

Monitoring > VPN > VPN Statistics > Sessions

Type	Active	Cumulative	Peak Concurrent	Ina
Clientless VPN	2	7	7	2
Browser	2	7	7	2

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

Username IP Address	Group Policy Connection Profile	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx
bob1 192.168.1.20	GroupPolicy1 TunnelGroup1	Clientless RC4	22:34:45 UTC Sun Oct 7 2012 0h:00m:37s	2836 7086
bob1 192.168.1.20	GroupPolicy1 TunnelGroup1	Clientless RC4	22:35:04 UTC Sun Oct 7 2012 0h:00m:18s	2836 7071

Clientless SSL VPN:

Implementing a working configuration

Decide on policy, and where to implement it
Create the group, con-profile and user
Test and verify

Requirement:

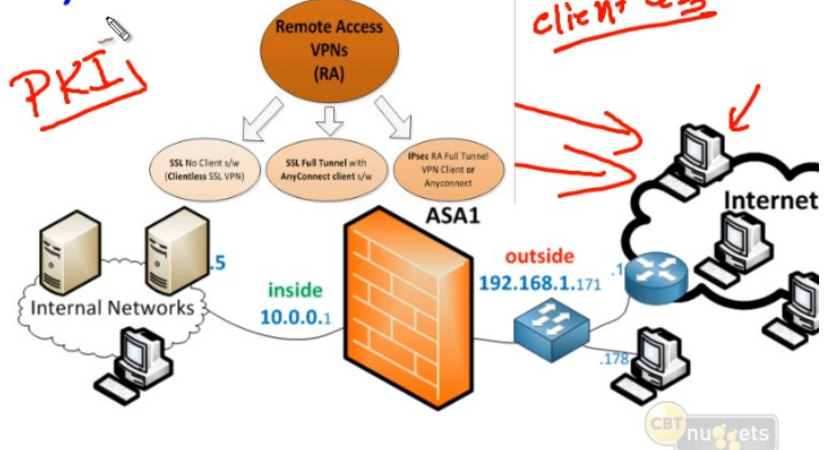
Type of VPN:
Random machines on Internet
They all support global PKI (SSL)
Not managed by company

Group Level:
Banner message
Custom bookmark
WebType ACL
Allow portal URL browsing

User Level:
New user in new Sales group
Require use of specific connection profile

Connection profile:
Use LOCAL AAA
Name: sales-con-prof
Alias: sales-con-alias
Custom URL: http://192.168.1.171/sales
Connections supported: SSL Clientless only
Connection profile linked to sales group

PKI



Requirement:

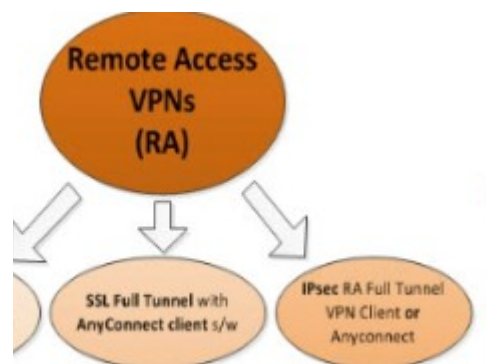
Requirement:

Type of VPN:
Random machines on Internet
They all support global PKI (SSL)
Not managed by company

Group Level:
Banner message
Custom bookmark
WebType ACL
Allow portal URL browsing

User Level:
New user in new Sales group
Require use of specific connection profile

Connection profile:
Use LOCAL AAA
Name: sales-con-prof
Alias: sales-con-alias
Custom URL: http://192.168.1.171/sales
Connections supported: SSL Clientless only
Connection profile linked to sales group



CISCO ASDM 5.4 101 AS

File View Tools Wizards

Home Configuration

Remote Access VPN

- Introduction
- Network (Client) Access
- Clientless SSL VPN Access
- Connection Profiles
- Portal
- Group Policies
- Dynamic Access Policy
- Advanced
- AAA/Local Users
- Host Scan Image
- Secure Desktop Management
- Certificate Management
- Language Localization
- DHCP Server
- DNS
- Advanced

Device Setup

Firewall

Remote Access VPN

Add Internal Group Policy

General

Portal

More Options

Name: Sales-Group

Banner: ☐ Inherit Welcome to sales. The Sales group policy is being applied.

More Options

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

Web ACL: ☐ Inherit Sales-web-acls [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 ☐ Unlimited minutes

Timeout Alerts

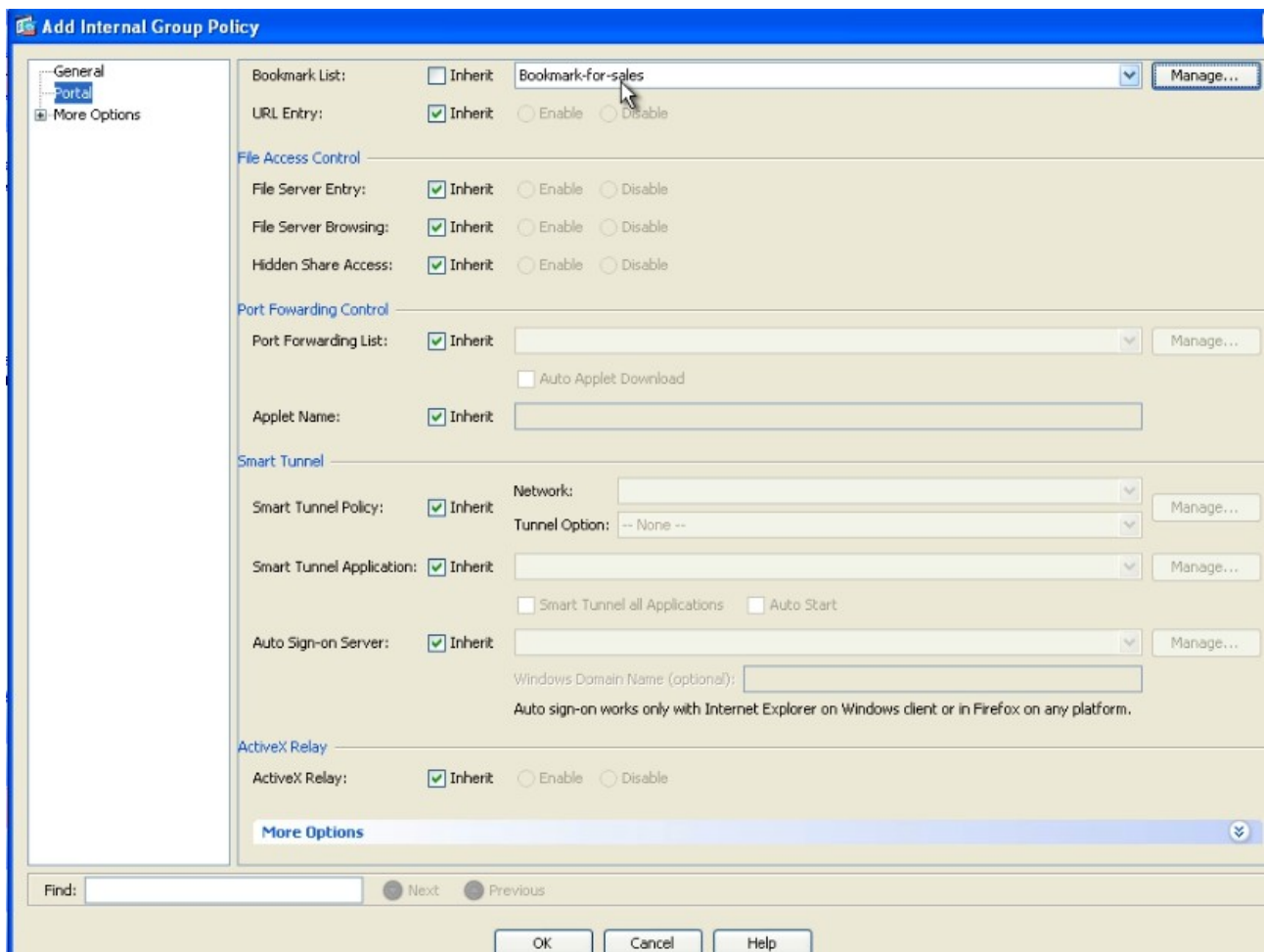
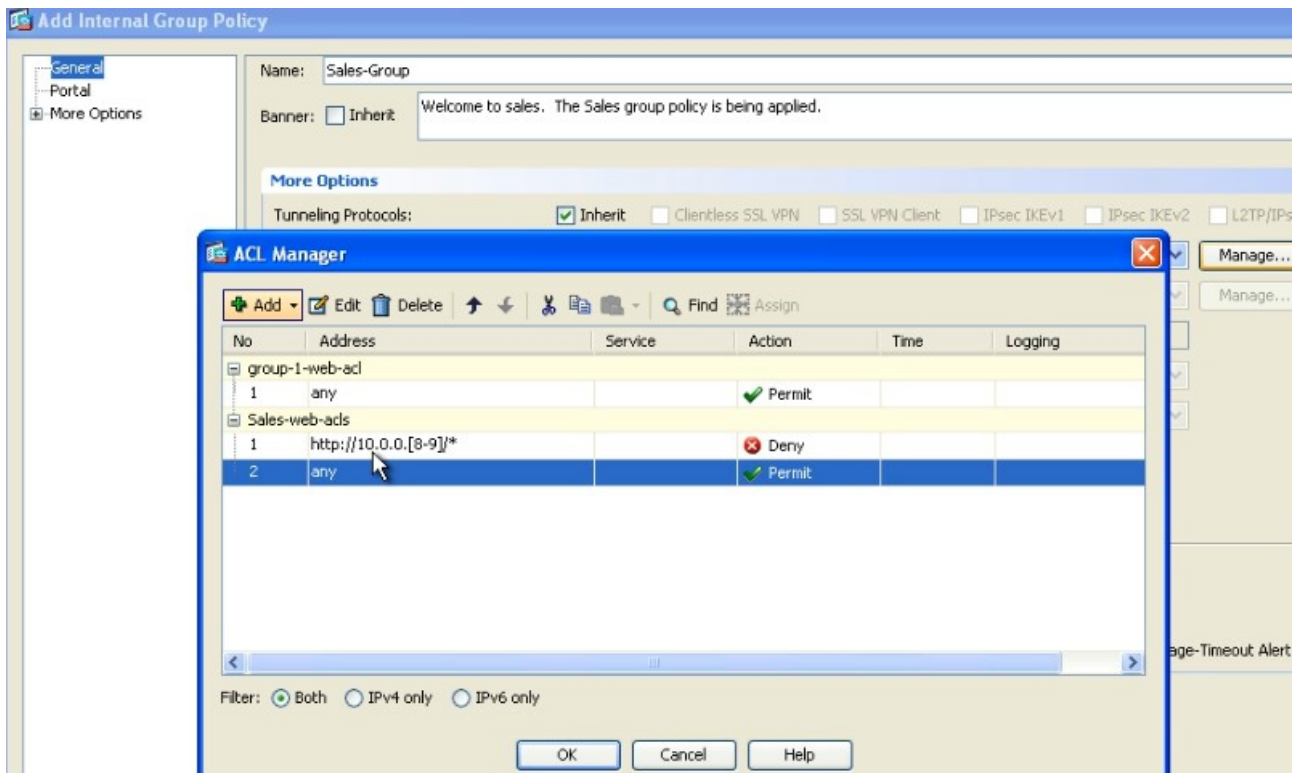
Session Alert Interval: ☒ Inherit ☐ Default minutes

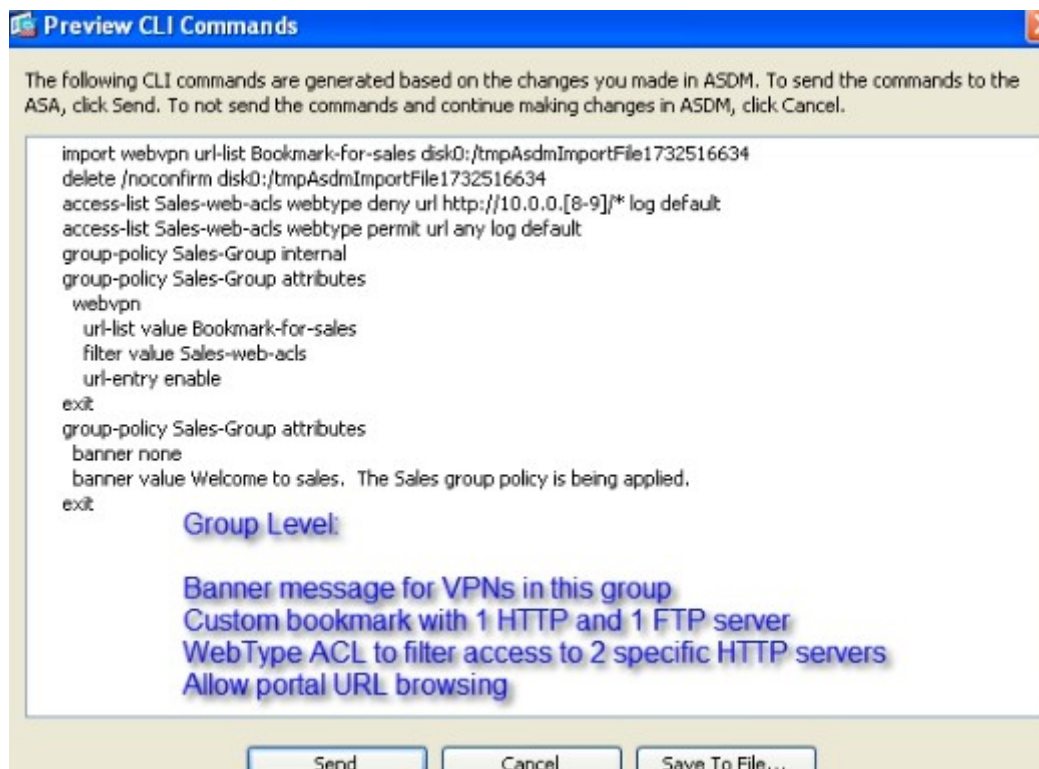
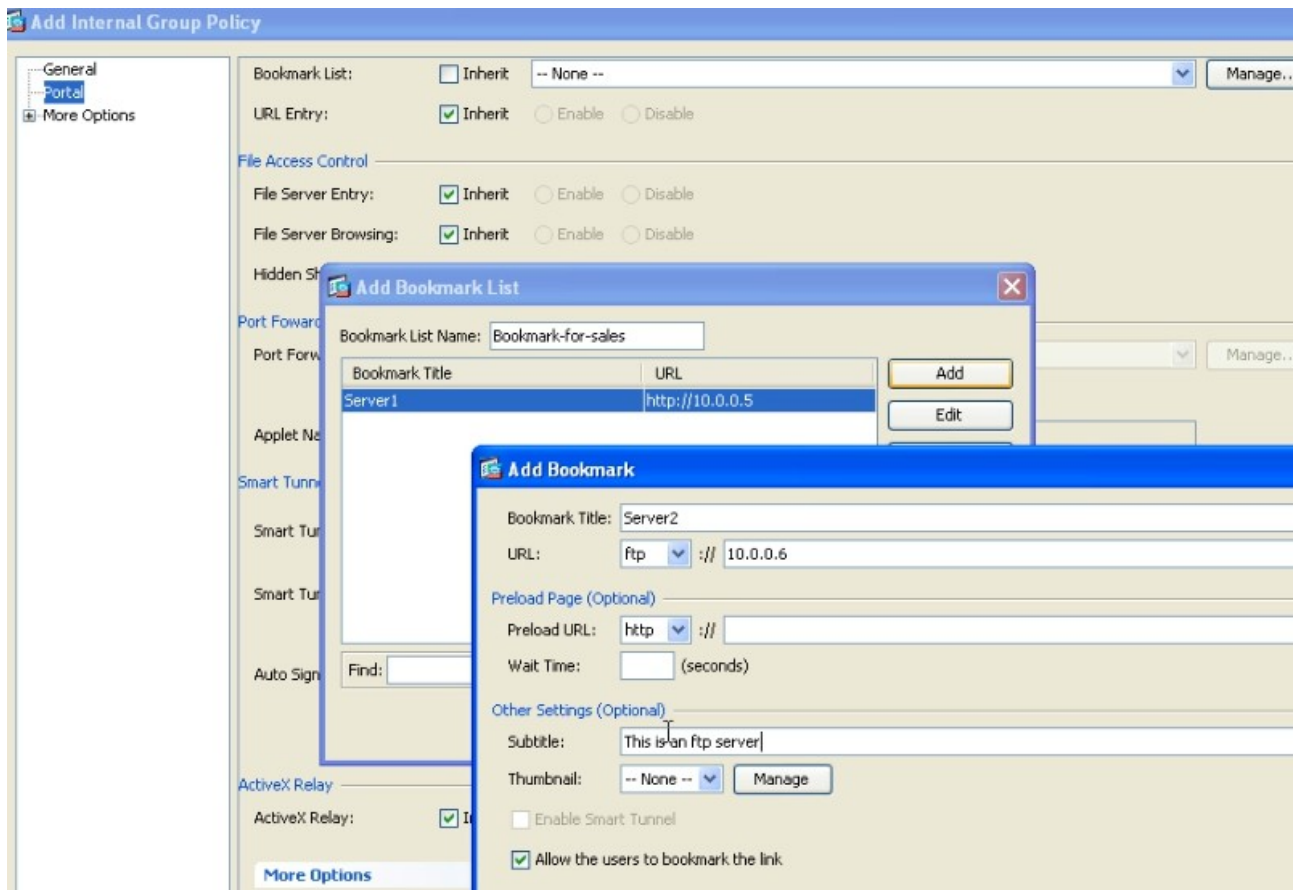
Idle Alert Interval: ☒ Inherit ☐ Default minutes

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

Group Level:

- Banner message for VPNs in this group
- Custom bookmark with 1 HTTP and 1 FTP server
- WebType ACL to filter access to 2 specific HTTP servers
- Allow portal URL browsing





We are using the same User Profile Group Policy and the Connection Profile Group Policy as the same: Sales-Group

Basic

Name: sales-con-profile
Aliases: sales-con-alias

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

DNS
Server Group: DefaultDNS
(Following fields are attributes of the DNS server group selected above.)
Servers: 10.0.0.40
Domain Name: CBTNuggets.com

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

Connection profile:
Use LOCAL AAA
Name: sales-con-profile
Alias: sales-con-alias
Custom URL: http://192.168.1.171/sales
Connections supported: SSL Clientless

Advanced

Login and Logout Page Customization: ☐ 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
sales-con-alias	<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://192.168.1.171/sales	<input checked="" type="checkbox"/>

☐ Do not 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.)

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"/>
inside	<input type="checkbox"/>
sales	<input type="checkbox"/>

☒ Enable inbound VPN sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

Login Page Setting

☒ Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

☐ 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: Match Case

Name	Enabled	Aliases	Authentication Method	Group Policy
DefaultRAGroup	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>		AAA(LOCAL)	DfltGrpPolicy
TunnelGroup1	<input checked="" type="checkbox"/>	TunnelGroup1-alias	AAA(LOCAL)	GroupPolicy2
TunnelGroup2	<input checked="" type="checkbox"/>	TunnelGroup2-alias	AAA(LOCAL)	GroupPolicy3
sales-con-profile	<input checked="" type="checkbox"/>	sales-con-alias	AAA(LOCAL)	Sales-Group

Preview CLI Commands

The following CLI commands are generated based on the changes you made in ASA, click Send. To not send the commands and continue making changes in ASA, click Cancel.

```

group-policy Sales-Group attributes
  vpn-tunnel-protocol ssl-clientless
exit
tunnel-group sales-con-profile type remote-access
tunnel-group sales-con-profile general-attributes
  default-group-policy Sales-Group
tunnel-group sales-con-profile webvpn-attributes
  group-alias sales-con-alias enable
group-url https://192.168.1.171/sales enable
  
```

Cisco ASDM 6.4.101 ASDM

Add User Account

Username: sales-users
Password: *****
Confirm Password: *****

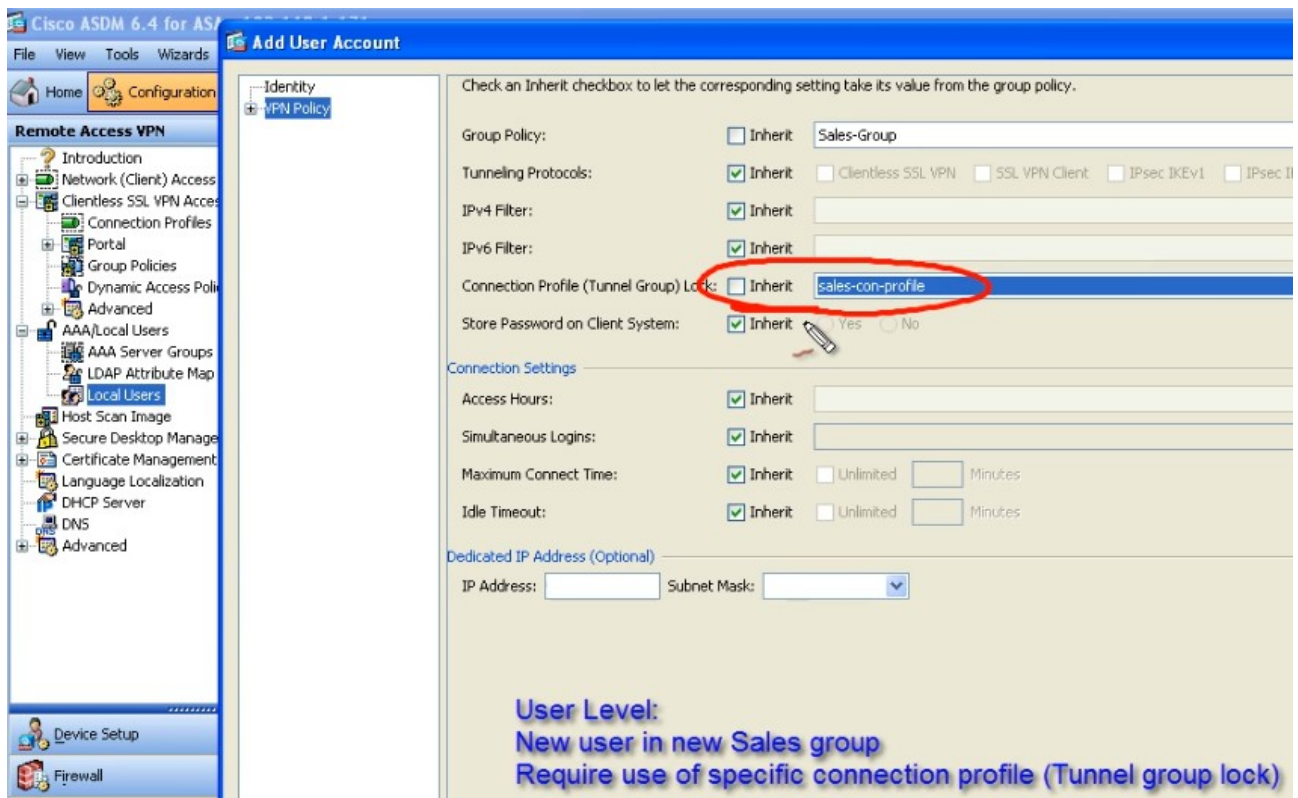
☐ User authenticated using MSCHAP

Access Restriction
Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
Note: All users have network access, regardless of these settings.

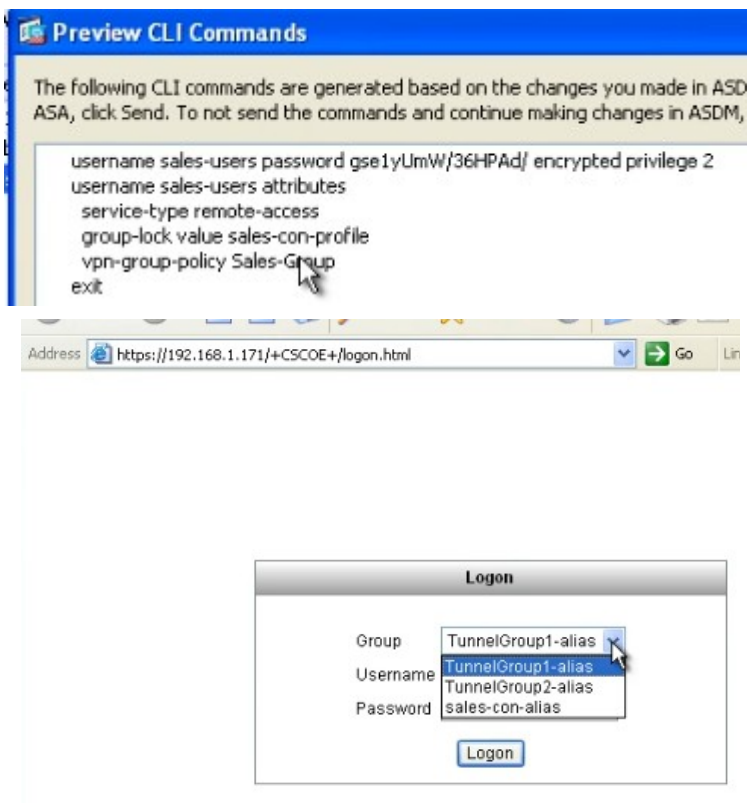
☐ Full access(ASDM, SSH, Telnet and Console)
Privilege level is used with command authorization.
Privilege Level: 2

☐ CLI login prompt for SSH, Telnet and console (no ASDM access)
This setting is effective only if "aaa authentication http console LOCAL" command is configured.

☒ No ASDM, SSH, Telnet or Console access
This setting is effective only if "aaa authentication http console LOCAL" and "aaa authorization exec" commands are configured.



Tunnel Group Lock is important.







Address  https://192.168.1.171/+CSCOE+/portal.html?next=portal 


Welcome to sales. The Sales group policy is being applied.

Cancel


Continue

Address  https://192.168.1.171/+CSCOE+/portal.html  Go Links >>  


Home
Web Access
File Access

Address http://  Browse

Web Bookmarks

 Server1
This is server1 it is a web server.

File Bookmarks

 Server2
This is an ftp server. Have fun.

10.0.0.8 is denied based on the WebTypeACL:

Connection failed

Access to this resource has been denied.

Back

Syslog Details				
Severity:	 6 (Informational)	Date:	Oct 08 2012	Source IP:
Syslog ID:	716004	Time:	20:17:11	Destination IP:
Description:	Group <Sales-Group> User <sales-user> IP <192.168.1.20> WebVPN access DENIED to specified location: http://10.0.0.8/			

```
ASA1(config)# show vpn-sessiondb webvpn
```

Session Type: WebVPN

Username	: sales-user	Index	: 14
Public IP	: 192.168.1.20		
Protocol	: Clientless		
License	: AnyConnect Premium		
Encryption	: RC4	Hashing	: SHA1
Bytes Tx	: 2848	Bytes Rx	: 15030
Group Policy	: Sales-Group	Tunnel Group	: sales-con-profile
Login Time	: 20:25:06 UTC Mon Oct 8 2012		
Duration	: 0h:04m:02s		
Inactivity	: 0h:00m:00s		
NAC Result	: Unknown		
VLAN Mapping	: N/A	VLAN	: none

```
ASA1(config)#
```