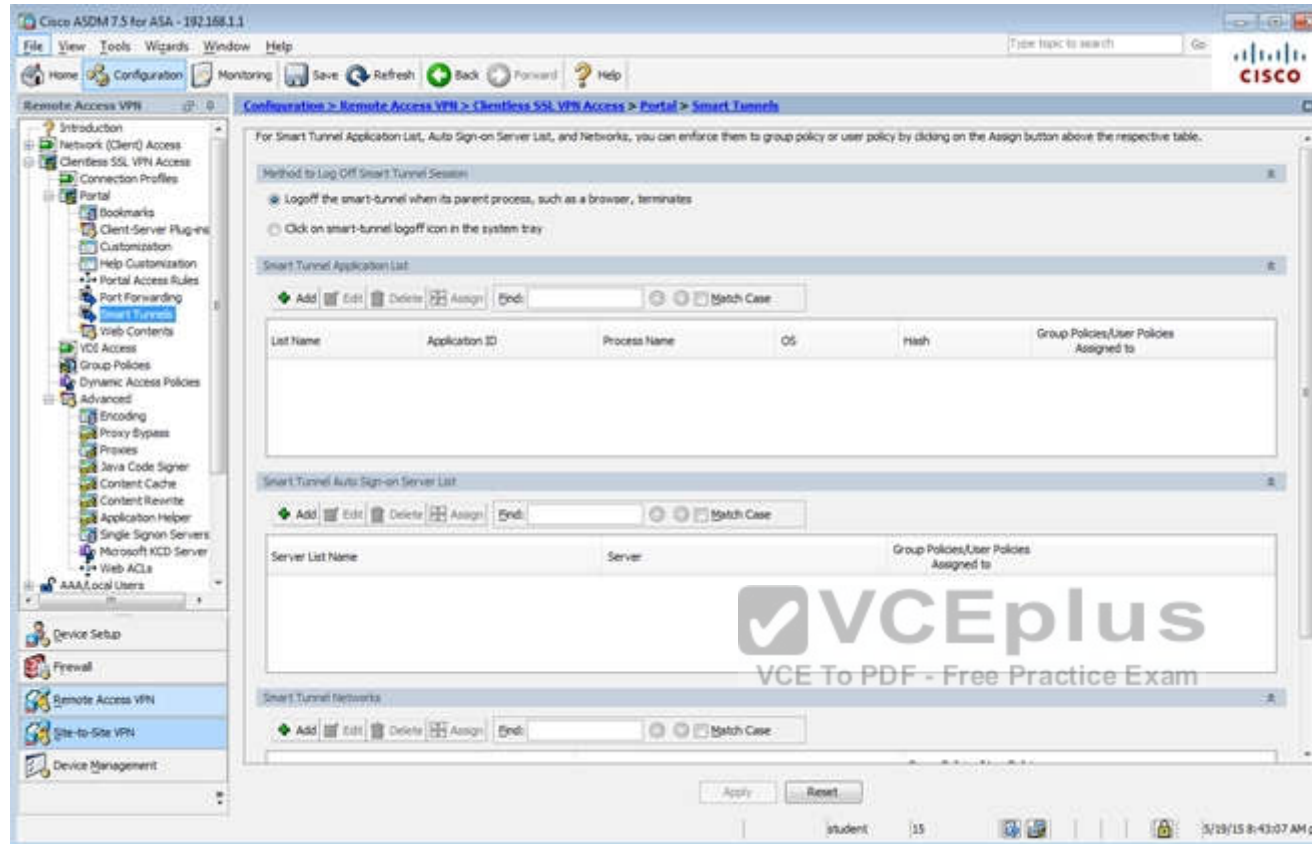
-- None -- + Add Edit Delete

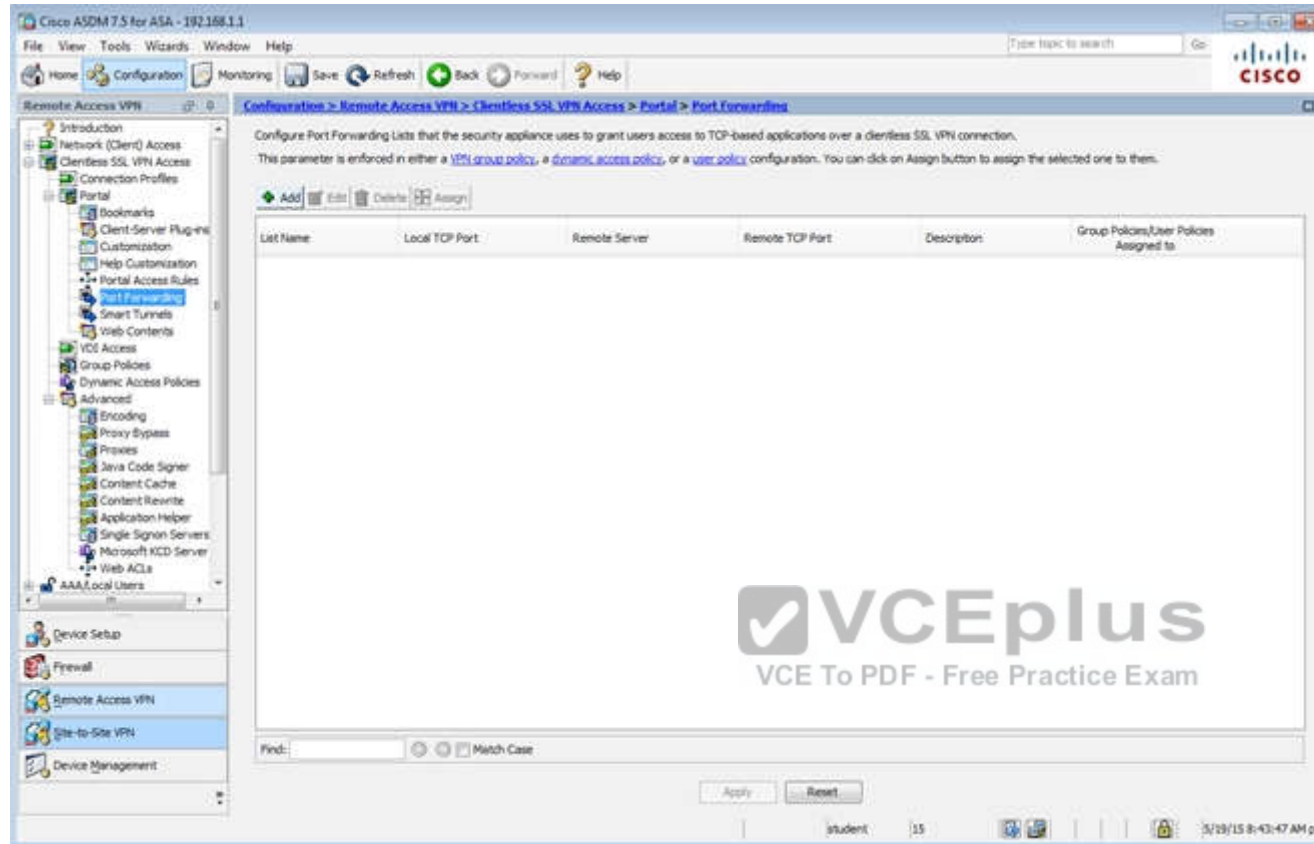
Find: Next Previous

OK Cancel Help









Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Clientless SSL VPN Access > 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 |
|--------------------------------|----------|------------------------------------|--|
| Swan | External | swan-clientless | Clientless |
| DefaultPolicy (System Default) | Internal | key1:key2:ssl-clientless/2tp-ipsec | DefaultRAGroup/DefaultL3Group/DefaultADMG/Def... |

End: Match Case

Apply Reset

student 15 3/19/15 8:49:27 AM pst

Edit Internal Group Policy: Sales

Name: Sales

Banner: ☒ Inherit

More Options

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

Web ACL: ☒ Inherit Manage...

Access Hours: ☒ Inherit Manage...

Simultaneous Logins: ☒ Inherit

Restrict access to VLAN: ☒ Inherit

Connection Profile (Tunnel Group) Lock: ☒ Inherit

Maximum Connect Time: ☒ Inherit ☐ Unlimited minutes

Idle Timeout: ☒ Inherit ☐ Use Global Default minutes

Timeout Alerts

Session Alert Interval: ☒ Inherit ☐ Default minutes

Idle Alert Interval: ☒ Inherit ☐ Default minutes

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

Find: ☒ Next ☐ Previous

OK Cancel Help

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

- IPsec/SSL Connection
- Secure Mobility Solution
- Address Assignment
- Advanced
- Clientless SSL VPN Access
- Connection Profiles
- Portal
- Bookmarks
- Client-Server Plug-ins
- Customization
- Help Customization
- Portal Access Rules
- Port Forwarding
- Smart Tunnels
- Web Contents
- Voice Access
- Group Policies**
- Dynamic Access Policies
- Advanced
- AAA/Local Users
- AAA Server Groups
- LDAP Attribute Map
- Local Users
- Host Scan Image
- Secure Desktop Manager

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

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

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

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

| Name | Type | Tunneling Protocol | Connection Profiles/Users Assigned To |
|--------------------------------|----------|---|---------------------------------------|
| Default | Internal | ssl-clientless | Default |
| DfltGrpPolicy (System Default) | Internal | Rev 1.0 Rev 2.0 ssl-clientless/2to-ipssec | DfltGrpPolicy |

Find:

student 15 10/15/14 9:15:40 AM pet

Edit Internal Group Policy: Sales

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

Bookmark List: ☐ Inherit Manage...

URL Entry: ☒ Inherit ☐ Enable ☐ Disable

File Access Control

File Server Entry: ☒ Inherit ☐ Enable ☐ Disable

File Server Browsing: ☒ Inherit ☐ Enable ☐ Disable

Hidden Share Access: ☒ Inherit ☐ Enable ☐ Disable

Port Forwarding Control

Port Forwarding List: ☒ Inherit Manage...

☐ Auto Applet Download

Applet Name: ☒ Inherit

Smart Tunnel

Smart Tunnel Policy: ☒ Inherit Manage...

Tunnel Option: Manage...

Smart Tunnel Application: ☒ Inherit Manage...

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

☐ Auto Start

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

Windows Domain Name (optional):

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

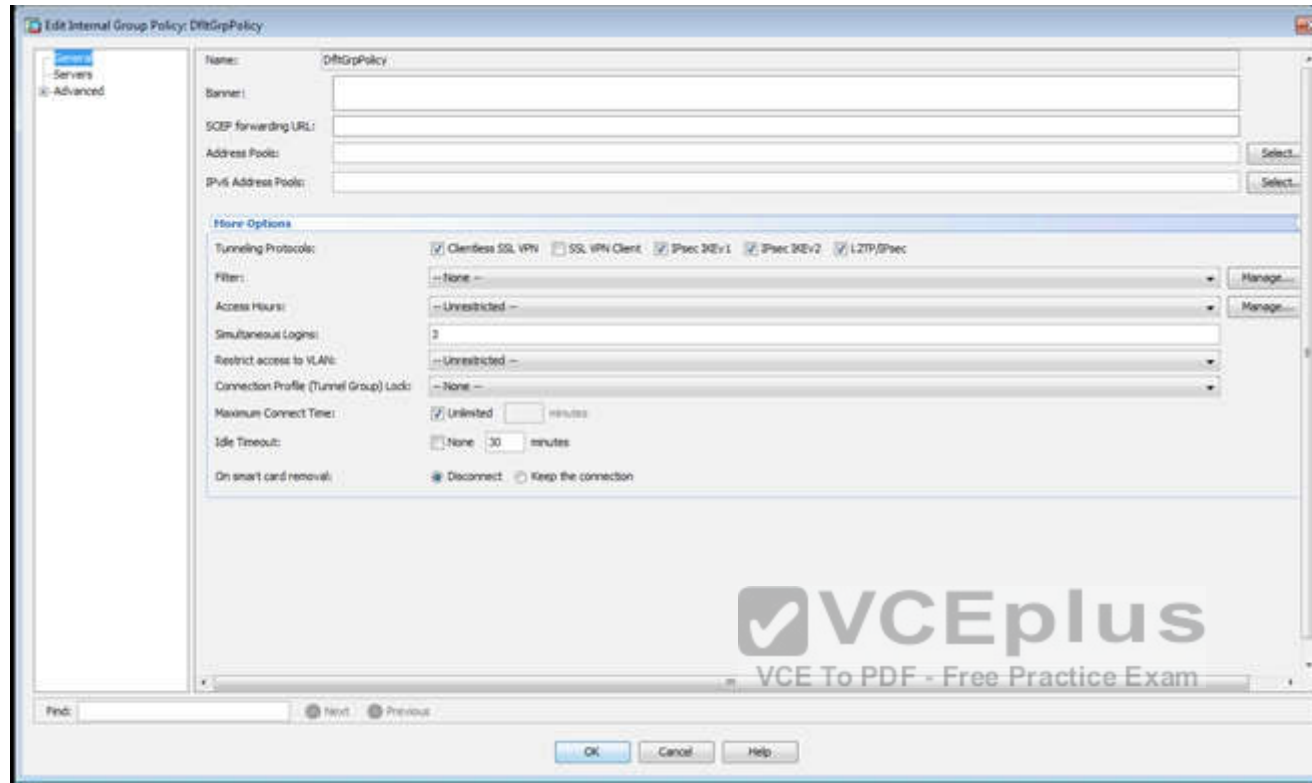
ActiveX Relay

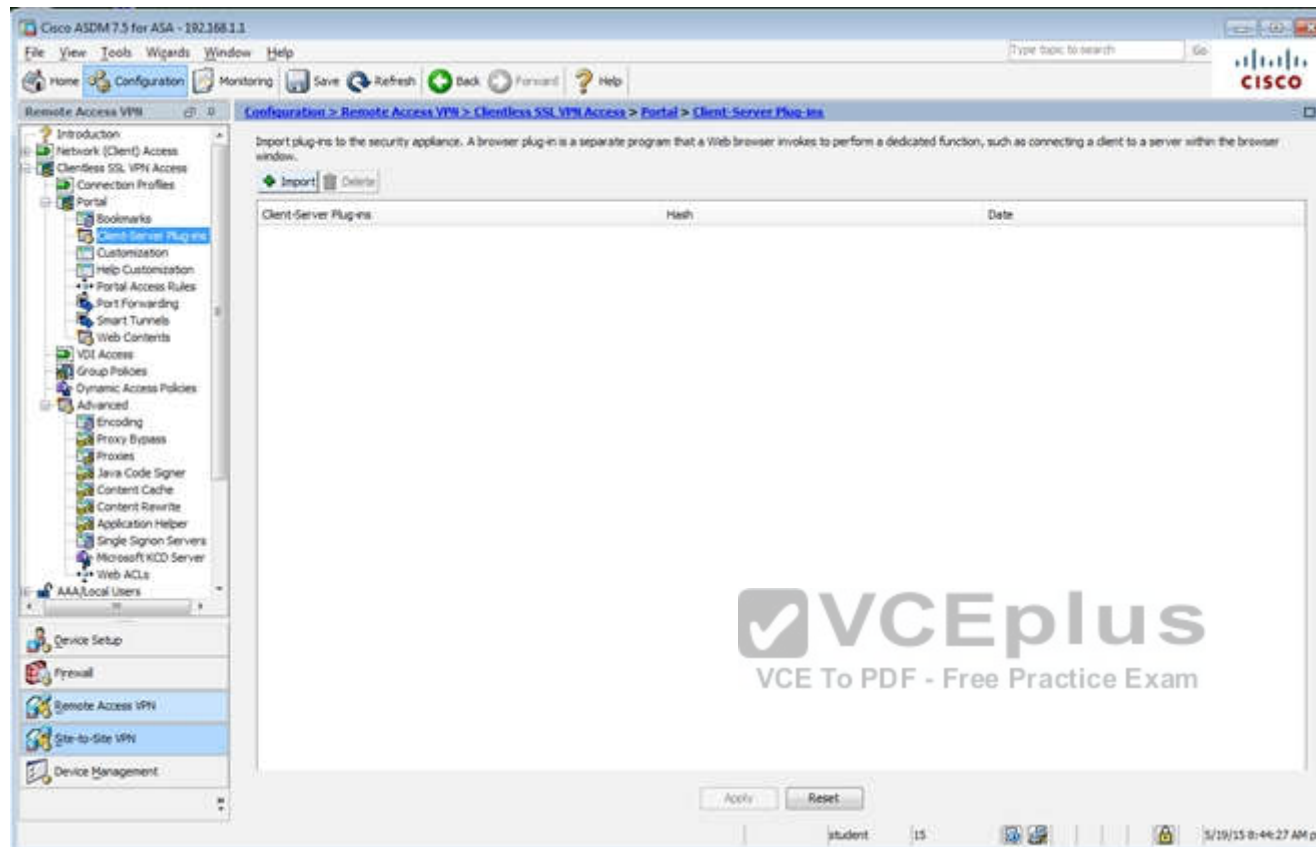
ActiveX Relay: ☒ Inherit ☐ Enable ☐ Disable

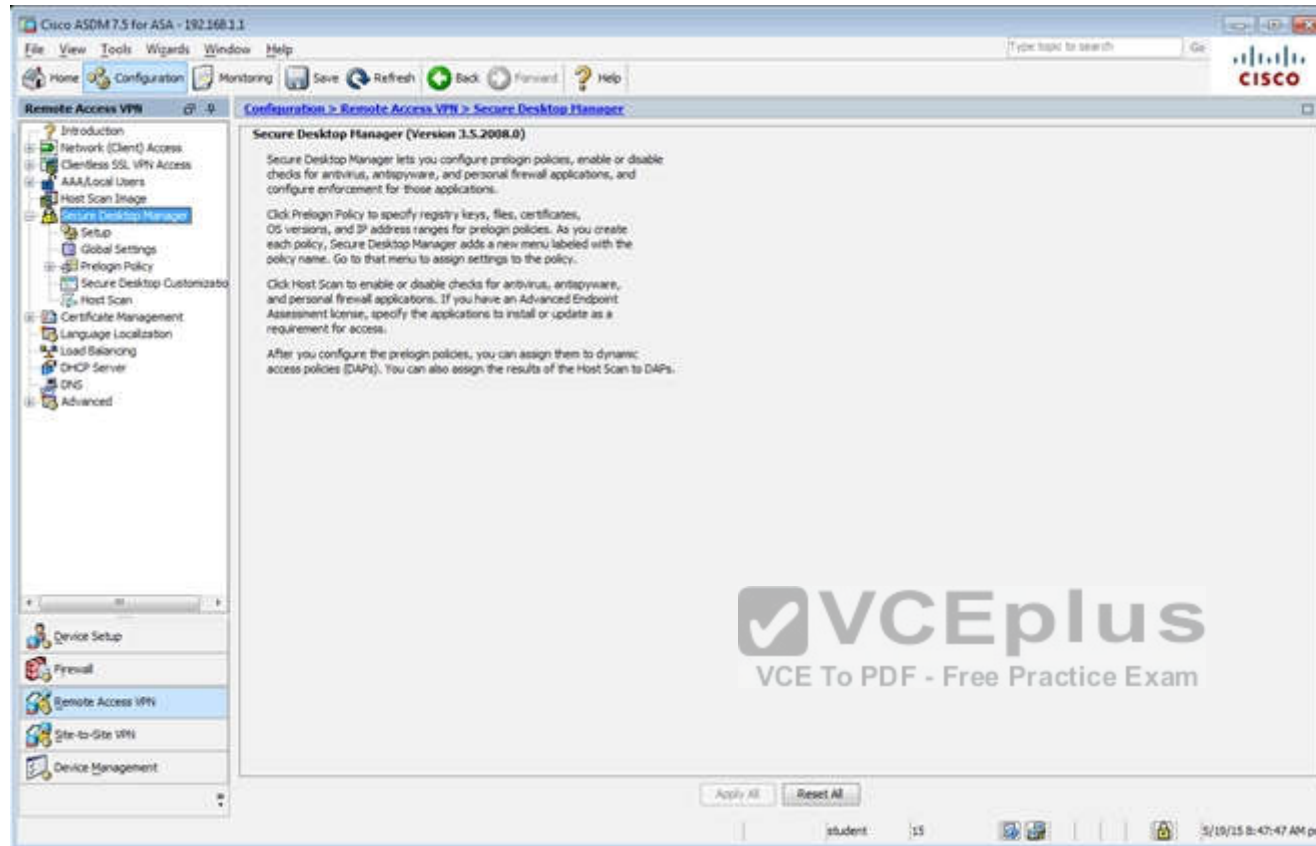
More Options

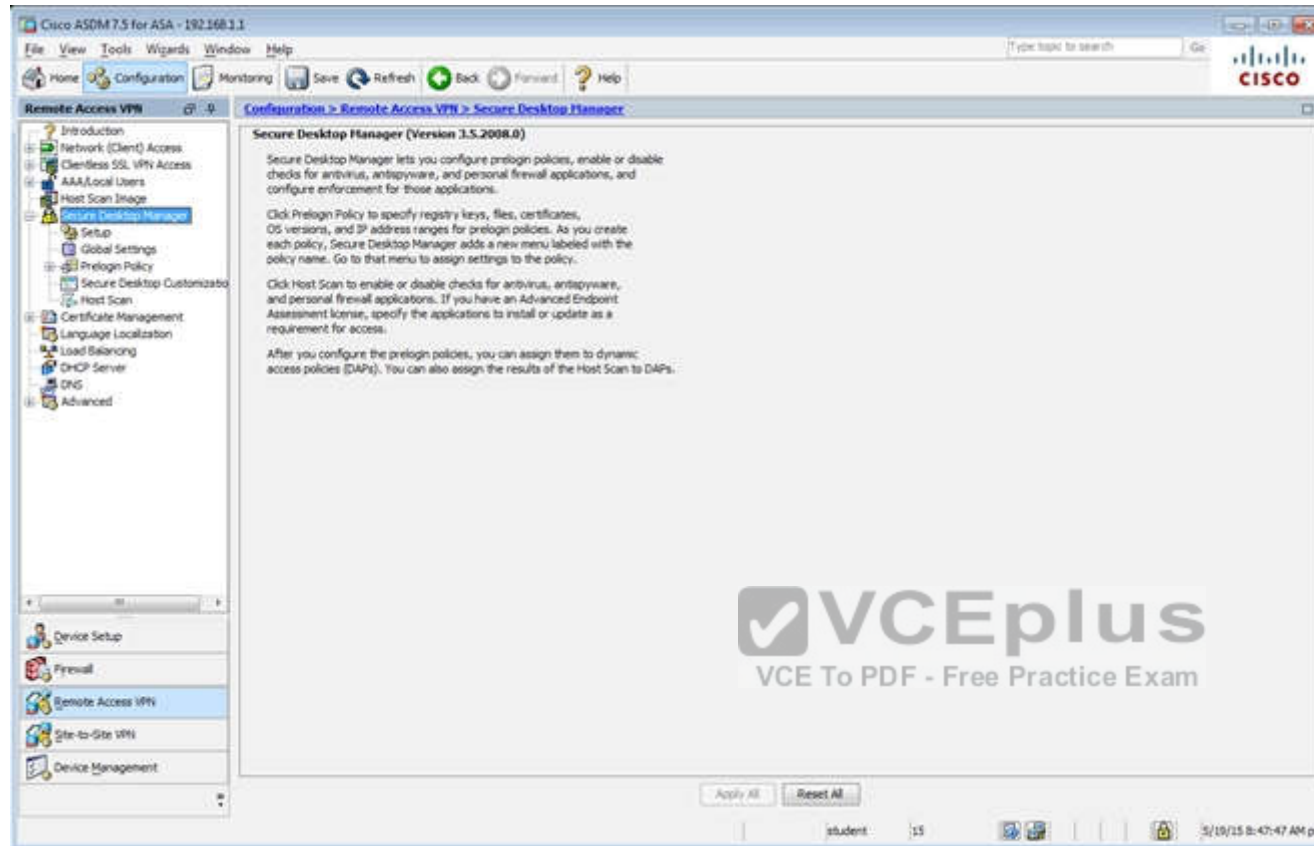
Find: Next Previous

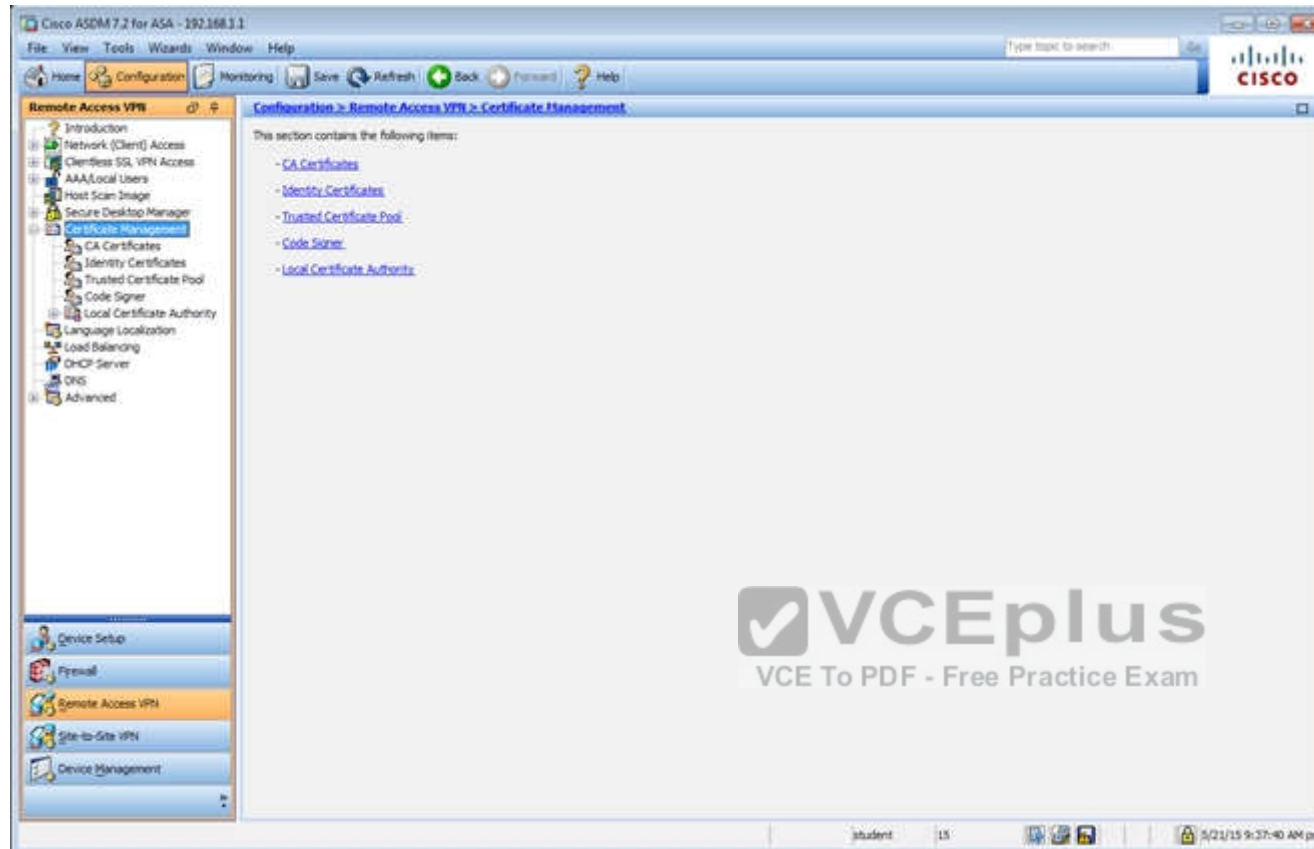
OK Cancel Help











Cisco ASDM 7.3 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Configuration > Remote Access VPN > Certificate Management > Identity Certificates

| Issued To | Issued By | Expiry Date | Associated Trustpoints | Usage | Public Key Type |
|----------------------------|----------------------------|----------------------------|------------------------|-----------------|-----------------|
| hostname-4P (17-ASA-sec... | hostname-4P (17-ASA-sec... | 11:59:33 pet 1 Dec 20 2024 | ASDM - Trustpoints | General Purpose | RSA 2048 bits |

Buttons: Add, Show Details, Delete, Export, Install

End: Match Case

Certificate Expiration Alerts

Send the first alert before: (days)

Repeat Alert Interval: (days)

Public CA Enrollment

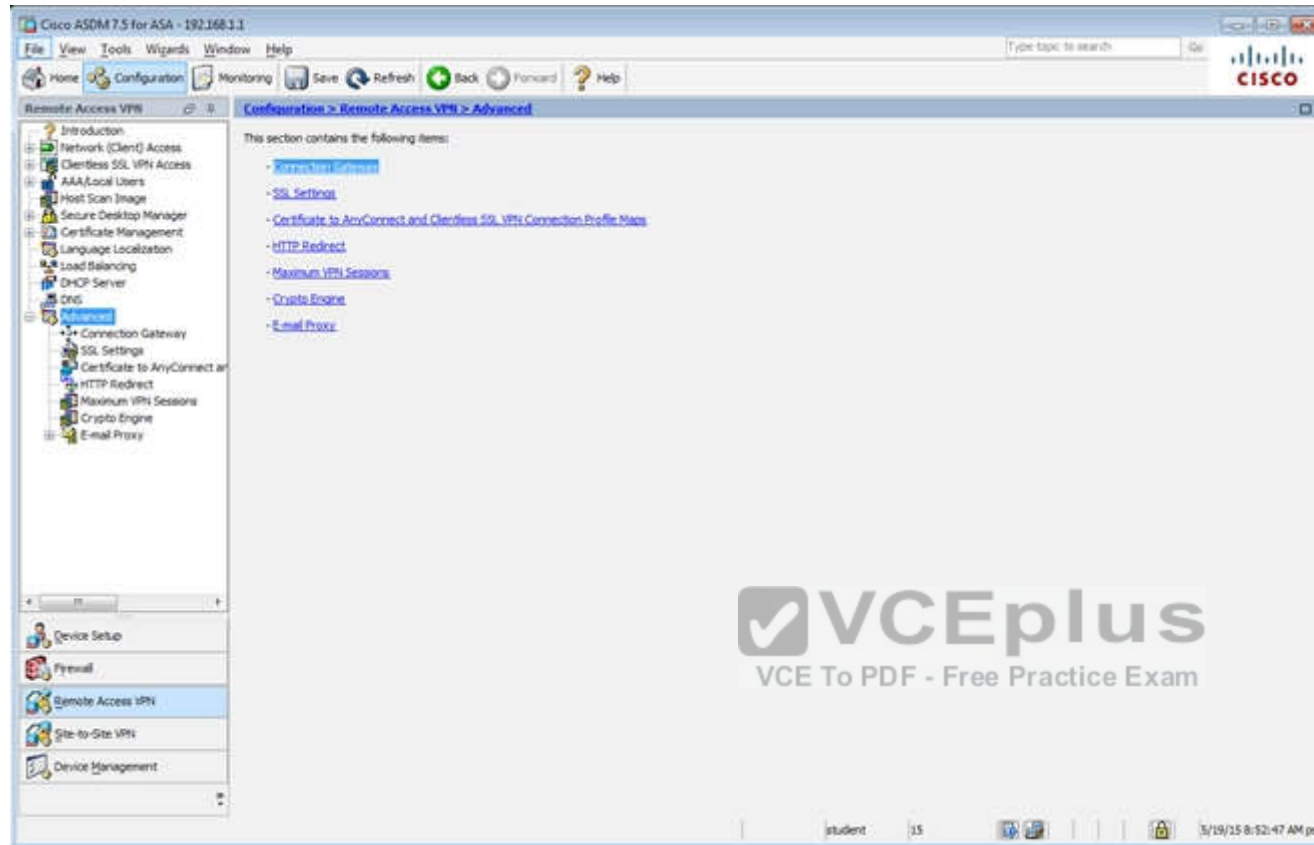
Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers Cisco customers a special promotional price for certificates and trial certificates for testing.

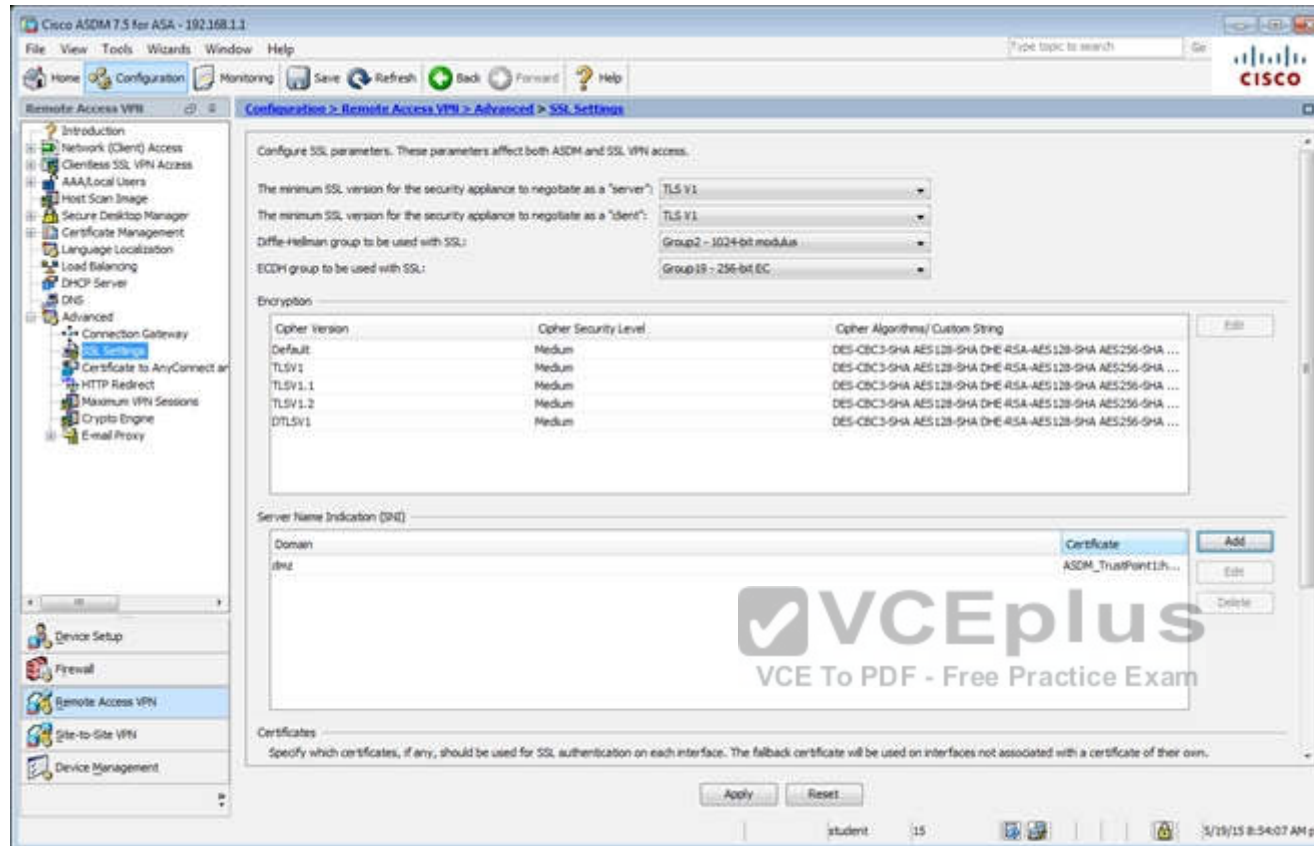
Using a previously saved certificate signing request, [enroll with Entrust](#).

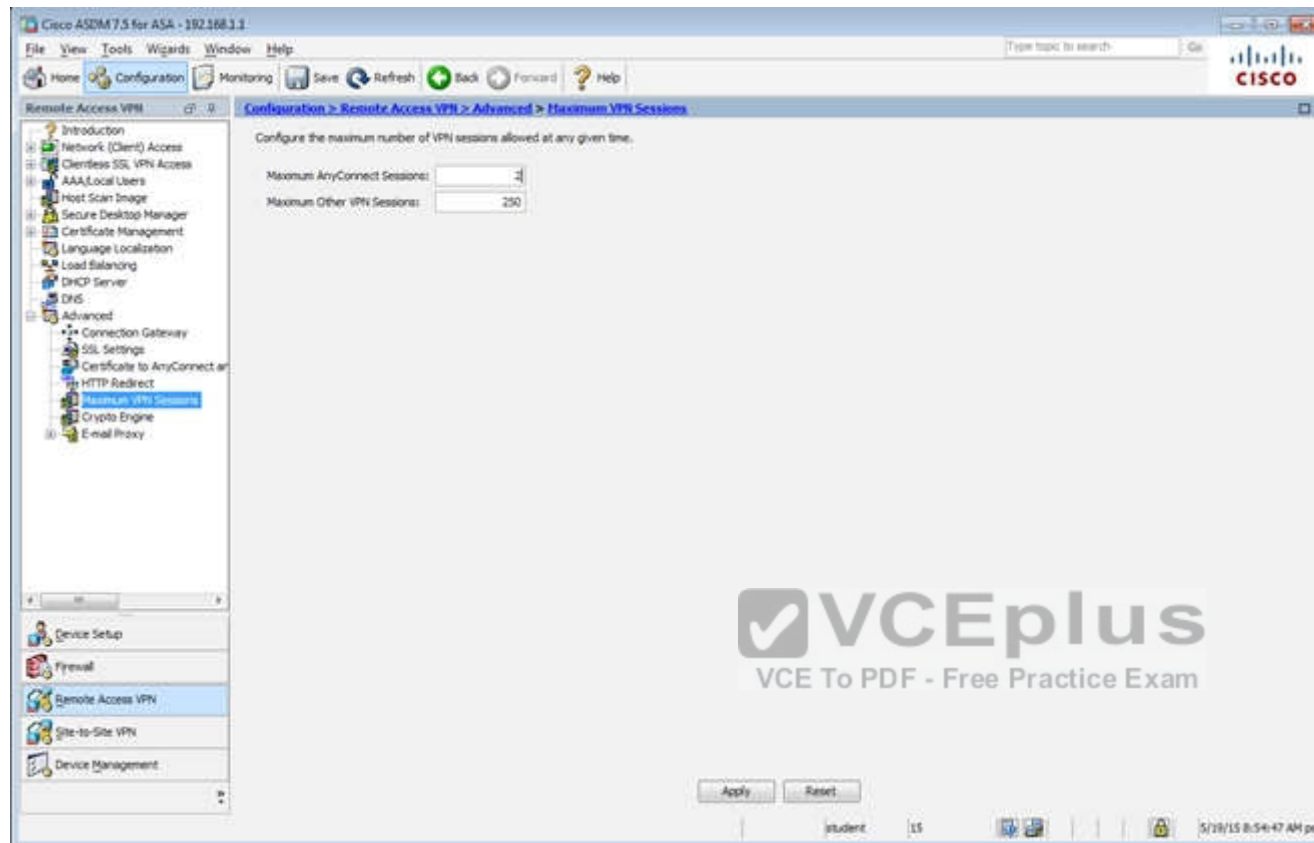
ASDM Identity Certificate Wizard

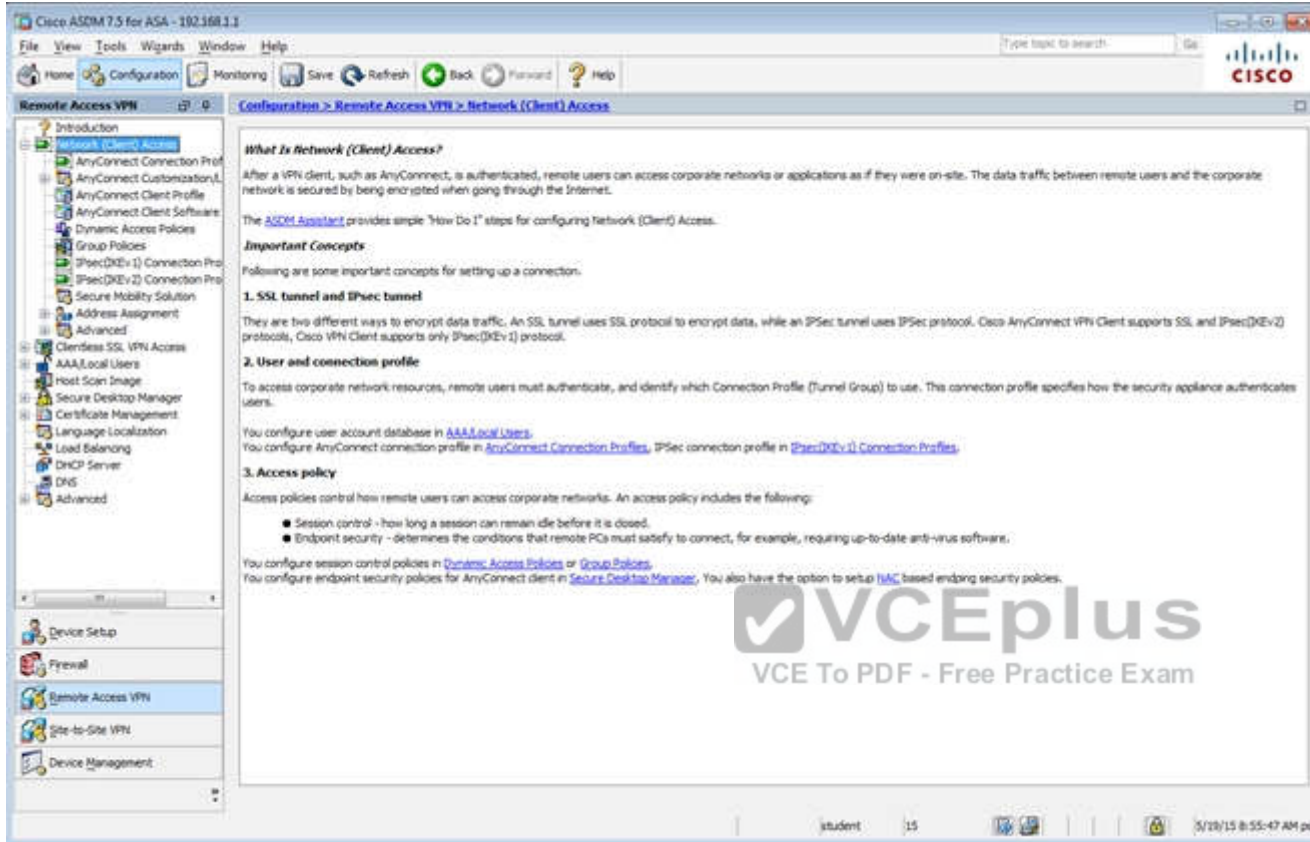
The Cisco ASDM Identity Certificate Wizard assists you in creating a self-signed certificate that is required for launching ASDM through launcher.

student 15 3/19/15 8:51:47 AM pet









Cisco ASDM 7.5 for ASA - 102.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Network (Client) Access

What Is Network (Client) Access?

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

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

Important Concepts

Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel

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

2. User and connection profile

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

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

3. Access policy

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

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

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

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

student 15 5/29/15 8:55:47 AM pct

The screenshot shows the Cisco ASDM 7.2 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Remote Access VPN' expanded, showing 'Network (Client) Access' and 'Group Policies'. The main pane shows the 'Group Policies' configuration page. It includes a description of VPN group policies and a table of existing policies.

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

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

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

Buttons: Add, Edit, Delete, Assign

| Name | Type | Tunneling Protocol | Connection Profiles/Users Assigned To |
|-----------------------------|----------|--|--|
| Sales | Internal | ssl-clientless | clientless |
| GroupPolicy: System Default | Internal | l2l3-clientless/ssl-clientless/zip-gwsec | DefaultGroupDefault, GroupDefaultWebVPNGroup |

Find: Match Case

Buttons: Apply, Reset

Taskbar: student 15 3/21/15 10:17:10 AM pet

Edit Internal Group Policy: DiffGrpPolicy

Settings

- Servers
- Advanced
 - Split Tunneling
 - Browser Proxy
 - AnyConnect Client
 - IPsec (IKEv1) Client

Name: DiffGrpPolicy

Banner:

SCDP forwarding URL:

Address Pools: Select...

IPv6 Address Pools: Select...

Home Options

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

Filter: -- None -- Manage...

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

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

Simultaneous Logins: 3

Restrict access to VLAN: -- Unrestricted --

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

Maximum Connect Time: ☒ Unlimited ☐ minutes

Idle Timeout: ☐ None ☐ 30 minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

VCEplus
VCE To PDF - Free Practice Exam

Find: Next Previous

OK Cancel Help

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction
Network (Client) Access
AnyConnect Connection Profile
AnyConnect Customization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec (IKEv1) Connection Profile
IPsec (IKEv2) Connection Profile
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced

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

Access Interfaces
Enable interfaces for IPsec access.

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

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

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

+ Add Edit Delete

| Name | IPsec Enabled | L2TP/IPsec Enabled | Authentication Server Group | Group Policy |
|--------------------|-------------------------------------|-------------------------------------|-----------------------------|---------------|
| DefaultRAGroup | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD | DiffGrpPolicy |
| DefaultWEBVPNGroup | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD | DiffGrpPolicy |
| Services | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | LOCAL | Local |

End: Match Case

Apply Reset

student 15 5/18/15 8:56:47 AM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec (IKEv2) 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

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

Access Interfaces

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

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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

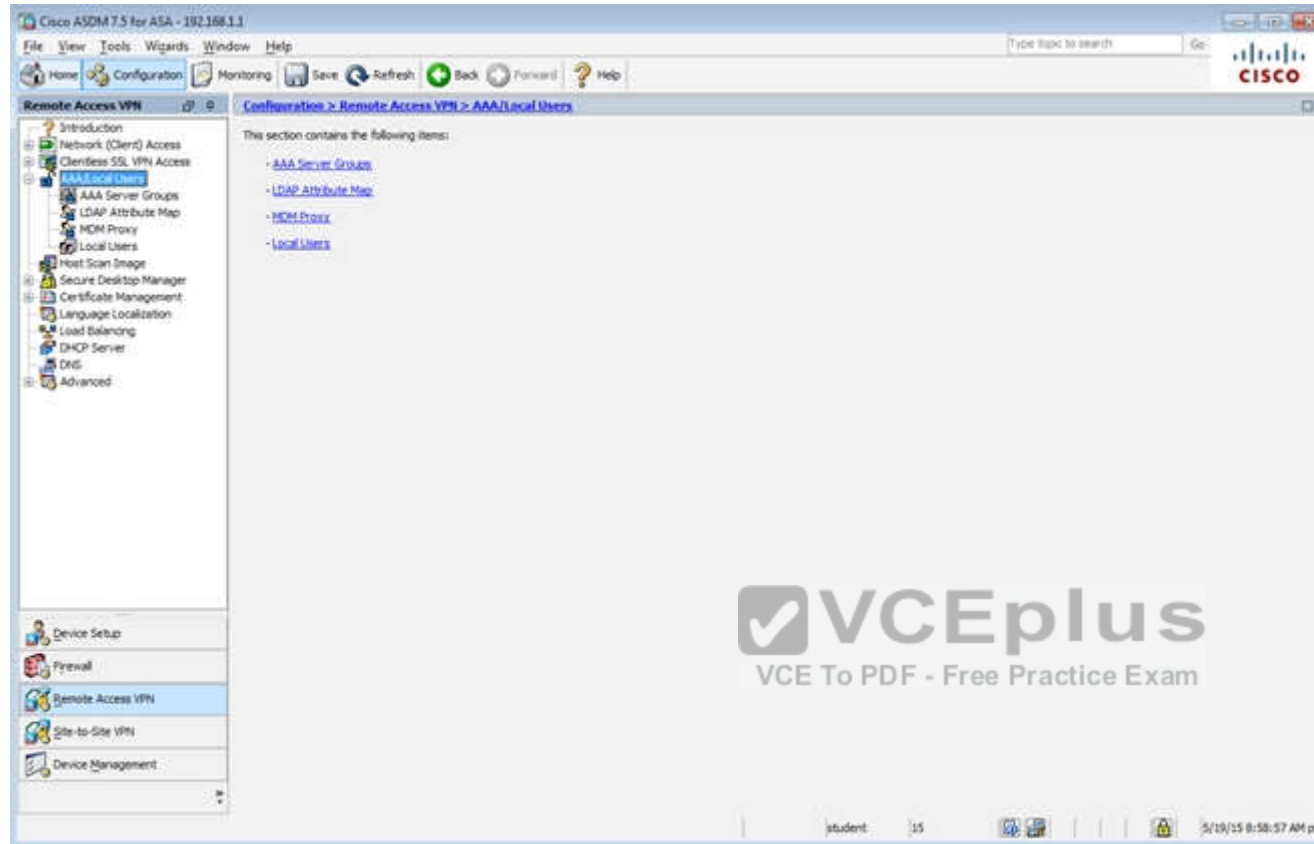
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Find:

| Name | SSL Enabled | IPsec Enabled | Authentication Method | Group Policy |
|--------------------|-------------------------------------|-------------------------------------|-----------------------|--------------------|
| DefaultRAGroup | <input type="checkbox"/> | <input type="checkbox"/> | AAA(RADIUS) | DefaultGroupPolicy |
| DefaultTNSVPNGroup | <input type="checkbox"/> | <input checked="" type="checkbox"/> | AAA(RADIUS) | DefaultGroupPolicy |
| Clientless | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | AAA(SSL-VPN) | DefaultGroupPolicy |

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

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
MDM Proxy
Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DnCP Server
DNS
Advanced

Create entries in the ASA local user database.

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

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

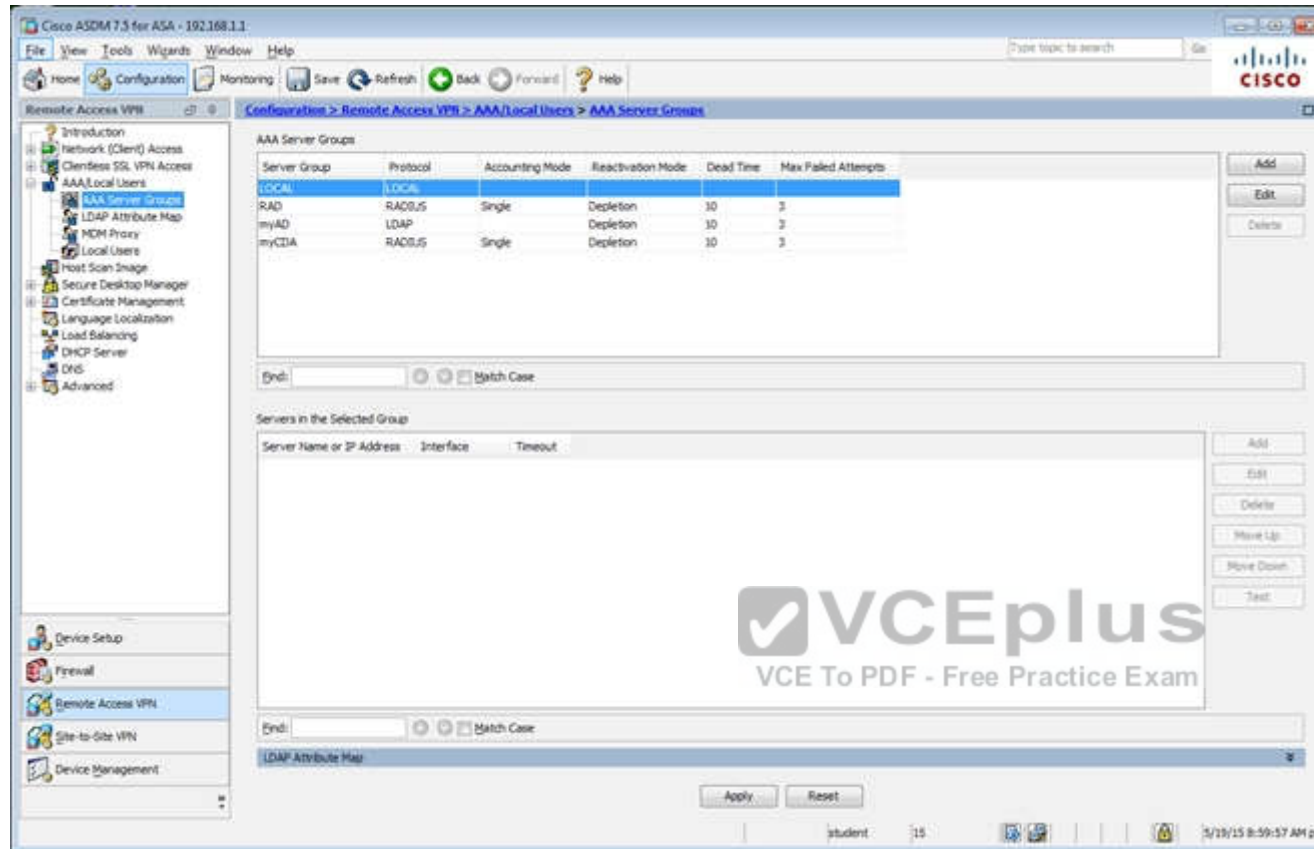
| Username | Privilege Level (Role) | Access Restrictions | VPN Group Policy | VPN Group Lock |
|-----------|------------------------|---------------------|----------------------------|----------------------------|
| student | 15 | Full | -- Inherit Group Policy -- | -- Inherit Group Policy -- |
| enable_15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

Add Edit Delete

End: Match Case

Apply Reset

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



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

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

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:
For B:



Virtual Terminal

- 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

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


Device Certificate ...

Port Setting ...

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

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

☐ Shutdown portal login page.

Connection Profiles

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

 Add  Edit  Delete Find:   ☐ Match Case

| Name | Enabled | Aliases | Authentication Method |
|--------------------|-------------------------------------|---------|-----------------------|
| DefaultRAGroup | <input checked="" type="checkbox"/> | | AAA(RAD) |
| DefaultWEBVPGGroup | <input checked="" type="checkbox"/> | | AAA(RAD) |
| clientless | <input checked="" type="checkbox"/> | test | AAA(LOCAL) |

For C, Navigate to the Bookmarks tab:

Virtual Terminal

Remote Access VPN

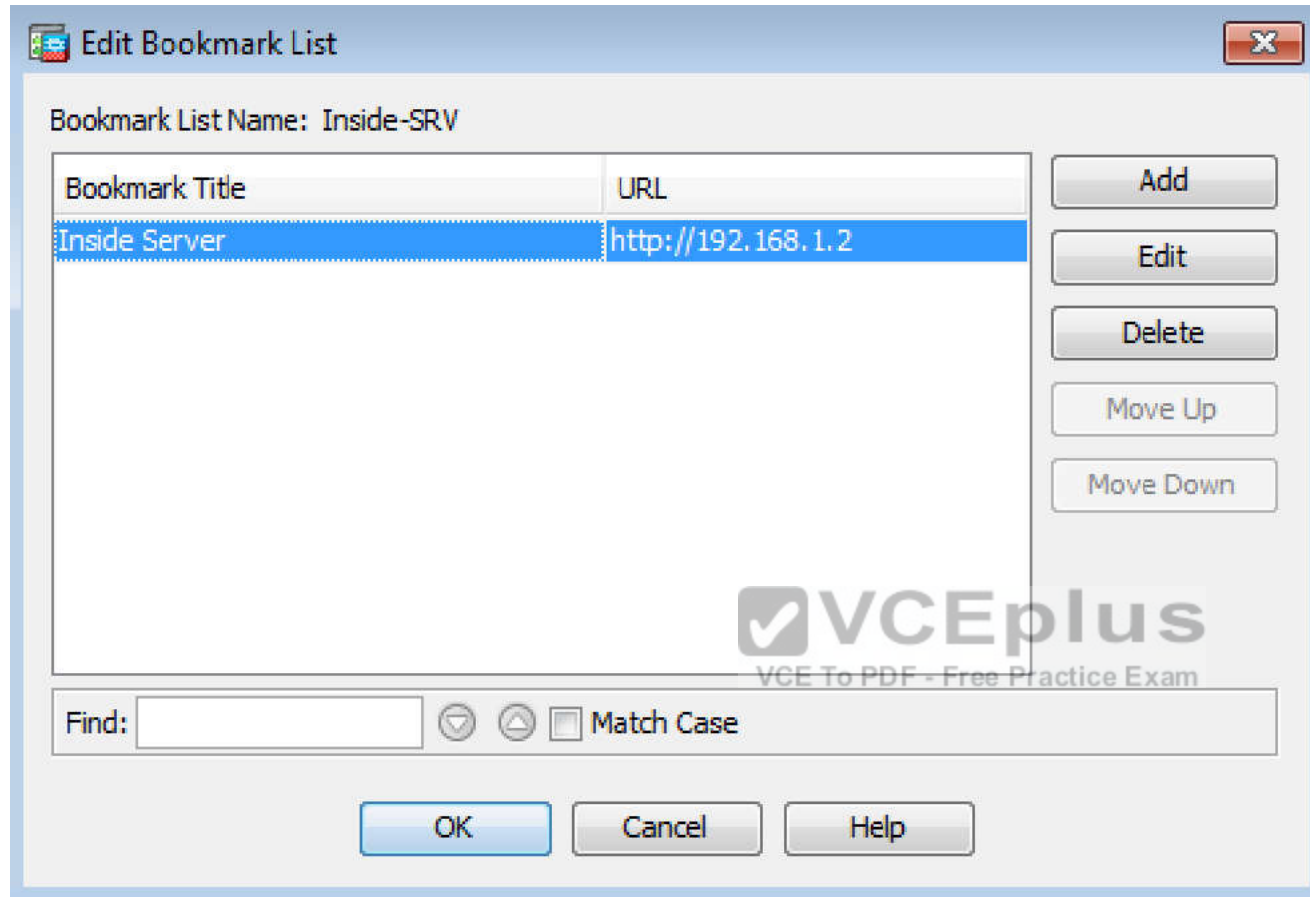
Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks

Configure Bookmark Lists that the security appliance displays on the SSL VPN portal page.
This parameter is enforced in either a [VPN group policy](#), a [dynamic access policy](#), or a [user](#).

[+ Add](#)
[✎ Edit](#)
[🗑 Delete](#)
[+ Import](#)
[✎ Export](#)
[🔗 Assign](#)

| Bookmarks | Group Policy |
|------------|--------------|
| Template | |
| Inside-SRV | Sales |

Then hit "edit" and you will see this:



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

Virtual Terminal

Remote Access VPN

- 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

Configuration > Remote Access VPN > Certificate Management > Identity Certificates

| Issued To | Issued By | Expiry Date | Associated Trustpoints | U |
|-------------------------|-------------------------|--------------------------|------------------------|---|
| hostname=P17-ASA.sec... | hostname=P17-ASA.sec... | 11:10:33 pst Dec 20 2024 | ASDM_TrustPoint1 | |



Find: ☐ Match Case

Certificate Expiration Alerts

Send the first alert before : (days)

Repeat Alert Interval : (days)

Public CA Enrollment

Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers certificates for testing.

Note E:



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View **Tools** Wizards Window Help

Home **Configuration** Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

- Introduction
- Network (Client) Access
 - AnyConnect Connection Prof**
 - AnyConnect Customization/L
 - AnyConnect Client Profile
 - AnyConnect Client Software
 - Dynamic Access Policies
 - Group Policies
 - IPsec(IKEv1) Connection Pro
 - IPsec(IKEv2) Connection Pro
 - Secure Mobility Solution
 - Address Assignment
 - Advanced
- Clientless SSL VPN Access
- AAA/Local Users
- Host Scan Image
- Secure Desktop Manager
- Certificate Management
- Language Localization
- Load Balancing
- DHCP Server
- DNS
- Advanced

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

Access Interfaces

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


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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

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

 Add  Edit  Delete Find:   ☐ Match Case

QUESTION 67**Scenario**

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

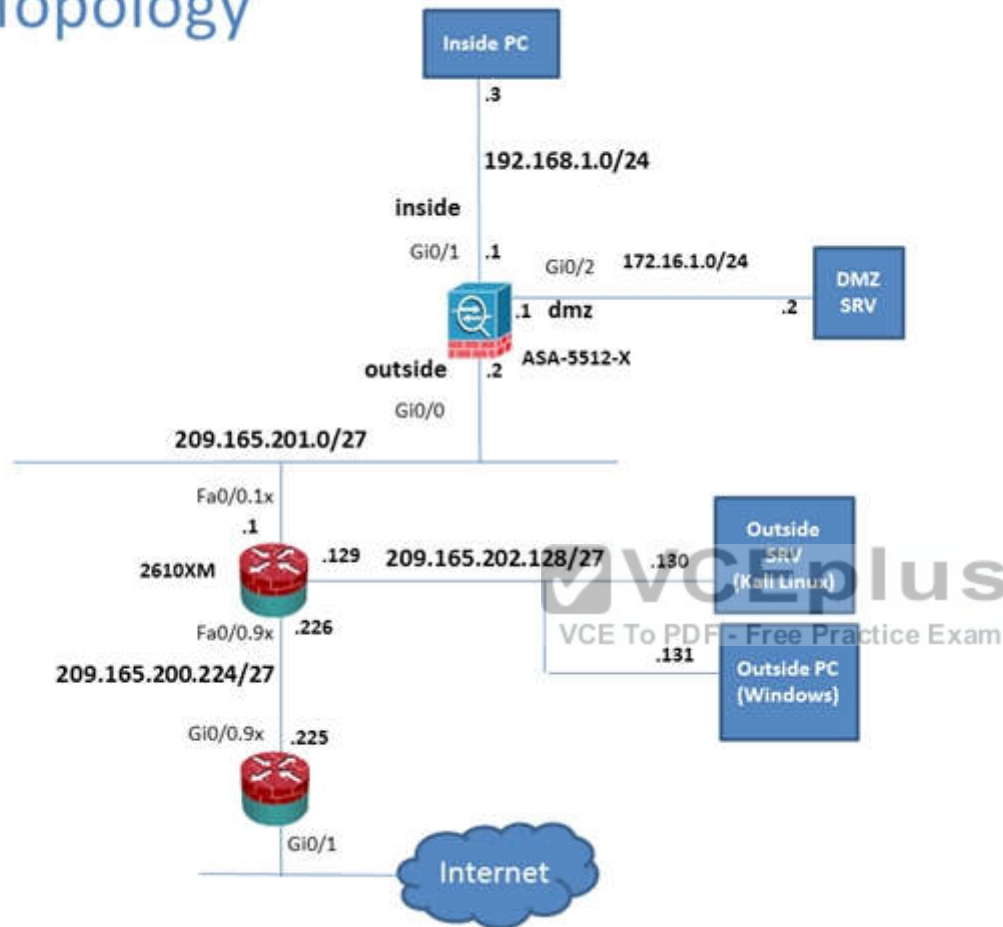
To access ASDM, click the ASA icon in the topology diagram.

Note: Not all ASDM functionalities are enabled in this simulation.

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



Lab Topology



Cisco ASDM 7.5 for ASA - 192.168.1.3

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Home

Device Dashboard Firewall Dashboard ASA PrePOWER Status

Device Information

General License

Host Name: **P17-ASA.secure-x.local**
 ASA Version: **100.14(6)13**
 ASDM Version: **7.5(1)1**
 Firewall Mode: **Routed**
 Environment Status: **OK**

Device Uptime: **11d 21h 42m 47s**
 Device Type: **ASA 5512**
 Context Mode: **Single**
 Total Flash: **4096 MB**

Interface Status

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

Select an interface to view input and output Kbps

VPN Sessions

IPsec: 0 Clientless SSL VPN: AnyConnect Client: 0 [Details](#)

Failover Status

Failover not configured. Click the link to configure it. [Configure](#)

System Resources Status

Total Memory Usage Total CPU Usage Core Usage [Details](#)

Memory Usage (MB)

Traffic Status

Connections Per Second Usage

UDP: 0 TCP: 0 Total: 0

'outside' Interface Traffic Usage (Kbps)

Input Kbps: 0 Output Kbps: 0

Latest ASDM Syslog Messages

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

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces c2 9 Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

| Interface | IP Address | MAC Address | Proxy Arp |
|-----------|---------------|----------------|-----------|
| outside | 209.165.201.1 | 000c.3014.3820 | No |
| inside | 192.168.1.4 | 0050.5633.3333 | No |
| inside | 192.168.1.3 | 0050.5611.1111 | No |
| inside | 192.168.1.2 | 0050.5622.2222 | No |
| inside | 192.168.1.56 | 0050.5692.5c7b | No |
| inside | 192.168.1.55 | 0006.80e6.90f3 | No |
| dmz | 172.16.1.2 | 0050.5644.4444 | No |
| mgmt | 10.10.10.1 | 000c.3014.3820 | No |

Clear Dynamic ARP Entries

Refresh

Data Refreshed Successfully.

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

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

VPN

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

Interfaces
VPN
Gigabit Traffic Filter
Routing
Properties
Logging

Monitoring > VPN > VPN Statistics > Sessions

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

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

| Username | IP Address | Group Policy | Connection Profile | Protocol | Encryption | Login Time | Duration | Bytes Tx | Bytes Rx |
|----------|-----------------|--------------|--------------------|---------------------|---------------------|------------------------------|----------|----------|----------|
| student | 209.165.202.131 | Sales | Clientless | Clientless: TLS/SSL | Clientless: TLS/SSL | 08:05:46 Sat Thu May 21 2013 | 00:00:10 | 216774 | 41633 |

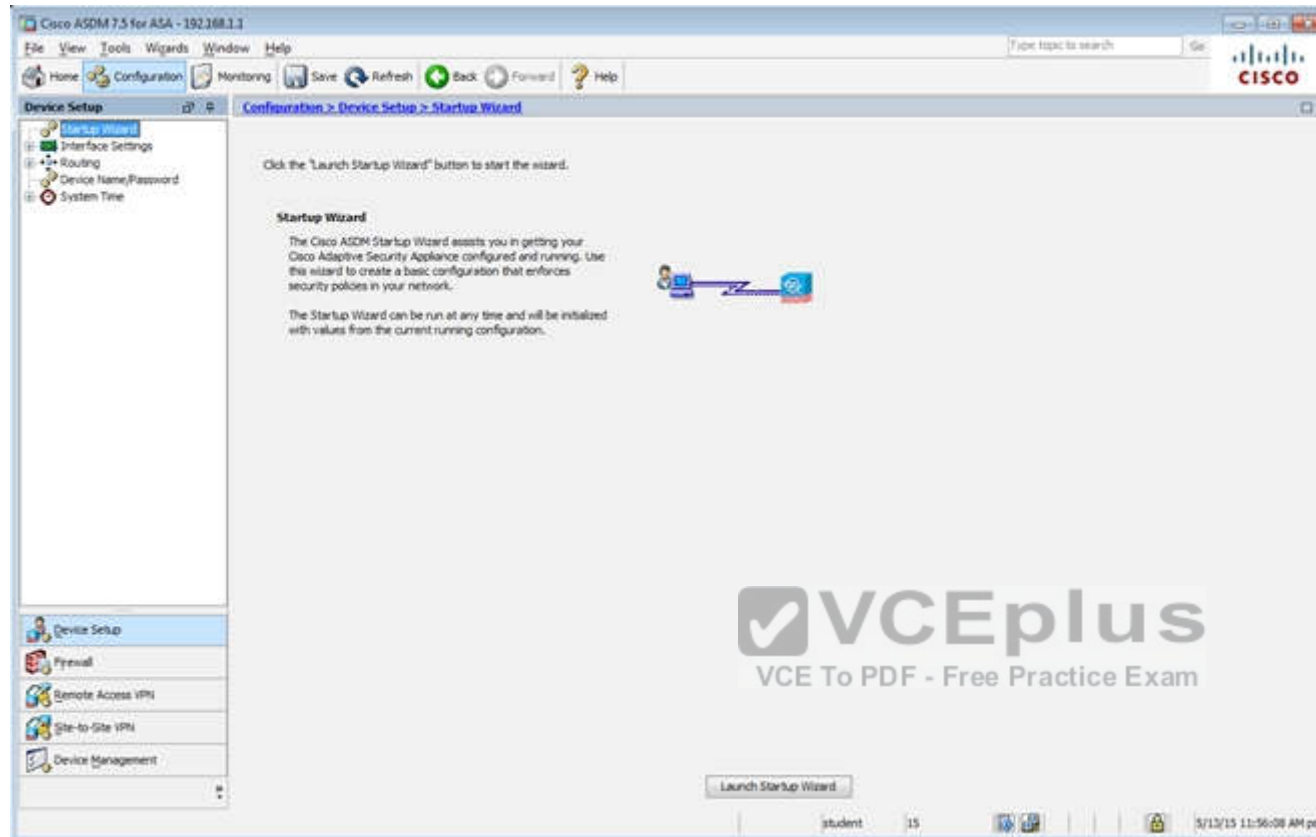
Details
Logout
Ping

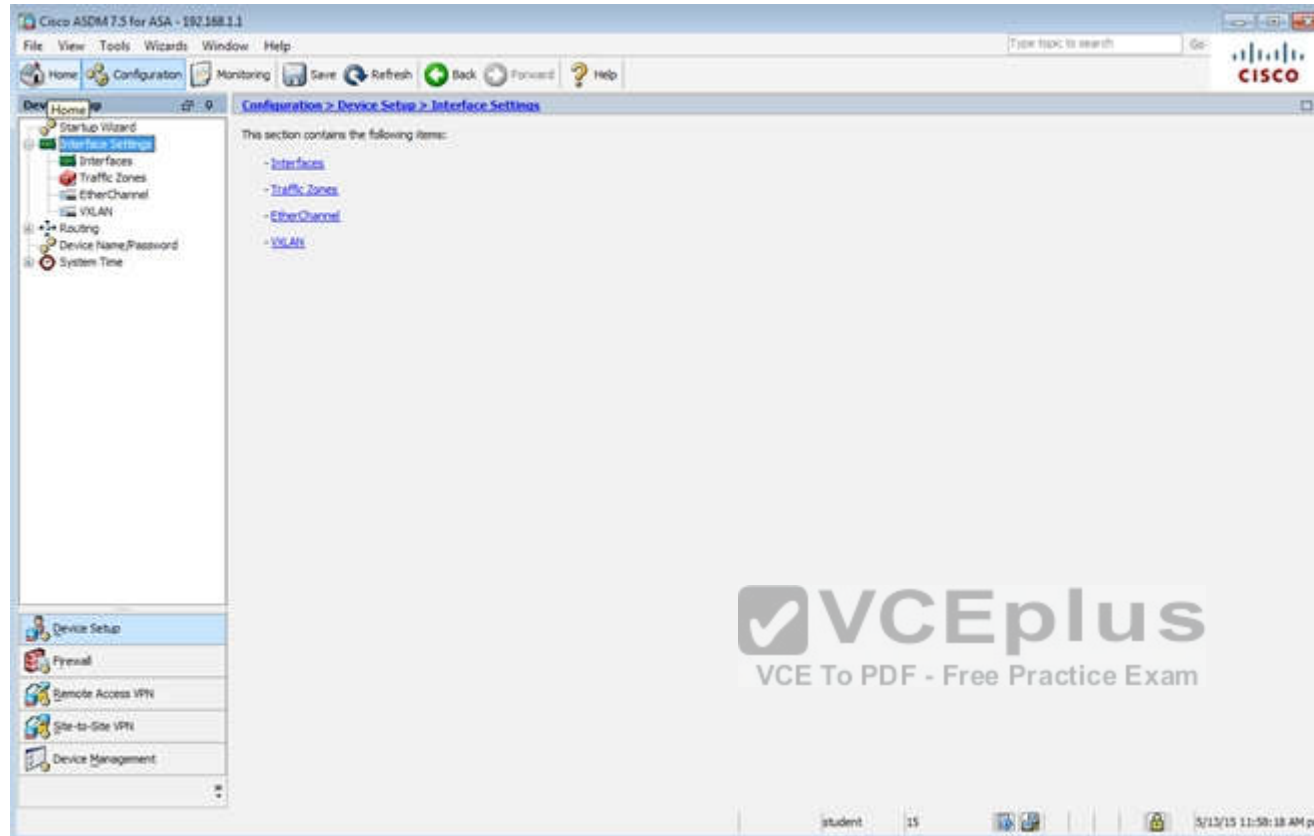
Refresh

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

Data Refreshed Successfully.

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





Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device Setup

Configuration > Device Setup > Interface Settings > Interfaces

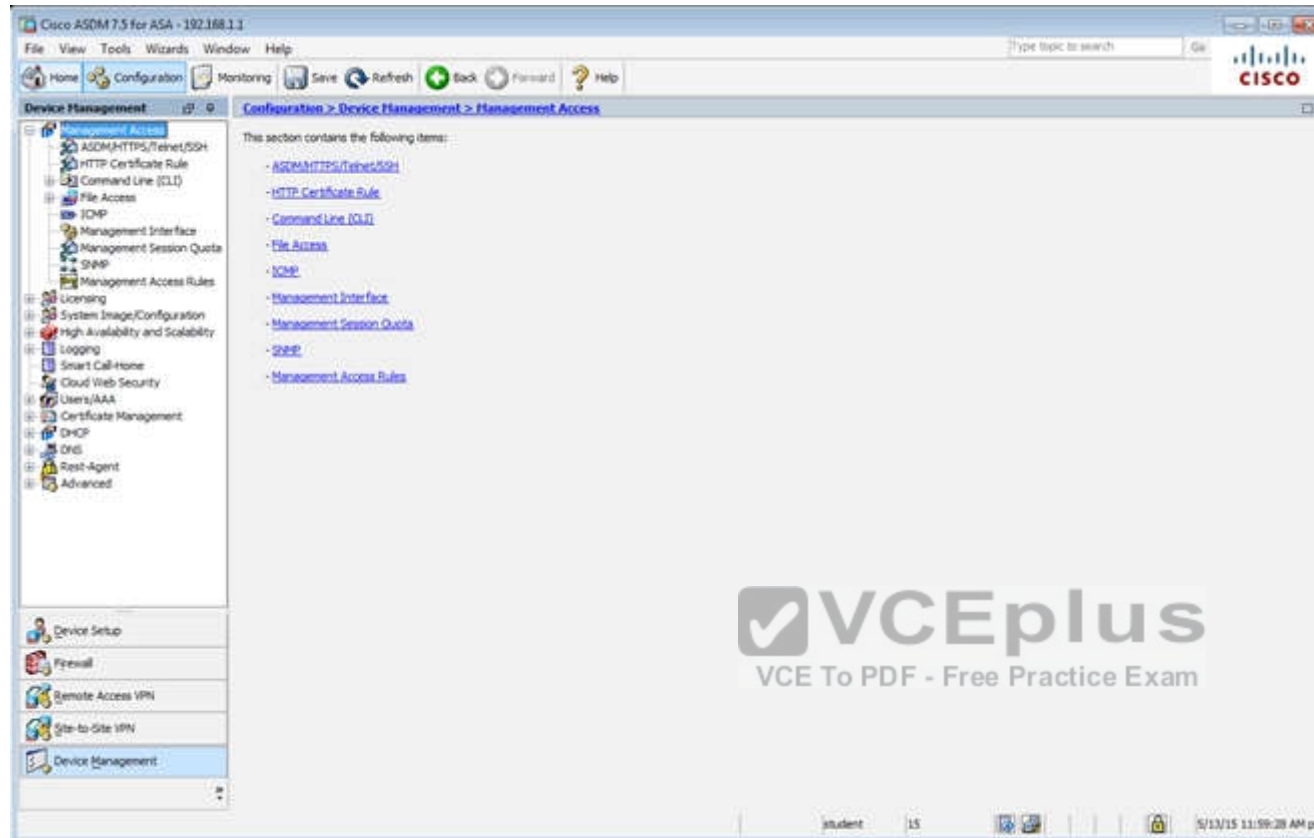
Startup Wizard
Interface Settings
Traffic Zones
EtherChannel
VLANs
Routing
Device Name/Password
System Time

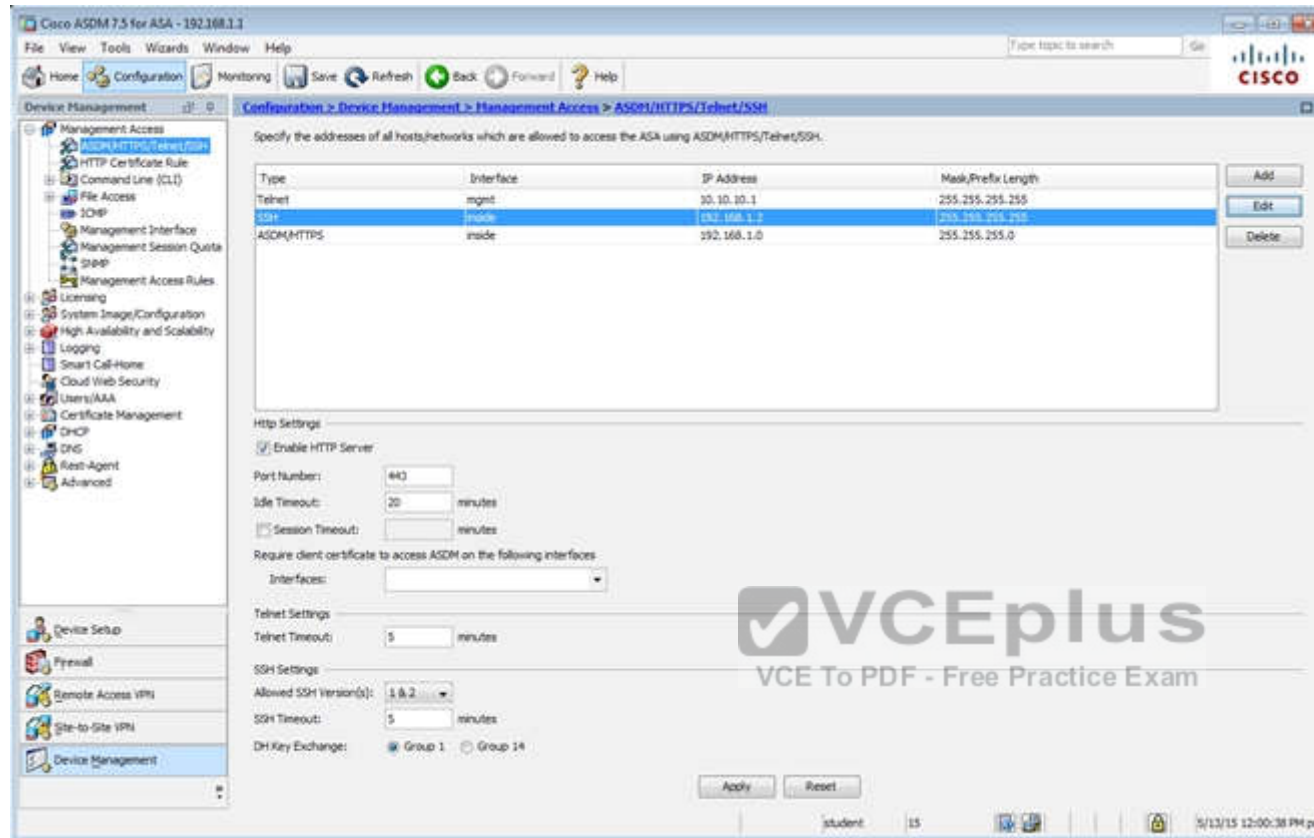
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management

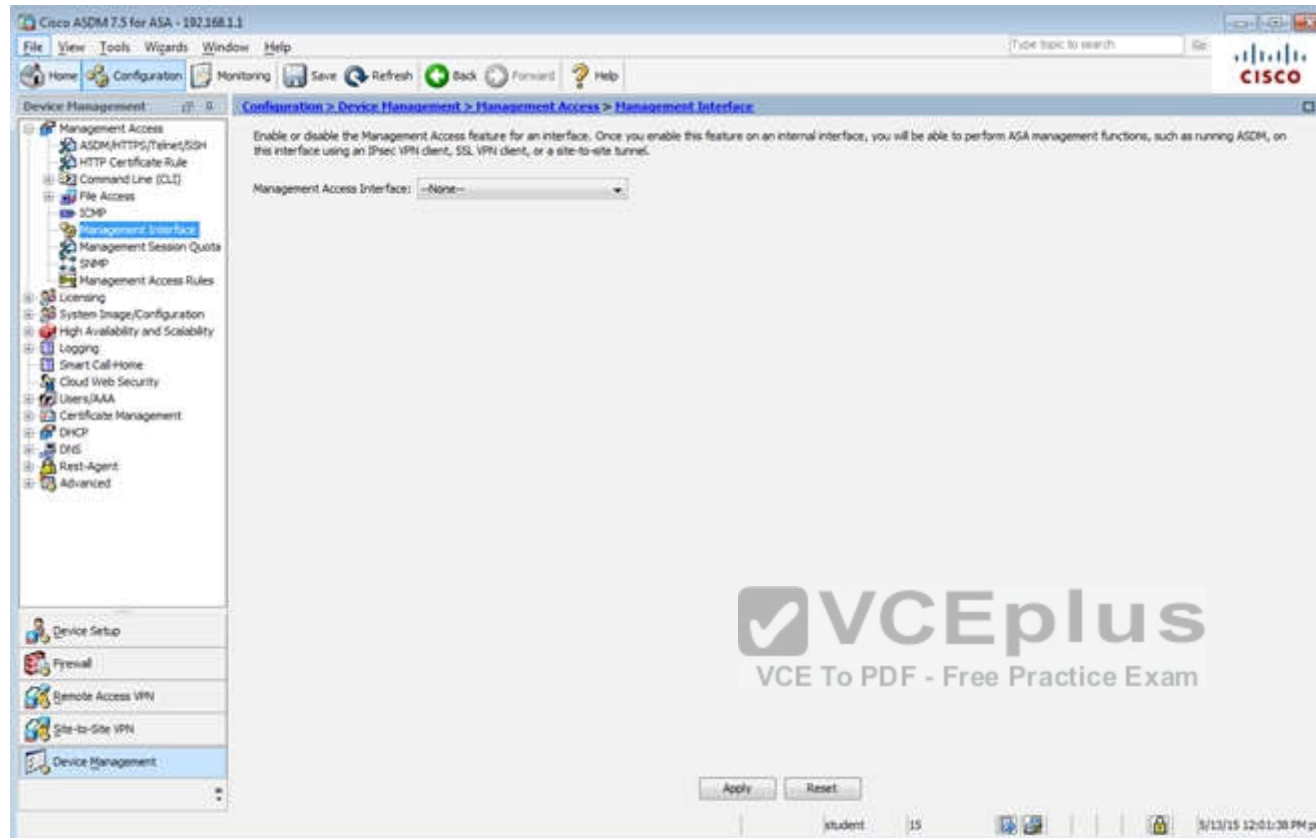
| Interface | Name | Zone | Route Map | State | Security Level | IP Address | Subnet Mask Prefix Length | Group | Type |
|--------------------|---------|------|-----------|---------|----------------|-----------------|---------------------------|-------|----------|
| GigabitEthernet0/0 | outside | | | Enabled | | 0.0.0.0/0.0.0.0 | 255.255.255.0 | | Hardware |
| GigabitEthernet0/1 | inside | | | Enabled | | 100.292.168.1.1 | 255.255.255.0 | | Hardware |
| GigabitEthernet0/2 | dmz | | | Enabled | | 172.16.1.1 | 255.255.255.0 | | Hardware |
| GigabitEthernet0/3 | | | | Enabled | | | | | Hardware |
| GigabitEthernet0/4 | | | | Enabled | | | | | Hardware |
| GigabitEthernet0/5 | mgmt | | | Enabled | | 100.10.10.10.2 | 255.255.255.0 | | Hardware |
| Management0/0 | | | | Enabled | | | | | Hardware |

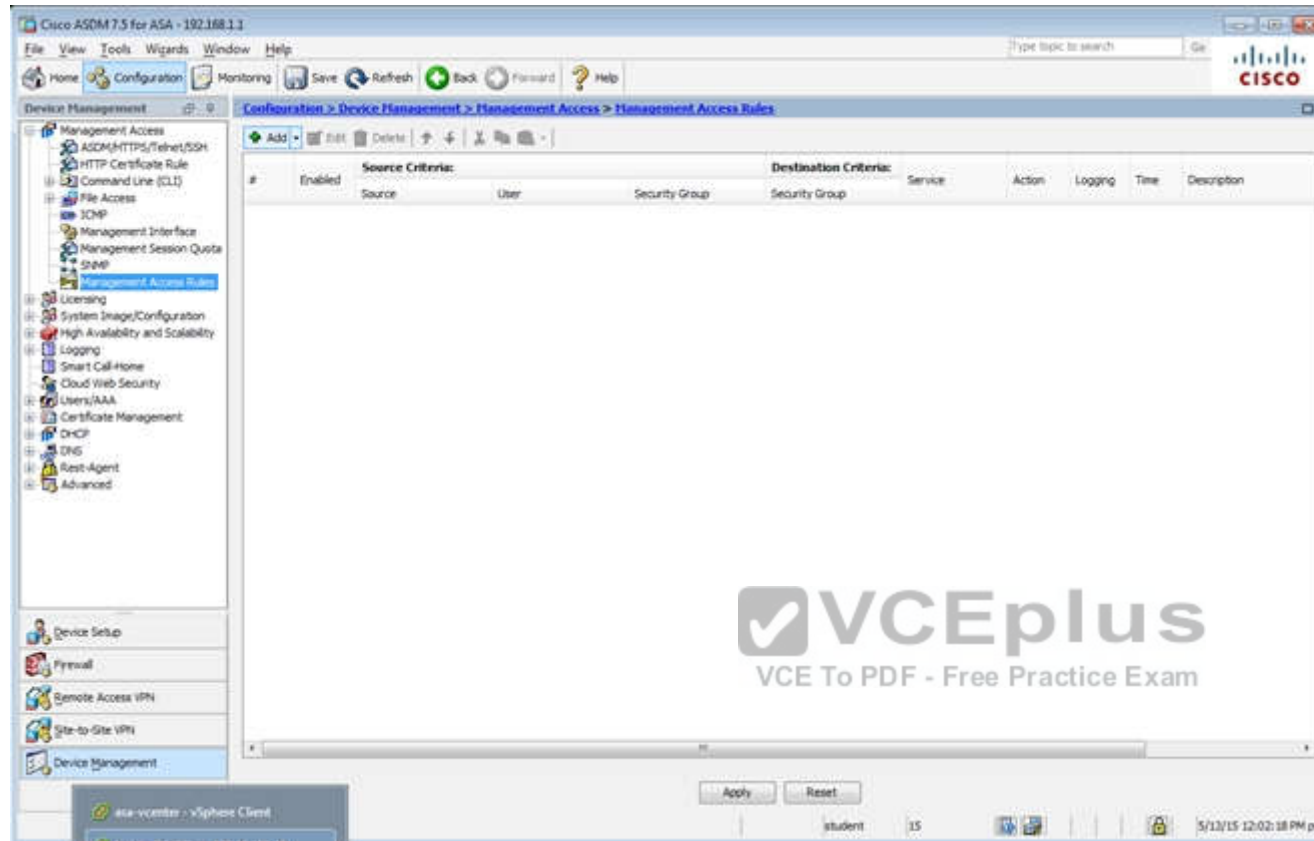
☐ Enable traffic between two or more interfaces which are configured with same security levels
☐ Enable traffic between two or more hosts connected to the same interface
☐ Enable jumbo frame reservation

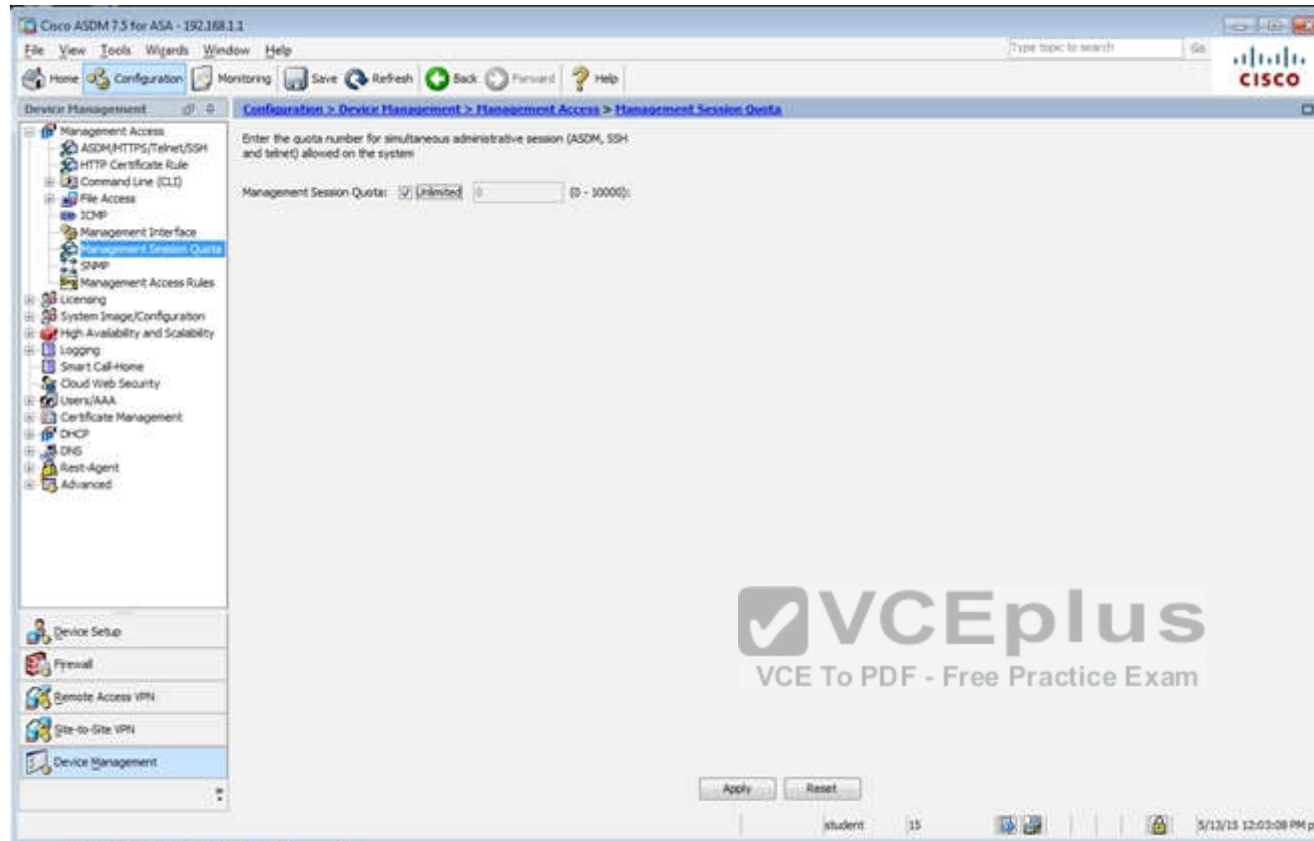
student 15 5/13/15 12:42:48 PM pst

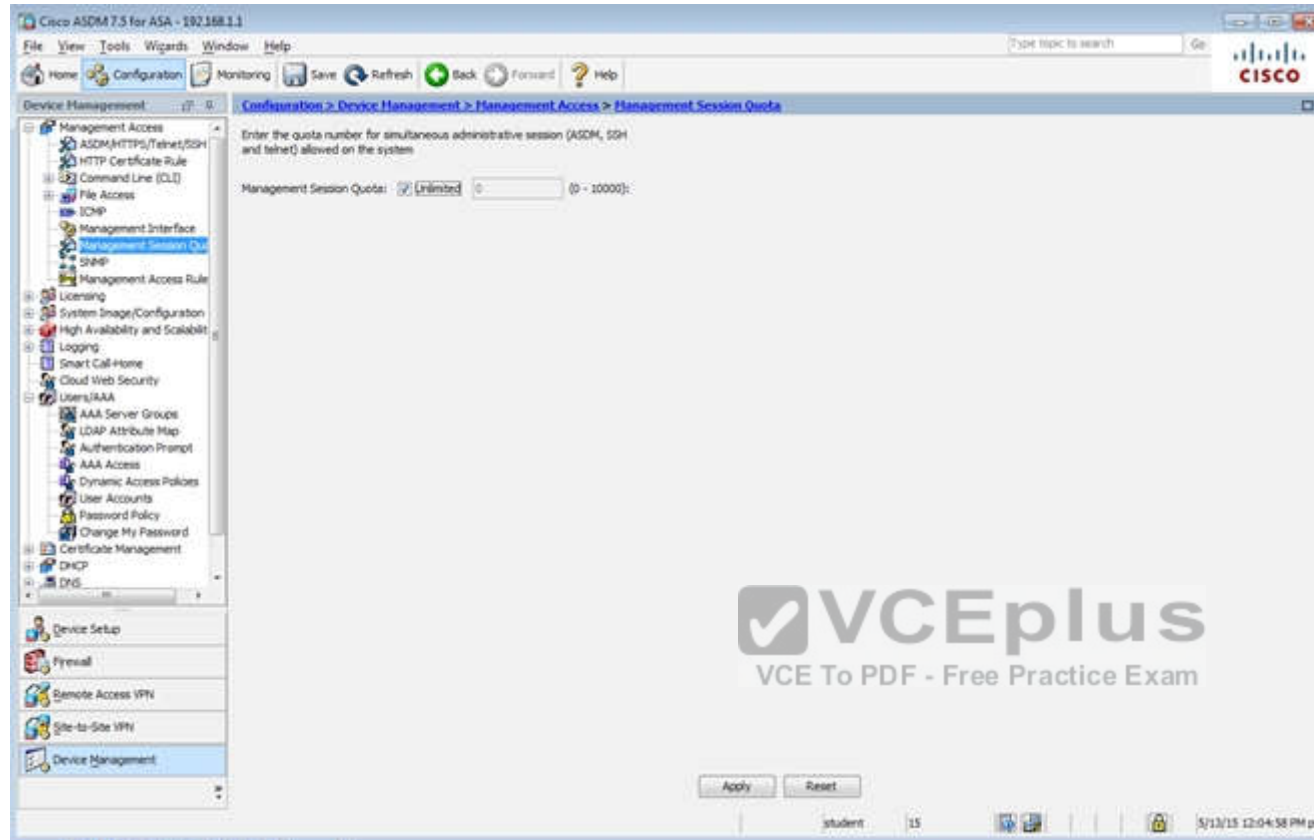


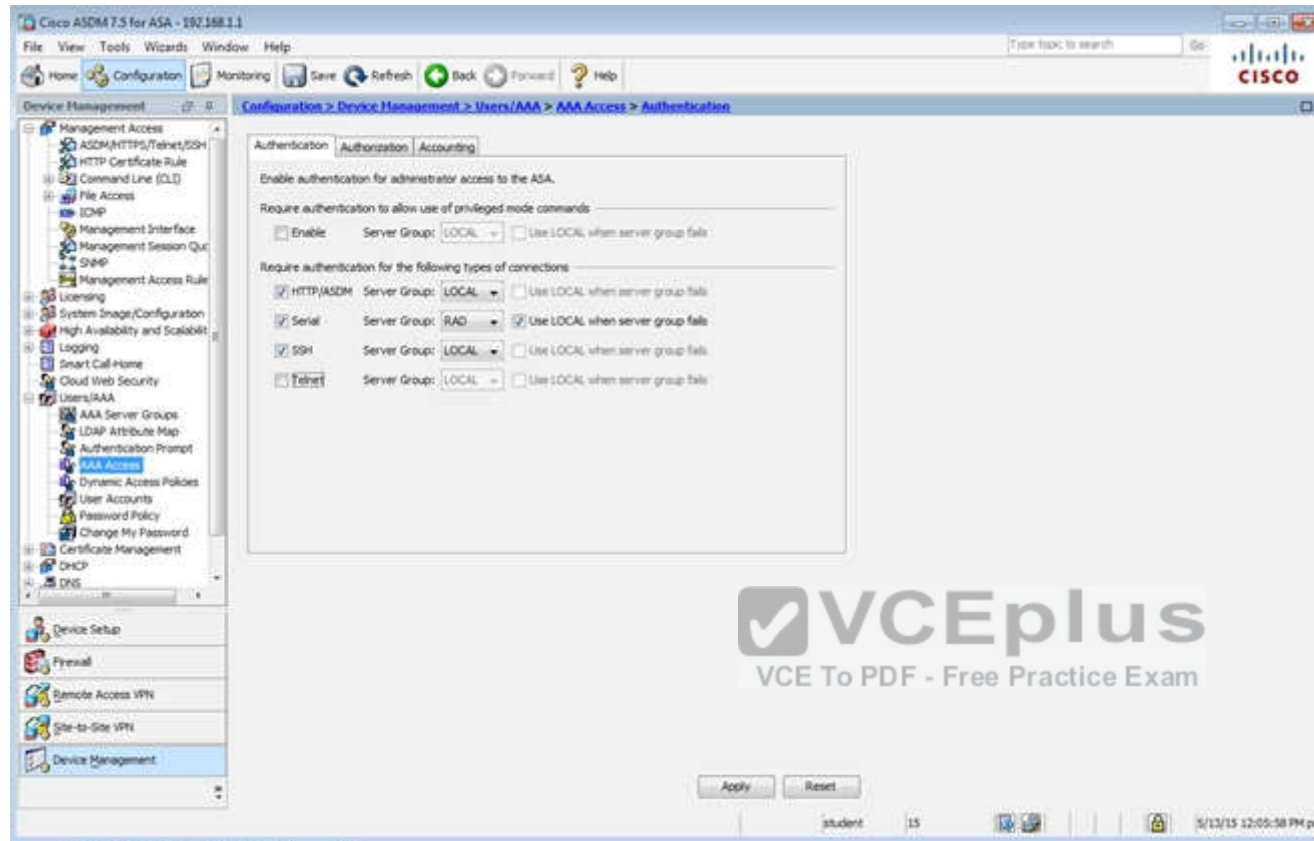


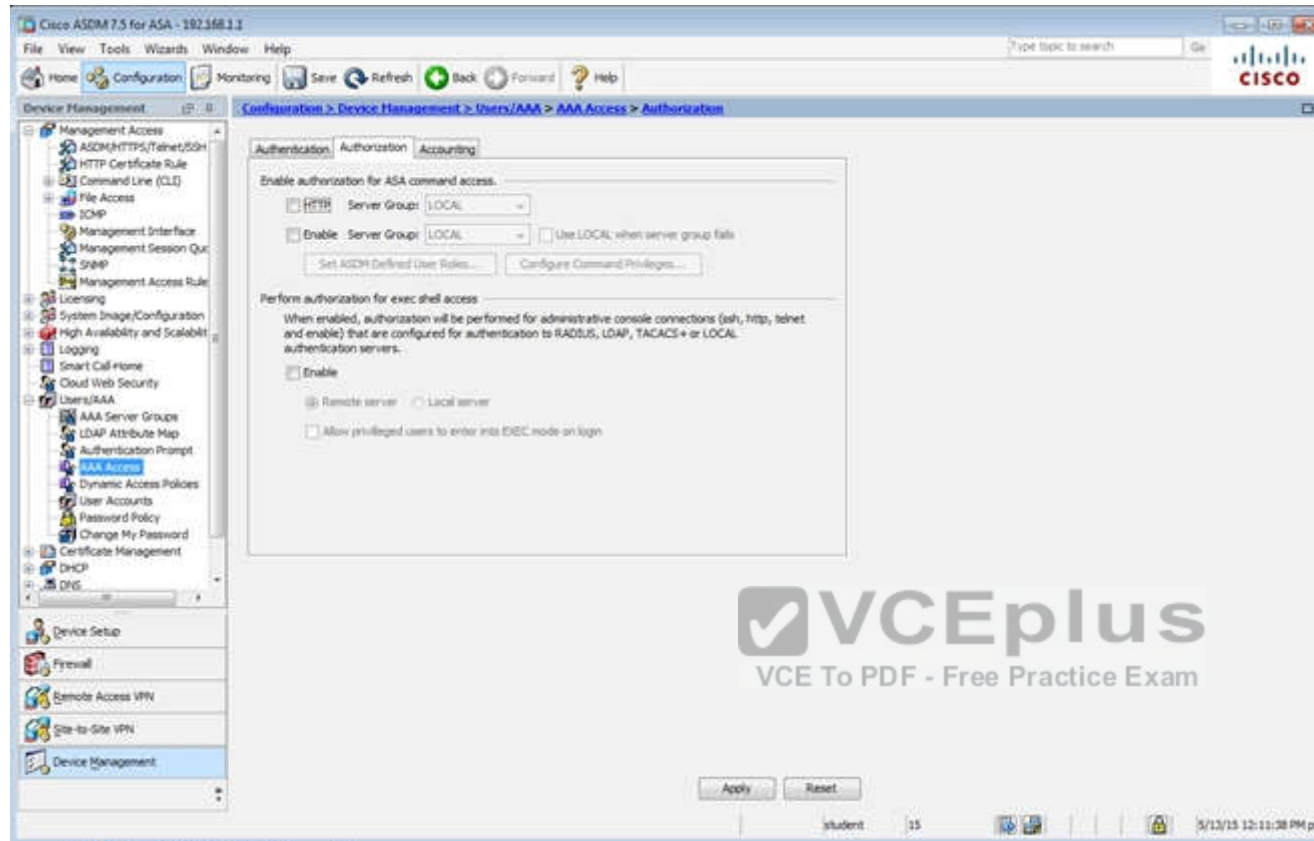


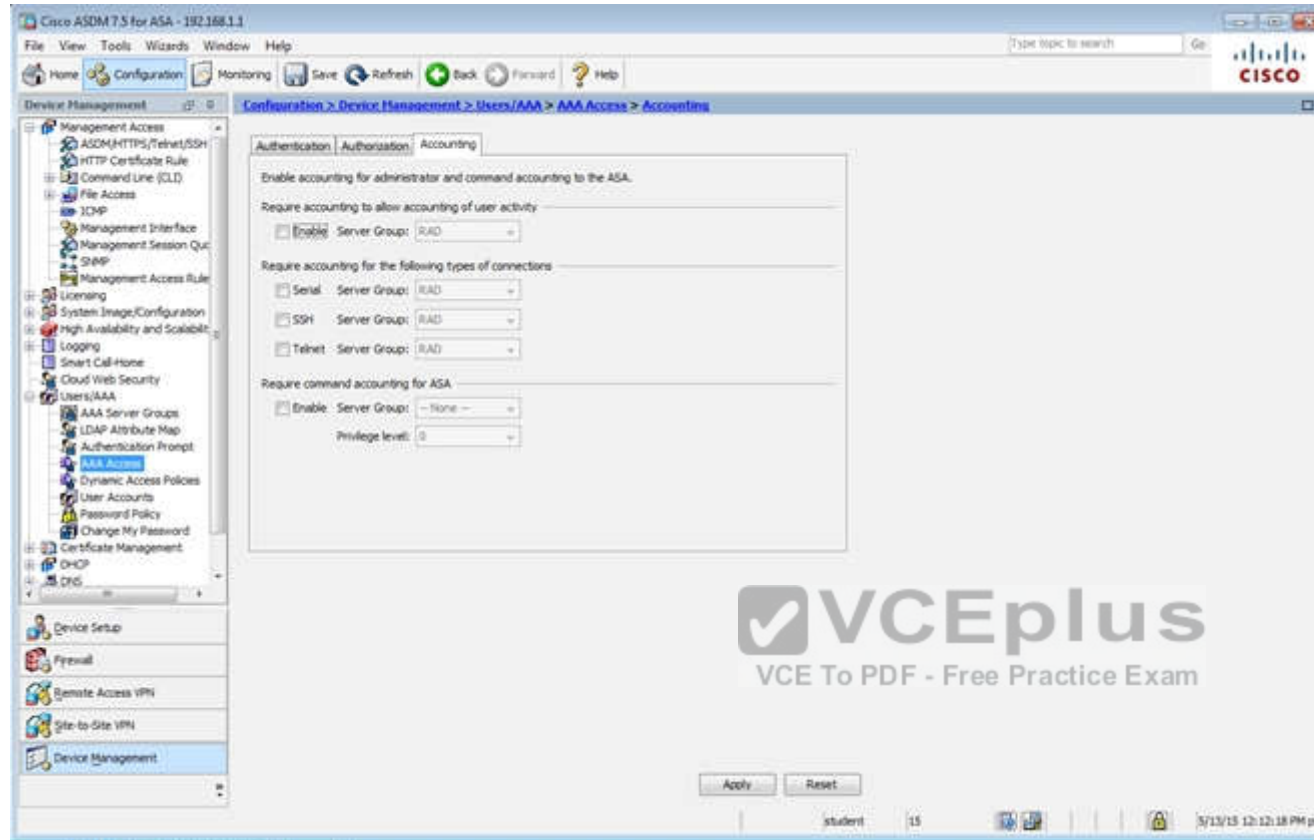


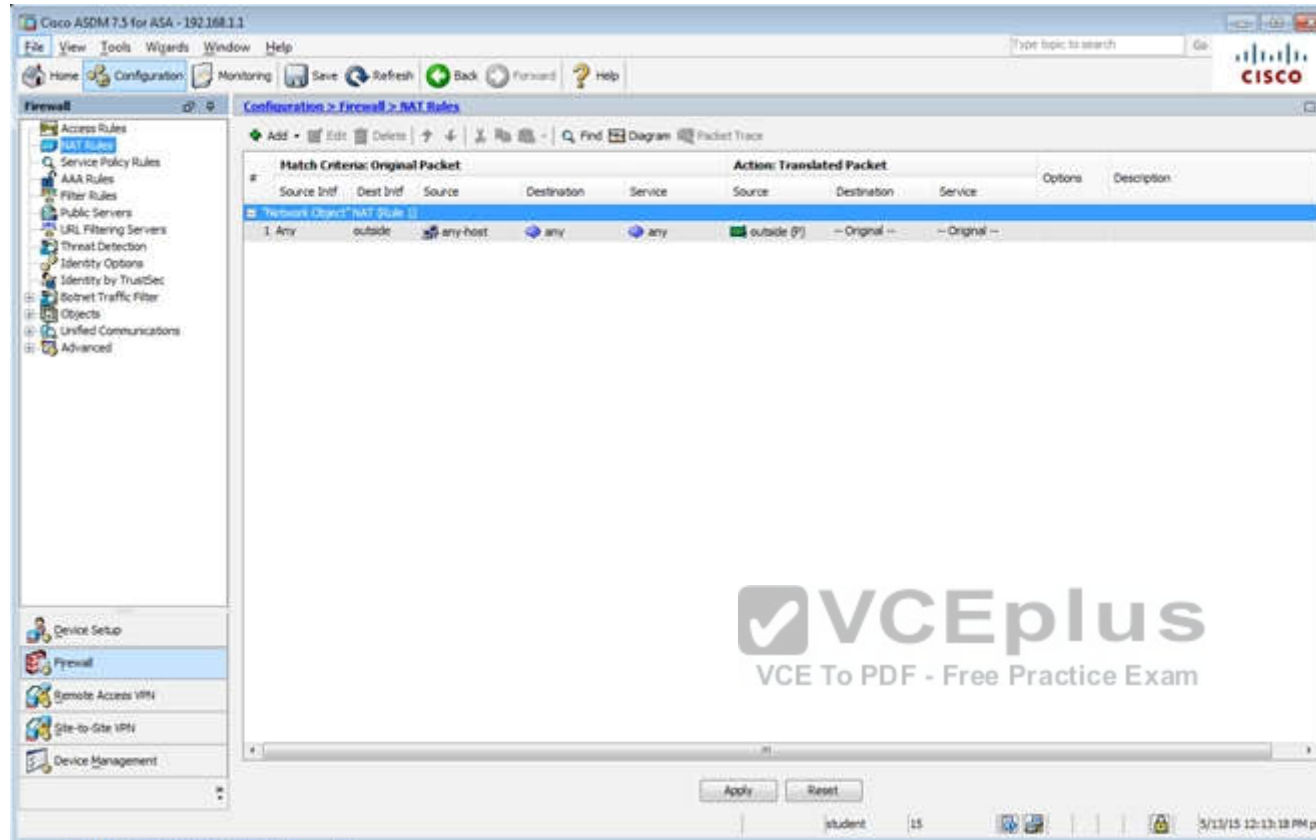


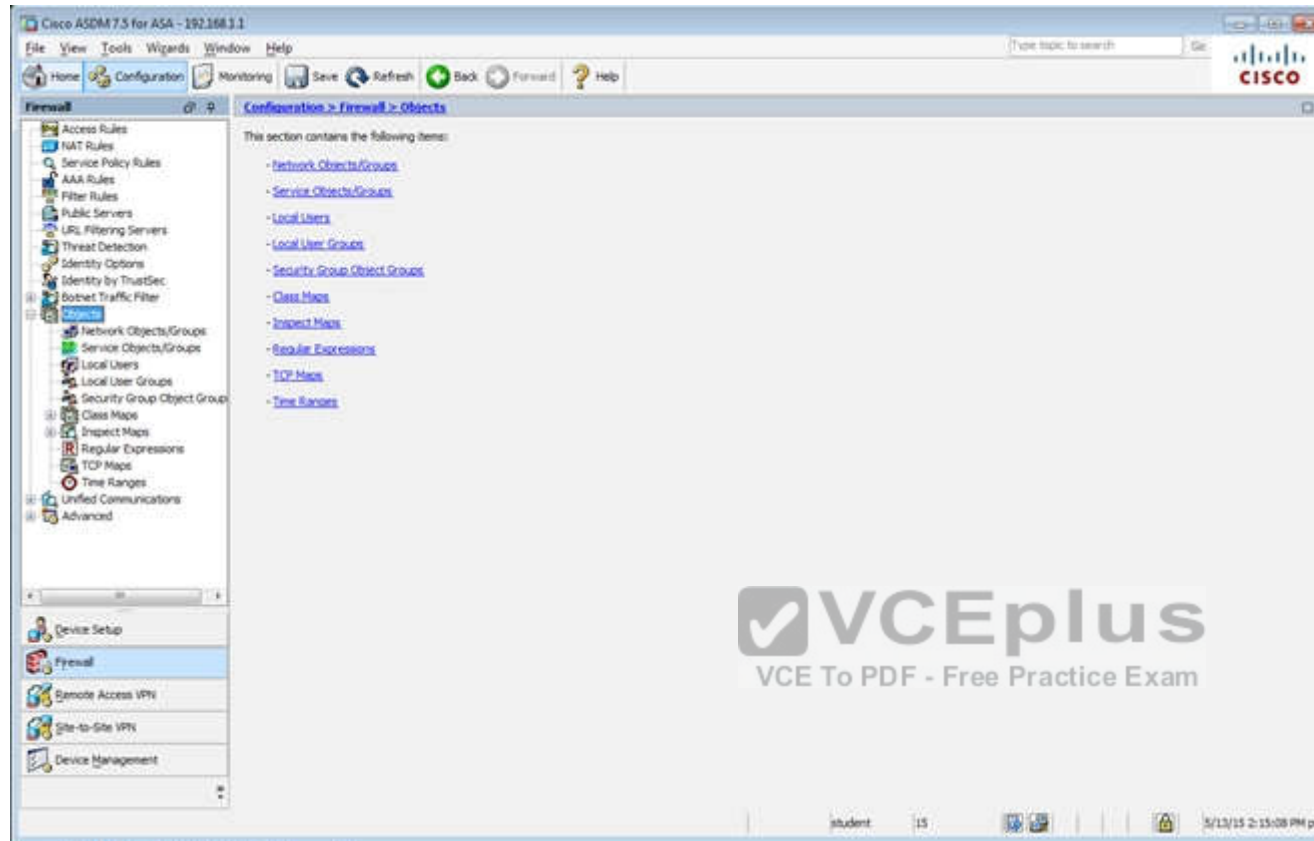












Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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 [Authentication](#).

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

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

Add Edit Delete

Ends: Match Case

Apply Reset

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

Cisco ASDM 7.3 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall 27 0 Configuration > Firewall > Objects > Network Objects/Groups

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

Configuration > Firewall > Objects > Network Objects/Groups

Filter: [] Where Used: [] Not Used: [] Filter (Clear)

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

Apply Reset

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

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 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

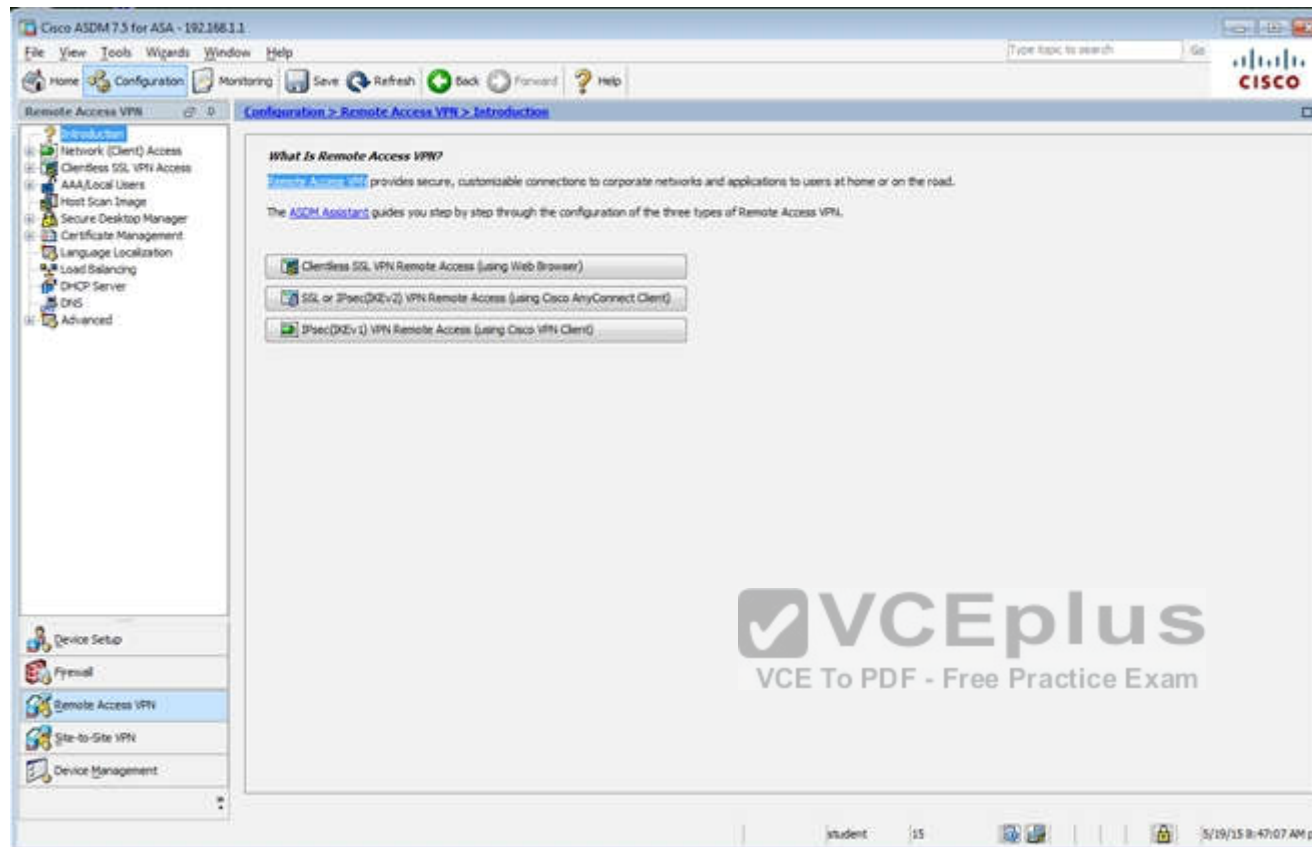
Traffic Classification

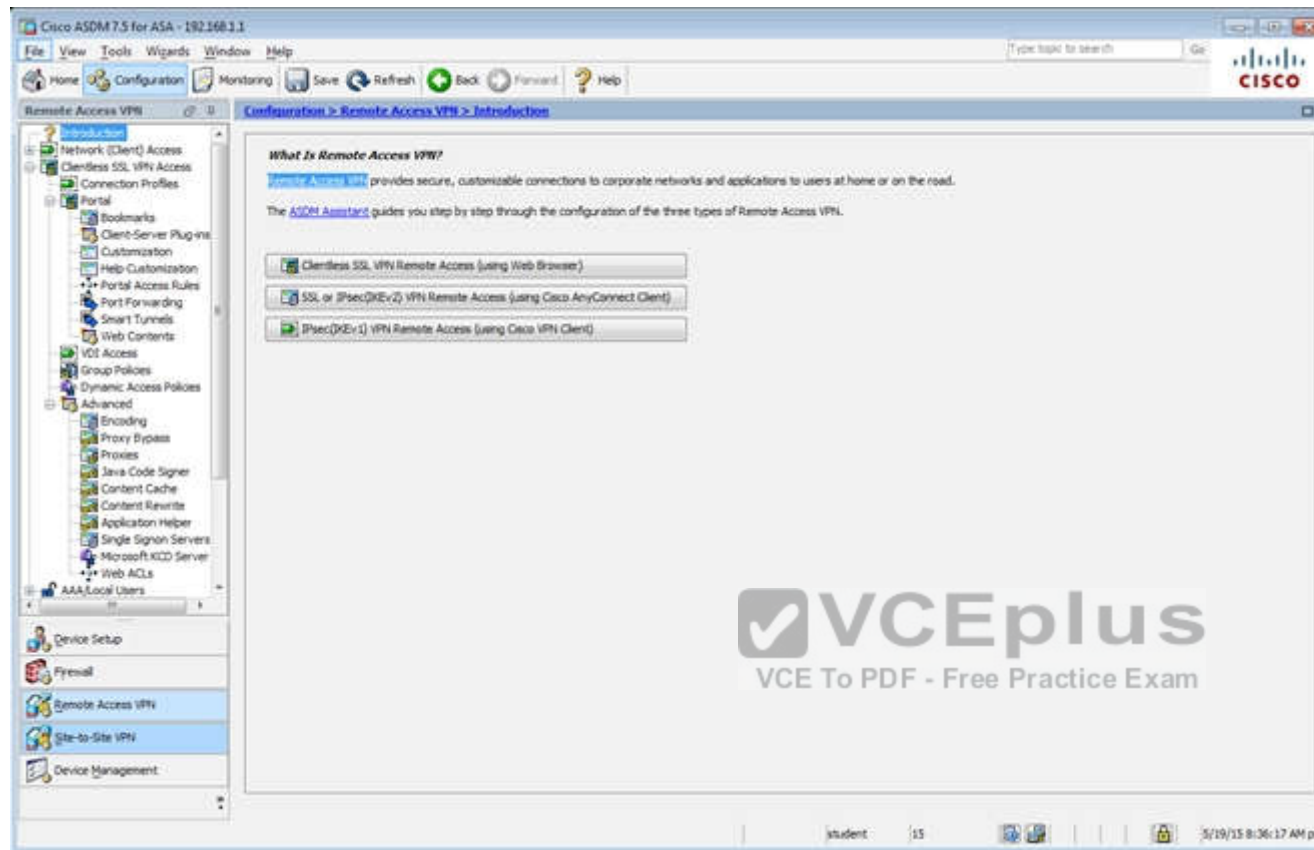
| Name | # | Enabled | Match | Source | Src Security Group | Destination | Dest Security Group | Service | Time | Rule Actions | Describe |
|--|---|---------|-------|--------|--------------------|-------------|---------------------|------------------------------|------|--|----------|
| Interface: dmz; Policy: dmz_policy | | | | | | | | | | | |
| class-default | | | Match | any | | any | | any traffic class-default | | | |
| Interface: inside; Policy: inside_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 SMTP (14 more inspect actions) | |

Apply Reset

student 15 5/13/15 12:15:48 PM pst







Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

| Interface | Allow Access |
|-----------|-------------------------------------|
| outside | <input checked="" type="checkbox"/> |
| dns | <input type="checkbox"/> |
| inside | <input type="checkbox"/> |

Device Certificate ...
Port Setting ...

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

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

☐ Shutdown portal login page.

Connection Profiles

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

Add Edit Delete Find: Match Case

| Name | Enabled | Aliases | Authentication Method | Group Policy |
|--------------------|-------------------------------------|---------|-----------------------|---------------|
| DefaultRAGroup | <input checked="" type="checkbox"/> | | AAA(RADIUS) | DefaultPolicy |
| DefaultWEBVpnGroup | <input checked="" type="checkbox"/> | | AAA(RADIUS) | DefaultPolicy |
| Clientless | <input checked="" type="checkbox"/> | test | AAA(RADIUS) | DefaultPolicy |

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

Apply Reset

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

Edit Clientless SSL VPN Connection Profile: clientless

Basic
Advanced

Name: clientless
Aliases: test

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

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

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

Find: ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

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

Login and Logout Page Customization: DfltCustomization Manage...

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

☐ Enable the display of SecurId messages on the login screen

Connection Aliases

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

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

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

Group URLs

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

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

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

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

☒ Always run CSD

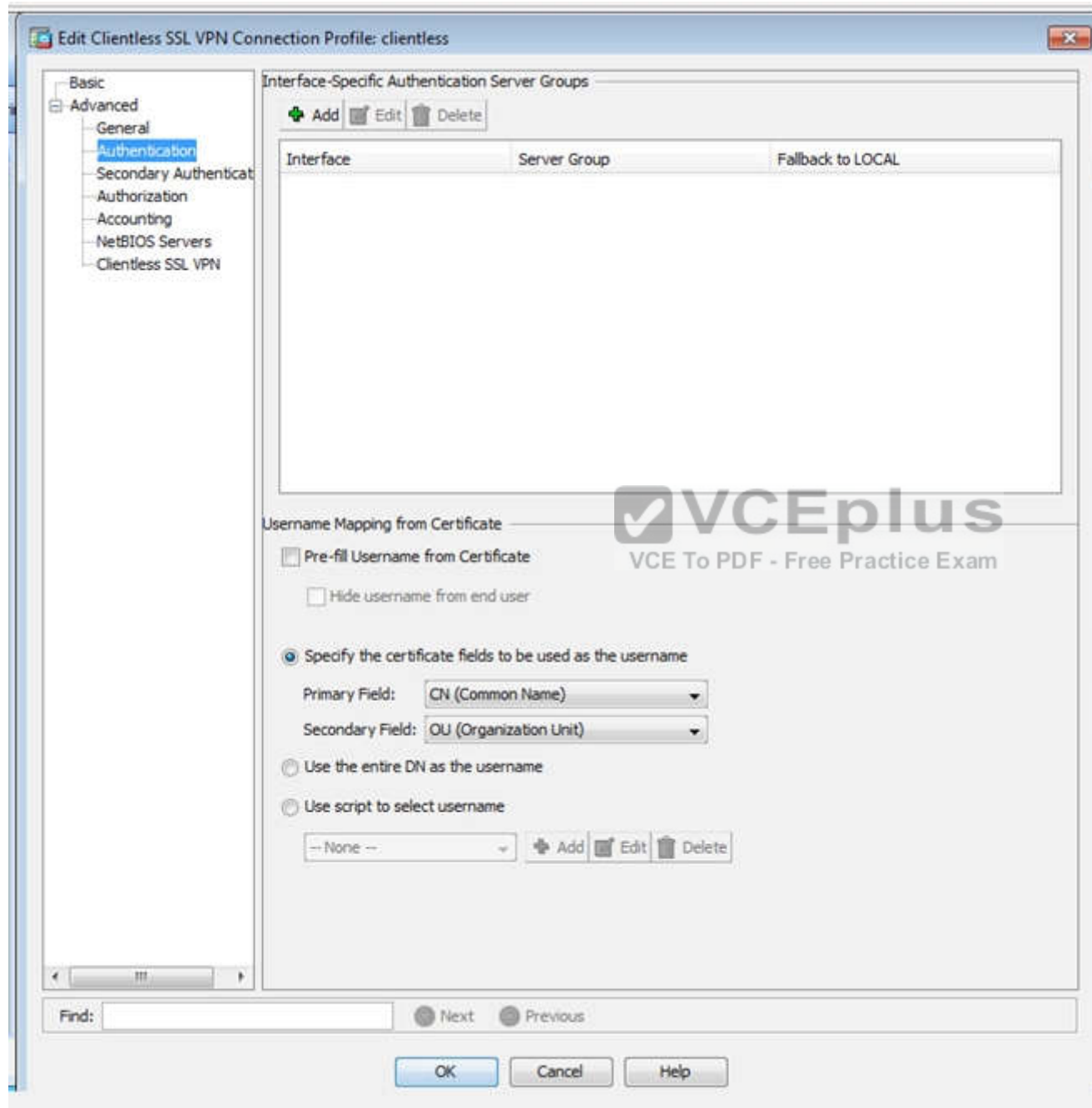
☐ Disable CSD for both AnyConnect and Clientless SSL VPN

☐ Disable CSD for AnyConnect only

Find: Next Previous

OK Cancel Help







Edit Clientless SSL VPN Connection Profile: clientless

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

Secondary Authentication Server Group

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

☐ Use LOCAL if Server Group fails

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

Attributes Server: ☒ Primary ☐ Secondary

Session Username Server: ☒ Primary ☐ Secondary

Interface-Specific Secondary Authentication Server Groups

+ Add Edit Delete

| Interface | Server Group | Fallback to LOCAL | Use primary username |
|-----------|--------------|-------------------|----------------------|
|-----------|--------------|-------------------|----------------------|

Username Mapping from Certificate

☐ Pre-fill username from certificate

☐ Hide username from end user

☐ Fallback when a certificate is unavailable

Password: ☒ Prompt ☐ Use primary ☐ Use

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

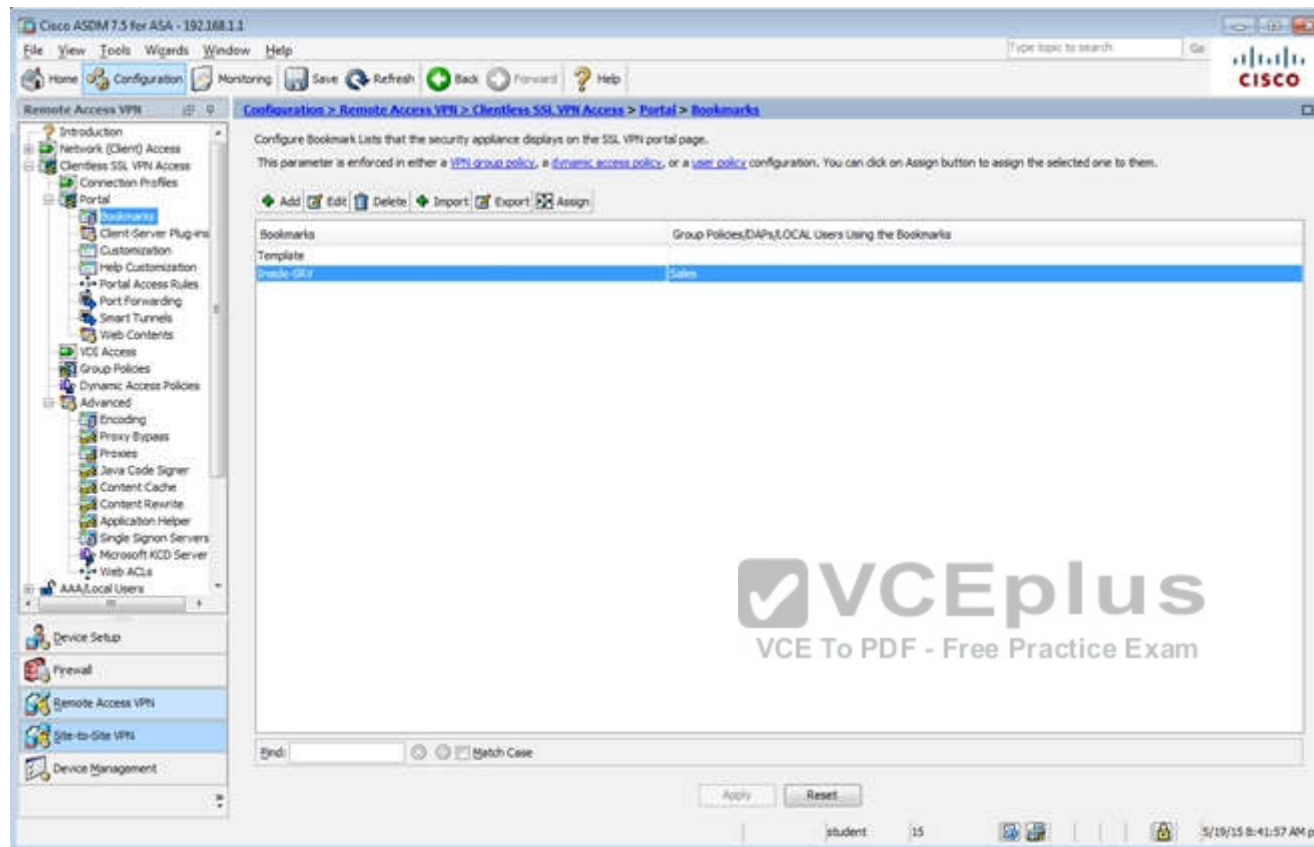
☐ Use the entire DN as the username

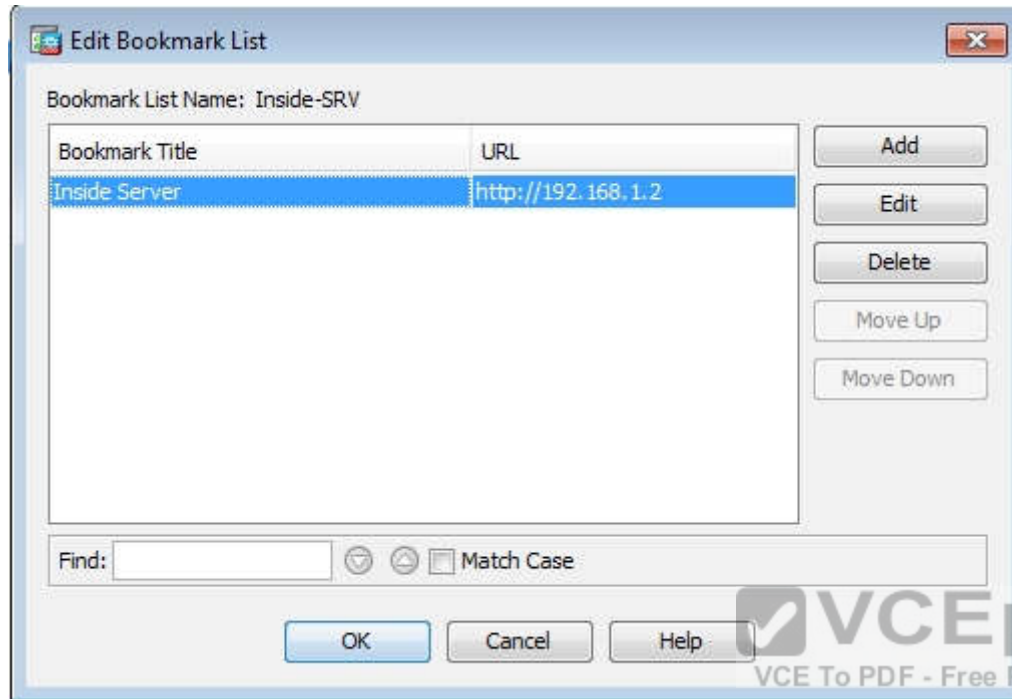
☐ Use script to select username

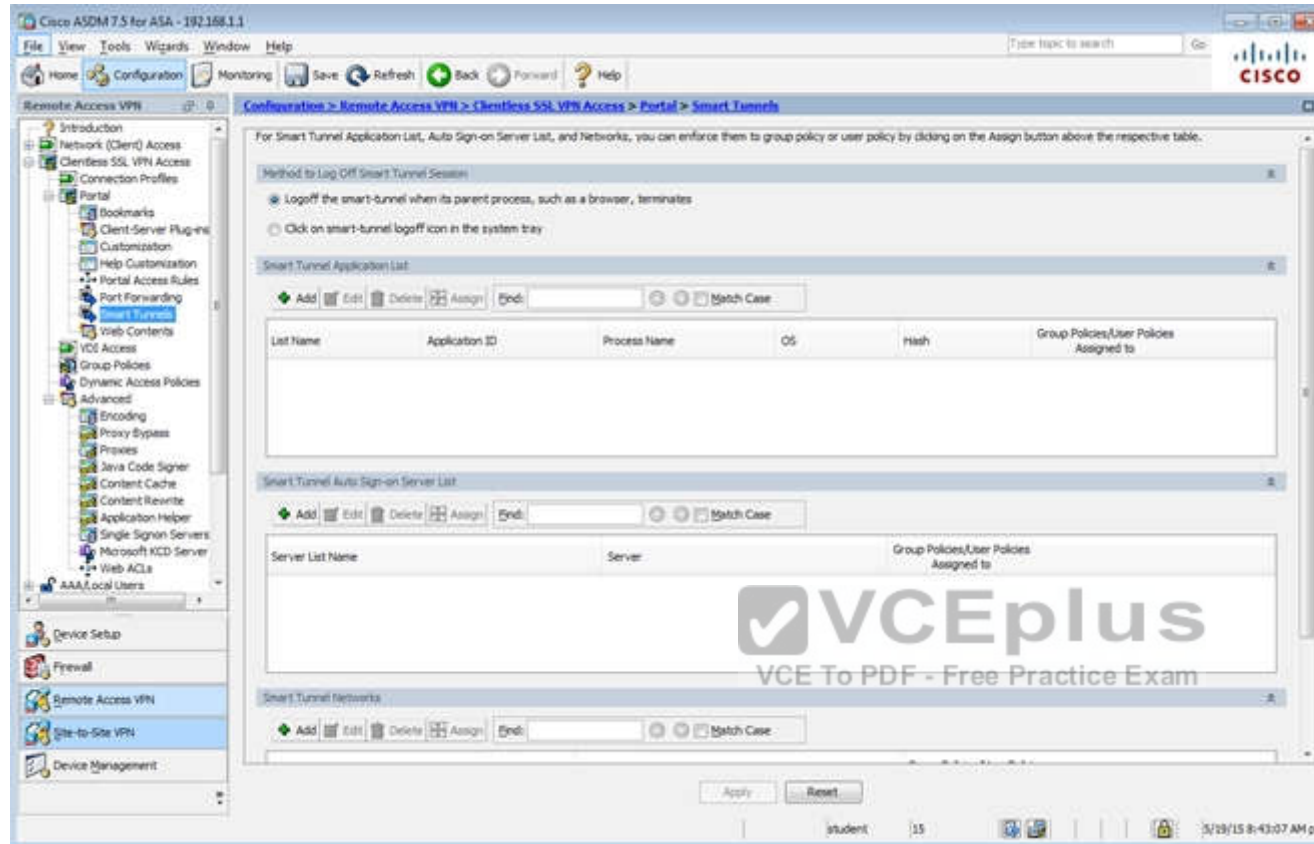
-- None -- + Add Edit Delete

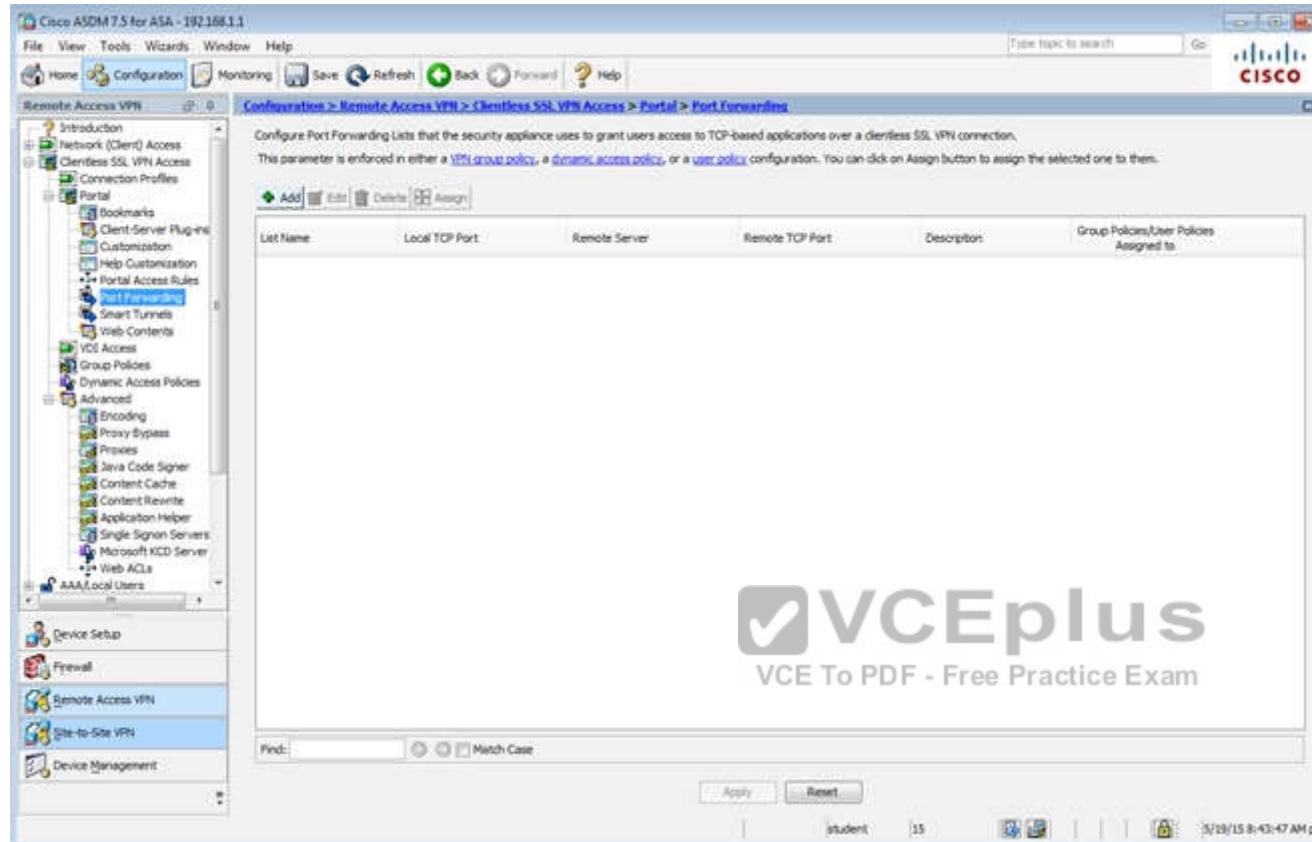
Find: Next Previous

OK Cancel Help









Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Clientless SSL VPN Access > 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 |
|--------------------------------|----------|------------------------------------|--|
| System | System | SSL-Clientless | Clientless |
| DefaultPolicy (System Default) | Internal | key1:key2:ssl-clientless/2tp-ipsec | DefaultRAGroup/DefaultL3Group/DefaultADMG/Def... |

End: Match Case

Apply Reset

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

Edit Internal Group Policy: Sales

Name: Sales

Banner: ☒ Inherit

More Options

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

Web ACL: ☒ Inherit Manage...

Access Hours: ☒ Inherit Manage...

Simultaneous Logins: ☒ Inherit

Restrict access to VLAN: ☒ Inherit

Connection Profile (Tunnel Group) Lock: ☒ Inherit

Maximum Connect Time: ☒ Inherit ☐ Unlimited minutes

Idle Timeout: ☒ Inherit ☐ Use Global Default minutes

Timeout Alerts

Session Alert Interval: ☒ Inherit ☐ Default minutes

Idle Alert Interval: ☒ Inherit ☐ Default minutes

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

Find: ☒ Next ☐ Previous

OK Cancel Help

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

- IPsec/SSL Connection
- Secure Mobility Solution
- Address Assignment
- Advanced
- Clientless SSL VPN Access
- Connection Profiles
- Portal
- Bookmarks
- Client-Server Plug-ins
- Customization
- Help Customization
- Portal Access Rules
- Port Forwarding
- Smart Tunnels
- Web Contents
- Voice Access
- Group Policies**
- Dynamic Access Policies
- Advanced
- AAA/Local Users
- AAA Server Groups
- LDAP Attribute Map
- Local Users
- Host Scan Image
- Secure Desktop Manager

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

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

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

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

| Name | Type | Tunneling Protocol | Connection Profiles/Users Assigned To |
|--------------------------------|----------|---|---------------------------------------|
| Default | Internal | ssl-clientless | Default |
| DfltGrpPolicy (System Default) | Internal | Rev 1.0 Rev 2.0 ssl-clientless/2to-ipssec | DfltGrpPolicy |

Find:

student 15 10/15/14 9:15:40 AM pet

Edit Internal Group Policy: Sales

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

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

URL Entry: ☒ Inherit ☐ Enable ☐ Disable

File Access Control

File Server Entry: ☒ Inherit ☐ Enable ☐ Disable

File Server Browsing: ☒ Inherit ☐ Enable ☐ Disable

Hidden Share Access: ☒ Inherit ☐ Enable ☐ Disable

Port Forwarding Control

Port Forwarding List: ☒ Inherit Manage...
☐ Auto Applet Download

Applet Name: ☒ Inherit

Smart Tunnel

Smart Tunnel Policy: ☒ Inherit Networks: Manage...
Tunnel Option: -- None --

Smart Tunnel Application: ☒ Inherit Manage...
☐ Smart Tunnel all Applications (This feature only works with Windows platform.)
☐ Auto Start

Auto Sign-on Server: ☒ Inherit Manage...
Windows Domain Name (optional):
Auto sign-on works only with Internet Explorer on Windows client or in Firefox on any platform.

ActiveX Relay

ActiveX Relay: ☒ Inherit ☐ Enable ☐ Disable

More Options

Find: Next Previous

OK Cancel Help

Edit Internal Group Policy: DfHGrpPolicy

Advanced

Name: DfHGrpPolicy

Banner:

SOCP forwarding URL:

Address Pools: Select

IPv6 Address Pools: Select

None Options

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

Filter: -- None -- Manage...

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

Simultaneous Logins: 3


Restrict access to VLANs: -- Unrestricted --

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

Maximum Connect Time: ☒ Unlimited ☐ 180/000

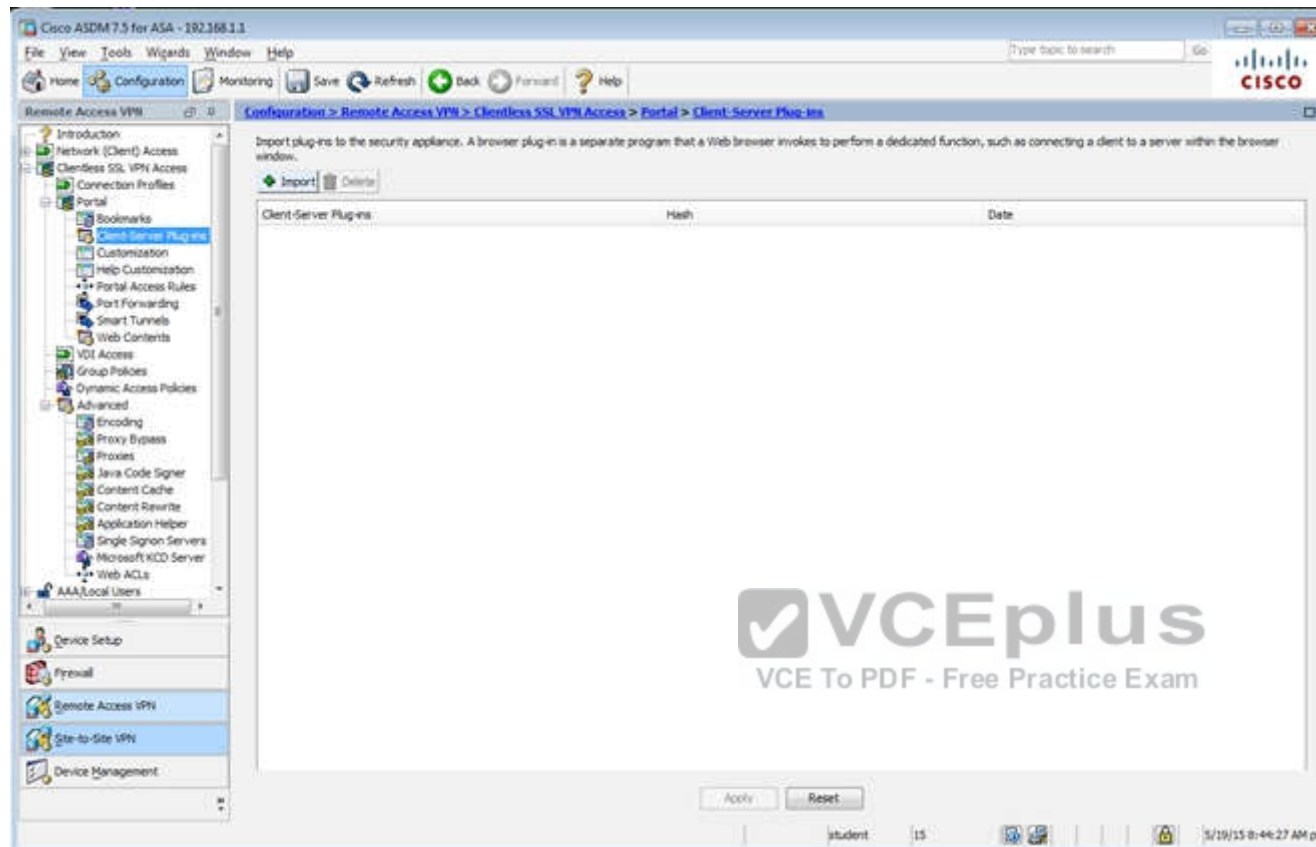
Idle Timeout: ☐ None 30 minutes

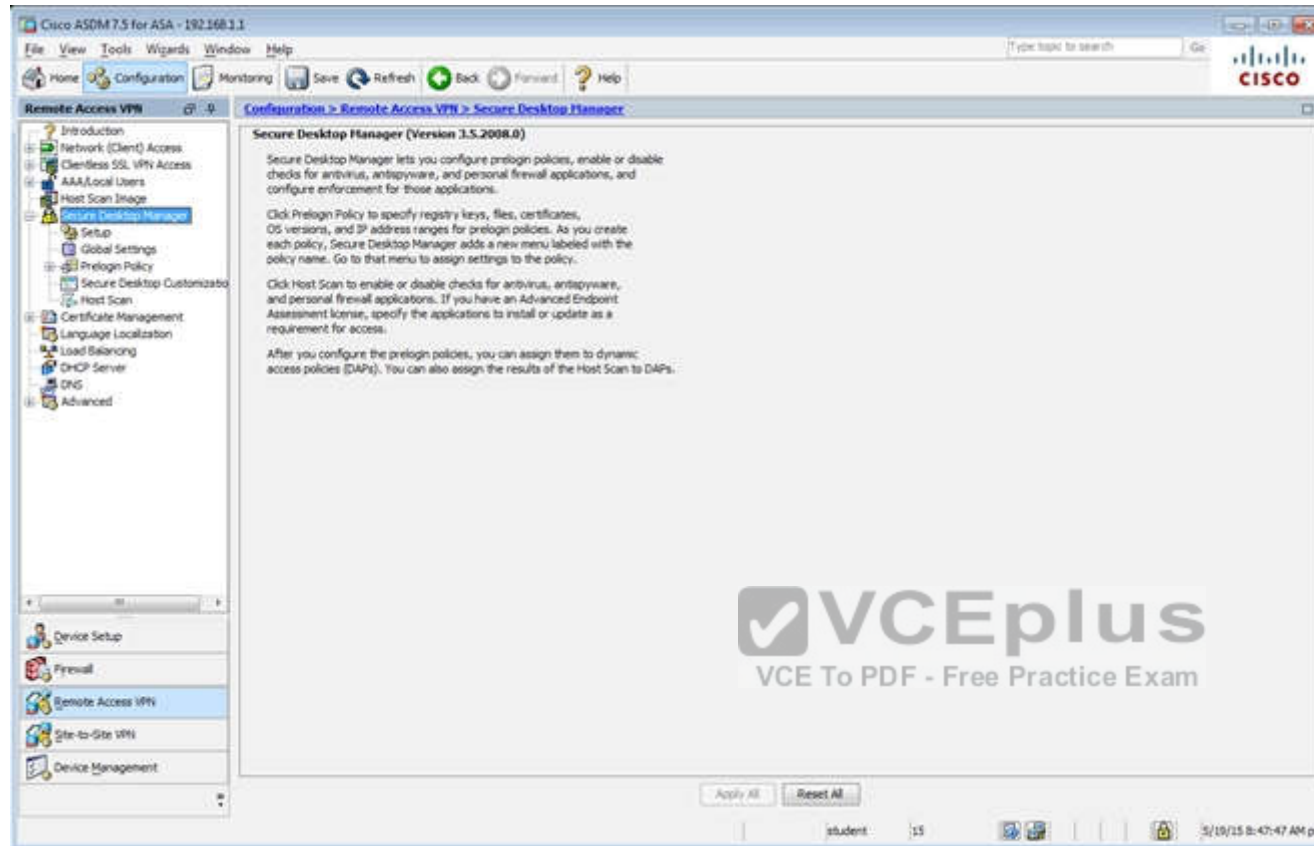
On smart card removal: ☒ Disconnect ☐ Keep the connection

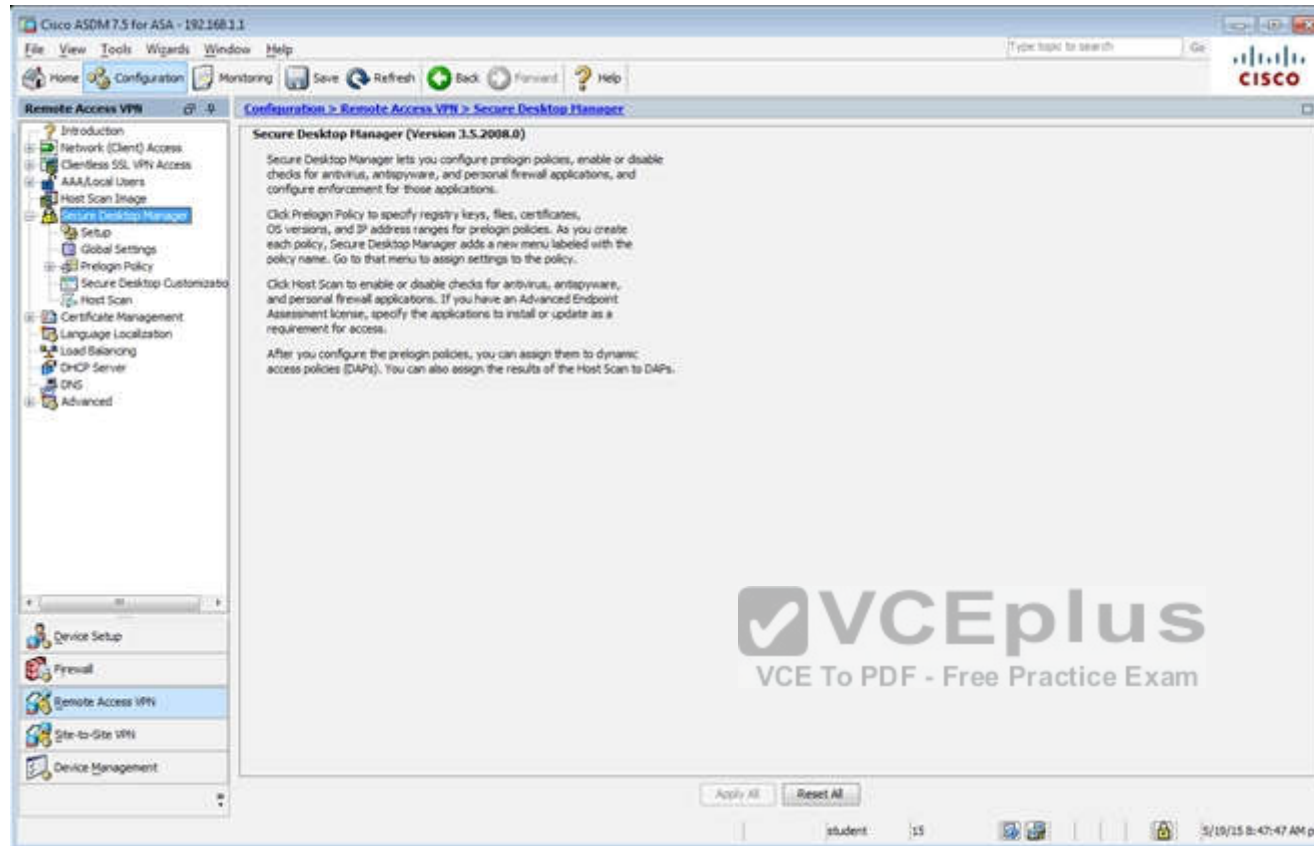
 **VCEplus**
VCE To PDF - Free Practice Exam

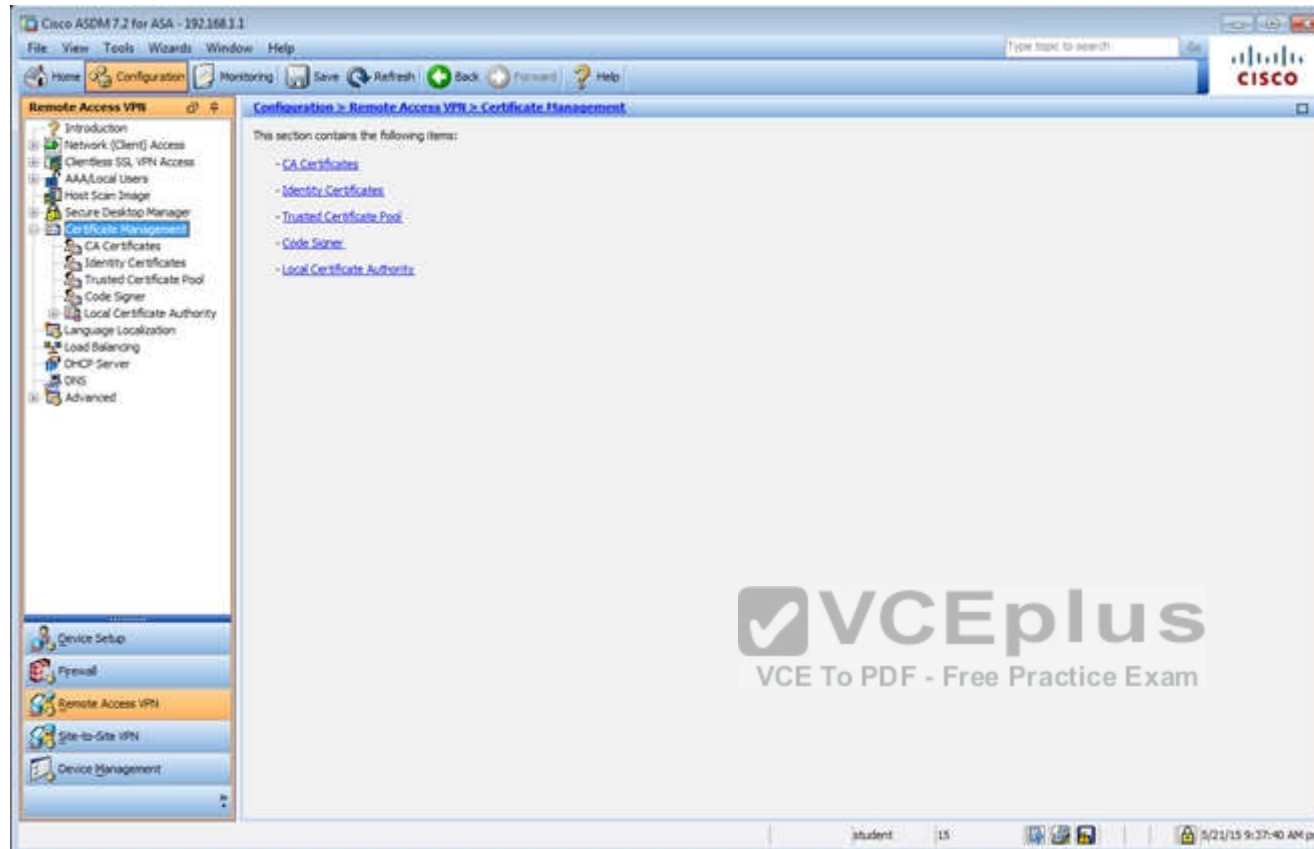
Find: Next Previous

OK Cancel Help

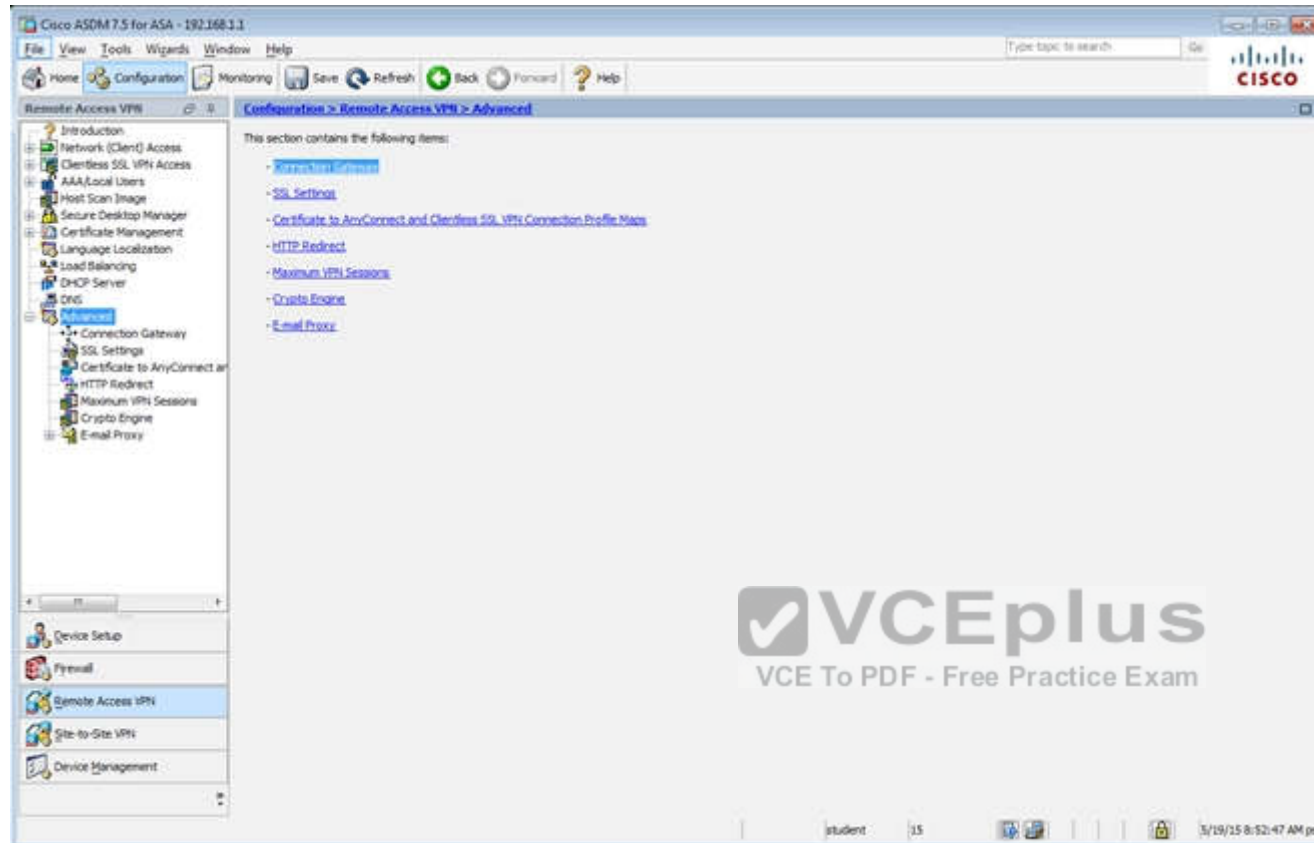


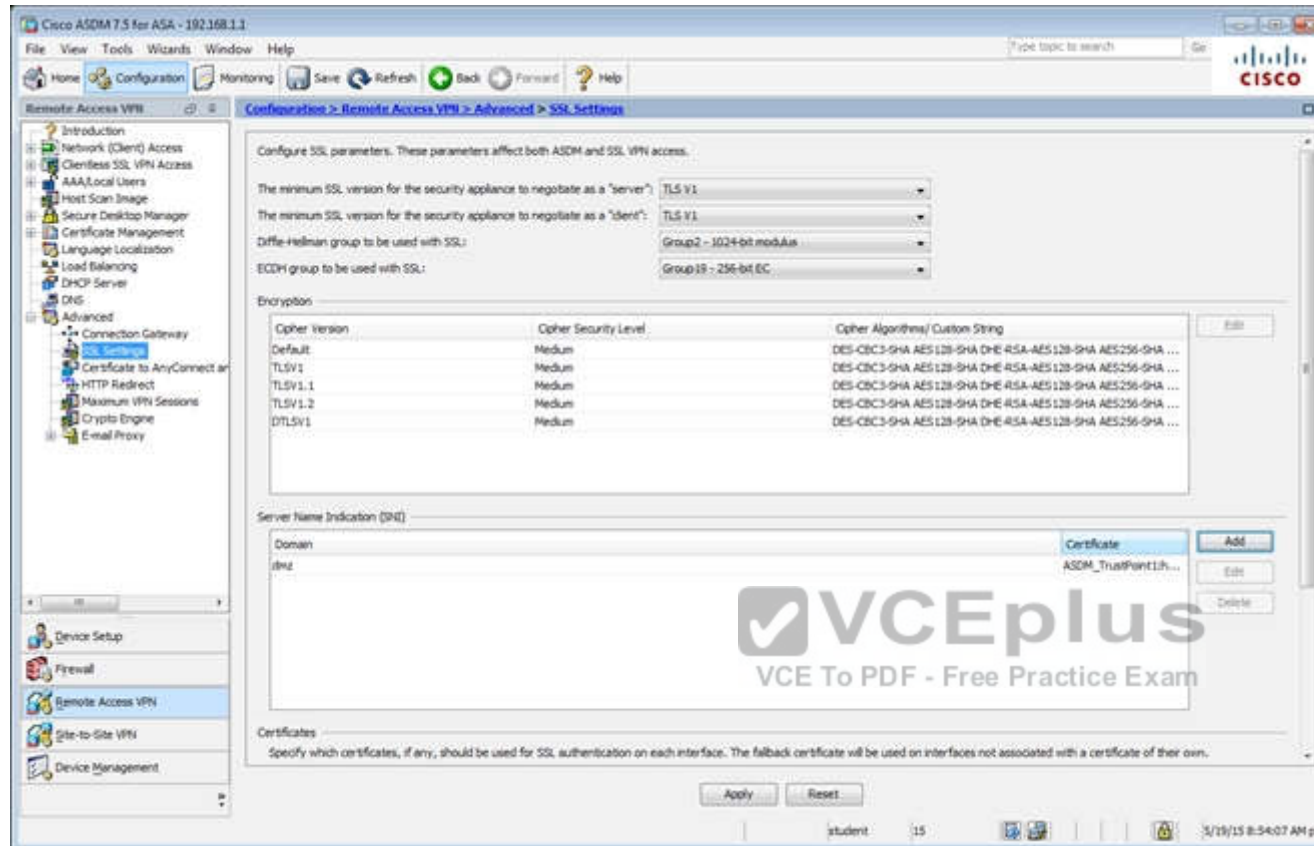


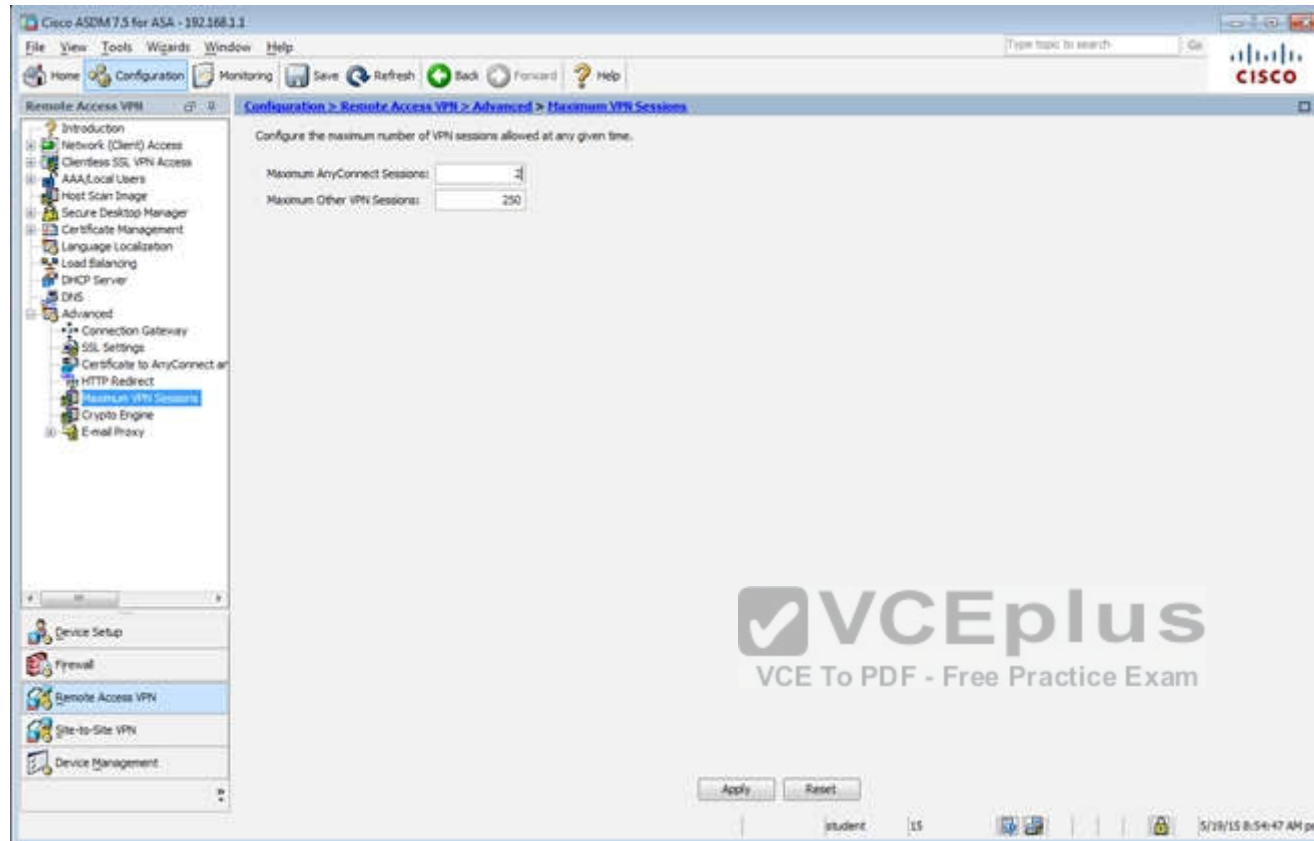


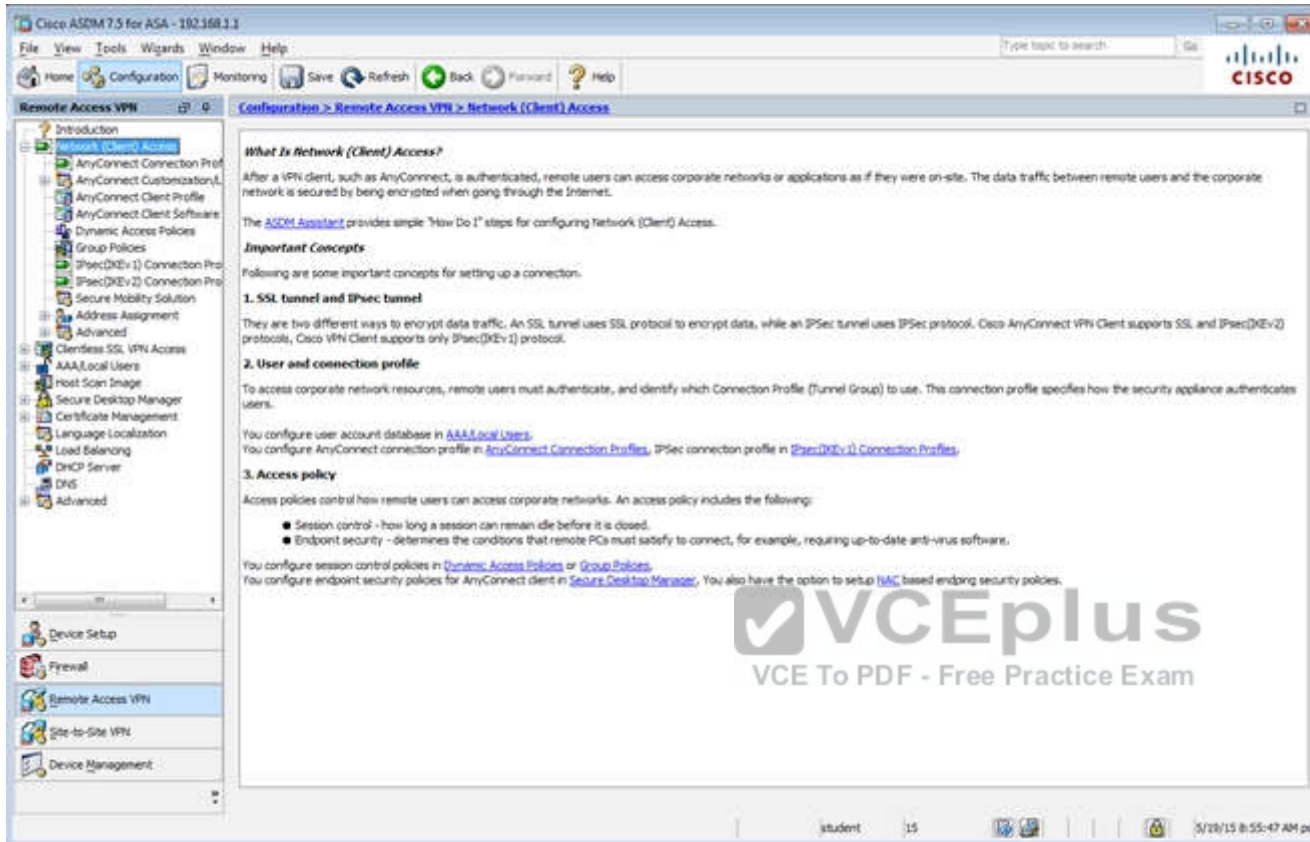


The screenshot shows the Cisco ASDM 7.3 for ASA - 192.168.1.1 interface. The left sidebar contains a tree view with categories like Remote Access VPN, Configuration, Monitoring, and Advanced. The main pane is titled 'Configuration > Remote Access VPN > Certificate Management > Identity Certificates'. It features a table with columns: Issued To, Issued By, Expiry Date, Associated Trustpoints, Usage, and Public Key Type. A single entry is visible: 'hostname-4P (17-ASA-sec...)' issued by 'hostname-4P (17-ASA-sec...)' on '11:00:33 pet 1 Dec 20 2024' using the 'ASDM-Trustpoint1' trustpoint for 'General Purpose' with 'RSA 2048 bits' public key type. Action buttons (Add, Show Details, Delete, Export, Install) are on the right. Below the table are sections for 'Certificate Expiration Alerts' (with input for days and a 'Set Default' button) and 'Public CA Enrollment' (with a description and an 'Enroll ASA SSL certificate with Enroll...' button). At the bottom, there's an 'ASDM Identity Certificate Wizard' section with a 'Launch ASDM Identity Certificate Wizard...' button and 'Apply'/'Reset' buttons. The status bar at the bottom shows 'student', '15', and the date/time '3/19/15 8:51:47 AM pet'.









Cisco ASDM 7.5 for ASA - 102.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Network (Client) Access

What Is Network (Client) Access?

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

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

Important Concepts

Following are some important concepts for setting up a connection.

1. SSL tunnel and IPsec tunnel

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

2. User and connection profile

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

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

3. Access policy

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

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

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

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

student 15 5/29/15 8:55:47 AM pct

The screenshot shows the Cisco ASDM 7.2 for ASA - 192.168.1.1 interface. The left sidebar displays the configuration tree with 'Remote Access VPN' selected. The main pane shows the 'Configuration > Remote Access VPN > Network (Client) Access > Group Policies' page. The page title is 'Group Policies'. Below the title, there is a description: '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](#).' Below this, there are buttons for 'Add', 'Edit', 'Delete', and 'Assign'. A table lists the configured group policies:

| Name | Type | Tunneling Protocol | Connection Profiles/Users Assigned To |
|-------------------------------------|----------|---|--|
| Sales | Internal | ssl-clientless | clientless |
| DefaultGroupPolicy (System Default) | Internal | l2l3-clientless/ssl-clientless/zip-gpsw | DefaultRAGroupDefault, & GroupDefaultWebVPNGroup |

At the bottom of the main pane, there is a 'Find:' search bar with a 'Match Case' checkbox. Below the search bar are 'Apply' and 'Reset' buttons. The bottom status bar shows the user 'student', the page number '15', and the date/time '3/21/15 10:17:10 AM pet'.

Edit Internal Group Policy: DiffGrpPolicy

Settings

- Servers
- Advanced
 - Split Tunneling
 - Browser Proxy
 - AnyConnect Client
 - IPsec (IKEv1) Client

Name: DiffGrpPolicy

Banner:

SCDP forwarding URL:

Address Pools: Select...

IPv6 Address Pools: Select...

Home Options

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

Filter: -- None -- Manage...

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

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

Simultaneous Logins: 3

Restrict access to VLAN: -- Unrestricted --

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

Maximum Connect Time: ☒ Unlimited ☐ minutes

Idle Timeout: ☐ None ☐ 30 minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

VCEplus
VCE To PDF - Free Practice Exam

Find: Next Previous

OK Cancel Help

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction
Network (Client) Access
AnyConnect Connection Profile
AnyConnect Customization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec (IKEv1) Connection Profile
IPsec (IKEv2) Connection Profile
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced

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

Access Interfaces
Enable interfaces for IPsec access.

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

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

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

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

| Name | IPsec Enabled | L2TP/IPsec Enabled | Authentication Server Group | Group Policy |
|--------------------|-------------------------------------|-------------------------------------|-----------------------------|---------------|
| DefaultRAGroup | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD | DiffGrpPolicy |
| DefaultWEBVPNGroup | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD | DiffGrpPolicy |
| Services | <input type="checkbox"/> | <input type="checkbox"/> | LOCAL | Local |

End:

student 15 5/18/15 8:56:47 AM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec (IKEv2) 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

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

Access Interfaces

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

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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

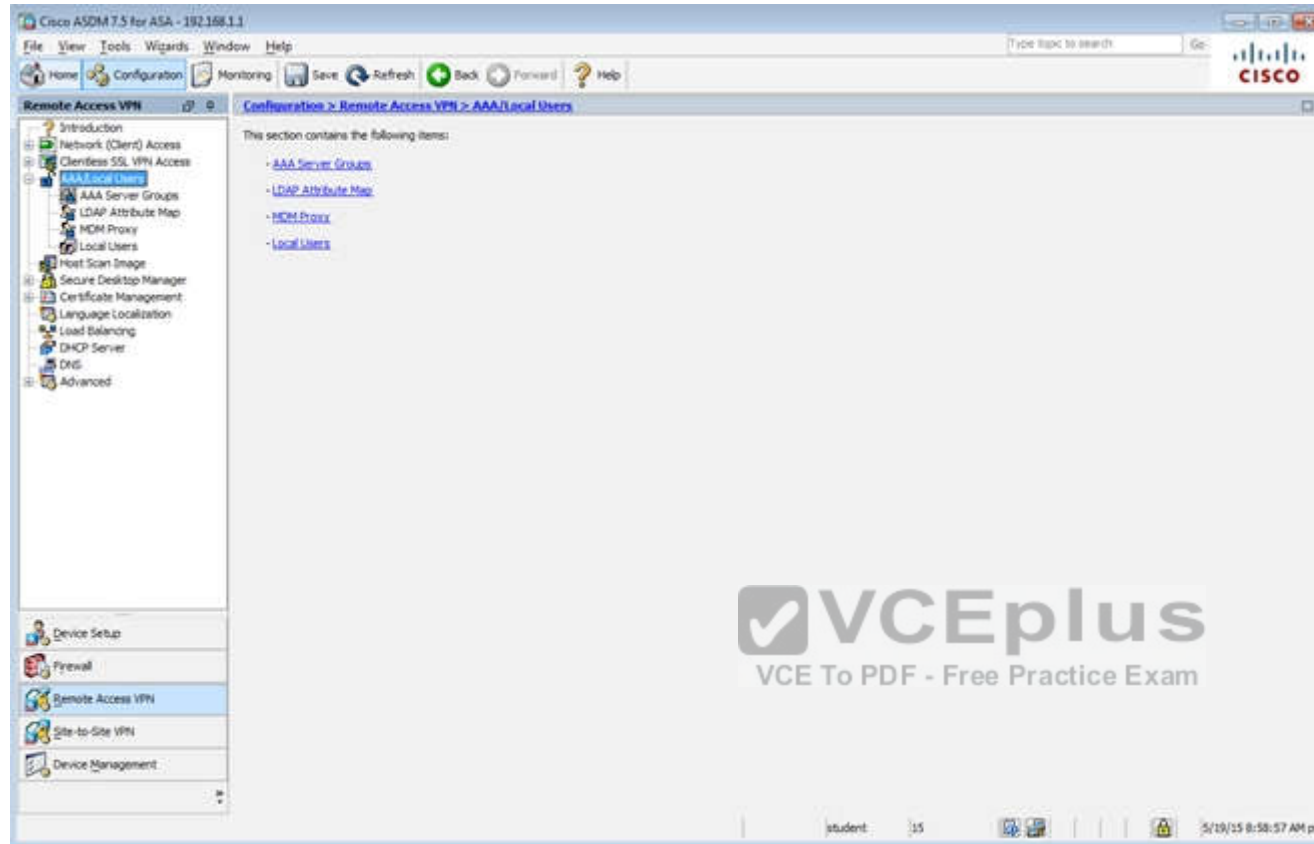
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile [here](#).

Find:

| Name | SSL Enabled | IPsec Enabled | Authentication Method | Group Policy |
|--------------------|-------------------------------------|-------------------------------------|-----------------------|--------------------|
| DefaultRAGroup | <input type="checkbox"/> | <input type="checkbox"/> | AAA(RADIUS) | DefaultGroupPolicy |
| DefaultTNSVPNGroup | <input type="checkbox"/> | <input checked="" type="checkbox"/> | AAA(RADIUS) | DefaultGroupPolicy |
| Clientless | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | AAA(SSL-HTTPS) | DefaultGroupPolicy |

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

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
MDM Proxy
Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced

Create entries in the ASA local user database.

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

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

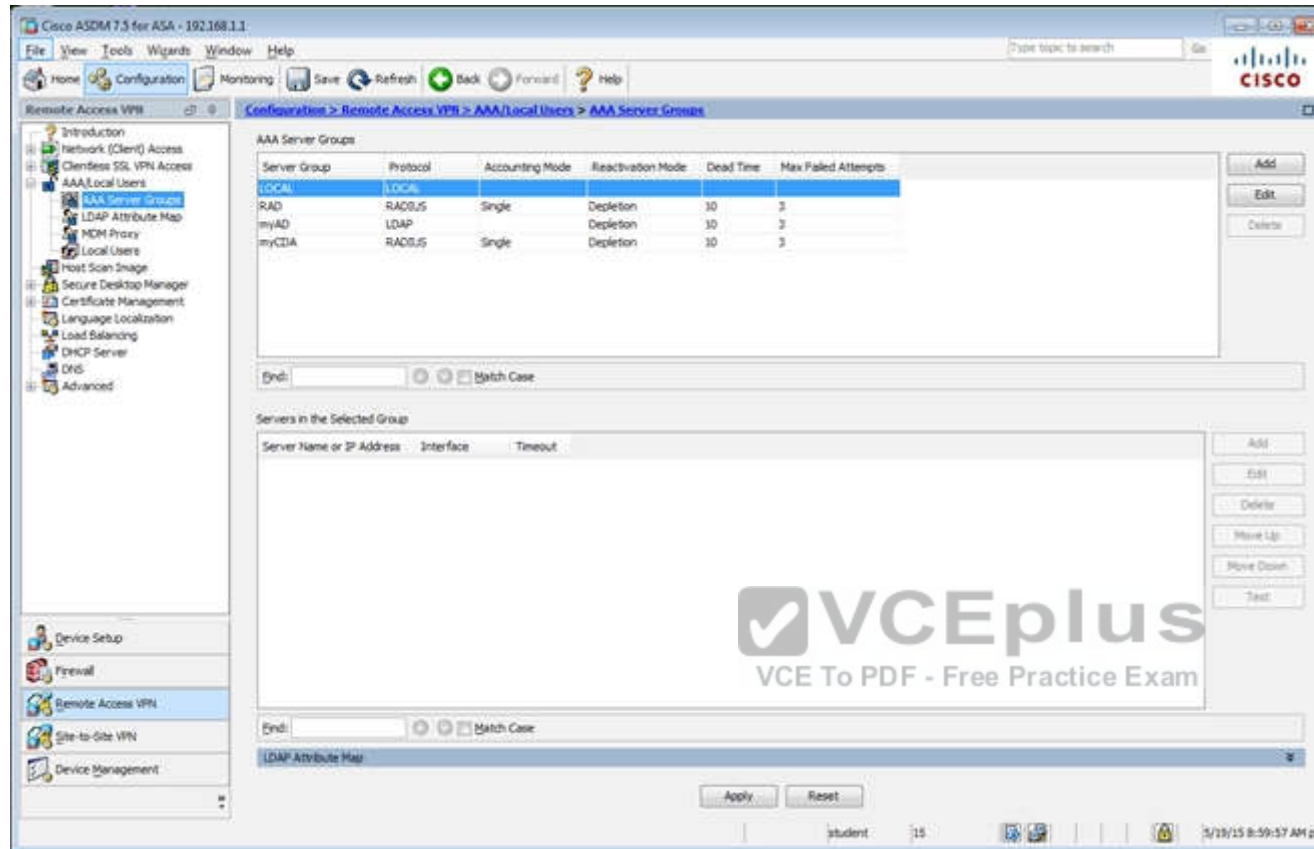
| Username | Privilege Level (Role) | Access Restrictions | VPN Group Policy | VPN Group Lock |
|-----------|------------------------|---------------------|----------------------------|----------------------------|
| student | 15 | Full | -- Inherit Group Policy -- | -- Inherit Group Policy -- |
| enable_15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

Add Edit Delete

End: Match Case

Apply Reset

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



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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

First navigate to the Connection Profiles tab as shown below, highlight the one with the test alias:



Virtual Terminal

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

- 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

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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

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

Device Certificate ...

Port Setting ...

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

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

☐ Shutdown portal login page.

Connection Profiles

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

+ Add Edit Delete Find: ☐ Match Case

| Name | Enabled | Aliases | Authentication Method |
|--------------------|-------------------------------------|---------|-----------------------|
| DefaultRAGroup | <input checked="" type="checkbox"/> | | AAA(RAD) |
| DefaultWEBVPNGroup | <input checked="" type="checkbox"/> | | AAA(RAD) |
| clientless | <input checked="" type="checkbox"/> | test | AAA(LOCAL) |

Then hit the “edit” button and you can clearly see the Sales Group Policy being applied.



Virtual Terminal

Remote Access

- Introduction
- Network ()
- Clientless
- Conne
- Portal
- Bo
- Cl
- CU
- He
- Pod
- Pod
- Sn
- W
- VDI Ad
- Group
- Dynan
- Advan
- En
- Pr
- Pr
- Ja
- Co
- Co
- Ap
- Sir
- Mi
- W
- AAA/Local
- Device Setu

Aliases:

Authentication

Method: ☒ AAA ☐ Certificate ☐ Both

AAA Server Group: Manage...

☐ Use LOCAL if Server Group fails

DNS

Server Group: Manage...

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

Servers:

Domain Name:

Default Group Policy

Group Policy: Manage...

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

☒ Enable clientless SSL VPN protocol

QUESTION 68**SIMULATION****Scenario**

Given the new additional connectivity requirements and the topology diagram, use ASDM to accomplish the required ASA configurations to meet the requirements.

New additional connectivity requirements:

- Currently, the ASA configurations only allow on the Inside and DMZ networks to access any hosts on the Outside. Your task is to use ASDM to configure the ASA to also allow any host only on the Outside to HTTP to the DMZ server. The hosts on the Outside will need to use the 209.165.201.30 public IP address when HTTPing to the DMZ server.
- Currently, hosts on the ASA higher security level interfaces are not able to ping any hosts on the lower security level interfaces. Your task in this simulation is to use ASDM to enable the ASA to dynamically allow the echo-reply responses back through the ASA.

Once the correct ASA configurations have been configured:

- You can test the connectivity to `http://209.165.201.30` from the Outside PC browser.
- You can test the pings to the Outside (`www.cisco.com`) by opening the inside PC command prompt window. In this simulation, only testing pings to `www.cisco.com` will work.

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.

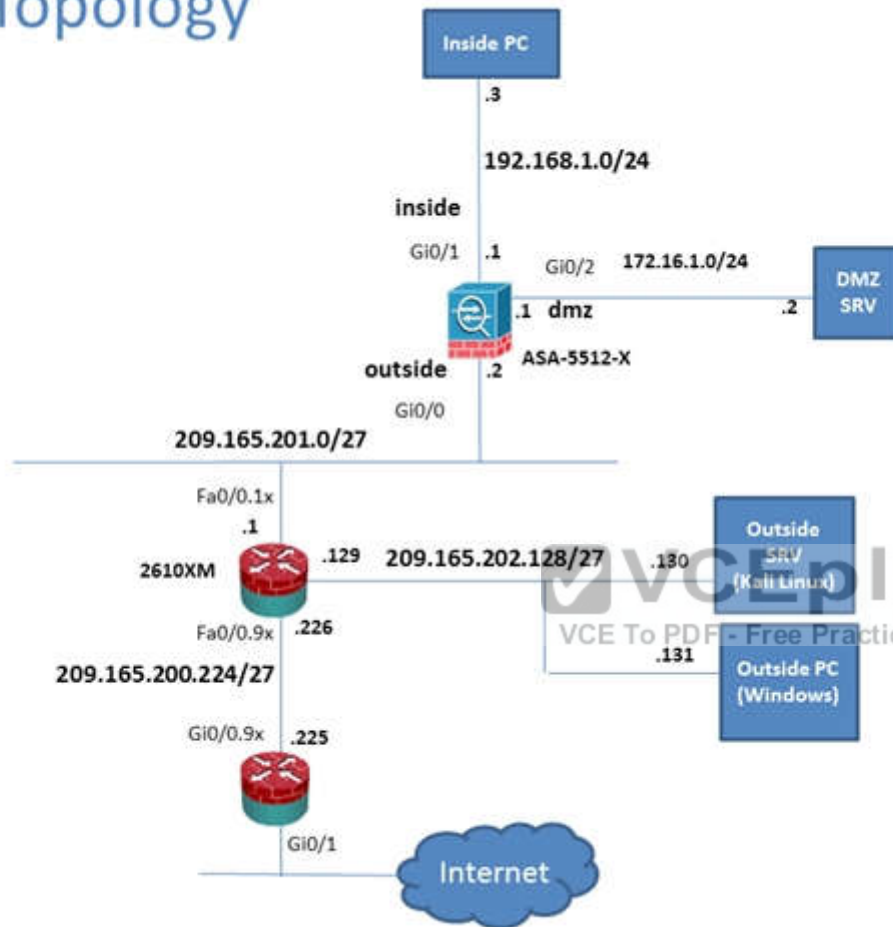
Note:

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



Cisco ASDM 7.5 for ASA - 192.168.1.3

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Home

Device Dashboard Firewall Dashboard ASA PrePOWER Status

Device Information

General License

Host Name: **P17-ASA.secure-x.local**
 ASA Version: **100.14(6)13**
 ASDM Version: **7.5(1)1**
 Firewall Mode: **Routed**
 Environment Status: **OK**

Device Uptime: **11d 21h 42m 47s**
 Device Type: **ASA 5512**
 Context Mode: **Single**
 Total Flash: **4096 MB**

Interface Status

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

Select an interface to view input and output Kbps

VPN Sessions

IPsec: 0 Clientless SSL VPN: AnyConnect Client: 0 [Details](#)

Failover Status

Failover not configured. Click the link to configure it. [Configure](#)

System Resources Status

Total Memory Usage Total CPU Usage Core Usage [Details](#)

Memory Usage (MB)

Traffic Status

Connections Per Second Usage

UDP: 0 TCP: 0 Total: 0

'outside' Interface Traffic Usage (Kbps)

Input Kbps: 0 Output Kbps: 0

Latest ASDM Syslog Messages

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

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Interfaces c2.9 Monitoring > Interfaces > ARP Table

ARP Table

Each row represents one ARP table entry.

| Interface | IP Address | MAC Address | Proxy Arp |
|-----------|---------------|----------------|-----------|
| outside | 209.165.201.1 | 000c.3014.3820 | No |
| inside | 192.168.1.4 | 0050.5633.3333 | No |
| inside | 192.168.1.3 | 0050.5611.1111 | No |
| inside | 192.168.1.2 | 0050.5622.2222 | No |
| inside | 192.168.1.56 | 0050.5692.5c7b | No |
| inside | 192.168.1.55 | 0006.80e6.90f3 | No |
| dmz | 172.16.1.2 | 0050.5644.4444 | No |
| mgmt | 10.10.10.1 | 000c.3014.3820 | No |

Clear Dynamic ARP Entries

Refresh

Data Refreshed Successfully.

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

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

VPN

Monitoring > VPN > VPN Statistics > Sessions

VPN Statistics

- VPN Cluster Loads
- Crypto Statistics
- Compression Statistics
- Encryption Statistics
- Global IKE/Phase Statistics
- Protocol Statistics
- VPN Mapping Sessions
- MDM Proxy Statistics
- MDM Proxy Sessions
- Clientless SSL VPN
- VPN Connection Graphs
- WSA Sessions

Interfaces

VPN

Global Traffic Filter

Routing

Properties

Logging

Type Active Cumulative Peak Concurrent Inactive

Clientless VPN

Browser

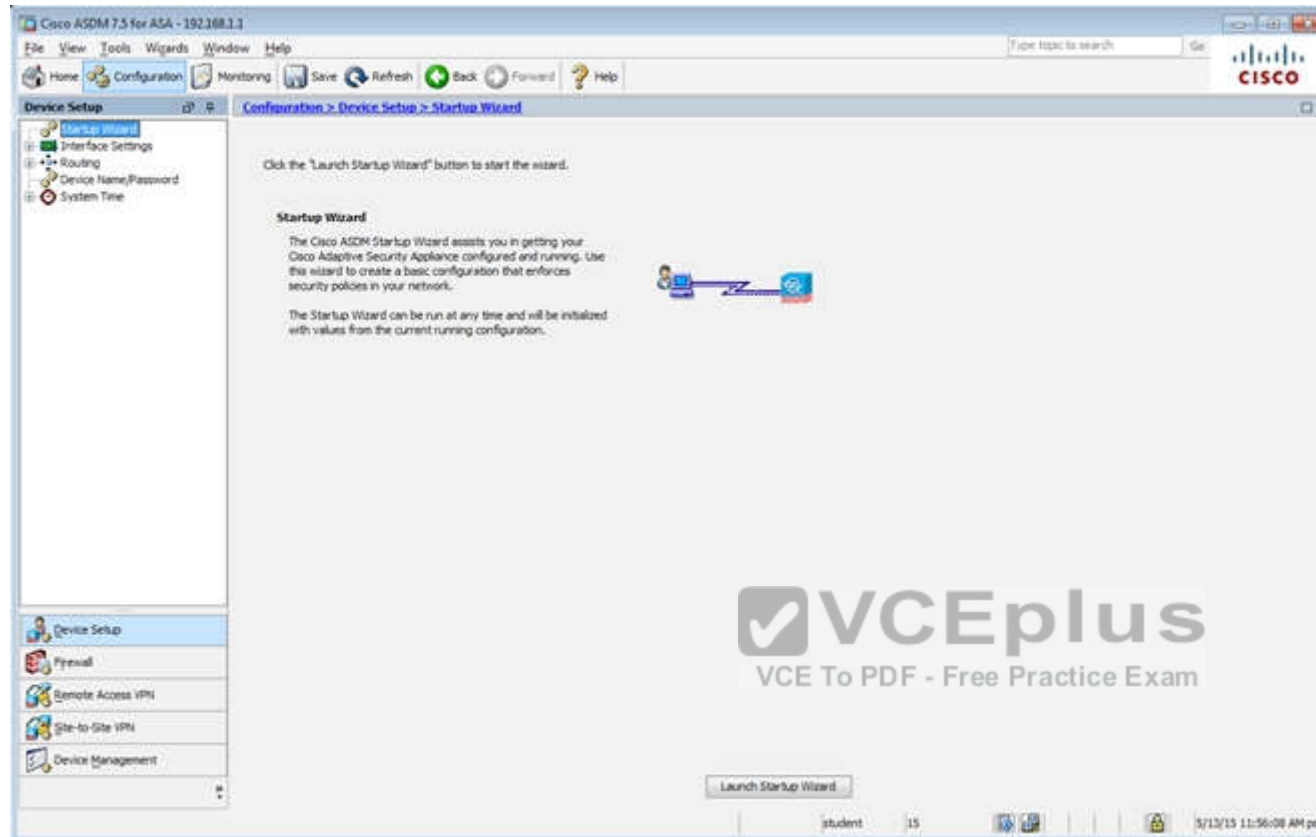
Filter By: Phase Site-to-Site -- All Sessions -- Filter

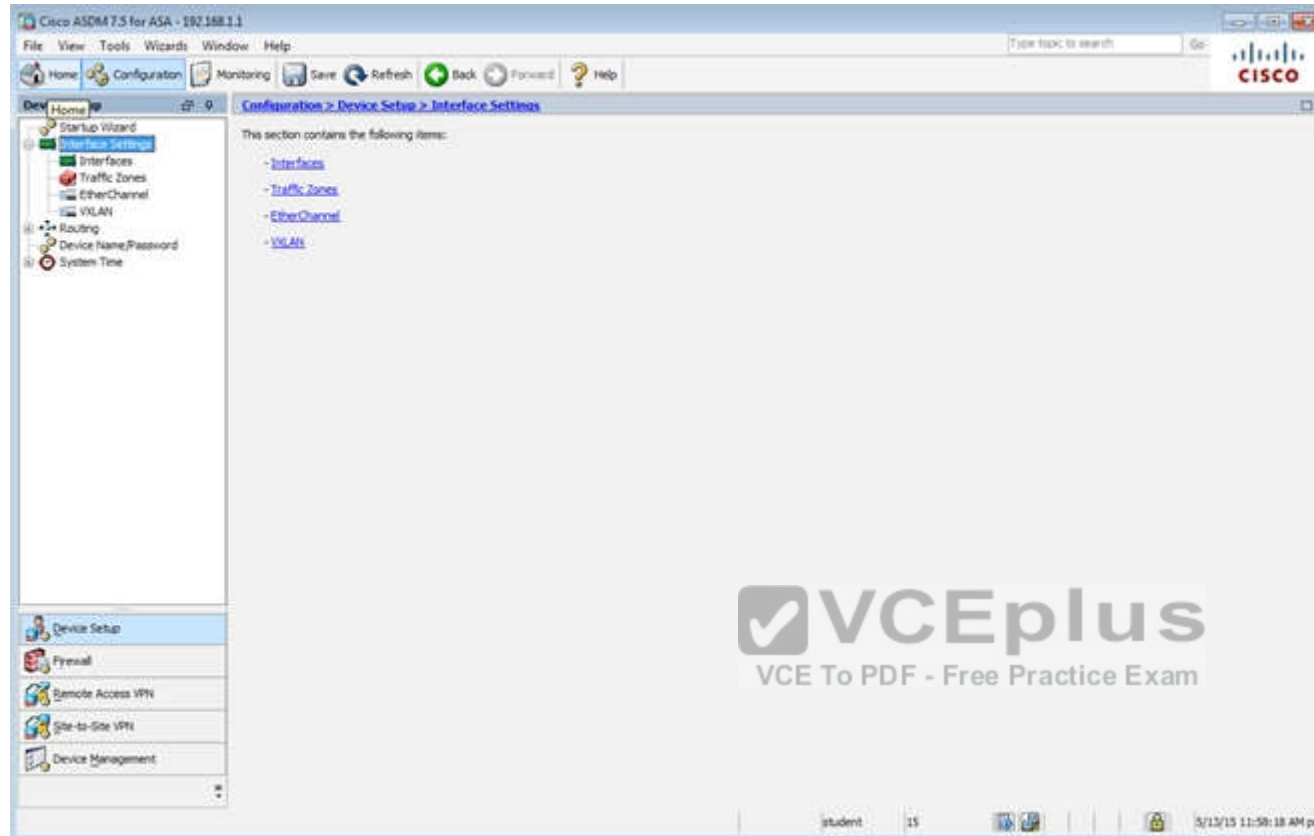
| Connection Profile | IP Address | Protocol | Encryption | Login Time | Duration | Bytes Tx | Bytes Rx | Cer Auth Int | Cer Auth Left |
|--|------------|----------|------------|------------|----------|----------|----------|--------------|---------------|
| <p>To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.</p> <p>Logout By: -- All Sessions -- Logout Sessions</p> <p>Refresh</p> <p>Last Updated: 5/19/15 9:33:12 AM</p> | | | | | | | | | |

Data Refreshed Successfully.

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

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

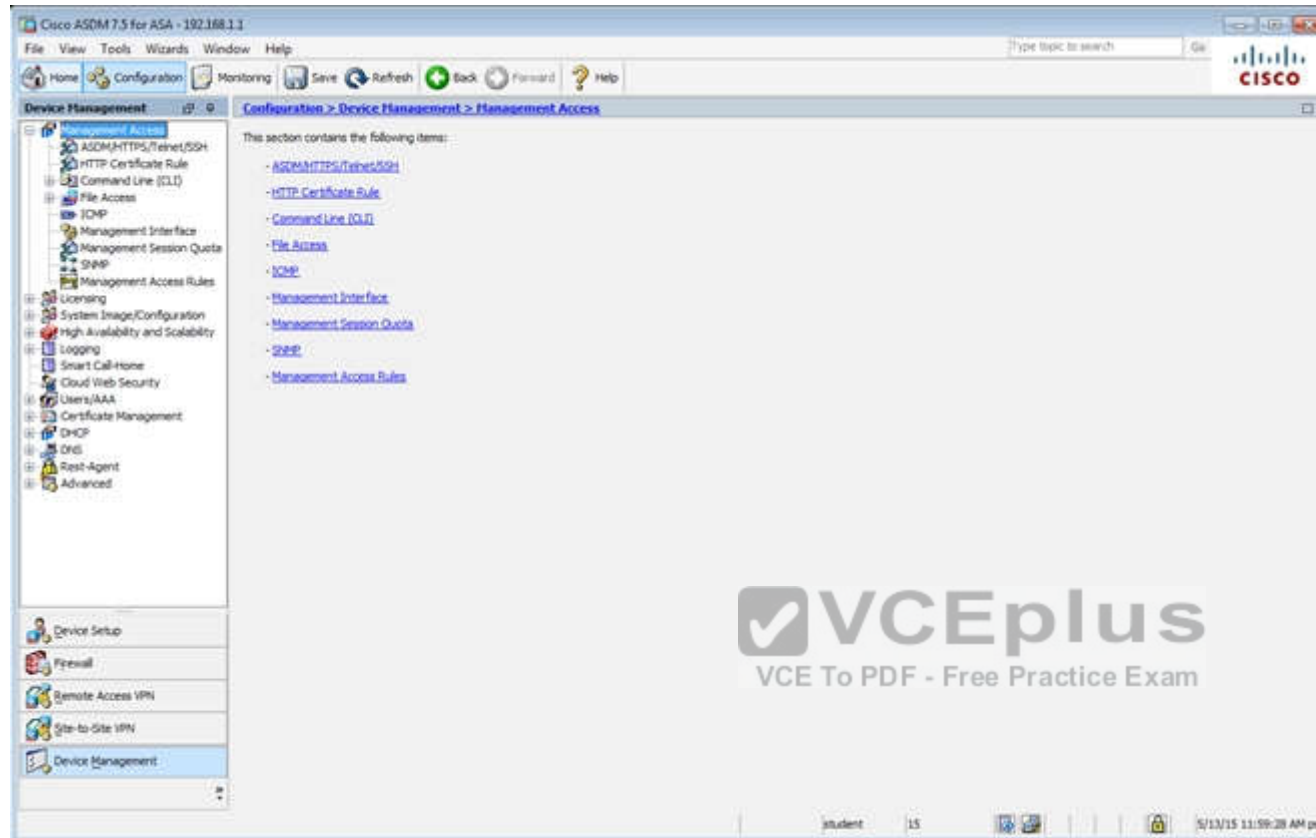
Device Setup

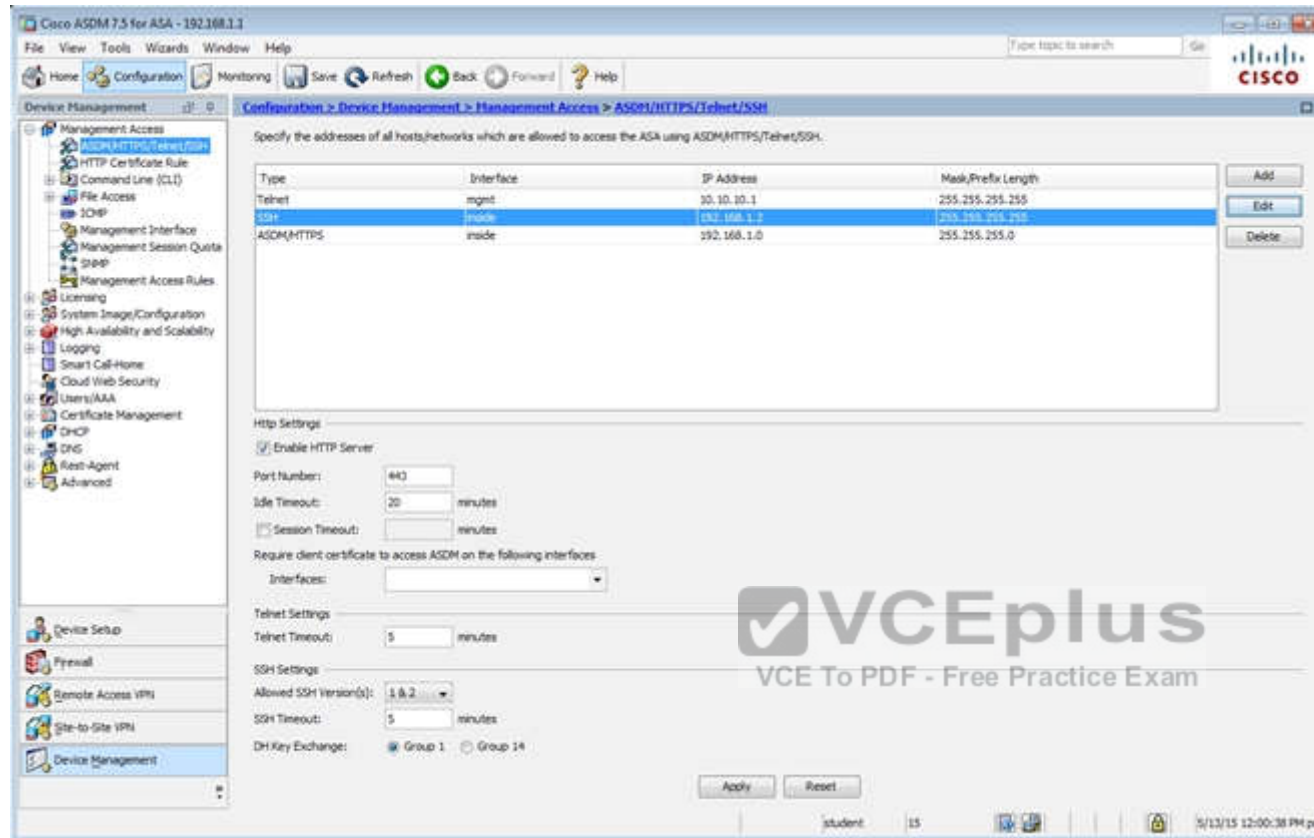
Configuration > Device Setup > Interface Settings > Interfaces

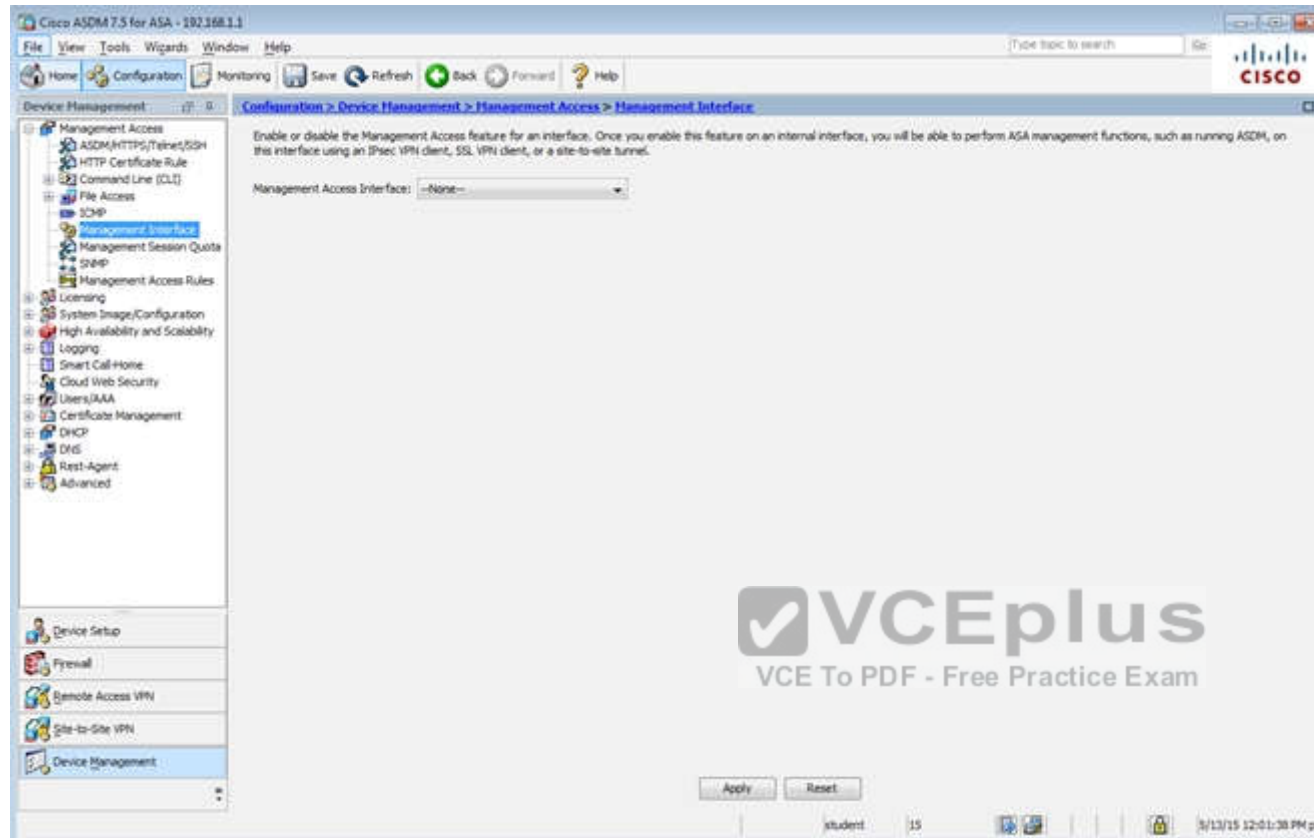
| Interface | Name | Zone | Route Map | State | Security Level | IP Address | Subnet Mask Prefix Length | Group | Type |
|--------------------|---------|------|-----------|---------|----------------|-----------------|---------------------------|-------|----------|
| GigabitEthernet0/0 | outside | | | Enabled | | 0.0.0.0/0.0.0.0 | 255.255.255.0 | | Hardware |
| GigabitEthernet0/1 | inside | | | Enabled | | 100.292.168.1.1 | 255.255.255.0 | | Hardware |
| GigabitEthernet0/2 | dmz | | | Enabled | | 172.16.1.1 | 255.255.255.0 | | Hardware |
| GigabitEthernet0/3 | | | | Enabled | | | | | Hardware |
| GigabitEthernet0/4 | | | | Enabled | | | | | Hardware |
| GigabitEthernet0/5 | mgmt | | | Enabled | | 100.10.10.10.2 | 255.255.255.0 | | Hardware |
| Management0/0 | | | | Enabled | | | | | Hardware |

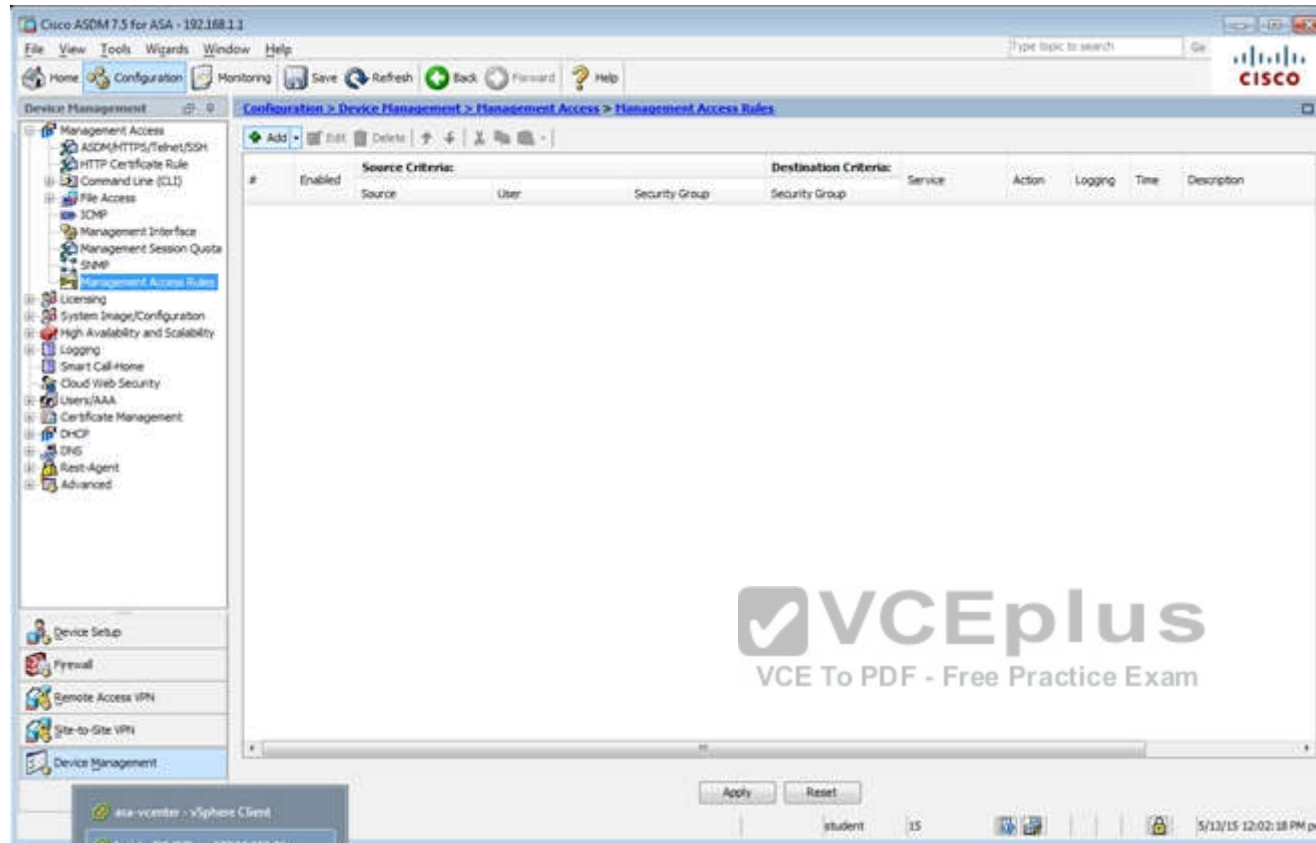
☐ Enable traffic between two or more interfaces which are configured with same security levels
☐ Enable traffic between two or more hosts connected to the same interface
☐ Enable jumbo frame reservation

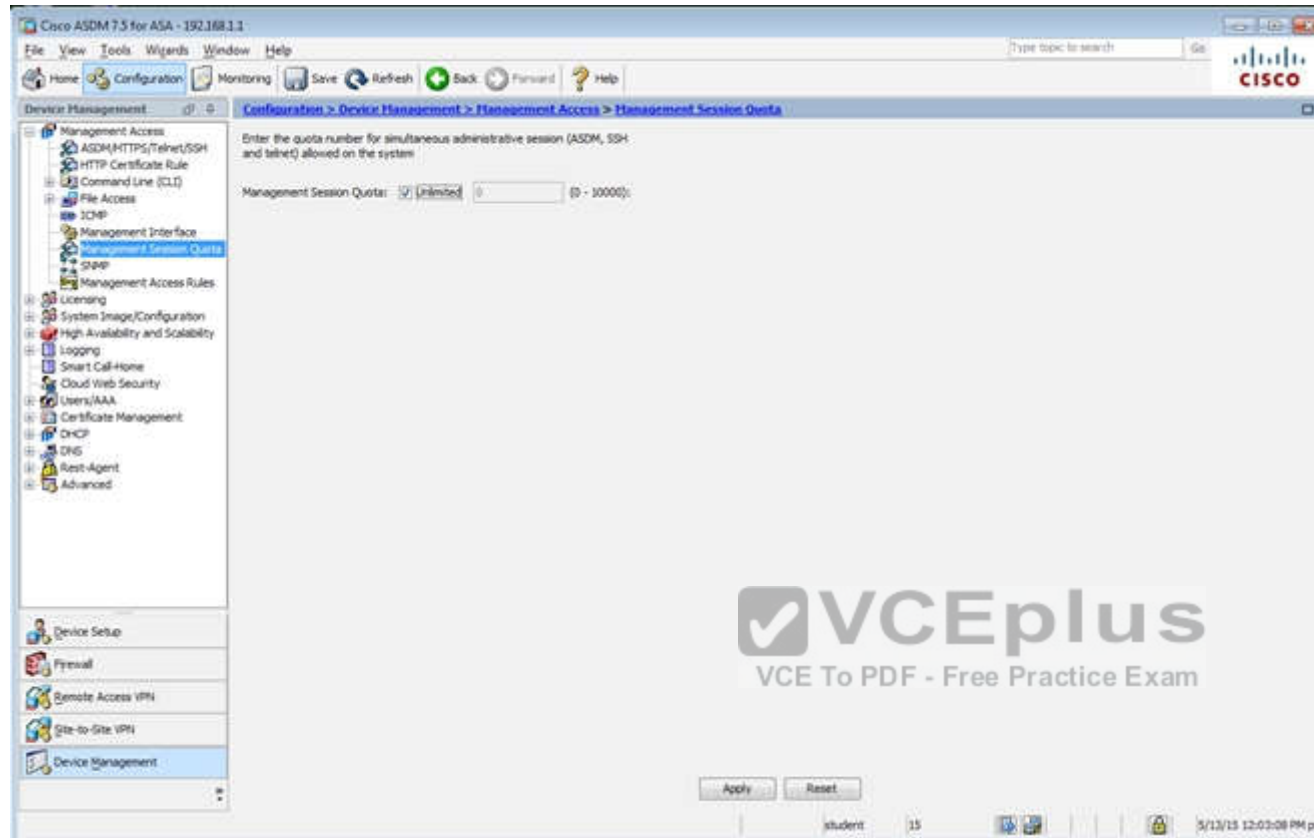
student 15 5/13/15 12:42:48 PM pst

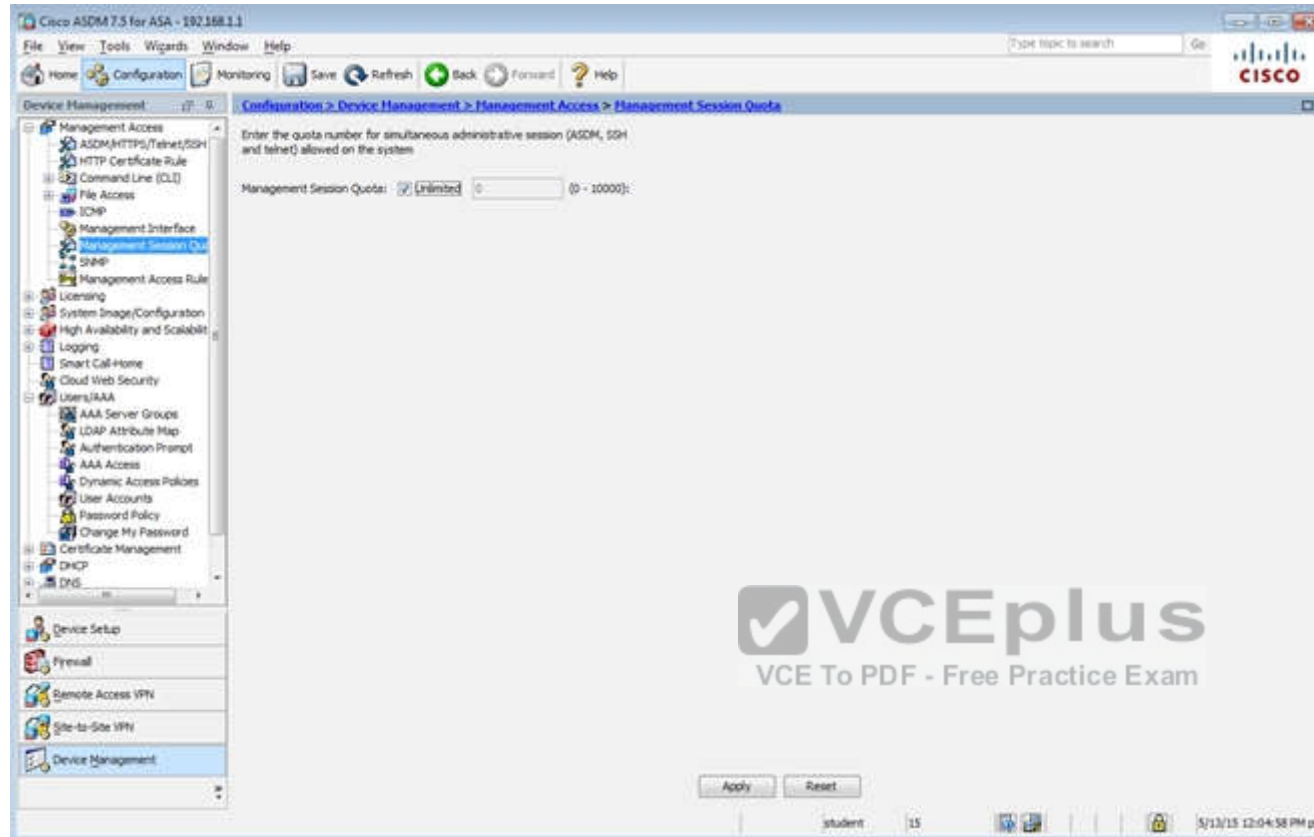


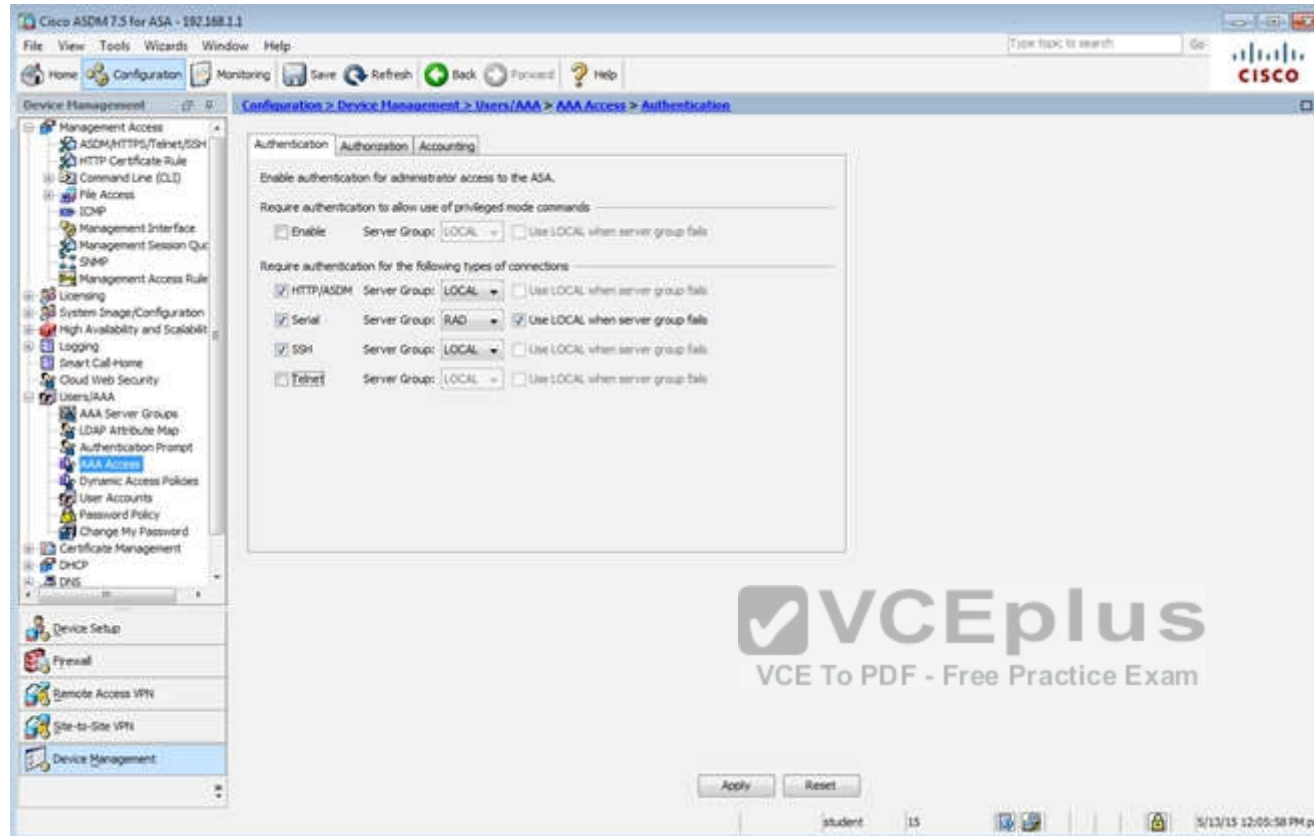


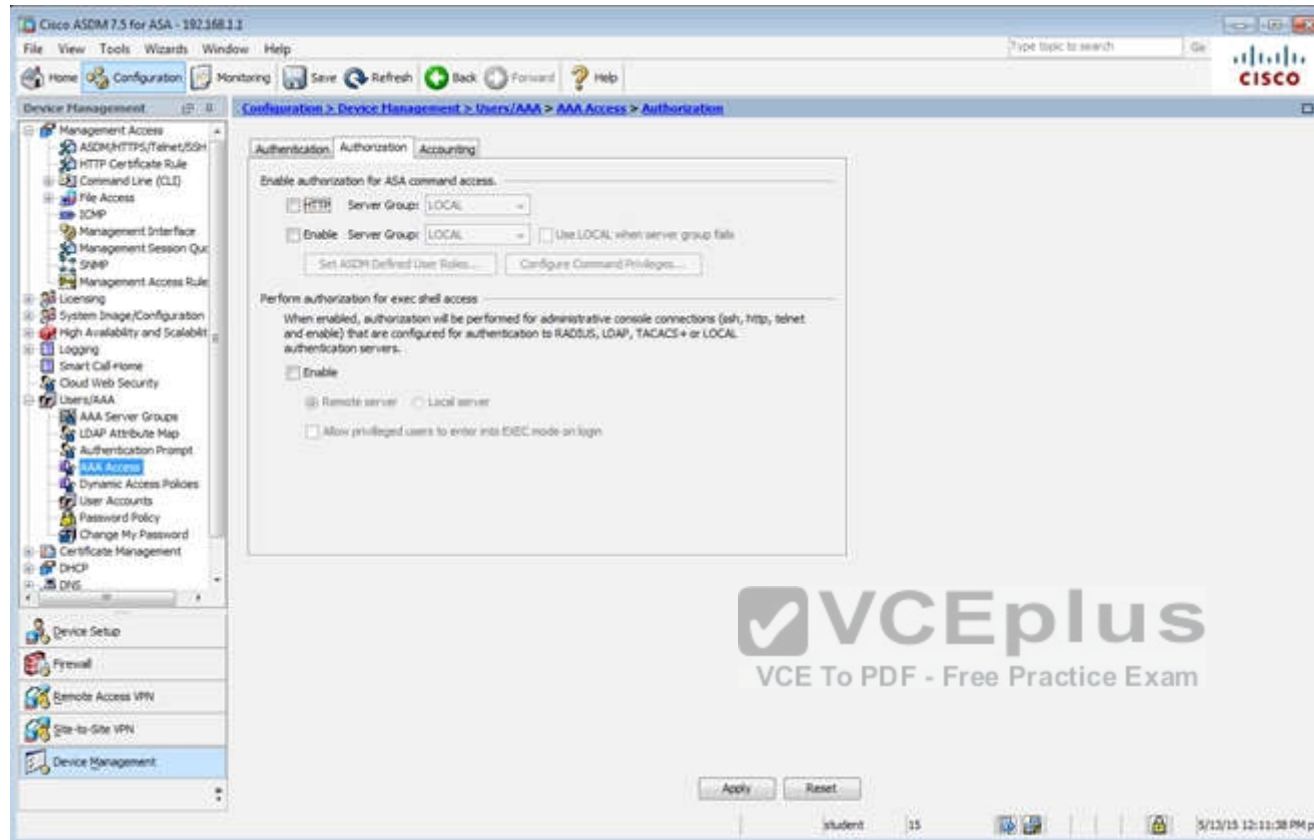


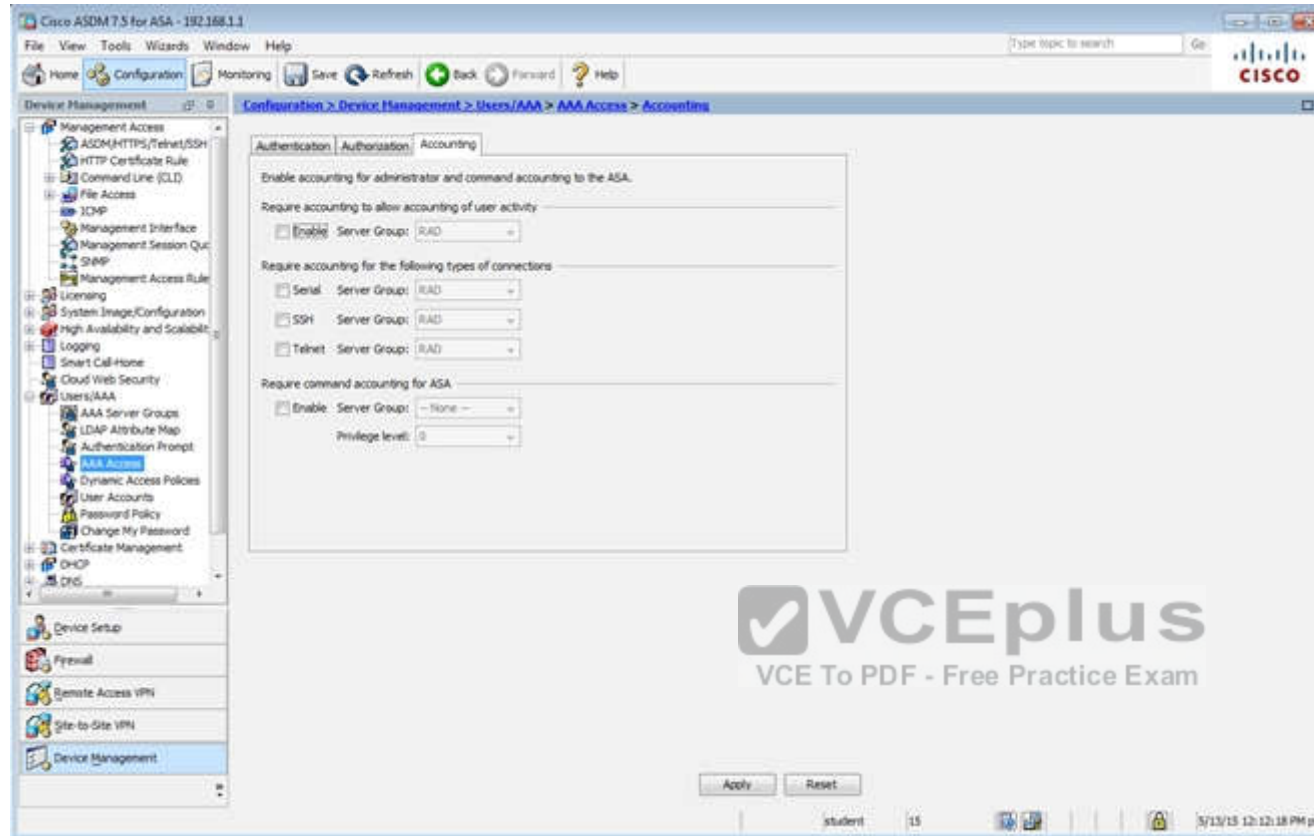












Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

AAA Server Groups

| Server Group | Protocol | Accounting Mode | Reactivation Mode | Dead Time | Max Failed Attempts |
|--------------|----------|-----------------|-------------------|-----------|---------------------|
| LOCAL | LOCAL | | | | |
| myAD | RADIUS | Single | Depletion | 10 | 3 |
| myCD4 | RADIUS | Single | Depletion | 10 | 3 |

Find: Match Case

Servers in the Selected Group

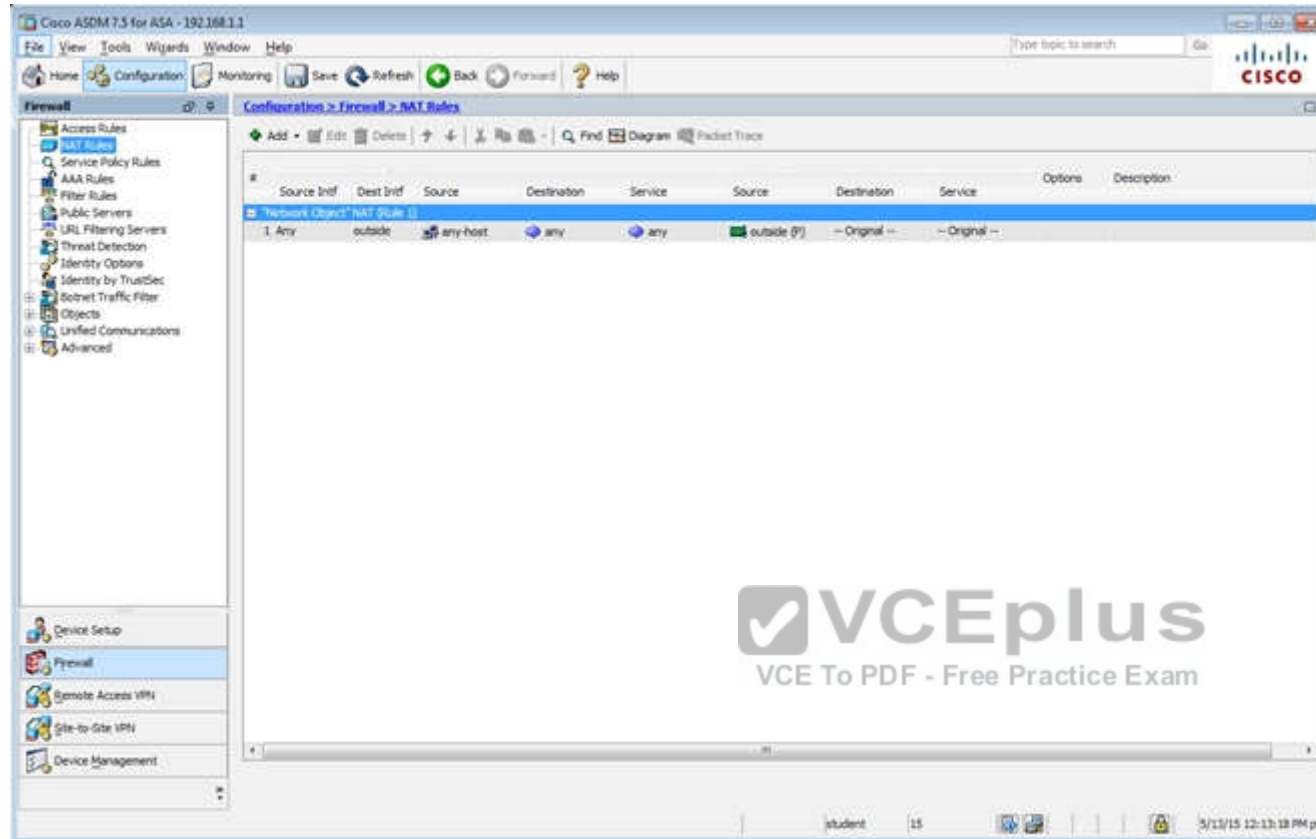
| Server Name or IP Address | Interface | Timeout |
|---------------------------|-----------|---------|
| 192.168.1.100 | inside | 10 |

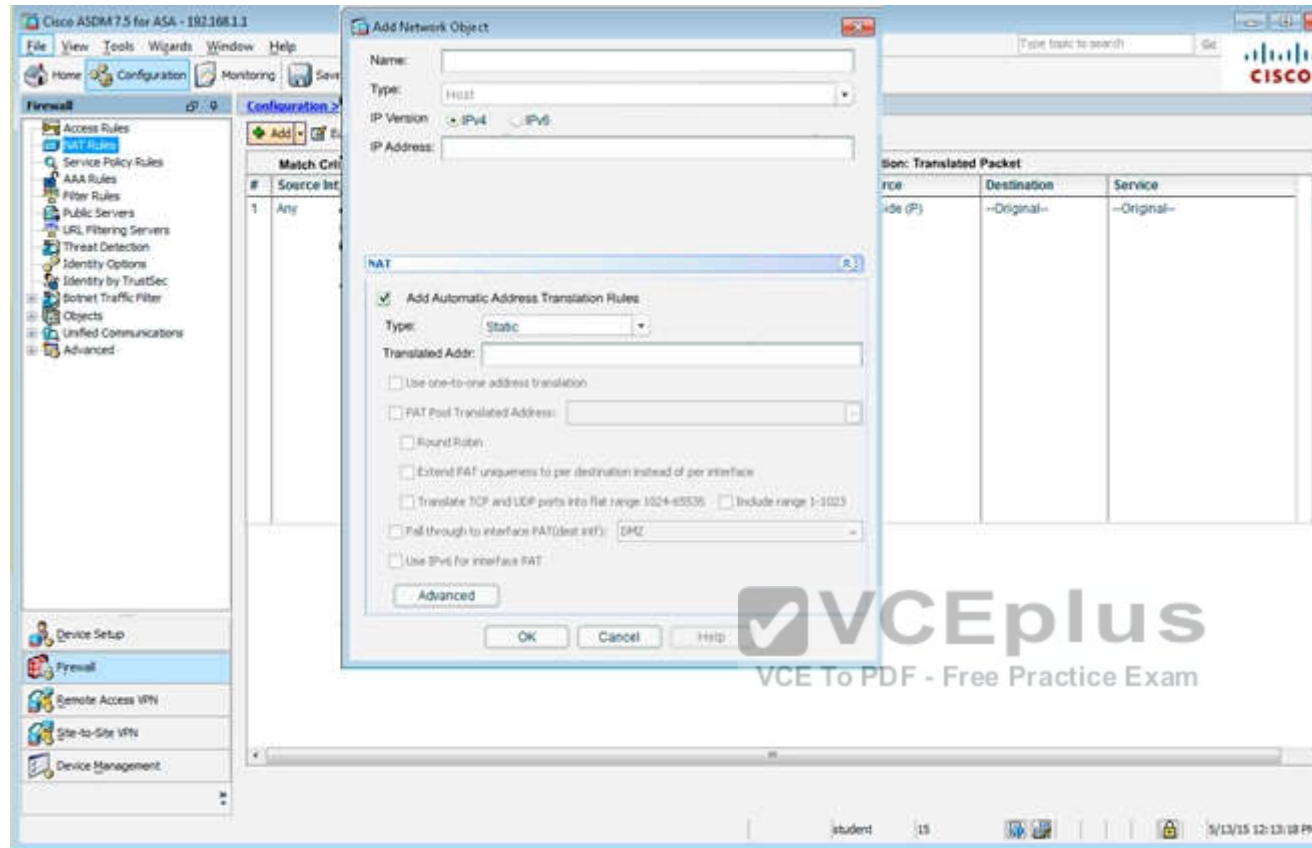
Find: Match Case



LDAP Attribute Map

Apply Reset

student 15 3/13/15 12:16:58 PM pst





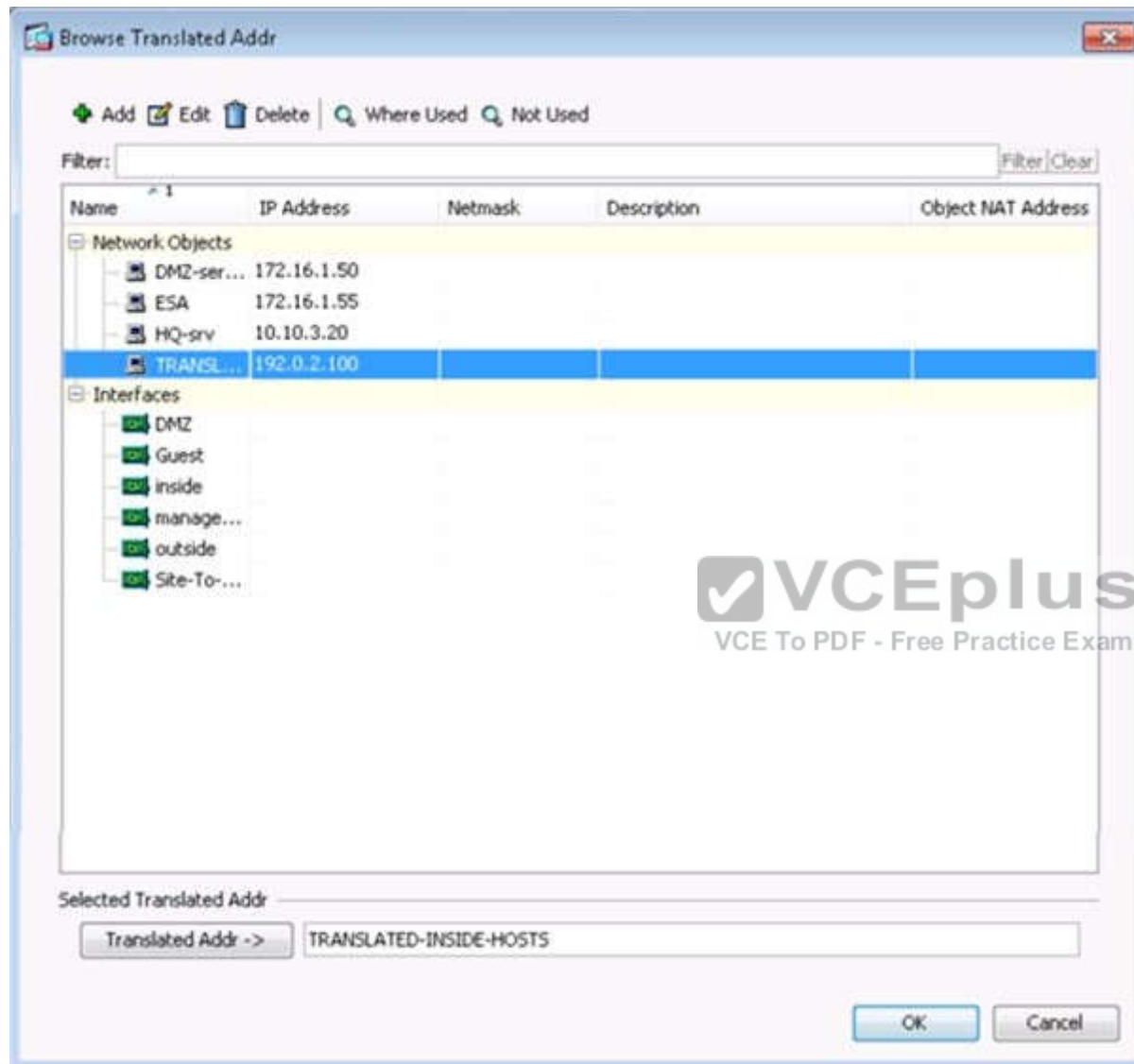
 Advanced NAT Settings 

Translate DNS replies for rule

Interface _____

Source Interface: _____

Destination Interface: _____



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall

Configuration > Firewall > Objects > Local Users

Create entries in the ASA local user database.

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

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

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

Add Edit Delete

Ends: Match Case

Apply Reset

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

Cisco ASDM 7.3 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall 27 0 Configuration > Firewall > Objects > Network Objects/Groups

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

Filter: [] Filter (Clear)

| Name | IP Address | Network | 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 | | |

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

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall (0)

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 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

Configuration > Firewall > Service Policy Rules

Add Edit Delete Find Diagram Packet Trace

| Name | # | Enabled | Match | Source | Src Security Group | Destination | Dest Security Group | Service | Time | Rule Actions | Describe |
|--|---|---------|-------|--------|--------------------|-------------|---------------------|-------------------|------|---------------------------|--------------|
| Interface: dmz; Policy: dmz_policy | | | | | | | | | | | |
| class-default | | | Match | any | | any | | any traffic | | | |
| | | | | | | | | class-default | | | |
| Interface: inside; Policy: inside_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 SMTP |

student 15 5/13/15 12:15:48 PM pst

 Edit Service Policy Rule ✕


Traffic Classification Default Inspections Rule Actions

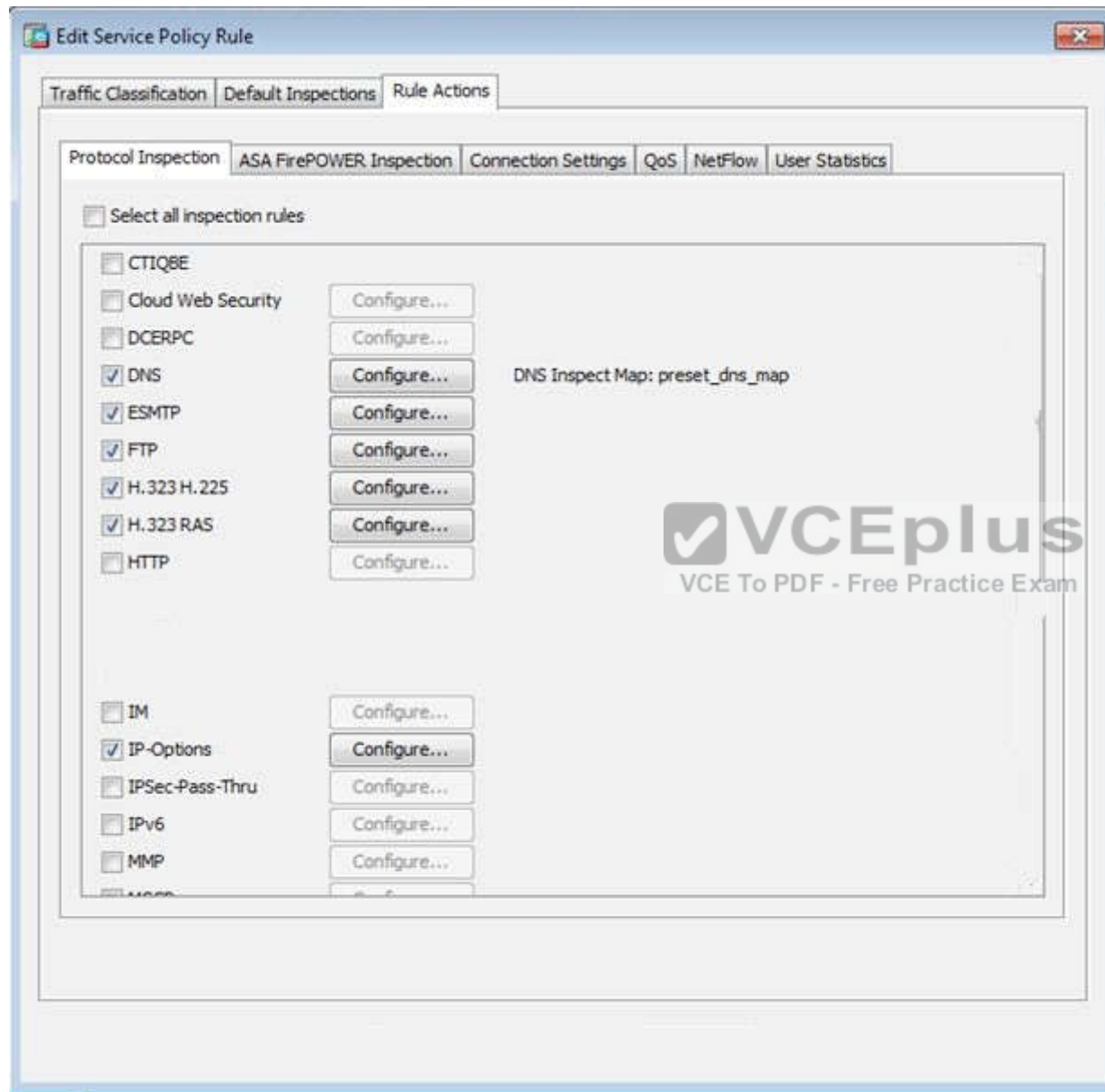
Name: inspection_default

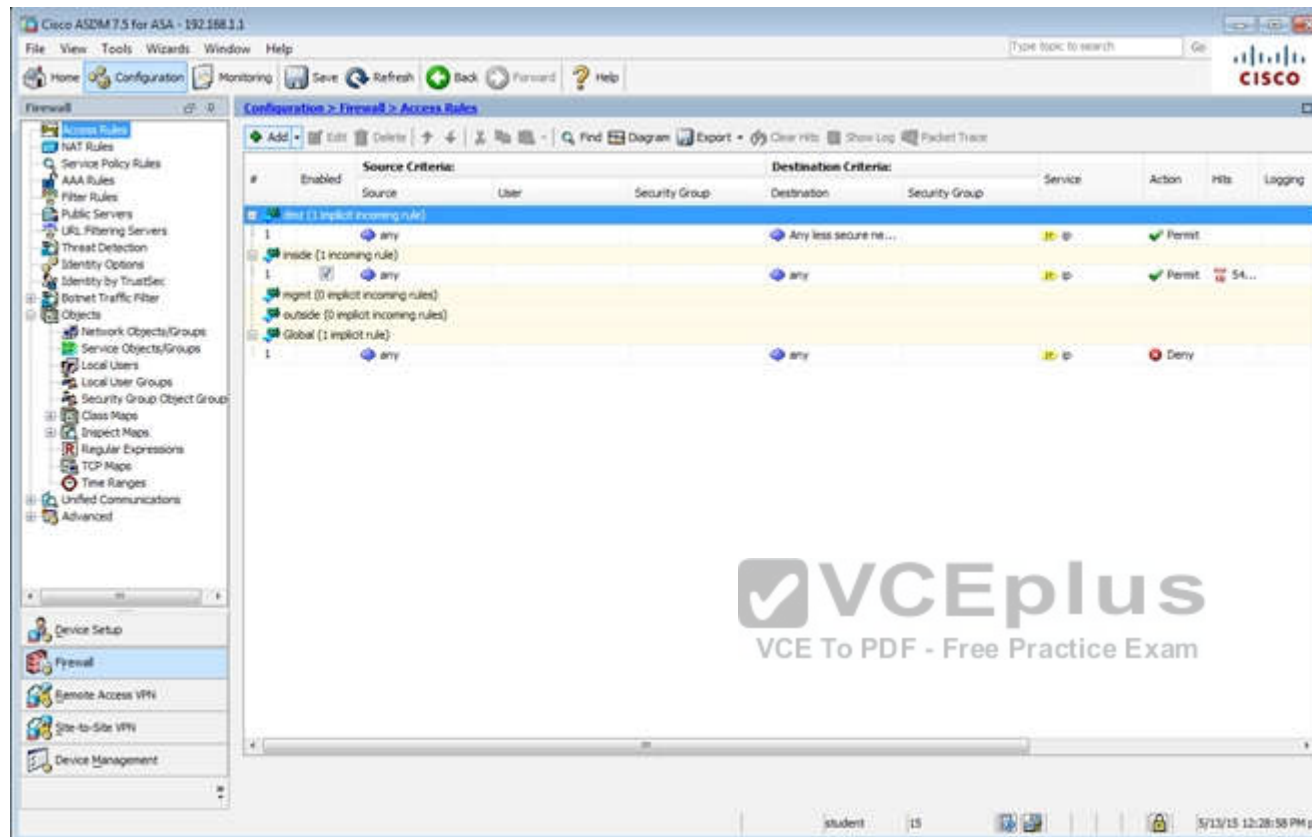
Description (optional):

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

 **VCEplus**
VCE To PDF - Free Practice Exam







Add Access Rule


Interface:

Action:

Source Criteria

Source: 

User: 

Security Group: 

Destination Criteria

Destination:


Security Group:

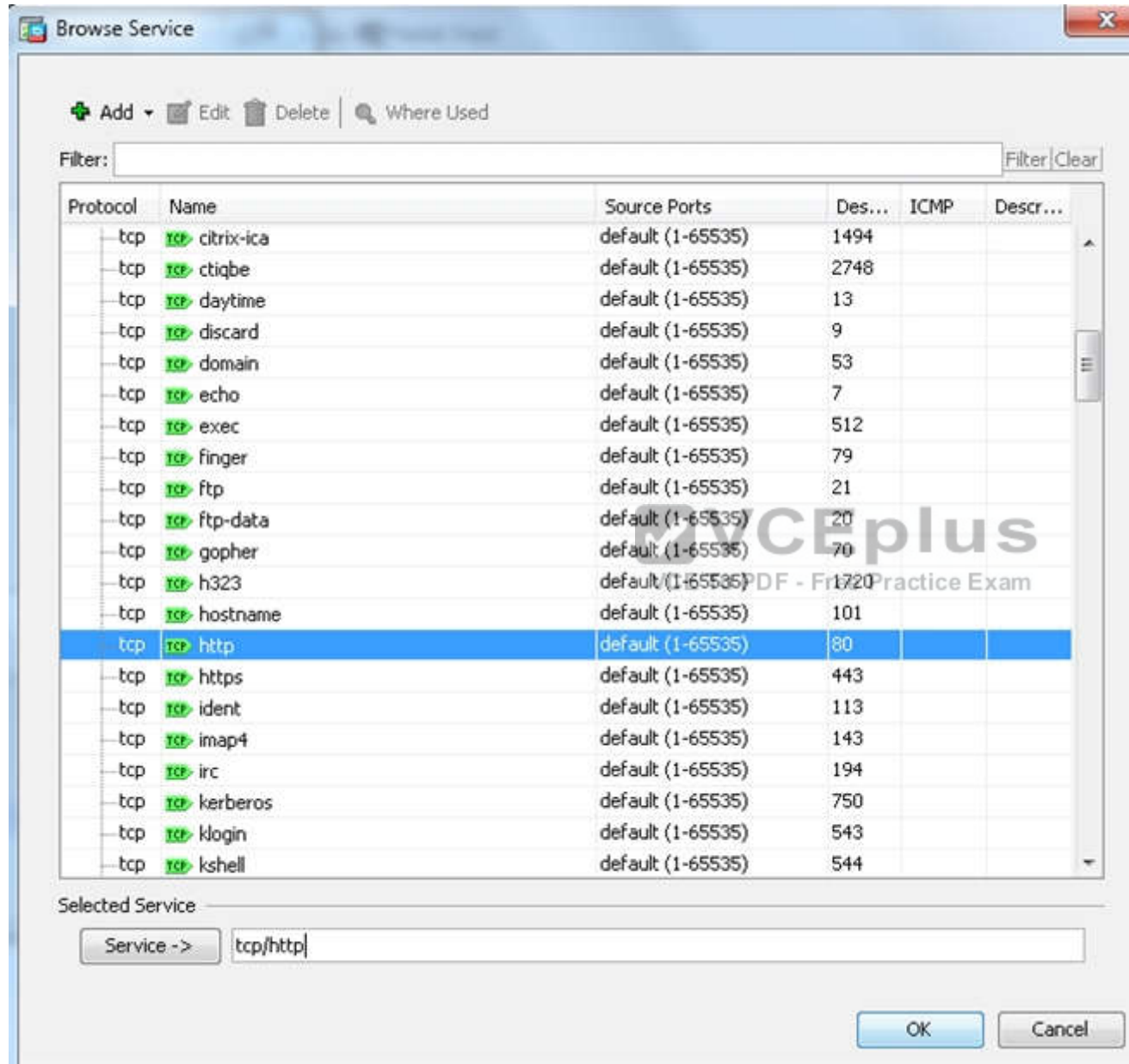
Service:

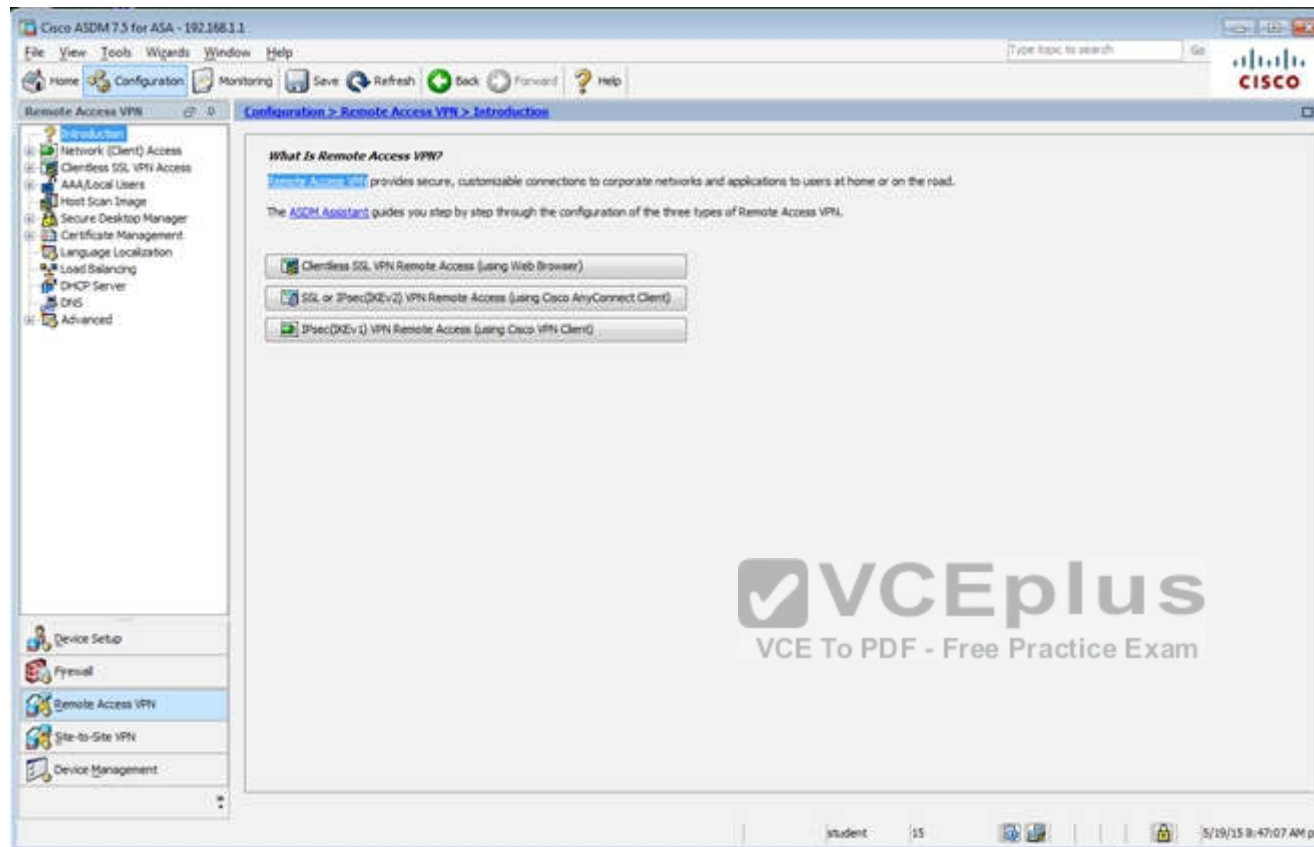
Description:

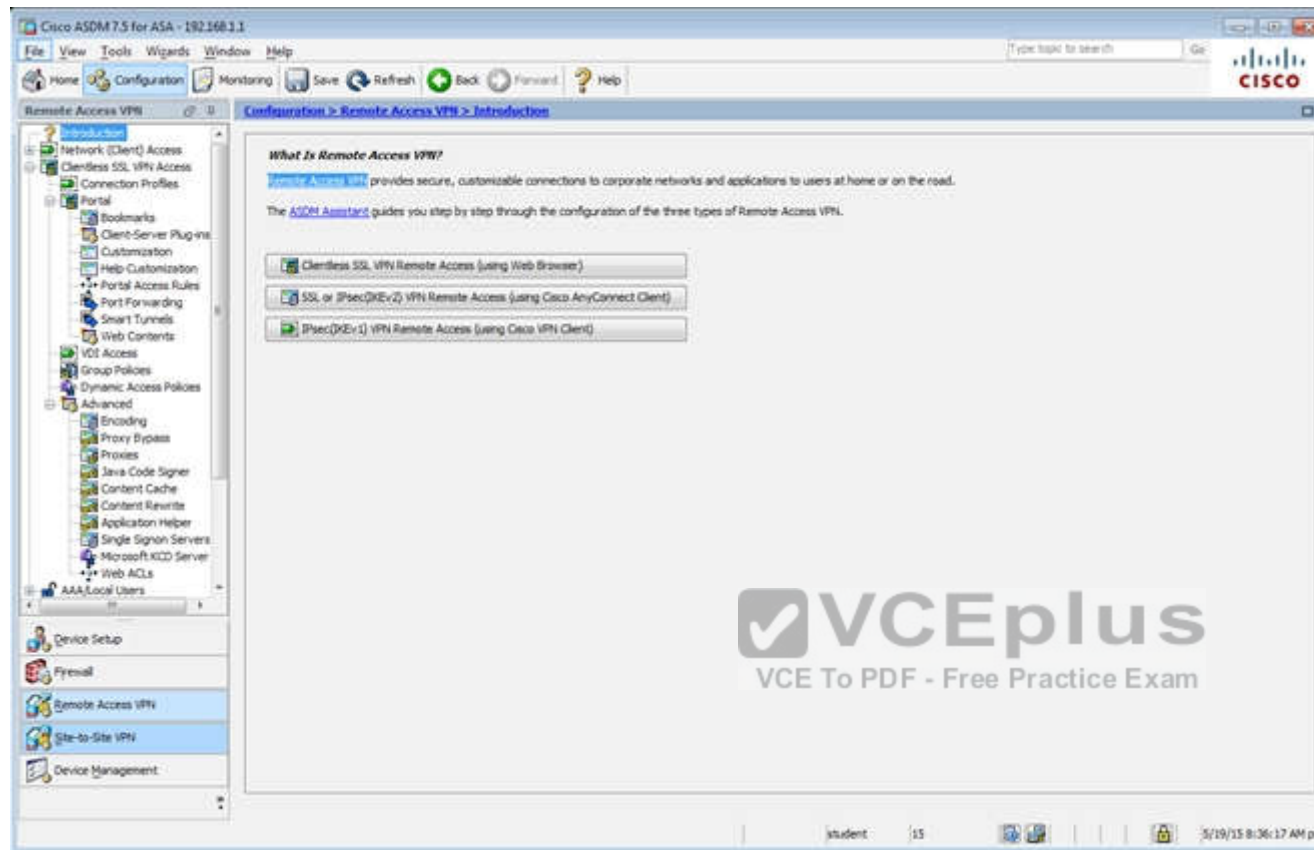
☒ Enable Logging

Logging Level:

More Options 







Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

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

Access Interfaces

Enable interfaces for clientless SSL VPN access.

| Interface | Allow Access |
|-----------|-------------------------------------|
| outside | <input checked="" type="checkbox"/> |
| dns | <input type="checkbox"/> |
| inside | <input type="checkbox"/> |

Device Certificate ...
Port Setting ...

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

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

☐ Shutdown portal login page.

Connection Profiles

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

Add Edit Delete Find: Match Case

| Name | Enabled | Aliases | Authentication Method | Group Policy |
|--------------------|-------------------------------------|---------|-----------------------|---------------|
| DefaultRAGroup | <input checked="" type="checkbox"/> | | AAA(RADIUS) | DefaultPolicy |
| DefaultWEBVpnGroup | <input checked="" type="checkbox"/> | | AAA(RADIUS) | DefaultPolicy |
| Clientless | <input checked="" type="checkbox"/> | test | AAA(RADIUS) | DefaultPolicy |

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

Apply Reset

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

Edit Clientless SSL VPN Connection Profile: clientless

Basic
Advanced

Name: clientless
Aliases: test

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

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

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

Find: ☐ Next ☐ Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

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

Login and Logout Page Customization: DfltCustomization Manage...

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

☐ Enable the display of SecurId messages on the login screen

Connection Aliases

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

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

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

Group URLs

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

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

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

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

☒ Always run CSD

☐ Disable CSD for both AnyConnect and Clientless SSL VPN

☐ Disable CSD for AnyConnect only

Find: Next Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

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

Interface-Specific Authentication Server Groups

+ Add Edit Delete

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

Username Mapping from Certificate

☐ Pre-fill Username from Certificate

☐ Hide username from end user

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

☐ Use the entire DN as the username

☐ Use script to select username

-- None -- + Add Edit Delete

Find: Next Previous

OK Cancel Help



Edit Clientless SSL VPN Connection Profile: clientless

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

Secondary Authentication Server Group

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

☐ Use LOCAL if Server Group fails

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

Attributes Server: ☒ Primary ☐ Secondary

Session Username Server: ☒ Primary ☐ Secondary

Interface-Specific Secondary Authentication Server Groups

+ Add Edit Delete

| Interface | Server Group | Fallback to LOCAL | Use primary username |
|-----------|--------------|-------------------|----------------------|
|-----------|--------------|-------------------|----------------------|

Username Mapping from Certificate

☐ Pre-fill username from certificate

☐ Hide username from end user

☐ Fallback when a certificate is unavailable

Password: ☒ Prompt ☐ Use primary ☐ Use

☒ Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

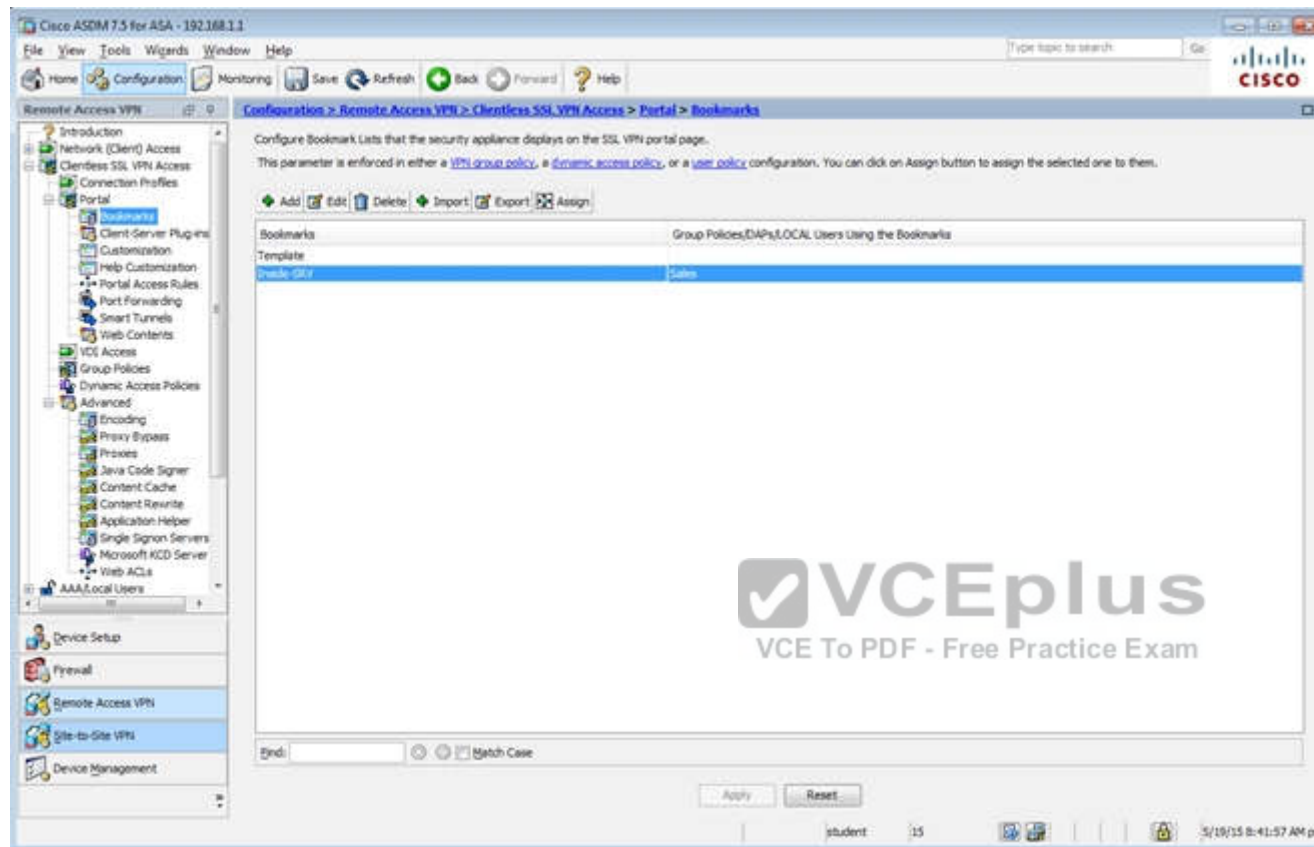
☐ Use the entire DN as the username

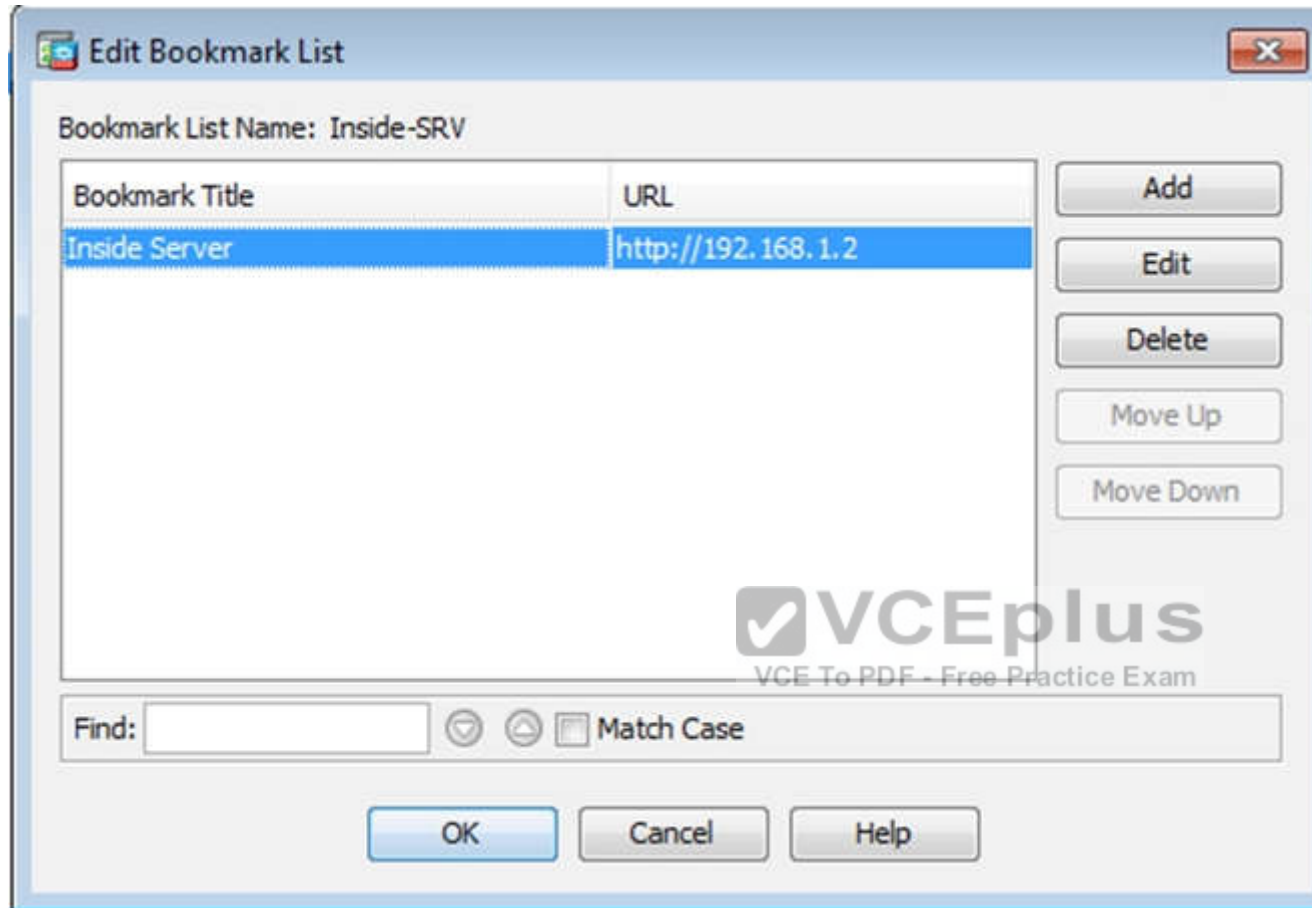
☐ Use script to select username

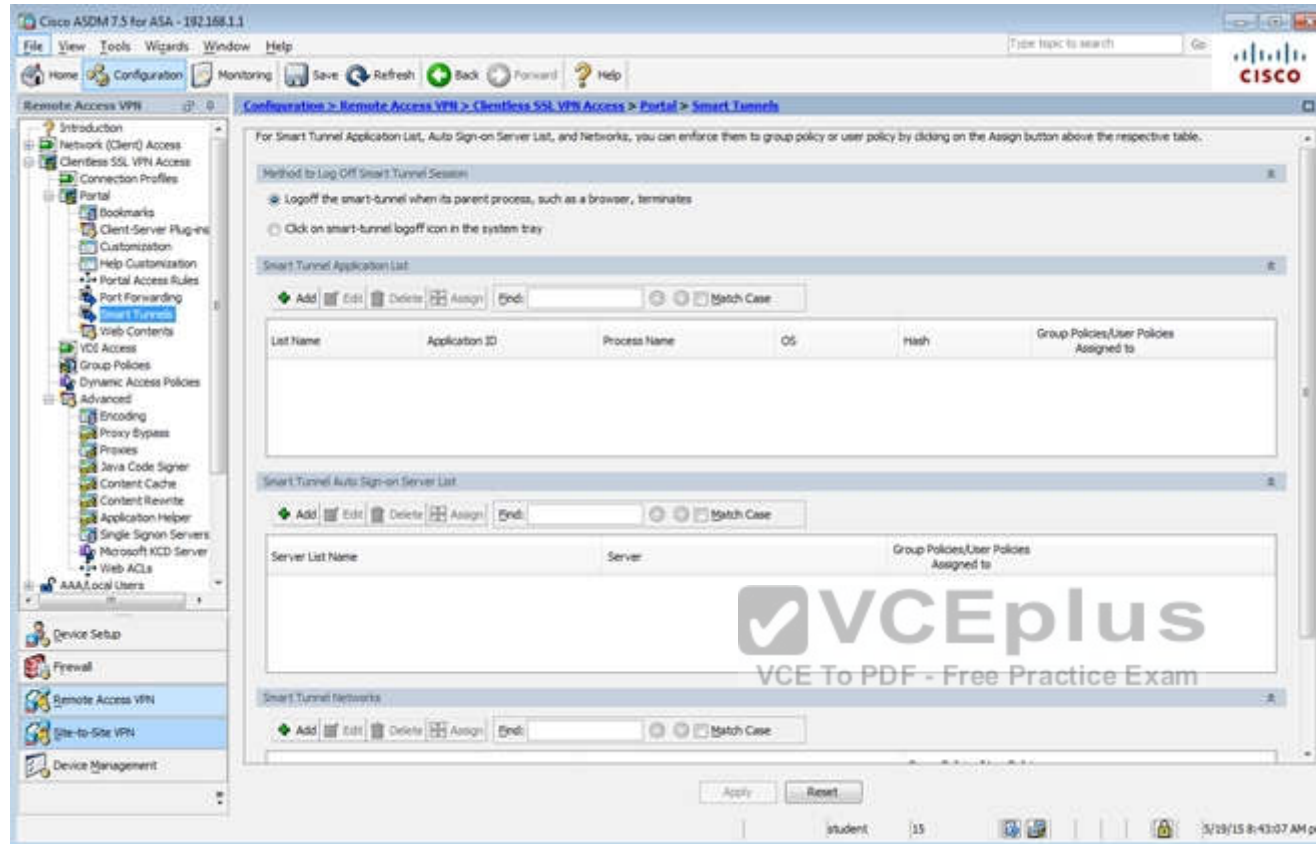
-- None -- + Add Edit Delete

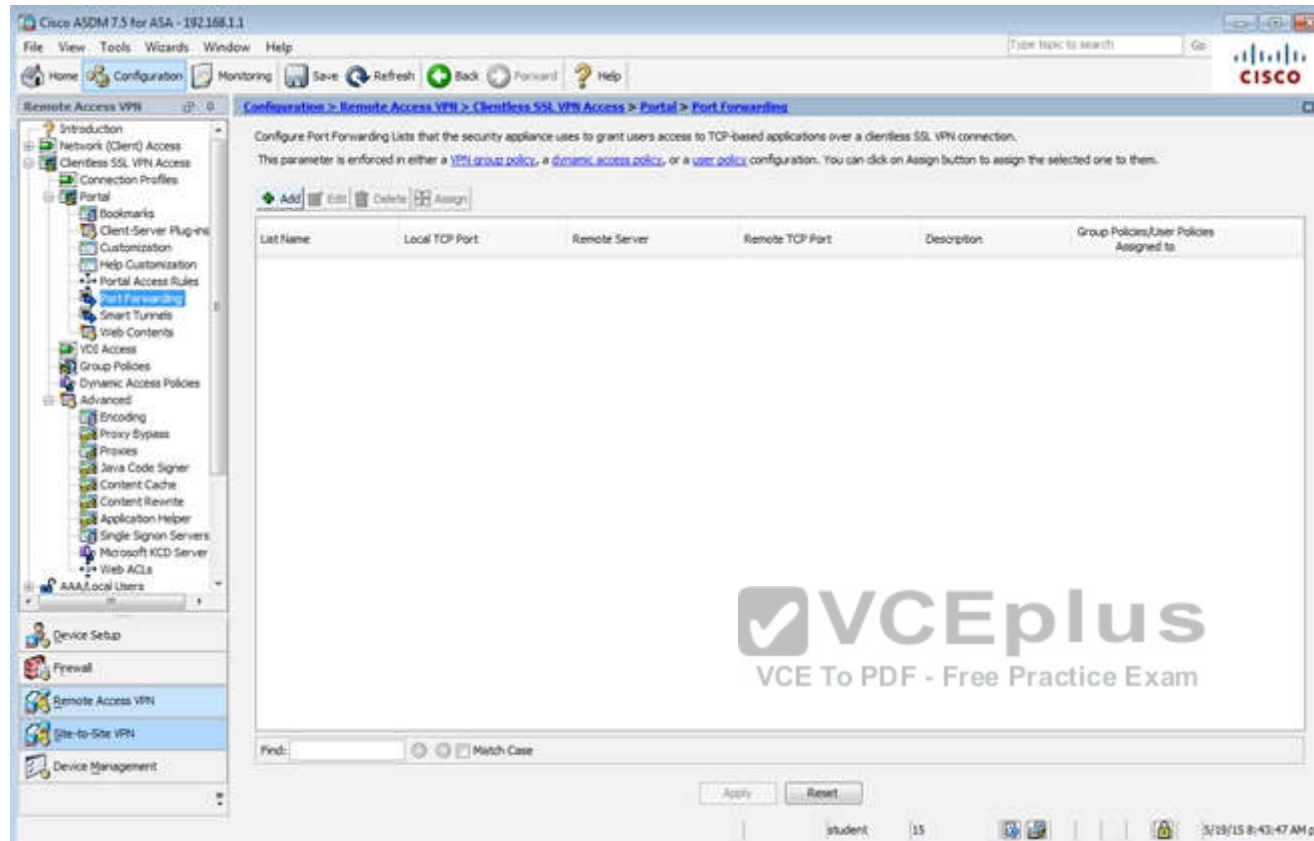
Find: ☒ Next ☐ Previous

OK Cancel Help









Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Clientless SSL VPN Access > 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 |
|--------------------------------|----------|------------------------------------|--|
| Salvo | Internal | ssl-clientless | Clientless |
| DiffGrpPolicy (System Default) | Internal | kev1:kev2:ssl-clientless/2tp-ipsec | DefaultRAGroup/DefaultL3Group/DefaultADMG/Def... |

End: Match Case

Apply Reset

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

Edit Internal Group Policy: Sales

Name: Sales

Banner: ☒ Inherit

More Options

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

Web ACL: ☒ Inherit Manage...

Access Hours: ☒ Inherit Manage...

Simultaneous Logins: ☒ Inherit

Restrict access to VLAN: ☒ Inherit

Connection Profile (Tunnel Group) Lock: ☒ Inherit

Maximum Connect Times: ☒ Inherit ☐ Unlimited minutes

Idle Timeout: ☒ Inherit ☐ Use Global Default minutes

Timeout Alerts

Session Alert Interval: ☒ Inherit ☐ Default minutes

Idle Alert Interval: ☒ Inherit ☐ Default minutes

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

Find: ☒ Next ☐ Previous

OK Cancel Help

Cisco ASDM 7.2 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

- Presecurity Connection
- Secure Mobility Solution
- Address Assignment
- Advanced
- Clientless SSL VPN Access
- Connection Profiles
- Portal
- Bookmarks
- Client-Server Plug-ins
- Customization
- Help Customization
- Portal Access Rules
- Port Forwarding
- Smart Tunnels
- Web Contents
- VDC Access
- Group Policies
- Dynamic Access Policies
- Advanced
- AAA Local Users
- AAA Server Groups
- LDAP Attribute Map
- Local Users
- Host Scan Image
- Secure Desktop Manager

Device Setup

Firewall

Remote Access VPN

Site-to-Site VPN

Device Management

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

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

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

| Name | Type | Tunneling Protocol | Connection Profiles/Users Assigned To |
|--------------------------------|----------|--------------------------------------|---------------------------------------|
| Default | Internal | ssl-clientless | Default |
| DefaultPolicy (System Default) | Internal | ikev1/ikev2/ssl-clientless/2tp-ipsec | DefaultPolicy |

Find:

student 15 10/15/14 9:15:40 AM pet

Edit Internal Group Policy: Sales

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

Bookmark List: ☐ Inherit Manage...

URL Entry: ☒ Inherit ☐ Enable ☐ Disable

File Access Control

File Server Entry: ☒ Inherit ☐ Enable ☐ Disable

File Server Browsing: ☒ Inherit ☐ Enable ☐ Disable

Hidden Share Access: ☒ Inherit ☐ Enable ☐ Disable

Port Forwarding Control

Port Forwarding List: ☒ Inherit Manage...

☐ Auto Applet Download

Applet Name: ☒ Inherit

Smart Tunnel

Smart Tunnel Policy: ☒ Inherit Manage...

Tunnel Option: Manage...

Smart Tunnel Application: ☒ Inherit Manage...

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

☐ Auto Start

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

Windows Domain Name (optional):

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

ActiveX Relay

ActiveX Relay: ☒ Inherit ☐ Enable ☐ Disable

More Options

Find: ☐ Next ☐ Previous

OK Cancel Help

Edit Internal Group Policy: DfHGrpPolicy

Advanced

Name: DfHGrpPolicy

Banner:

SCP forwarding URL:

Address Pools: Select...

IPv6 Address Pools: Select...

More Options

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

Filter: -- None -- Manage...

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

Simultaneous Logins: 3

Restrict access to VLANs: -- Unrestricted --

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

Maximum Connect Time: ☒ Unlimited ☐ 1000/000

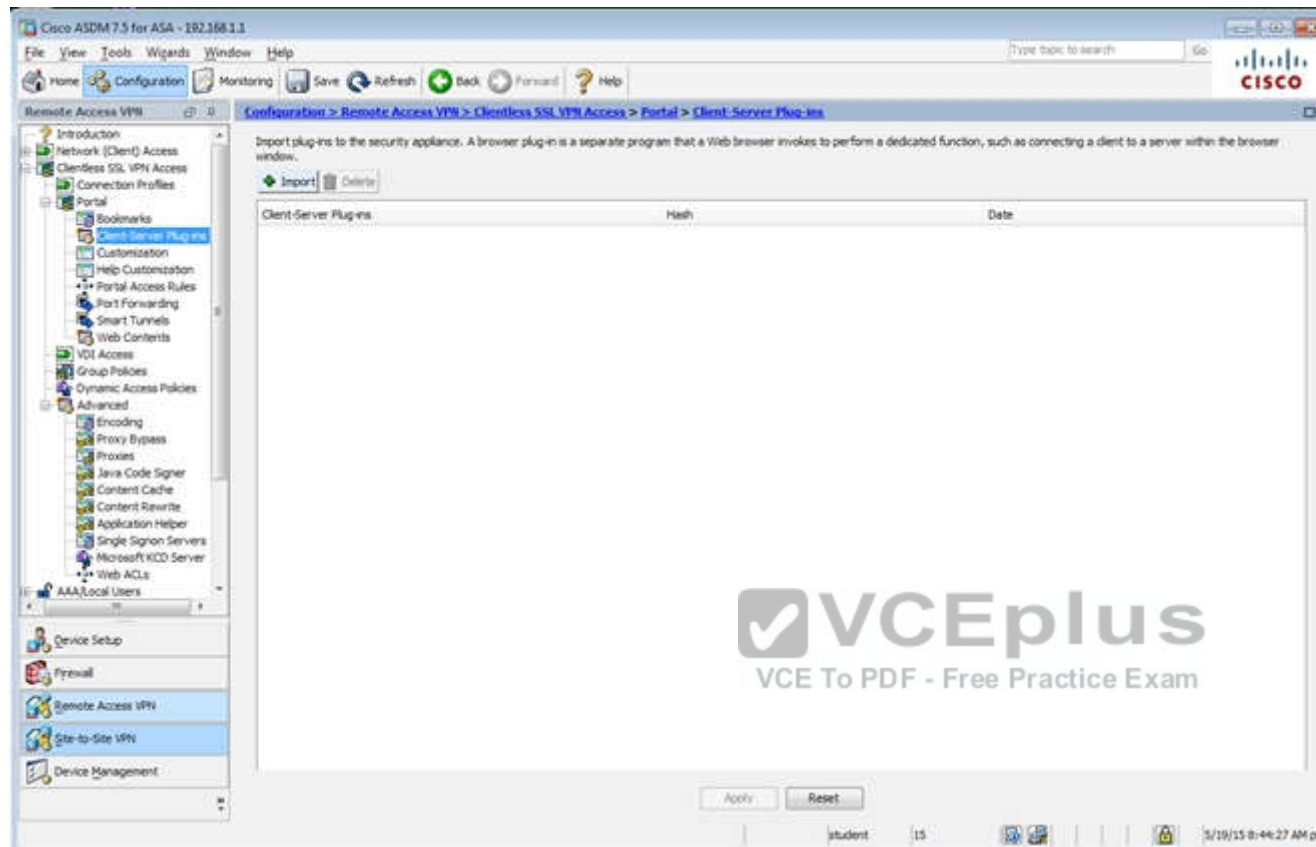
Idle Timeout: ☐ None minutes

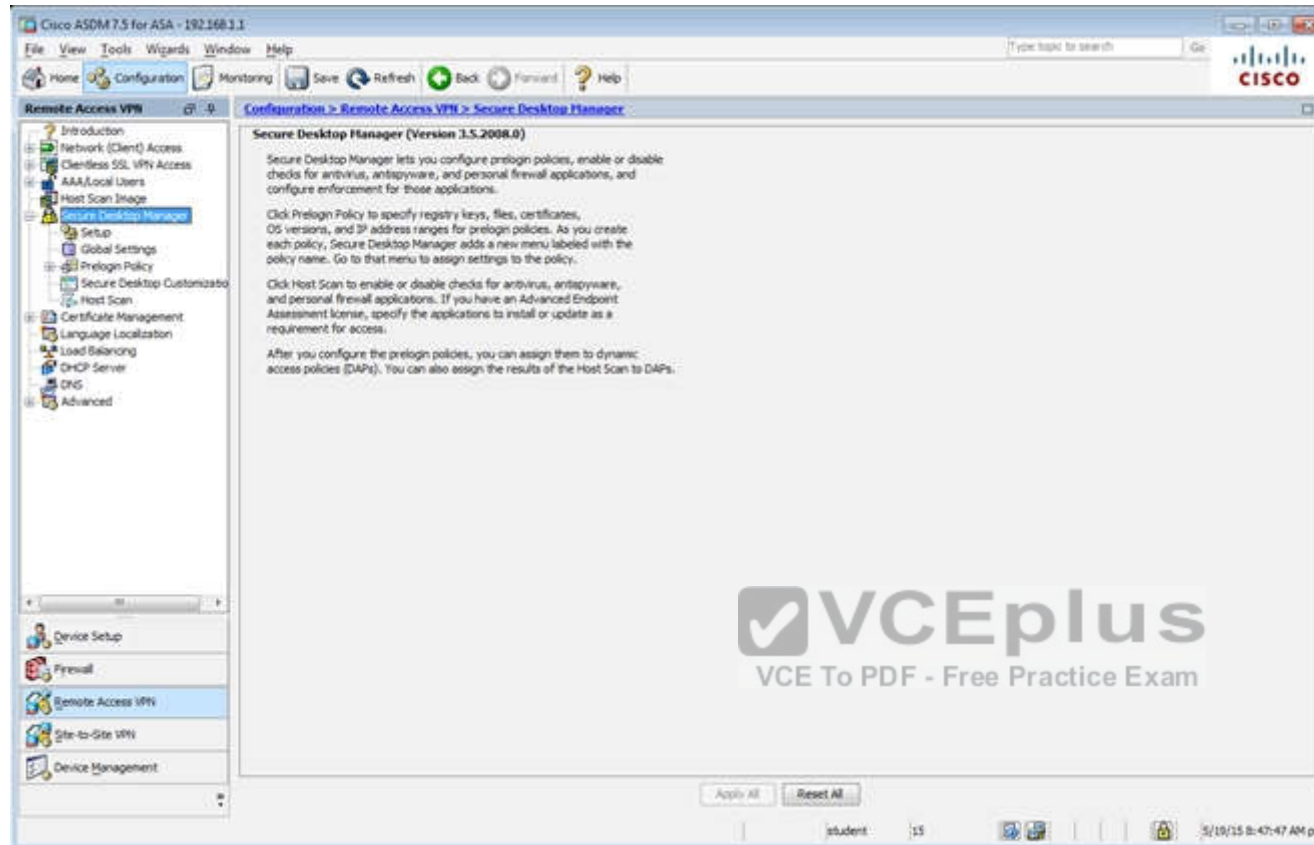
On smart card removal: ☒ Disconnect ☐ Keep the connection

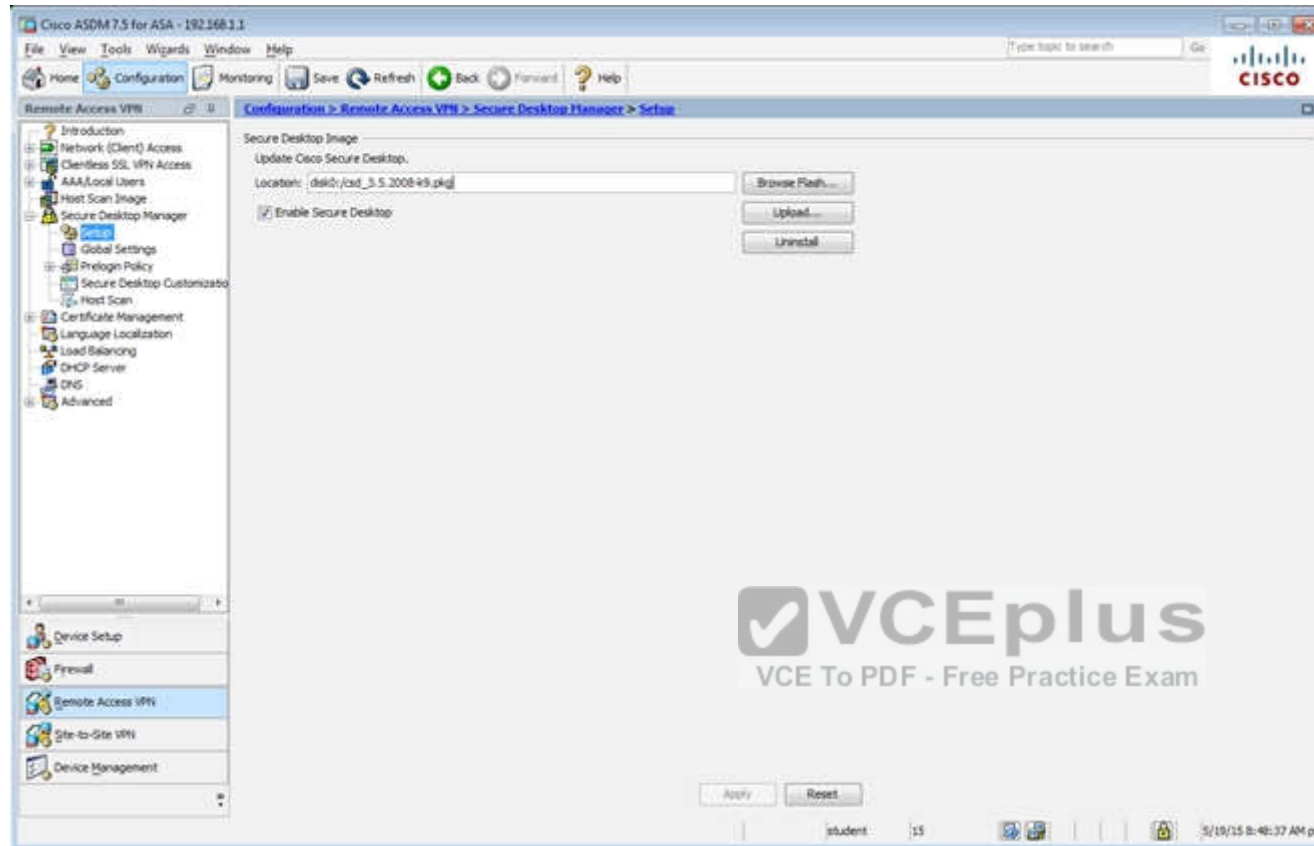
VCEplus
VCE To PDF - Free Practice Exam

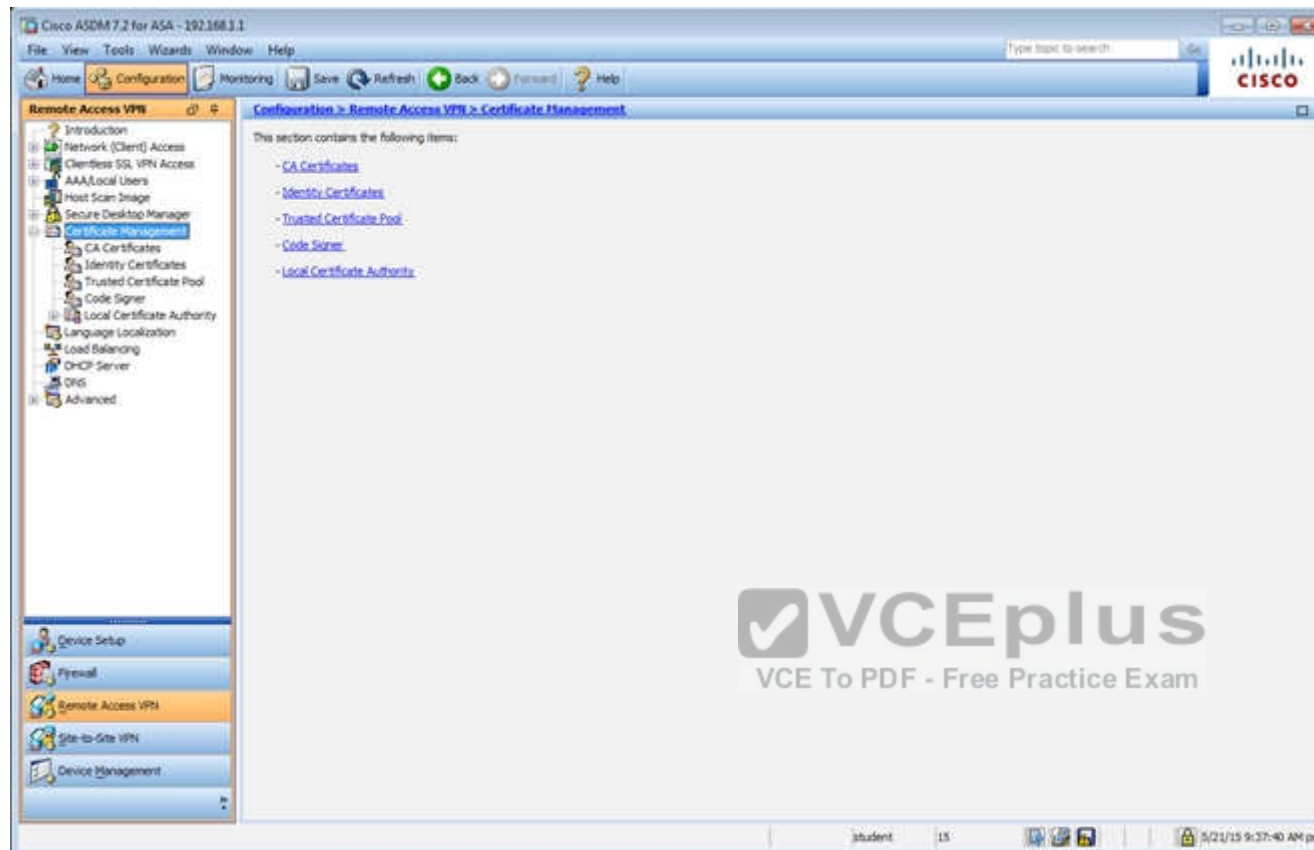
Find: Next Previous

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

Configuration > Remote Access VPN > Certificate Management > Identity Certificates

| Issued To | Issued By | Expiry Date | Associated Trustpoints | Usage | Public Key Type |
|----------------------------|----------------------------|----------------------------|------------------------|-----------------|-----------------|
| hostname-4P (17-ASA-sec... | hostname-4P (17-ASA-sec... | 11:59:33 pet 1 Dec 20 2024 | ASDM-Trustpoint1 | General Purpose | RSA 2048 bits |

Buttons: Add, Show Details, Delete, Export, Install

Find: Match Case

Certificate Expiration Alerts

Send the first alert before: (days)

Repeat Alert Interval: (days)

Public CA Enrollment

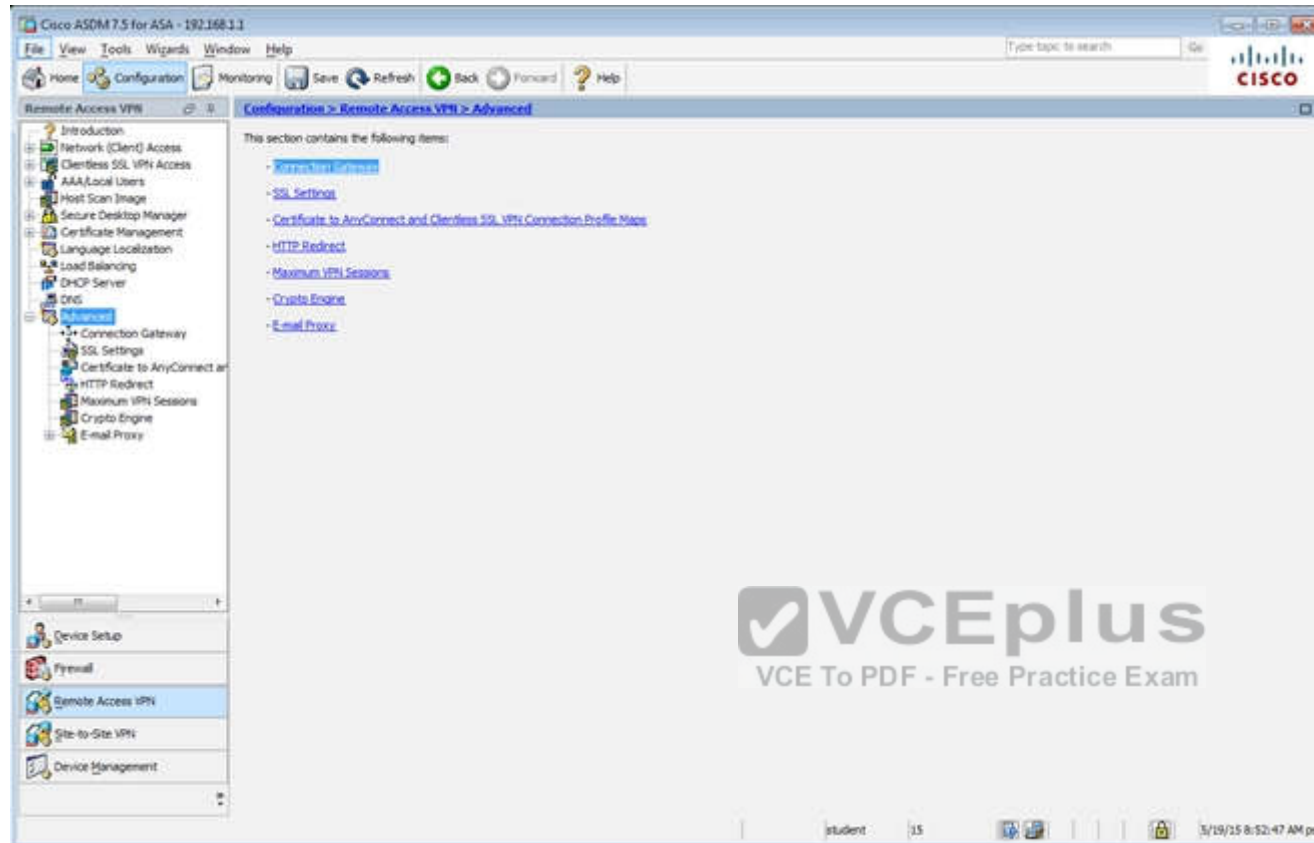
Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers Cisco customers a special promotional price for certificates and trial certificates for testing.

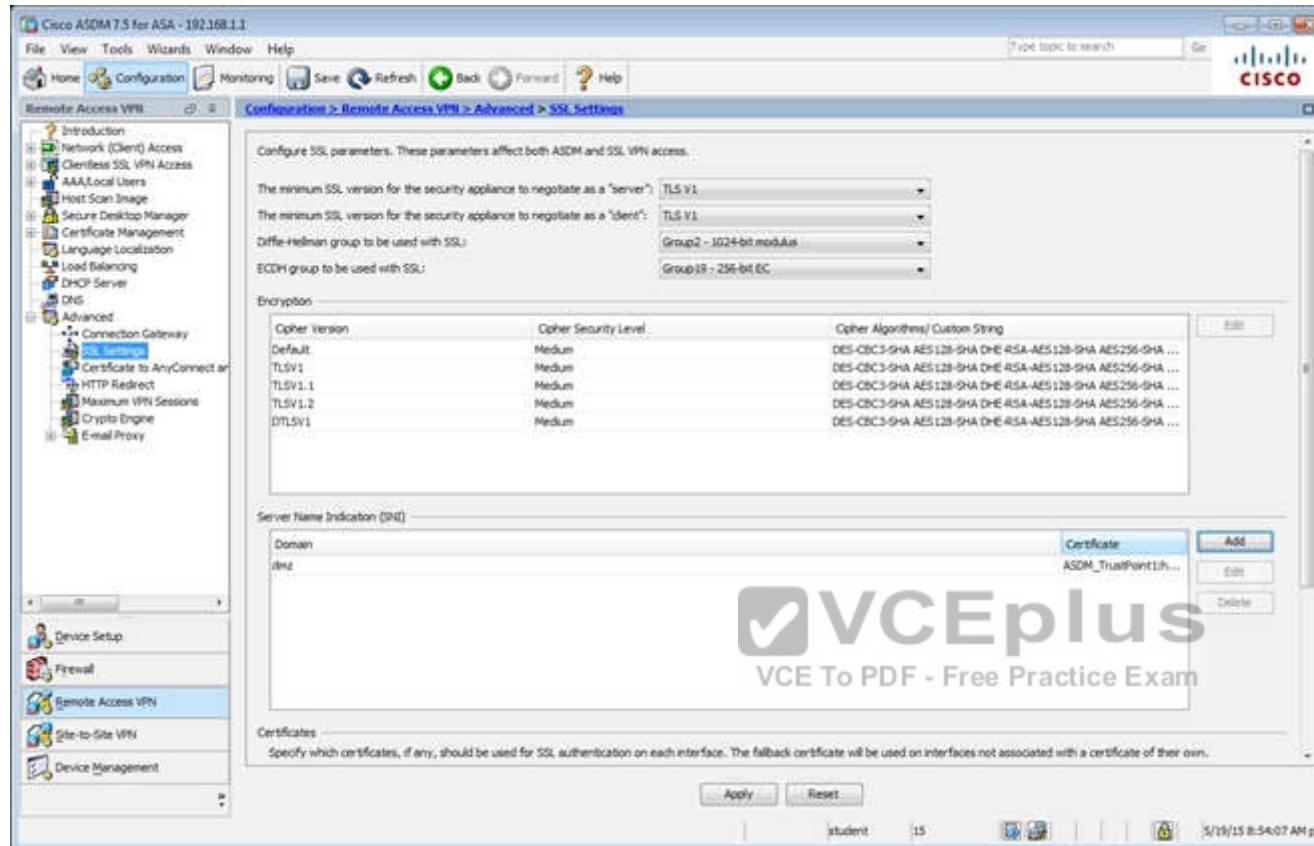
Using a previously saved certificate signing request, [enroll with Entrust](#).

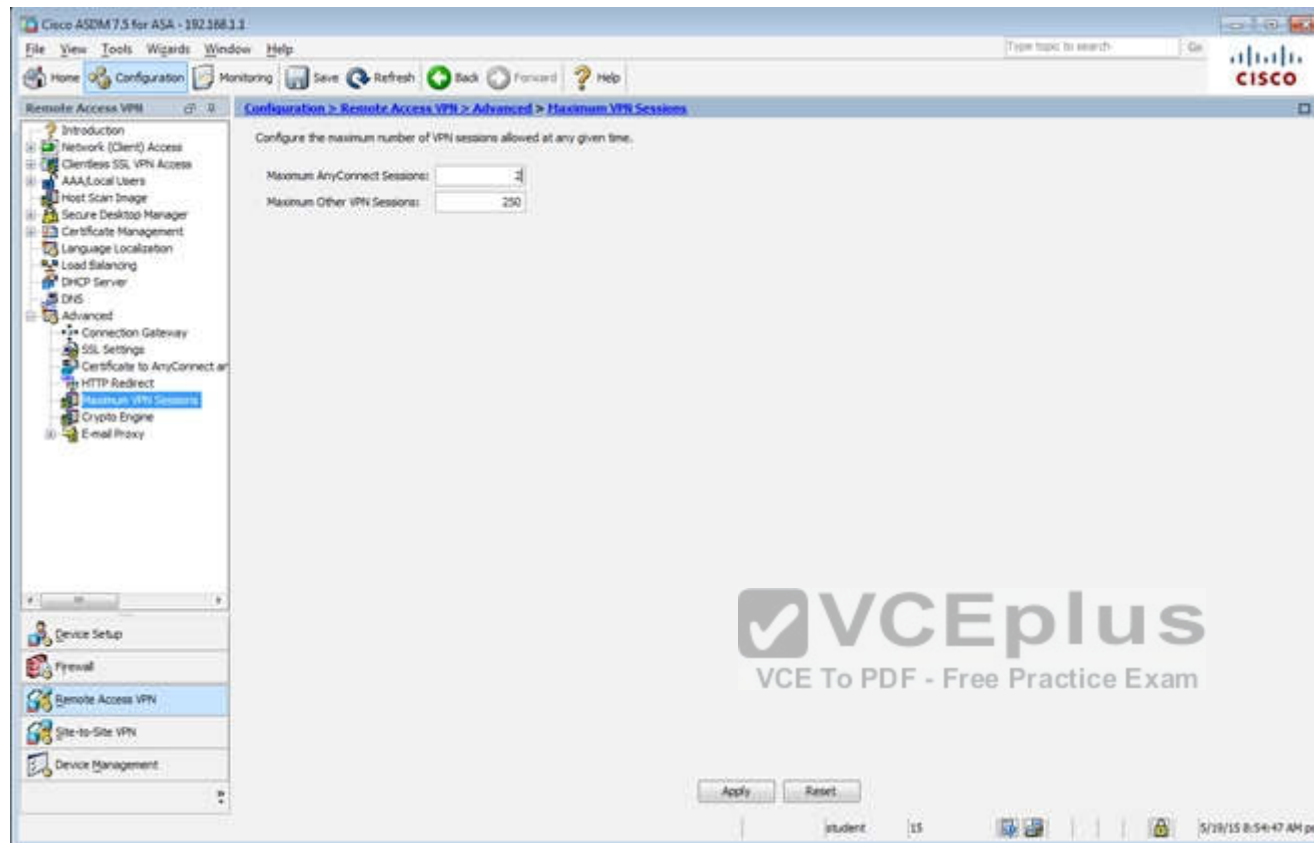
ASDM Identity Certificate Wizard

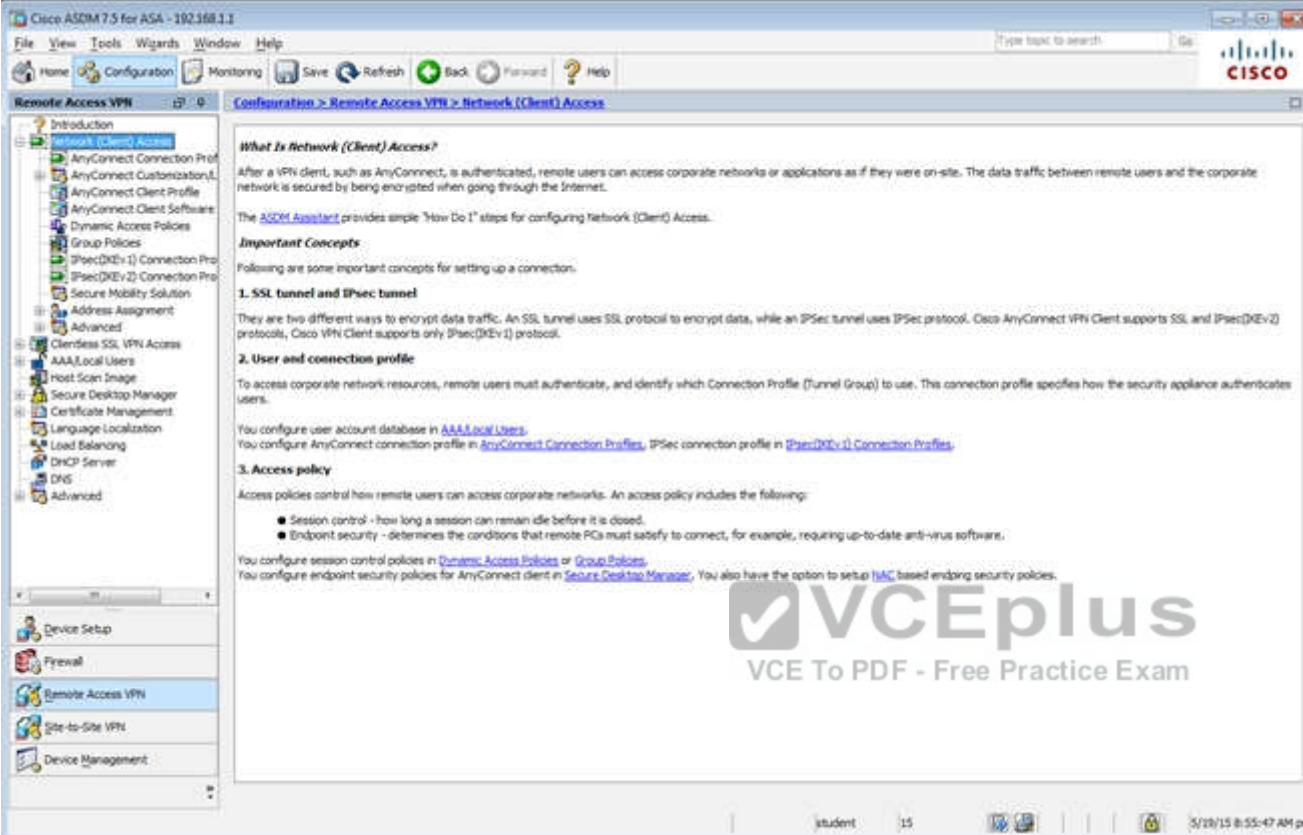
The Cisco ASDM Identity Certificate Wizard assists you in creating a self-signed certificate that is required for launching ASDM through launcher.

student 15 3/19/15 8:31:47 AM pet









Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Network (Client) Access

Network (Client) Access

What Is Network (Client) Access?

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

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

Important Concepts

Following are some important concepts for setting up a connection:

1. SSL tunnel and IPsec tunnel

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

2. User and connection profile

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

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

3. Access policy

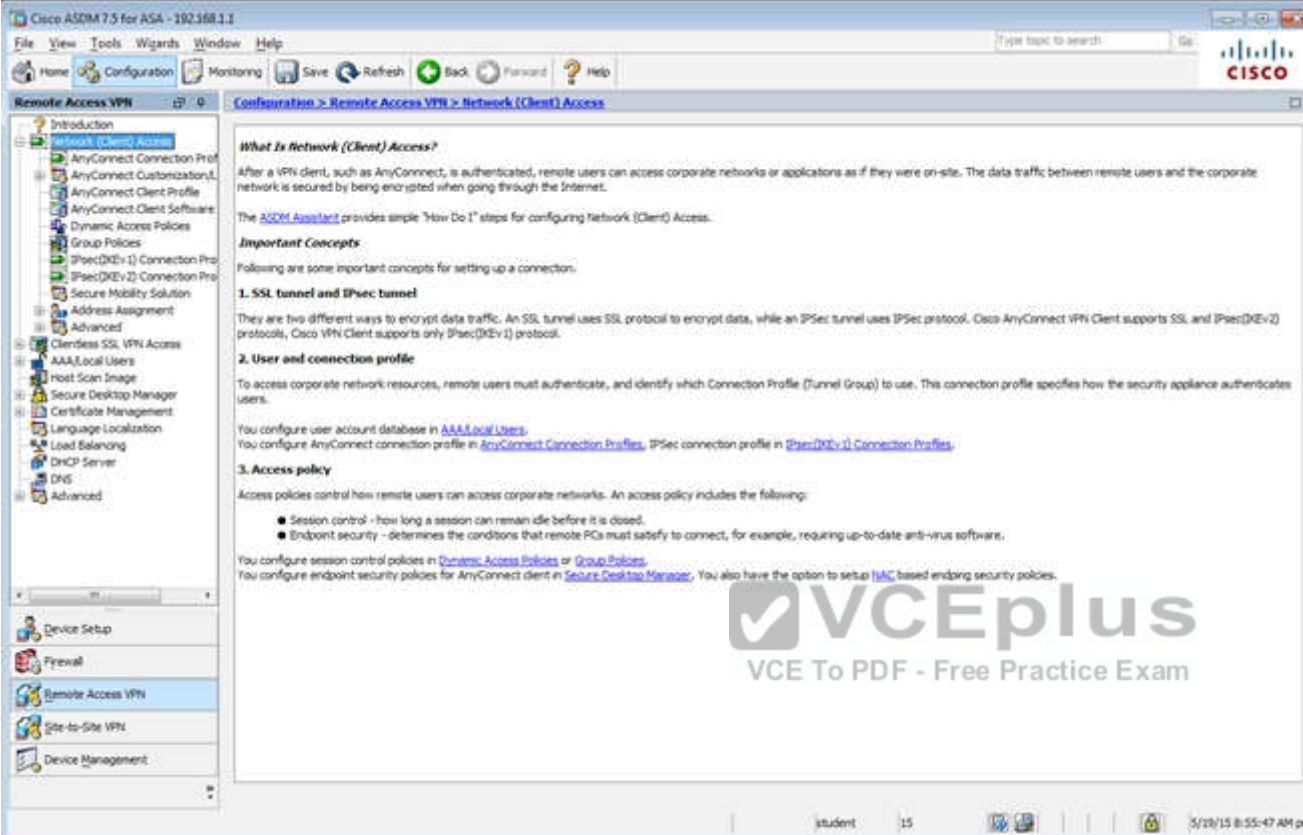
Access policies control how remote users can access corporate networks. An access policy includes the following:

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

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

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

student 15 5/29/15 8:55:47 AM pct



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Remote Access VPN

Configuration > Remote Access VPN > Network (Client) Access

Network (Client) Access

What Is Network (Client) Access?

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

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

Important Concepts

Following are some important concepts for setting up a connection:

1. SSL tunnel and IPsec tunnel

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

2. User and connection profile

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

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

3. Access policy

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

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

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

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

student 15 5/29/15 8:55:47 AM pct

Edit Internal Group Policy: DfBGrpPolicy

Advanced

Servers

Advanced

- Split Tunneling
- Browser Proxy
- AnyConnect Client
- IPsec (IKEv1) Client

Name: DfBGrpPolicy

Banner:

SCDP forwarding URL:

Address Pools: Select...

IPv6 Address Pools: Select...

None Options

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

Filter: -- None -- Manage...

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

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

Simultaneous Logins: 3

Restrict access to VLAN: -- Unrestricted --

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

Maximum Connect Time: ☒ Unlimited ☐ minutes

Idle Timeout: ☐ None ☐ 30 minutes

On smart card removal: ☒ Disconnect ☐ Keep the connection

VCEplus
VCE To PDF - Free Practice Exam

Find: Next Previous

OK Cancel Help

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction
Network (Client) Access
AnyConnect Connection Profile
AnyConnect Customization
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

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

Access Interfaces
Enable interfaces for IPsec access.

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

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

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

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

| Name | IPsec Enabled | L2TP/IPsec Enabled | Authentication Server Group | Group Policy |
|--------------------|-------------------------------------|-------------------------------------|-----------------------------|---------------|
| DefaultVRAGroup | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD | DiffGrpPolicy |
| DefaultWEBVPNGroup | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | RAD | DiffGrpPolicy |
| Servers | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | LOCAL | Sales |

Find: Match Case

Apply Reset

student 15 5/18/15 8:56:47 AM pst

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec (IKEv2) 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

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

Access Interfaces

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

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

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

☒ Bypass interface access lists for inbound VPN sessions

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

Login Page Setting

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

☐ Shutdown portal login page.

Connection Profiles

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

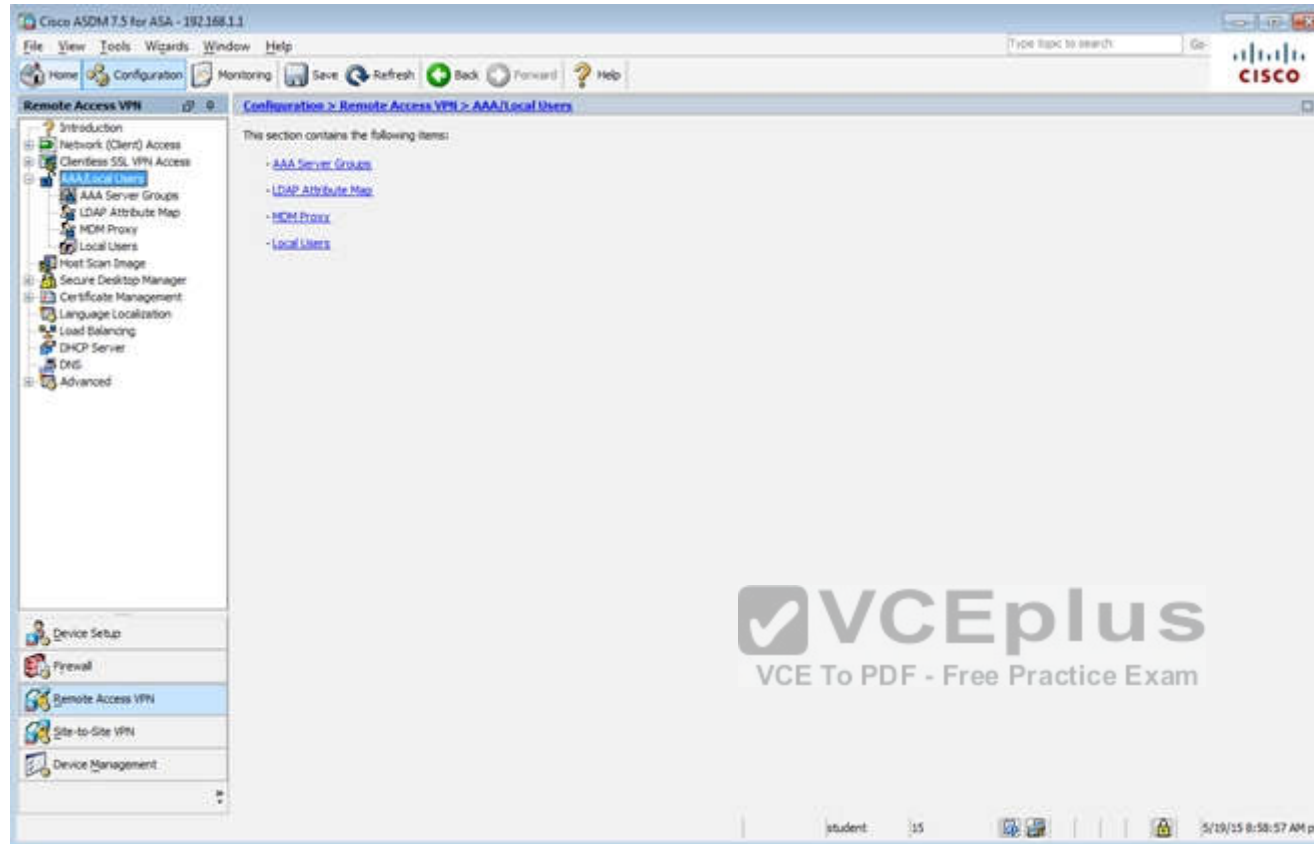
+ Add Edit Delete Find: Match Case

| Name | SSL Enabled | IPsec Enabled | Authentication Method | Group Policy |
|--------------------|-------------------------------------|-------------------------------------|-----------------------|--------------------|
| DefaultRAGroup | <input type="checkbox"/> | <input type="checkbox"/> | AAA(RADIUS) | DefaultGroupPolicy |
| DefaultWEBVPNGroup | <input type="checkbox"/> | <input checked="" type="checkbox"/> | AAA(RADIUS) | DefaultGroupPolicy |
| AnyConnect | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | AAA(RADIUS) | DefaultGroupPolicy |

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

Apply Reset

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



Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

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

Introduction
Network (Client) Access
Clientless SSL VPN Access
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
MDM Proxy
Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced

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

Create entries in the ASA local user database.

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

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

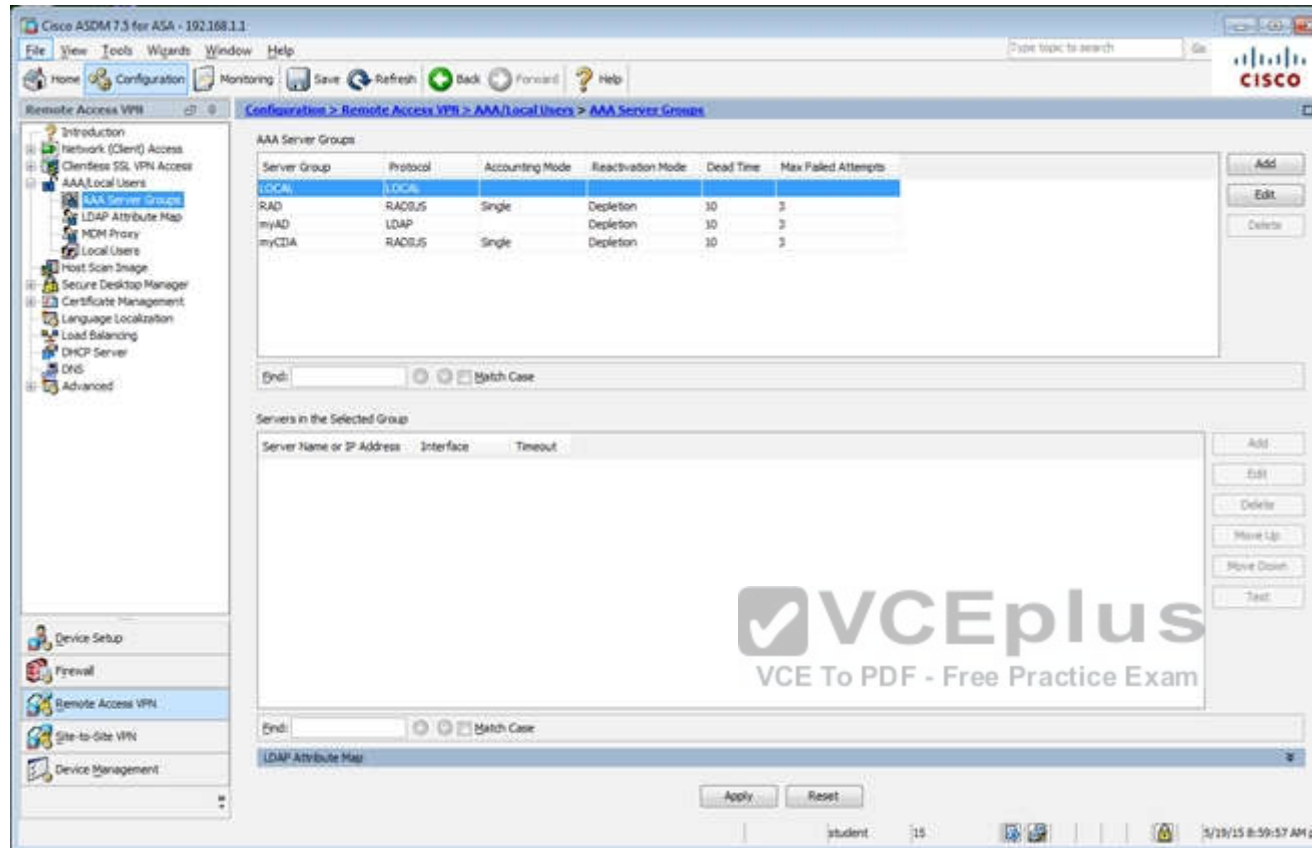
| Username | Privilege Level (Role) | Access Restrictions | VPN Group Policy | VPN Group Lock |
|-----------|------------------------|---------------------|----------------------------|----------------------------|
| student | 15 | Full | -- Inherit Group Policy -- | -- Inherit Group Policy -- |
| enable_15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

Add
Edit
Delete

End: Match Case

Apply Reset

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



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

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

Virtual Terminal

Cisco ASDM 7.5 for ASA - 192.168.1.1

File
View
Tools
Wizards
Window
Help

Home
Configuration
Monitoring
Save

Firewall

Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
Public Servers
URL Filtering Servers
Threat Detection
Identity Options
Identity by TrustSec
Botnet Traffic Filter
Objects
Unified Communications
Advanced

Add
Edit

| # | Source Int |
|---|------------|
| 1 | Any |

Add Network Object

Name: HTTP
Type: Host
IP Version: ☒ IPv4 ☐ IPv6
IP Address: 209.165.201.30

NAT
☒ Add Automatic Address Translation Rules

Type: Static
Translated Addr: 172.16.1.2

☐ Use one-to-one address translation
☐ PAT Pool Translated Address:
☐ Round Robin
☐ Extend PAT uniqueness to per destination instead of per interface
☐ Translate TCP and UDP ports into flat range 1024-65535 ☐ Include range 1-1023
☐ Fall through to interface PAT(dest intf): DMZ
☐ Use IPv6 for interface PAT

Scenario
TOPOLOGY

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



Virtual Terminal

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring

Firewall

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
 - 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

Add Access Rule

Interface:

Action: ☒ Permit ☐ Deny

Source Criteria

Source:

User:

Security Group:

Destination Criteria

Destination:

Security Group:

Service:

Description:

☒ Enable Logging

Logging Level:

More Options

OK Cancel Help

Scenario **TOPOLOGY**



Virtual Terminal

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall

Configuration > Firewall > Access Rules

+ Add Edit Delete Where Used Not Used

Diagram Export Clear Hits Show Log Pack

Source Criteria:

Destination Criteria:

| # | Enabled | Source | User | Security Gi | Destination | Security Gi | Service | Act |
|---------------------------|-------------------------------------|--------|------|-------------|----------------------|-------------|----------|------|
| dmz (1) implicity incomi | | | | | | | | |
| 1 | | any | | | Any less secure ne.. | | ip | Perm |
| inside (1 implicit incomi | | any | | | Any less secure ne.. | | ip | Perm |
| 1 | | any | | | Any less secure ne.. | | ip | Perm |
| outside (1 incoming rule | | | | | | | | |
| 1 | <input checked="" type="checkbox"/> | any | | | 209.165.201.30 | | tcp/http | Perm |
| Global (1 implicit rule | | | | | | | | |
| 1 | | any | | | any | | ip | Den |

Apply

Reset

Advanced

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:



Virtual Terminal

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Firewall

- Access Rules
- NAT Rules
- Service Policy Rules
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
 - Network Objects/Groups
 - Service Objects/Groups
 - Local Users
 - Local User Groups
 - Security Group Object Group
- Class Maps
- Inspect Maps
- Regular Expressions
- TCP Maps
- Time Ranges
- Unified Communications
- Advanced

Configuration > Firewall > Service Policy Rules

+ Add Edit Delete Up Down Copy Paste Find Diagram Packet Trace

Traffic Classification

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

Apply

Reset

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



Virtual Terminal

Cisco ASDM 7.5 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring

Firewall

- Access Rules
- NAT Rules
- Service Policy Rules**
- AAA Rules
- Filter Rules
- Public Servers
- URL Filtering Servers
- Threat Detection
- Identity Options
- Identity by TrustSec
- Botnet Traffic Filter
- Objects
 - 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

Edit Service Policy Rule

Traffic Classification Default Inspections Rule Actions

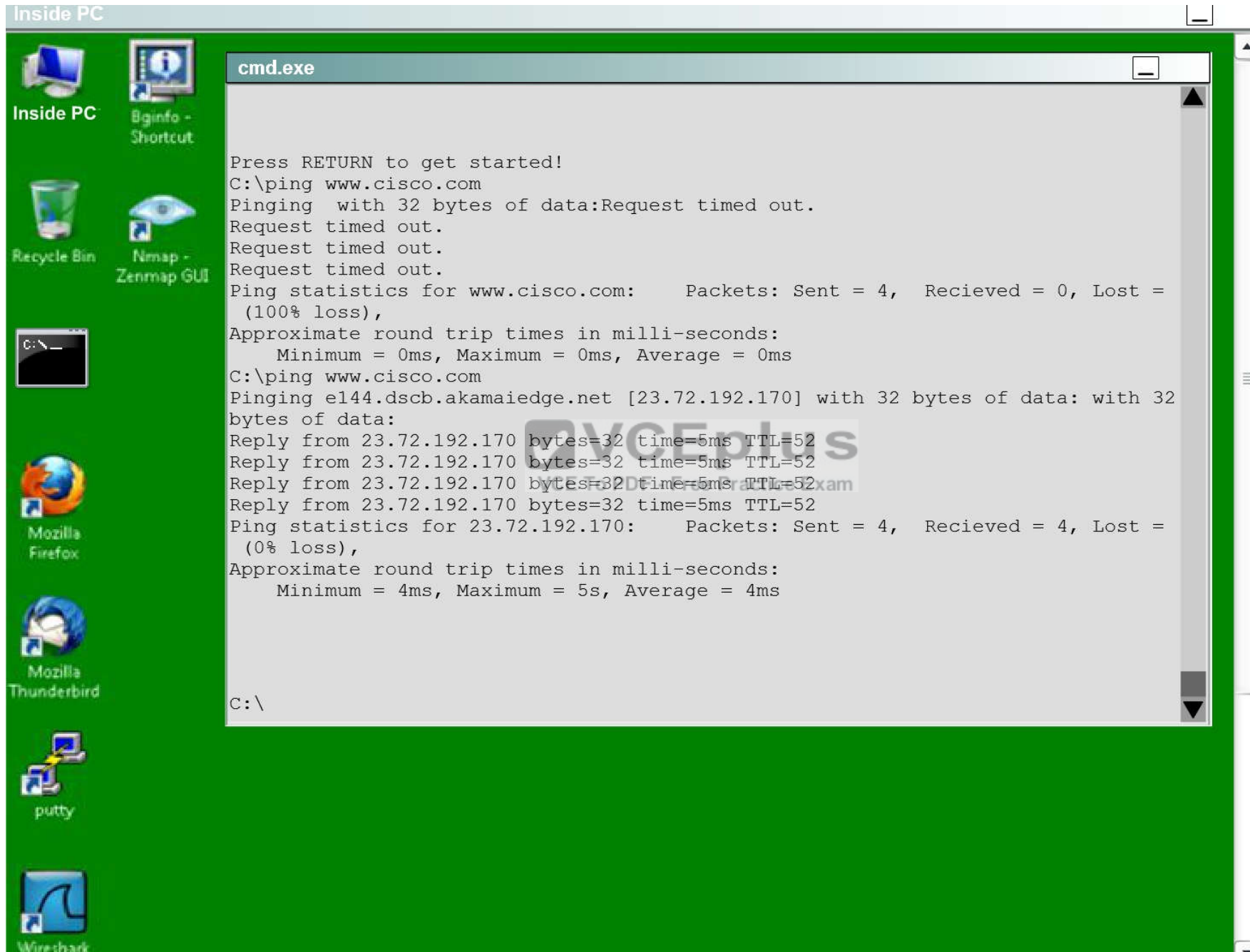
Protocol Inspection ASA FirePOWER Inspection Connection Settings QoS NetFlow User Statistics

☐ Select all inspection rules

| | |
|---|--|
| <input type="checkbox"/> CTIQBE | |
| <input type="checkbox"/> Cloud Web Security | Configure... |
| <input type="checkbox"/> DCERPC | Configure... |
| <input checked="" type="checkbox"/> DNS | Configure... DNS Inspect Map: preset_dns_map |
| <input checked="" type="checkbox"/> ESMTP | Configure... |
| <input checked="" type="checkbox"/> FTP | Configure... |
| <input checked="" type="checkbox"/> H.323 H.225 | Configure... |
| <input checked="" type="checkbox"/> H.323 RAS | Configure... |
| <input type="checkbox"/> HTTP | Configure... |
| <input checked="" type="checkbox"/> ICMP | |
| <input type="checkbox"/> ICMP Error | |
| <input type="checkbox"/> ILS | |
| <input type="checkbox"/> IM | Configure... |
| <input checked="" type="checkbox"/> IP-Options | Configure... |
| <input type="checkbox"/> IPSec-Pass-Thru | Configure... |
| <input type="checkbox"/> IPv6 | Configure... |
| <input type="checkbox"/> MMP | Configure... |

After that is done, we can ping www.cisco.com again to verify:





QUESTION 69

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

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

Correct Answer: BDF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Data plane security can be implemented using the following features:

Access control lists

Access control lists (ACLs) perform packet filtering to control which packets move through the network and where.

Antispoofing

ACLs can be used as an antispoofing mechanism that discards traffic that has an invalid source address.

Layer 2 security features

Cisco Catalyst switches have integrated features to help secure the Layer 2 infrastructure.

Reference: <http://www.ciscopress.com/articles/article.asp?p=1924983&seqNum=5>

QUESTION 70

How many crypto map sets can you apply to a router interface?

- A. 3
- B. 2
- C. 4
- D. 1

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

These commands apply the crypto map to the interface. You can assign only one crypto map set to an interface. If multiple crypto map entries have the same map-name but a different seq-num, they are part of the same set and are all applied to the interface. The security appliance evaluates the crypto map entry with the lowest seq-num first.

```
dt3-45a(config)#interface e0
```

```
dt3-45a(config-if)#crypto map armadillo
```

Reference: <http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/16439-IPSECpart8.html>

QUESTION 71

What is the transition order of STP states on a Layer 2 switch interface?

- A. listening, learning, blocking, forwarding, disabled
- B. listening, blocking, learning, forwarding, disabled
- C. blocking, listening, learning, forwarding, disabled
- D. forwarding, listening, learning, blocking, disabled

Correct Answer: C

Section: (none)

Explanation

**Explanation/Reference:**

Explanation:

Each interface on a access point using spanning tree exists in one of these states:

- Blocking—The interface does not participate in frame forwarding.
- Listening—The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.
- Learning—The interface prepares to participate in frame forwarding.
- Forwarding—The interface forwards frames.
- Disabled—The interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.

Reference: http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-3_7_JA/configuration/guide/i1237sc/s37span.html#wp1040509

QUESTION 72

Which sensor mode can deny attackers inline?

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

D. fail-open

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can configure certain aspects of the deny attackers inline event action. You can configure the number of seconds you want to deny attackers inline and you can limit the number of attackers you want denied in the system at any one time.

Reference: <http://www.cisco.com/c/en/us/td/docs/security/ips/5-1/configuration/guide/cli/cliguide/cliEvAct.html>

QUESTION 73

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

A. stop

B. none

C. error

D. all

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Secure Device Event Exchange (SDEE) messages report on the progress of Cisco IOS IPS initialization and operation. Click to display the Edit IPS: SDEE Messages window, where you can review SDEE messages and filter them to display only error, status, or alert messages.

Reference: http://www.cisco.com/c/en/us/td/docs/routers/access/cisco_router_and_security_device_manager/24/software/user/guide/IPS.html

QUESTION 74

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A security policy is used to minimize risk by allocating company's resources to eliminate risk and focus on growth and revenues.

Reference: <http://searchsecurity.techtarget.com/definition/security-policy>

QUESTION 75

Which wildcard mask is associated with a subnet mask of /27?

- A. 0.0.0.31
- B. 0.0.0.27
- C. 0.0.0.224
- D. 0.0.0.255

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

On Cisco router, wildcard subnet mask is used in the following occasion

* Defining subnet in ACL

* Defining subnet member in OSPF area

Reference: <http://www.dslreports.com/faq/15216>

QUESTION 76

Which statements about reflexive access lists are true? (Choose three.)

- A. Reflexive access lists create a permanent ACE
- B. Reflexive access lists approximate session filtering using the established keyword
- C. Reflexive access lists can be attached to standard named IP ACLs
- D. Reflexive access lists support UDP sessions
- E. Reflexive access lists can be attached to extended named IP ACLs
- F. Reflexive access lists support TCP sessions

Correct Answer: DEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Reflexive access lists allow IP packets to be filtered based on upper-layer session information. You can use reflexive access lists to permit IP traffic for sessions originating from within your network but to deny IP traffic for sessions originating from outside your network. This is accomplished by reflexive filtering, a kind of session filtering.

Reflexive access lists can be defined with extended named IP access lists only. You cannot define reflexive access lists with numbered or standard named IP access lists or with other protocol access lists.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfreflx.html

QUESTION 77

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

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

Correct Answer: BDE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The following event actions can be deployed in Promiscuous mode. These actions are in affect for a user-configurable default time of 30 minutes. Because the IPS sensor must send the request to another device or craft a packet, latency is associated with these actions and could allow some attacks to be successful. Blocking through usage of the Attack Response Controller (ARC) has the potential benefit of being able to perform to the network edge or at multiple places within the network.

Request block host: This event action will send an ARC request to block the host for a specified time frame, preventing any further communication. This is a severe action that is most appropriate when there is minimal chance of a false alarm or spoofing.

Request block connection: This action will send an ARC response to block the specific connection. This action is appropriate when there is potential for false alarms or spoofing.

Reset TCP connection: This action is TCP specific, and in instances where the attack requires several TCP packets, this can be a successful action. However, in some cases where the attack only needs one packet it may not work as well. Additionally, TCP resets are not very effective with protocols such as SMTP that consistently try to establish new connections, nor are they effective if the reset cannot reach the destination host in time.

Reference: <http://www.cisco.com/c/en/us/about/security-center/ips-mitigation.html>

QUESTION 78

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The CONSOLE list overrides the default method list default on line con 0. You need to enter the password "cisco" (configured on line con 0) to get console access.

The default list is still used on tty, vty and aux.

Note: To have console access authenticated by a local username and password, use:

Router(config)# aaa authentication login CONSOLE local

Reference: http://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html#login_auth

QUESTION 79

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Health and Performance Monitor (HPM) periodically polls monitored ASA devices, IPS devices, and ASA-hosted VPN services for key health and performance data, including critical and non-critical issues, such as memory usage, interface status, dropped packets, tunnel status, and so on. This information is used for alert generation and email notification, and to display trends based on aggregated data, which is available for hourly, daily, and weekly periods.

Reference: http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-4/user/guide/CSMUserGuide_wrapper/wfplan.html

QUESTION 80

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

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Start-stop and stop-only notices are used to send a failed authentication attempt record to AAA server.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/xr-3s/sec-usr-aaa-xr-3s-book/sec-cfg-accountg.html

QUESTION 81

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

1. Configure the **hostname** command.
2. Configure the DNS domain.
3. Generate the SSH key to be used.
4. Enable SSH transport support for the virtual type terminal (vty).

If you want to have one device act as an SSH client to the other, you can add SSH to a second device called Reed. These devices are then in a client-server arrangement, where Carter acts as the server, and Reed acts as the client. The Cisco IOS SSH client configuration on Reed is the same as required for the SSH server configuration on Carter.

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

QUESTION 82

Which protocol provides security to Secure Copy?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The Secure Copy (SCP) feature provides a secure and authenticated method for copying device configurations or device image files. SCP relies on Secure Shell (SSH), an application and protocol that provide a secure replacement for the Berkeley r-tools suite (Berkeley university's own set of networking applications).

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/15-s/sec_usr-ssh-15-s-book/sec-secure-copy.html

QUESTION 83

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The RDP plug-in is only one of the plug-ins available to users, along with others such as Secure Shell (SSH), Virtual Network Computing (VNC), and Citrix. The RDP plug-in is one of the most frequently used plug-ins in this collection. This document provides more details about the deployment and troubleshoot procedures for this plug-in.

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

QUESTION 84

Which security zone is automatically defined by the system?

- A. The source zone
- B. The self zone
- C. The destination zone
- D. The inside zone

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The self zone is a system-defined zone which does not have any interfaces as members. A zone pair that includes the self zone, along with the associated policy, applies to traffic directed to the device or traffic generated by the device. It does not apply to traffic through the device.

The most common usage of firewall is to apply them to traffic through a device, so you need at least two zones (that is, you cannot use the self zone).

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-2mt/sec-zone-pol-fw.html

QUESTION 85

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

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Using the channel created in phase 1, this phase establishes IPsec security associations and negotiates information needed for the IPsec tunnel. This phase can be seen in the above figure as "IPsec-SA established." Note that two phase 2 events are shown, this is because a separate SA is used for each subnet configured to traverse the VPN.

Reference: https://documentation.meraki.com/zGeneral_Administration/Tools_and_Troubleshooting/Networking_Fundamentals%3A_IPSec_and_IKEv

QUESTION 86

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Using one of the common Unique Local IPv6 global prefix generators, the Acme corporate network was assigned the global prefix of 6D8D64AF0C; when pushed together with the common unique local locally assigned prefix (FD00::/8) the prefix expands to FD6D:8D64:AF0C::/48; this leaves Acme with an additional 16 bits of space to use for subnetting across their sites.

Reference: <http://www.ciscopress.com/articles/article.asp?p=2154678&seqNum=2>

QUESTION 87

What is a possible reason for the error message?Router(config)#aaa server?% Unrecognized command

- A. The command syntax requires a space after the word “server”
- B. The command is invalid on the target device
- C. The router is already running the latest operating system
- D. The router is a new device on which the aaa new-model command must be applied before continuing

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

It means that the router is a new device on which aaa new model command must be applied before inducting it into the system.

Reference: <http://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html>

QUESTION 88

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

- A. Smart tunnels can be used by clients that do not have administrator privileges

- B. Smart tunnels support all operating systems
- C. Smart tunnels offer better performance than port forwarding
- D. Smart tunnels require the client to have the application installed locally

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

- Tunnel offers better performance than browser plug-ins.
- Port forwarding is the legacy technology for supporting TCP-based applications over a Clientless SSL VPN connection. Unlike port forwarding, Smart Tunnel simplifies the user experience by not requiring the user connection of the local application to the local port.
- Smart Tunnel does not require users to have administrator privileges.
- Smart Tunnel does not require the administrator to know application port numbers in advance.

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

QUESTION 89

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If the native VLAN on a trunk is different on each end of the link, STP loops may occur.

Reference: <https://supportforums.cisco.com/discussion/12477986/using-different-native-vlans-different-ports-switch-configured-trunks>

QUESTION 90

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

- A. Protocol used for filtering
- B. Direction of the access class

- C. Direction of the access group
- D. Direction of the access list

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You use direction of the access group when you apply an access list to a physical interface.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/xr-3s/sec-data-acl-xr-3s-book/sec-create-ip-apply.html

QUESTION 91

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Take the common case of the initiator behind the NAT. The initiator must quickly change to port 4500 once the NAT has been detected to minimize the window of IPsec-aware NAT problems.

Reference: <https://tools.ietf.org/html/rfc3947>

QUESTION 92

Which of the following are features of IPsec transport mode? (Choose three.)

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

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

IPSec can be run in either tunnel mode or transport mode. Each of these modes has its own particular uses and care should be taken to ensure that the correct one is selected for the solution:

- *Tunnel mode* is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.
- *Transport mode* is used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host—for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.

Reference: <http://www.ciscopress.com/articles/article.asp?p=25477>

QUESTION 93

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

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



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Configure routed ports by putting the interface into Layer 3 mode with the no switchport interface configuration command. Then assign an IP address to the port, enable routing, and assign routing protocol characteristics by using the ip routing and router protocol global configuration commands.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750/swint.html

QUESTION 94

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

- A. EAP
- B. ASCII
- C. PAP

- D. PEAP
- E. MS-CHAPv1
- F. MS-CHAPv2

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The ASA supports TACACS+ server authentication with the following protocols: ASCII, PAP, CHAP, and MS-CHAPv1.

Reference: <http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/asdm72/general/asa-general-asdm/aaa-tacacs.html>

QUESTION 95

Which type of IPS can identify worms that are propagating in a network?

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



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cisco's best-in-class anomaly detection feature detects worms by learning the "normal" traffic patterns of the network, and then scanning for anomalous behavior. Fast-propagating network worms scan the network in order to infect other hosts. For each protocol or service, the anomaly detection program studies what is normal scanning activity, and accumulates this information in a threshold histogram and an absolute scanner threshold. The scanner threshold specifies the absolute scanning rate above which any source is considered malicious.

Reference: http://www.cisco.com/c/en/us/products/collateral/security/ips-4200-series-sensors/prod_brochure0900aecd805baea7.html

QUESTION 96

Which command verifies phase 1 of an IPsec VPN on a Cisco router?

- A. show crypto map
- B. show crypto ipsec sa

- C. show crypto isakmp sa
- D. show crypto engine connection active

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When a problem exist with the connectivity, even phase 1 of VPN does not come up. On the ASA, if connectivity fails, the SA output is similar to this example, which indicates possibly an incorrect crypto peer configuration and/or incorrect ISAKMP proposal configuration:

Router#**show crypto isakmp sa**

1 IKE Peer: XX.XX.XX.XX

Type : L2L Role : initiator

Rekey : no State : MM_WAIT_MSG2

Reference: <http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/81824-common-ipsec-trouble.html>

QUESTION 97

What is the purpose of a honeypot IPS?

- A. To create customized policies
- B. To detect unknown attacks
- C. To normalize streams
- D. To collect information about attacks



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Honeypot systems use a dummy server to attract attacks. The purpose of the honeypot approach is to distract attacks away from real network devices. By staging different types of vulnerabilities in the honeypot server, you can analyze incoming types of attacks and malicious traffic patterns. You can use this analysis to tune your sensor signatures to detect new types of malicious network traffic.

Honeypot systems are used in production environments, typically by large organizations that come across as interesting targets for hackers, such as financial enterprises, governmental agencies, and so on. Also, antivirus and other security vendors tend to use them for research.

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

QUESTION 98

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Local session termination allows routers to act as proxies for remote systems that represent session endpoints. (A proxy is a device that acts on behalf of another device.)

Reference: http://docwiki.cisco.com/wiki/Internetwork_Design_Guide_-_Internetworking_Design_Basics

QUESTION 99

Which syslog severity level is level number 7?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

| Level | Description |
|-------------------|----------------------------------|
| 0 - emergency | System unusable |
| 1 - alert | Immediate action needed |
| 2 - critical | Critical condition |
| 3 - error | Error condition |
| 4 - warning | Warning condition |
| 5 - notification | Normal but significant condition |
| 6 - informational | Informational message only |
| 7 - debugging | Appears during debugging only |

Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/system_management/configuration/guide/sm_nx_os_cg/sm_5syslog.html

QUESTION 100

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

Reference: <https://en.wikipedia.org/wiki/Phishing>

QUESTION 101

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The traffic for each RSPAN session is carried as Layer 2 nonroutable traffic over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. All participating switches must be trunk-connected at Layer 2.

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/span.html>

QUESTION 102

Which tasks is the session management path responsible for? (Choose three.)

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

Correct Answer: BDF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The session management path is responsible for the following tasks:

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

Reference: http://www.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/intro_f.html

QUESTION 103

Which network device does NTP authenticate?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

NTP authentication, the device synchronizes to a time source only if the source carries one of the authentication keys specified by the ntp trusted-key command. The device drops any packets that fail the authentication check and prevents them from updating the local clock. NTP authentication is disabled by default.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5-x/nx-os/system_management/configuration/guide/sm_nx_os_cg/sm_3ntp.html#wp1100303

QUESTION 104

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

To protect against the growing breadth and diversity of threats in today's business climate, you need a modern approach. That means a variety of protections that can block hidden malware from both suspicious and legitimate sites before it reaches you. We think the best Web security solutions today should be backed by the best real-time security intelligence available to help you stay abreast of this changing threat landscape and prevent the latest exploits from turning into issues. And modern Web security should be able to support policies that give employees access to the sites they need to use to do their jobs while selectively denying the use of undesired sites and features like web-based file-sharing.

You get all of those features and more with the Cisco® Web Security Appliance (WSA), Figure 1. Cisco WSA safeguards businesses through broad threat

intelligence, multiple layers of malware defense, and vital data loss prevention (DLP) capabilities across the attack continuum. It's an all-in-one web gateway that brings you broad protection, extensive controls, and investment value. It also offers an array of competitive web security deployment options, each of which includes Cisco's market-leading global threat intelligence infrastructure.

Reference: <http://www.cisco.com/c/en/us/products/collateral/security/web-security-appliance/solution-overview-c22-732948.html>

QUESTION 105

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains, allowing you to isolate the ports on the switch from each other. A subdomain consists of a primary VLAN and one or more secondary VLANs

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

QUESTION 106

What hash type does Cisco use to validate the integrity of downloaded images?

- A. Sha1
- B. Sha2
- C. Md5
- D. Md1

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

The MD5 File Validation feature allows you to generate the MD5 checksum for the Cisco IOS image stored on your router and compare it to the value posted on Cisco.com to verify that the image on your router is not corrupted.

Reference: <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sys-image-mgmt/configuration/15-s/sysimgmgmt-15-s-book/sysimgmgmt-md5.html#GUID-9E5A6790-5E81-442B-8F6F-54271B25A9F8>

QUESTION 107

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

The Unicast RPF feature helps to mitigate problems that are caused by malformed or forged IP source addresses that are passing through a router.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfrpf.html

QUESTION 108

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

The older version of CDP v1 are vulnerable to DoS attacks, such that an attacker could flood the network segment with large CDP frames containing random device ID's causing Cisco devices running this version to crash. Targeting a vulnerable router using this attack could allow the attacker to send spoofed CDP frames with new route information with a higher priority so that traffic is rerouted to an unauthorised device. Although this form of DoS only affects older versions of the protocol many older platforms cannot upgrade to newer releases due to flash ROM size constraints, so I'm sure there are many devices still at risk to this exploit.

Reference: <http://packetbuddha.blogspot.com/2009/12/cdp-attacks.html>

QUESTION 109

What is the Cisco preferred countermeasure to mitigate CAM overflows?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Port Security on a Cisco switch enables you to control how the switch port handles the learning and storing of MAC addresses on a per-interface basis. The main use of this command is to set a limit to the maximum number of concurrent MAC addresses that can be learned and allocated to the individual switch port.

Reference: <http://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=2>

QUESTION 110

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet-inspection-based feature that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. While it is common practice to defend against attacks by inspecting traffic at the data centers and corporate headquarters, it is also critical to distribute the network-level defense to stop malicious traffic close to its entry point at the branch or telecommuter offices.

Reference: http://www.cisco.com/c/en/us/products/collateral/security/ios-intrusion-prevention-system-ips/prod_white_paper0900aecd8062acfb.html

QUESTION 111

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

- A. The user will be prompted to authenticate using the enable password
- B. Authentication attempts to the router will be denied

- C. Authentication will use the router's local database
- D. Authentication attempts will be sent to the TACACS+ server

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 does not respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern would continue through the remaining designated methods until the user is either authenticated or rejected, or until the session is terminated.

It is important to remember that a FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

Suppose the system administrator wants to apply a method list only to a particular interface or set of interfaces. In this case, the system administrator creates a named method list and then applies this named list to the applicable interfaces.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfathen.html

QUESTION 112

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Cisco's IPS sensors support event retrieval using the Security Device Event Exchange (SDEE) protocol. SDEE is an industry standard protocol and there are several open-source libraries available for using in the creation of an event collection and storage solution.

Reference: <https://supportforums.cisco.com/discussion/10988211/how-monitor-cisco-ids-4215-v60>

QUESTION 113

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

To prevent loops when a switch has multiple links connected to a downstream switch, STP will elect Root Bridge to prevent loops in the process.

Reference: <http://networkengineering.stackexchange.com/questions/114/how-is-the-stp-root-bridge-and-path-to-the-root-bridge-determined>

QUESTION 114

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

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Using NAT on a security appliance operating in transparent mode eliminates the need for upstream or downstream routers to perform NAT for their networks.

Reference: http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-1/user/guide/CSMUserGuide_wrapper/NATchap.html#51621

QUESTION 115

Which components does HMAC use to determine the authenticity and integrity of a message? (Choose two.)

- A. The password
- B. The hash
- C. The key
- D. The transform set

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

An HMAC is a MAC which is based on a hash function. The basic idea is to concatenate the key and the message, and hash them together. Since it is impossible, given a cryptographic hash, to find out what it is the hash of, knowing the hash (or even a collection of such hashes) does not make it possible to find the key. The basic idea doesn't quite work out, in part because of length extension attacks, so the actual HMAC construction is a little more complicated.

Reference: <http://security.stackexchange.com/questions/20129/how-and-when-do-i-use-hmac/20301>

QUESTION 116

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can set a global timeout interval for all TACACS+ servers. The timeout interval determines how long the Cisco CG-OS router waits for responses from TACACS+ servers before declaring a timeout failure.



| | |
|--|---|
| acacs-server timeoutseconds | Specifies the timeout interval for TACACS+ servers. The range is from 1 to 60 seconds. The default timeout interval is 5 seconds. |
|--|---|

Reference: http://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/security/security_Book/sec_tacacspl_cgr1000.html

QUESTION 117

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

- A. EAP

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

Correct Answer: CEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The ASA supports the following authentication methods with RADIUS servers:

- PAP—For all connection types.
- CHAP and MS-CHAPv1—For L2TP-over-IPsec connections.
- MS-CHAPv2—For L2TP-over-IPsec connections, and for regular IPsec remote access connections when the password management feature is enabled. You can also use MS-CHAPv2 with clientless connections.
- Authentication Proxy modes—For RADIUS-to-Active-Directory, RADIUS-to-RSA/SDI, RADIUS- to-Token server, and RSA/SDI-to-RADIUS connections,

Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/aaa_radius.html#pgfid-1211697

QUESTION 118

Which command initializes a lawful intercept view?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Parser view cisco li-view is the command that initializes lawful intercept view.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/xr-3s/sec-usr-cfg-xr-3s-book/sec-role-base-cli.html#GUID-682CE43D-C9FC-4F47-848E-0DBC84ED6F32

QUESTION 119

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

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The best measure is to enable DHCP snooping and dynamic ARP inspection for ARP spoofing attacks.

Reference: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/white_paper_c11_603839.html

QUESTION 120

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

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

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Standard ACLs

A standard IP ACL is simple; it filters based on source address only. You can filter a source network or a source host, but you cannot filter based on the destination of a packet, the particular protocol being used such as the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP), or on the port number. You can permit or deny only source traffic.

Extended ACLs:

An extended ACL gives you much more power than just a standard ACL. Extended IP ACLs check both the source and destination packet addresses. They can also check for specific protocols, port numbers, and other parameters, which allow administrators more flexibility and control.

Named ACLs

One of the disadvantages of using IP standard and IP extended ACLs is that you reference them by number, which is not too descriptive of its use. With a named ACL, this is not the case because you can name your ACL with a descriptive name. The ACL named DenyMike is a lot more meaningful than an ACL simply numbered 1. There are both IP standard and IP extended named ACLs.

Another advantage to named ACLs is that they allow you to remove individual lines out of an ACL. With numbered ACLs, you cannot delete individual statements. Instead, you will need to delete your existing access list and re-create the entire list.

Reference: <http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/access-control-list.html>

QUESTION 121

Which statement about extended access lists is true?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

An extended ACL gives you much more power than just a standard ACL. Extended IP ACLs check both the source and destination packet addresses. They can also check for specific protocols, port numbers, and other parameters, which allow administrators more flexibility and control.

Reference: <http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/access-control-list.html>

QUESTION 122

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

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Starting with Cisco IOS Software release 12.4(4)T, Control Plane Protection (CPPr) can be used to restrict and/or police control plane traffic destined to the route processor of the Cisco IOS device. Although it is similar to Control Plane Policing (CoPP), CPPr has the ability to restrict/police traffic using finer granularity than that used by CoPP. CPPr divides the aggregate control plane into three separate control plane categories, known as subinterfaces: (1) host, (2) transit, and (3) CEF-exception. In addition, CPPr includes the following additional control plane protection features:

- The port-filtering feature provides for policing/dropping of packets going to closed or nonlistening TCP/UDP ports
- Queue thresholding limits the number of packets for a specified protocol that will be allowed in the control plane IP input queue

Reference: <http://www.cisco.com/c/en/us/about/security-center/understanding-cppr.html>

QUESTION 123

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

Correct Answer: A

Section: (none)

Explanation

**Explanation/Reference:**

Explanation:

Knowledge is power goes the old and equally wise saying. This axiom is applicable to the arena of network attacks as well. The reconnaissance attack is one where the main purpose of the attacker is to find out information about the vulnerable points of the network which is being targeted.

Reference: <https://www.certificationkits.com/cisco-certification/ccna-security-certification-topics/ccna-security-describe-security-threats/ccna-security-common-network-attacks/>

QUESTION 124

Which protocols use encryption to protect the confidentiality of data transmitted between two parties? (Choose two.)

- A. FTP
- B. SSH
- C. Telnet
- D. AAA
- E. HTTPS
- F. HTTP

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

An encrypted connection becomes useless if you've unknowingly connected to a bogus server or a malicious client. While SSH and SSL use symmetric cryptography to preserve the confidentiality of transmitted data, they use another form of encryption for authentication. Authentication allows one party to verify whether the other party is really who it claims it is.

Reference: <http://www.jscape.com/blog/ssl-vs-ssh-simplified>

QUESTION 125

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

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

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

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. Both attack vectors can be easily mitigated with proper switchport configuration.

Reference: https://en.wikipedia.org/wiki/VLAN_hopping

QUESTION 126

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To enable permanent client installation for a specific group or user, use the **anyconnect keep-installer** command from group-policy or username webvpn modes:

anyconnect keep-installer installer

The default is that permanent installation of the client is enabled. The client remains on the remote computer at the end of the session. The following example configures the existing group-policy *sales* to remove the client on the remote computer at the end of the session:

```
hostname(config)# group-policy sales attributes  
hostname(config-group-policy)# webvpn  
hostname(config-group-policy)# anyconnect keep-installer installed none
```

Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/vpn_anyconnect.html

QUESTION 127

Which type of security control is defense in depth?

- A. Threat mitigation
- B. Risk analysis
- C. Botnet mitigation
- D. Overt and covert channels

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Defense in-depth is a technique that uses many layers of network defense to secure a network and all devices connected to that network. The theory behind defense in-depth is to deploy different layers of security in key parts of the network to detect, contain and ultimately stop an attack.

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

QUESTION 128

On which Cisco Configuration Professional screen do you enable AAA

- A. AAA Summary
- B. AAA Servers and Groups

- C. Authentication Policies
- D. Authorization Policies

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

AAA summary screen is used to enable AAA authentication.

Reference: https://books.google.com.pk/books?id=V8kmEemJPlkC&pg=PA81&lpg=PA81&dq=enable+AAA+AAA+summary+screen&source=bl&ots=Yw_pFKTbZ&sig=GxQD3FnhFotUeDenrA4Ssg4oQxg&hl=en&sa=X&ved=0ahUKEwjdlACcoKPNAhUK6xQKH9OAV0Q6AEIMjAE#v=onepage&q=enable%20AAA%20AAA%20summary%20screen&f=false

QUESTION 129

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



Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

SIEM can be used collecting and archiving syslog data and alerting administrators to security events in real time.

Reference: http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-smart-business-architecture/sbaSIEM_deployG.pdf

QUESTION 130

What are the three layers of a hierarchical network design? (Choose three.)

- A. access
- B. core
- C. distribution
- D. user

- E. server
- F. Internet

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Hierarchical network design has access, core and distribution layers.

Reference: <http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4>

QUESTION 131

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

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



Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In-band management can be used when management applications need concurrent access to the device. In-band management can also be used to gain administrator access from multiple locations.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/hubs/fhub316c_t/bmm/install_config/guide/bmmicg/bmminbn.pdf

QUESTION 132

What are two ways to prevent eavesdropping when you perform device-management tasks? (Choose two.)

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

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To prevent eavesdropping during device management tasks, you can use SSH and SNMPv3 to get info on eavesdropping if any.

Reference: <https://www.ietf.org/rfc/rfc5592.txt>

QUESTION 133

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

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

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Two prominent security protocols used to control access into networks are Cisco TACACS+ and RADIUS. The RADIUS specification is described in RFC 2865 leavingcisco.com, which obsoletes RFC 2138 leavingcisco.com. Cisco is committed to supporting both protocols with the best of class offerings. It is not the intention of Cisco to compete with RADIUS or influence users to use TACACS+. You should choose the solution that best meets your needs.

Reference: <http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html>

QUESTION 134

Which three statements describe DHCP spoofing attacks? (Choose three.)

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

F. They can physically modify the network gateway.

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

DHCP spoofing attacks modify traffic in transit and they use man-in-the-middle attacks along with ARP poisoning.

Reference: <https://learningnetwork.cisco.com/thread/67229>

QUESTION 135

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

IF the data breach is occurred within the company and the database has been copied, the confidentiality has been breached.

An employee may steal valuable trade secret information as seen at DuPont. However, not every business has these types of trade secrets. The type of information an employee is most likely to steal is the information needed to do his or her specific job, usually information that is readily available to them. To maintain a competitive advantage, the electronic information an employee uses everyday must be protected. Everyday employees have access to a wide variety of electronic information which range from important (email lists and non-financial business information), to confidential (customer information), to private (employee records), through the most sensitive and potentially damaging data: financial records, databases with enormous company history, trade secrets and intellectual property.

Reference: <https://www.nowsecure.com/blog/2010/08/31/departing-employees-and-data-theft/>

QUESTION 136

In which type of attack does an attacker send email messages that ask the recipient to click a link such as <https://www.cisco.net.cc/securelogon?>

- A. phishing
- B. pharming
- C. solicitation

D. secure transaction

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 137

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

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

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

Explanation:

Phishing attempts most often take the form of an email that seemingly comes from a company the recipient knows or does business with. The most recognized type of phishing attack is similar to the bank example described above, where the email asks the recipient to enter his account credentials on a website.

Reference: <https://digitalguardian.com/blog/what-phishing-attack-defining-and-identifying-different-types-phishing-attacks>

QUESTION 138

Which statement provides the best definition of malware?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Malware" is short for malicious software and used as a single term to refer to virus, spy ware, worm etc. Malware is designed to cause damage to a stand alone computer or a networked pc. So wherever a malware term is used it means a program, which is designed to damage your computer it may be a virus, worm, or Trojan.

Reference: <http://www.symantec.com/connect/articles/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them>

QUESTION 139

What mechanism does asymmetric cryptography use to secure data?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

Reference: <http://searchsecurity.techtarget.com/definition/asymmetric-cryptography>

QUESTION 140

Refer to the exhibit.

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

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

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

With which NTP server has the router synchronized?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

192.168.10.7 is clearly shown in the exhibit. It is NTP server address which is synchronized with router.

QUESTION 141

Refer to the exhibit.

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

tacacs server tacacs2
  address ipv4 2.2.2.2
  timeout 20
  single-connection

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



Which statement about the given configuration is true?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The single connection command cause the device to establish a connection for all TACACS transations.

QUESTION 142

What is the best way to confirm that AAA authentication is working properly?

- A. Use the test aaa command.

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

To associate a dialed number identification service (DNIS) or calling line identification (CLID) user profile with the record that is sent to the RADIUS server or to manually test load-balancing server status, use the test aaa group command in privileged EXEC mode.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-xe-3se-3850-cr-book/sec-s1-xe-3se-3850-cr-book_chapter_0101.html#wp1375904793

QUESTION 143

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.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Protected Extensible Authentication Protocol (PEAP) is an 802.1X authentication type for wireless LANs (WLANs). PEAP provides strong security, user database extensibility, and support for one-time token authentication and password change or aging.

Reference: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-series/prod_qas0900aecd801764fa.html

QUESTION 144

What improvement does EAP-FASTv2 provide over EAP-FAST?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The one improvement EAP-FASTv2 provides is that it allows multiple credentials to be passed in a single EAP exchange. EAP-FAST was unable to do that in a single EAP exchange.

Reference: <https://tools.ietf.org/html/draft-zhou-emu-eap-fastv2-00>

QUESTION 145

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

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

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

Explanation:

The device uses ISE in a way that it acts as a SCEP proxy to enable device to receive a certificate from a central CA server.

Reference: <http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/116068-configure-product-00.html>

QUESTION 146

When an administrator initiates a device wipe command from the ISE, what is the immediate effect?

- A. It requests the administrator to choose between erasing all device data or only managed corporate data.
- B. It requests the administrator to enter the device PIN or password before proceeding with the operation.
- C. It notifies the device user and proceeds with the erase operation.
- D. It immediately erases all data on the device.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In this case, ISE will ask the admin to choose between erasing all device data or only managed corporate data.

QUESTION 147

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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.

Reference: http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/anyconnectadmin30/ac03vpn.html

QUESTION 148

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

One of the main functions of NAT is to enable private IP networks to connect to the Internet. Network address translation replaces a private IP address with a public IP address, translating the private addresses in the internal network into legal, routable addresses that can be used on the public Internet. In this way, NAT

conserves public addresses; for example, NAT rules can be configured to utilize only one public address for the entire network in communications with the outside world.

Reference: http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-3/user/guide/CSMUserGuide_wrapper/NATchap.pdf

QUESTION 149

Refer to the exhibit.

```
R1
Interface GigabitEthernet 0/0
Ip address 10.20.20.4 255.255.255.0

crypto isakmp policy 1
authentication pre-share
lifetime 84600
crypto isakmp key test67890 address 10.20.20.4

R2
Interface GigabitEthernet 0/0
Ip address 10.20.20.4 255.255.255.0

crypto isakmp policy 10
authentication pre-share
lifetime 84600
crypto isakmp key test12345 address 10.30.30.5
```



You have configured R1 and R2 as shown, but the routers are unable to establish a site-to-site VPN tunnel. What action can you take to correct the problem?

- A. Edit the crypto keys on R1 and R2 to match.
- B. Edit the ISAKMP policy sequence numbers on R1 and R2 to match.
- C. Set a valid value for the crypto key lifetime on each router.
- D. Edit the crypto isakmp key command on each router with the address value of its own interface.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Routers will establish a site-to-site VPN tunnel when you edit the crypto keys on R1 and R2 to match.

Reference: http://www.cs.rpi.edu/~kotfid/secvoice10/labs/Security_Ch8_Lab-A-Site2Site-VPN_Instructor.doc

QUESTION 150

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.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The crypto ipsec transform-set myset esp-md5-hmac esp-aes-256 command merges authentication and encryption methods to protect traffic that matches an ACL.

QUESTION 151

Refer to the exhibit.

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The IKE phase 1 main mode was created on 10.1.1.5 but it failed to negotiate with 10.10.10.2.

Reference: http://www.juniper.net/techpubs/software/screenos/screenos6.3.0/630_ce_VPN.pdf

QUESTION 152

Which statement about IOS privilege levels is true?

- A. Each privilege level supports the commands at its own level and all levels below it.
- B. Each privilege level supports the commands at its own level and all levels above it.
- C. Privilege-level commands are set explicitly for each user.
- D. Each privilege level is independent of all other privilege levels.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Use either of these commands with the level option to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the privilege level configuration command to specify commands accessible at various levels.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfpass.html

QUESTION 153

Refer to the exhibit.

```
Username Engineer privilege 9 password 0 configure
Username Monitor privilege 8 password 0 watcher
Username HelpDesk privilege 6 password help
Privilege exec level 6 show running
Privilege exec level 7 show start-up
Privilege exec level 9 configure terminal
Privilege exec level 10 interface
```

Which line in this configuration prevents the HelpDesk user from modifying the interface configuration?

- A. Privilege exec level 9 configure terminal
- B. Privilege exec level 10 interface
- C. Username HelpDesk privilege 6 password help
- D. Privilege exec level 7 show start-up

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To enable a privileged user to view the entire configuration in memory, the user needs to modify privileges for all commands that are configured on the router. For example:

```
aaa new-model
```

```
aaa authentication login default local
```

```
aaa authorization exec default local
```

```
username john privilege 9 password 0 doe
```

```
username six privilege 6 password 0 six
```

```
username poweruser privilege 15 password poweruser
```

```
username inout password inout
```

```
username inout privilege 15 autocommand show running
```

```
privilege configure level 8 snmp-server community
```

```
privilege exec level 6 show running
```

```
privilege exec level 8 configure terminal
```

Reference: <http://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/23383-showrun.html>

QUESTION 154

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

This command performs the same function as the distance command used with an access list. However, the distance ospf command allows you to set a distance for an entire group of routes, rather than a specific route that passes an access list.

A common reason to use the distance ospf command is when you have multiple OSPF processes with mutual redistribution, and you want to prefer internal routes from one over external routes from the other.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfospf.html

QUESTION 155

Which feature filters CoPP packets?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Access control lists (ACLs) cannot be applied directly to the control plane subinterfaces. Instead, ACLs are used within the MQC policies (that is, class maps) and the service policy is then applied to the individual control plane subinterfaces.

Reference: <http://www.cisco.com/c/en/us/about/security-center/understanding-cppr.html>

QUESTION 156

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

MAC flooding is the act of attempting to overload the switches content addressable memory (CAM) table. By sending a large stream of packets with random addresses, the CAM table of the switch will evenly fill up and the switch can hold no more entries; some switches might divert to a "fail open" state. This means that all frames start flooding out all ports of the switch.

Reference: <http://howdoesinternetwork.com/2011/mac-address-flooding>

QUESTION 157

Which type of PVLAN port allows hosts in the same VLAN to communicate directly with each other?

- A. community for hosts in the PVLAN
- B. promiscuous for hosts in the PVLAN
- C. isolated for hosts in the PVLAN
- D. span for hosts in the PVLAN

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Private VLANs (PVANs) allow splitting the domain into multiple isolated broadcast "subdomains", introducing sub-VLANs inside a VLAN. As we know, Ethernet VLANs can not communicate directly with each other – they require a L3 device to forward packets between separate broadcast domains. The same restriction applies to PVLANS – since the subdomains are isolated at Level 2, they need to communicate using an upper level (L3/packet forwarding) device – such as router.

Reference: <http://blog.ine.com/tag/private-vlan/>

QUESTION 158

What is a potential drawback to leaving VLAN 1 as the native VLAN?

- A. It may be susceptible to a VLAN hopping attack.
- B. Gratuitous ARPs might be able to conduct a man-in-the-middle attack.
- C. The CAM might be overloaded, effectively turning the switch into a hub.
- D. VLAN 1 might be vulnerable to IP address spoofing.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If you leave VLAN 1 as native, your network might be susceptible to a VLAN hopping attack.

Reference: <http://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=3>

QUESTION 159

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

- A. You must configure two zone pairs, one for each direction.
- B. You can configure a single zone pair that allows bidirectional traffic flows for any zone.
- C. You can configure a single zone pair that allows bidirectional traffic flows for any zone except the self zone.
- D. You can configure a single zone pair that allows bidirectional traffic flows only if the source zone is the less secure zone.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If there are two zones and you require policies for traffic going in both directions (from Z1 to Z2 and Z2 to Z1), you must configure two zone pairs (one for each direction).

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xr-3s/sec-data-zbf-xr-book/sec-zone-pol-fw.html#GUID-16FD9685-CB43-45AF-9D24-F6E2E6467FF3

QUESTION 160

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.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

QUESTION 161

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

If you have "same-security-traffic permit inter-interface" configured and have 2 interfaces with same "security-level" value and you have "access-list" configured on both interfaces then the ACLs will handle the decision of what traffic is allowed and what is not.

Reference: <https://supportforums.cisco.com/discussion/11852506/asa-91-code-enable-traffic-between-interfaces-same-security-levels>

QUESTION 162

Which IPS mode provides the maximum number of actions?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

IPS inline provides maximum number of actions.

Reference: <http://www.cisco.com/c/en/us/td/docs/security/ips/5-1/configuration/guide/cli/cliguide/cliEvAct.html>

QUESTION 163

How can you detect a false negative on an IPS?

- A. View the alert on the IPS.
- B. Review the IPS log.
- C. Review the IPS console.
- D. Use a third-party system to perform penetration testing.
- E. Use a third-party to audit the next-generation firewall rules.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You need a third party system to perform penetration testing to identify false negative on IPS.

Reference: <http://airccse.org/journal/ijstpm/papers/4115ijstpm04.pdf>

QUESTION 164

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

You can choose from the following summarization options:

- fire-all—Fires an alert each time the signature is triggered. If the threshold is set for summarization, alerts are fired for each execution until summarization occurs. After summarization starts, only one alert every summary interval fires for each address set. Alerts for other address sets are either all seen or separately summarized. The signature reverts to fire all mode after a period of no alerts for that signature.
- summary—Fires an alert the first time a signature is triggered, and then additional alerts for that signature are summarized for the duration of the summary interval. Only one alert every summary interval should fire for each address set. If the global summary threshold is reached, the signature goes into global summarization mode.
- global-summarization—Fires an alert for every summary interval. Signatures can be preconfigured for global summarization.
- fire-once—Fires an alert for each address set. You can upgrade this mode to global summarization mode.

Reference: http://www.cisco.com/c/en/us/td/docs/security/ips/7-0/configuration/guide/cli/cliguide7/cli_event_action_rules.html

QUESTION 165

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

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Choose allow with inspection to block only malicious traffic from a specific end user.

Reference: <https://popravak.wordpress.com/2015/05/20/sourcefire-access-control-policies-part-two/>

QUESTION 166

How can FirePOWER block malicious email attachments?

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

D. It sends an alert to the administrator to verify suspicious email messages.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

FirePOWER forwards email request to an external signature engine

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

QUESTION 167

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

- **Enable policy**—Enables or disables the individual policy; the global URL Filtering setting overrides the specifications of an individual policy.
- **URL Category**—Choose a filtering action for the URL categories to which you want to restrict access. There are over 80 categories segmented in seven logical groups. You can create custom categories in **HTTP > Configuration > Custom Categories**.

The following describes the available filtering actions:

- **Allow**—Connection to the target server is allowed and users can access the Web site.

- **Block**—Connection to the target server is not established and users are not allowed to access the Web site. A log entry is also created for this event.

- **Block w/Override**—Connection to target service is not established unless the user can type a specific password to override the category blocking.

Reference: https://docs.trendmicro.com/all/ent/iwsva/v5.5/en-us/iwsva_5.5_olh/urlf_policy_rule.htm

QUESTION 168

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

File analysis rate data fidelity to provide an authenticated hash for data.

Reference: http://www.cisco.com/c/en/us/td/docs/security/ips/7-1/configuration/guide/idm/idmguide71/idm_collaboration.html

QUESTION 169

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

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Software encryption has the broadest platform support to protect operating systems

Reference: <https://marketplace.cisco.com/catalog/companies/vormetric/products/vormetric-data-security>

QUESTION 170

A proxy firewall protects against which type of attack?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Cross-site scripting involves the injection of malicious scripts into web pages, where they can be used to gain access to user's systems or to sensitive information. The Cisco ACE Web Application Firewall provides rules that inspect messages for JavaScript, ECMAScript, VBScript and other types of code artifacts that could indicate a cross-site scripting attack.

Reference: http://www.cisco.com/c/en/us/td/docs/app_ntwk_services/data_center_app_services/ace_waf/v60/gettingstarted/guide/acewafgsg/waf_gs_XSS_attacks.html

QUESTION 171

What is a benefit of a web application firewall?

- A. It blocks known vulnerabilities without patching applications.
- B. It simplifies troubleshooting.
- C. It accelerates web traffic.
- D. It supports all networking protocols.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Web application firewall blocks a cache of known vulnerabilities without patching applications

Reference: <http://searchsecurity.techtarget.com/feature/Introduction-to-Web-application-firewalls-in-the-enterprise>

QUESTION 172

Which feature of the Cisco Email Security Appliance can mitigate the impact of snowshoe spam and sophisticated phishing attacks?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

The Email Security Appliance is the industry's first proven zero-hour antivirus solution. It offers a best-in-class capability to control and encrypt sensitive outbound email. At the same time, its layered defense, built into a single appliance, quickly blocks incoming attacks. It provides:

- Contextual analysis against phishing and snowshoe spam attacks
- A superior spam-capture rate (more than 99 percent) with few false positives (less than one in one million)
- File reputation, dynamic analysis (sandboxing), and retrospective security with Cisco AMP Threat Grid
- Graymail management and web interaction tracking

Reference: <http://www.cisco.com/c/en/us/products/security/email-security-appliance/index.html>

QUESTION 173

Which NAT type allows only objects or groups to reference an IP address?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Dynamic PAT translates multiple real addresses to a single mapped IP address by translating the real source address and source port to the mapped address and unique mapped port. Each connection requires a separate translation session because the source port differs for each connection.

Reference: <http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/111842-asa-dynamic-pat-00.html>

QUESTION 174

Which feature allows a dynamic PAT pool to select the next address in the PAT pool instead of the next port of an existing address?

- A. next IP
- B. round robin
- C. dynamic rotation
- D. NAT address rotation

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Check the Round Robin check box to assign addresses/ports in a round-robin fashion. By default without round robin, all ports for a PAT address will be allocated before the next PAT address is used. The round-robin method assigns one address/port from each PAT address in the pool before returning to use the first address again, and then the second address, and so on.

Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/asdm65/configuration_guide/asa_cfg_asdm_65/nat_objects.html

QUESTION 175

Your security team has discovered a malicious program that has been harvesting the CEO's email messages and the company's user database for the last 6 months. What are two possible types of attacks your team discovered? (Choose two.)

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

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In this case, advanced persistent threat and targeted malware might do the damage according to the scenario given in the question.

Reference: <http://www.spamtitan.com/blog/category/phishing-email-spam/>

QUESTION 176

Refer to the exhibit.

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

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

- A. It configures authentication to use AES 256.

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

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

To define a transform set—an acceptable combination of security protocols and algorithms—use the **crypto ipsec transform-set** global configuration command. To delete a transform set, use the **no** form of the command.

crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]

no crypto ipsec transform-set transform-set-name

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srfipsec.html#wp1017694

QUESTION 177

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

- A. when a matching TCP connection is found
- B. when the firewall requires strict HTTP inspection
- C. when the firewall receives a FIN packet
- D. when matching ACL entries are configured
- E. when the firewall requires HTTP inspection
- F. when matching NAT entries are configured

Correct Answer: ADF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

During normal operations, ASA firewall permit inbound HTTP GET requests when a matching TCP connection is found and a matching ACL entries are configured or when the firewall requires HTTP inspection.

Reference: <https://supportforums.cisco.com/document/69281/asa-using-packet-capture-troubleshoot-asa-firewall-configuration-and-scenarios>

QUESTION 178

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The **Root Guard** feature can be enabled on all switch ports in the network off of which the root bridge should not appear (that is, every port that is not a root port, the port on each switch that is considered to be closest to the root bridge). If a port configured for Root Guard receives a superior BPDU, instead of believing the BPDU, the port goes into a root-inconsistent state. While a port is in the root-inconsistent state, no user data is sent across it. However, after the superior BPDUs stop, the port returns to the forwarding state.

The **BPDU Guard** feature is enabled on ports configured with the Cisco PortFast feature. The PortFast feature is enabled on ports that connect to end-user devices, such as PCs. It reduces the amount of time required for the port to go into forwarding state after being connected. The logic of PortFast is that a port that connects to an end-user device does not have the potential to create a topology loop. Therefore, the port can go active sooner by skipping STP's listening and learning states, which by default take 15 seconds each. Because these PortFast ports are connected to end-user devices, they should never receive a BPDU. Therefore, if a port enabled for BPDU Guard receives a BPDU, the port is disabled.

Reference: <https://learningnetwork.cisco.com/thread/4575>