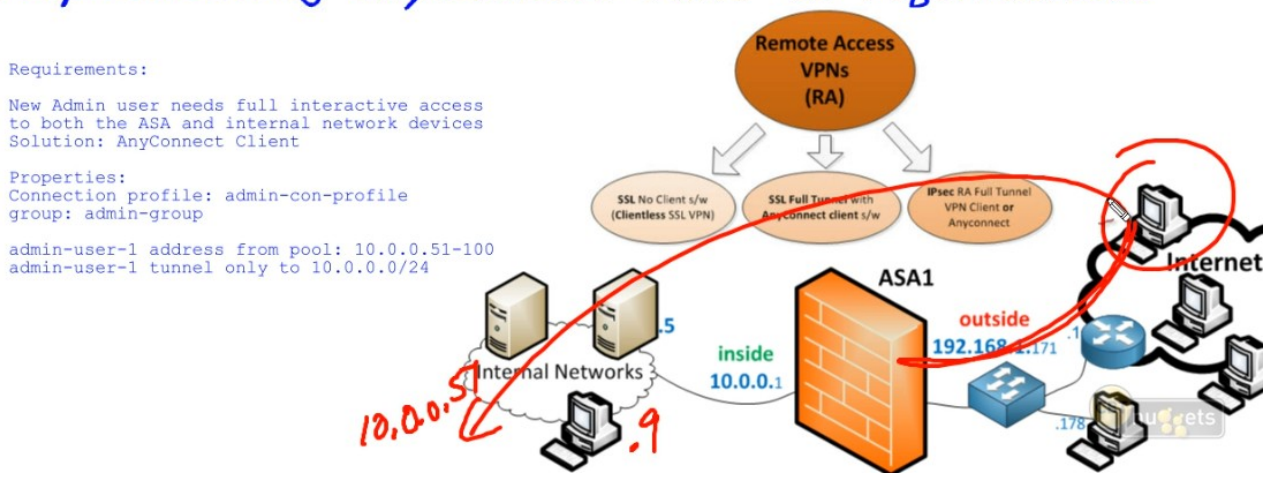
There are so many custom applications or some applications that require the users to be on the same network as the internal network as opposed to clientless ssl vpn so we use AnyConnect SSL full tunnel VPN or IPSec on Anyconnect or IPSec on legacy cisco vpn client.

AnyConnect SSL VPN Client:

Using the client for a "full" tunnel

Review of "when" we would use this option
Implementing AnyConnect based on requirements



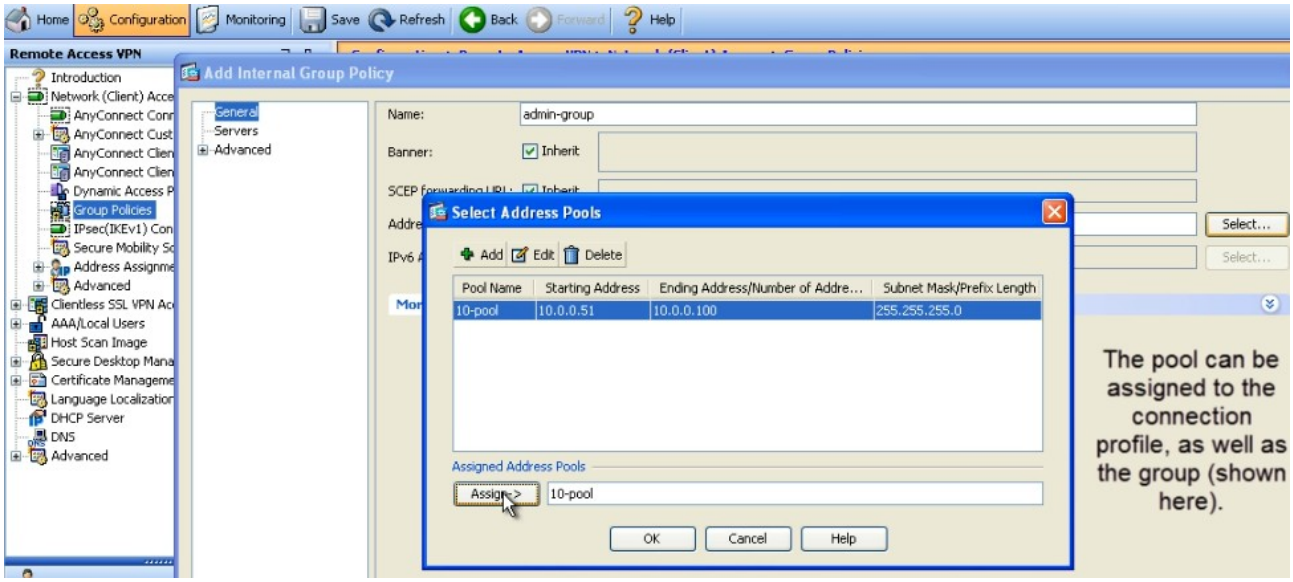
Requirements:

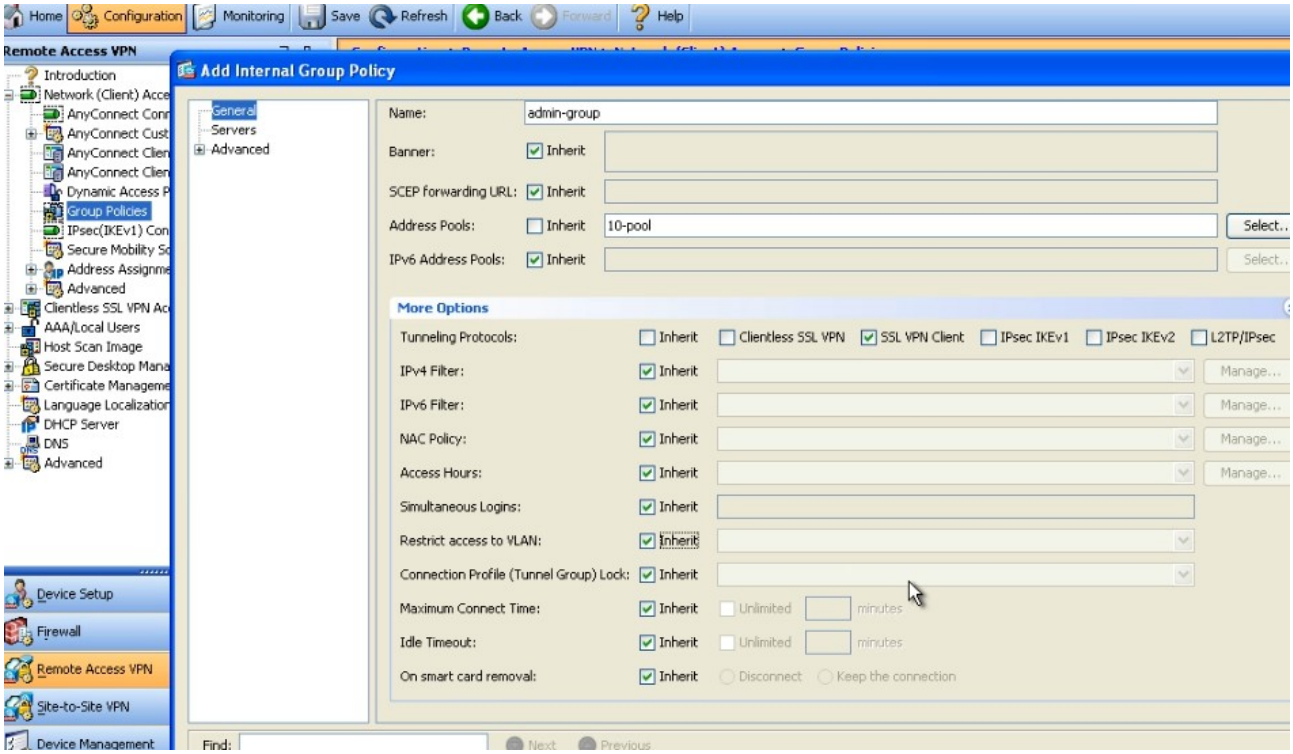
New Admin user needs full interactive access
to both the ASA and internal network devices
Solution: AnyConnect Client

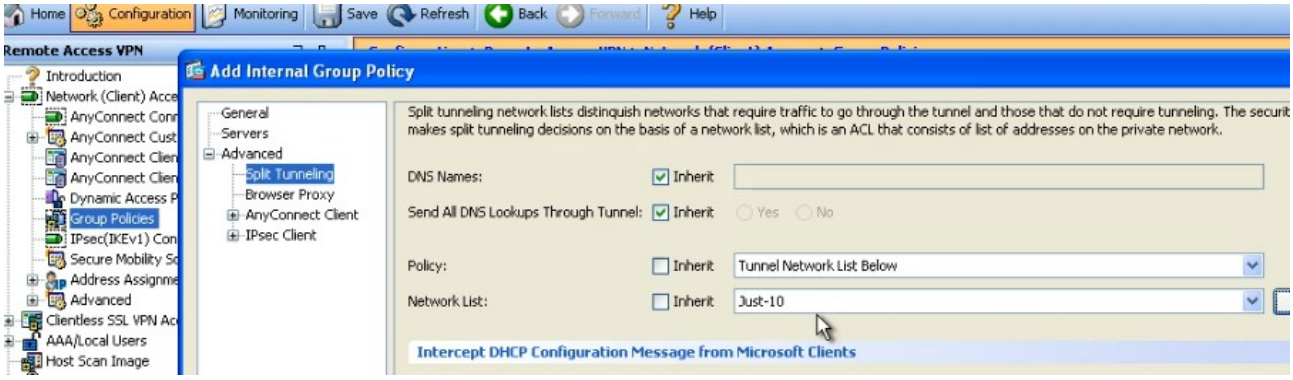
Properties:
Connection profile: admin-con-profile
group: admin-group

admin-user-1 address from pool: 10.0.0.51-100
admin-user-1 tunnel only to 10.0.0.0/24

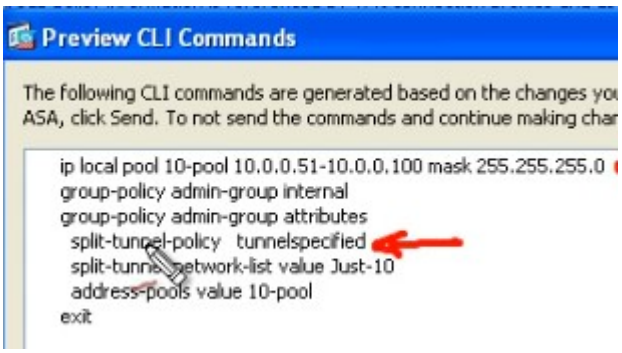
Split tunnel (don't send the traffic over the SSL VPN unless it is destined for the corporate network), so rest of the traffic including the internet traffic doesn't go across the SSL VPN.
Or we can tunnel everything except the local subnet of the client.
By default it is a full tunnel.

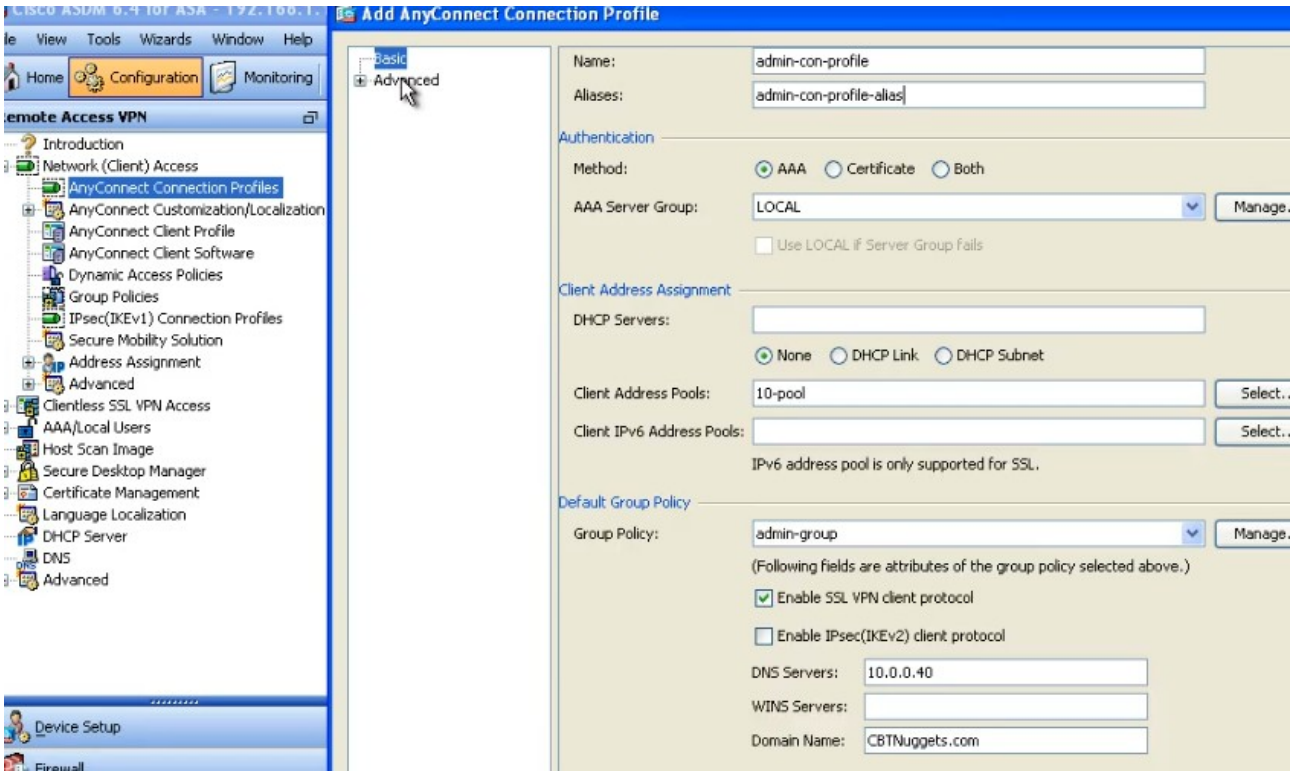

Add Internal Group Policy
General
Servers
Advanced
Name: admin-group
Banner: Inherit
Select Address Pools
Add Edit Delete
Pool Name | Starting Address | Ending Address/Number of Addre... | Subnet Mask/Prefix Length
10-pool | 10.0.0.51 | 10.0.0.100 | 255.255.255.0
Assigned Address Pools
Assign >
10-pool
OK Cancel Help
The pool can be assigned to the connection profile, as well as the group (shown here).

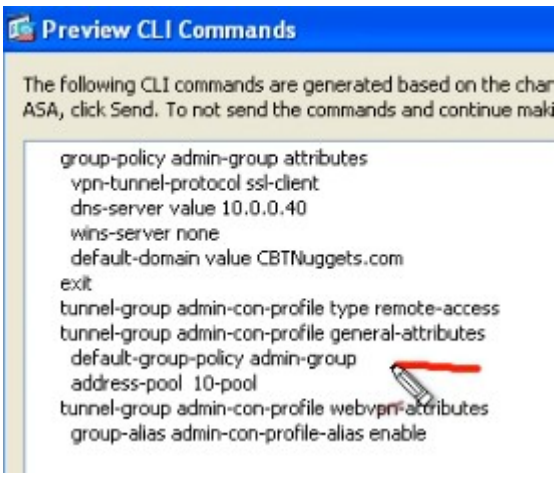

Add Internal Group Policy
General
Servers
Advanced
Name: admin-group
Banner: Inherit
SCEP forwarding URL: Inherit
Address Pools: Inherit 10-pool
IPv6 Address Pools: Inherit
More Options
Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/IPsec
IPv4 Filter: Inherit
IPv6 Filter: Inherit
NAC Policy: Inherit
Access Hours: Inherit
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
On smart card removal: Inherit Disconnect Keep the connection

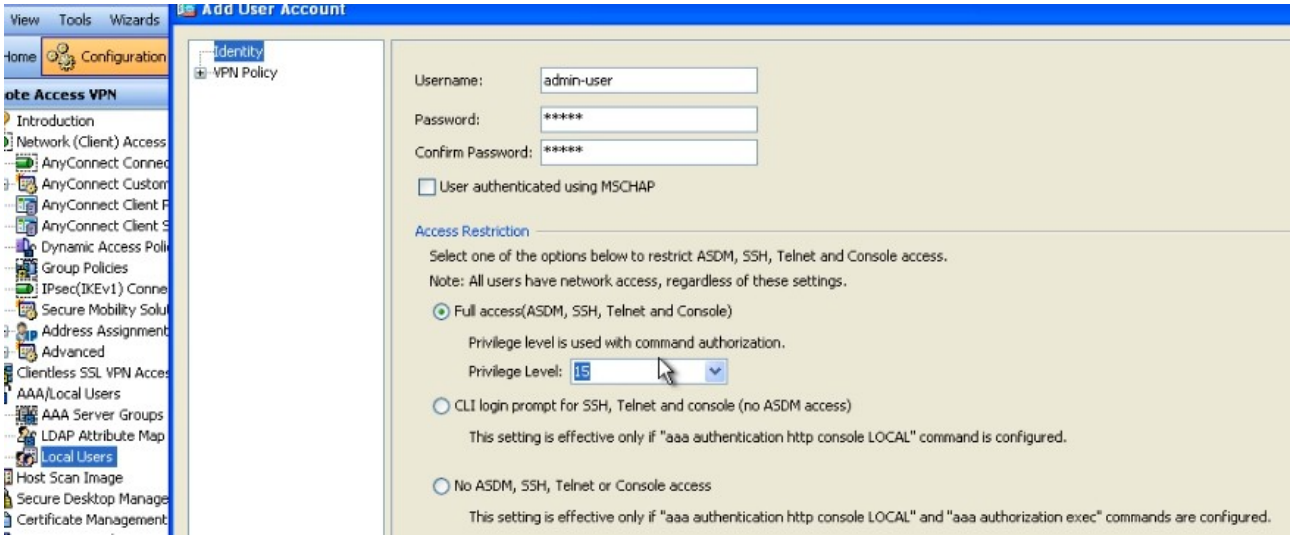

Add Internal Group Policy
General
Servers
Advanced
Split Tunneling
Browser Proxy
AnyConnect Client
IPsec Client
Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The securit
makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.
DNS Names: Inherit
Send All DNS Lookups Through Tunnel: Inherit Yes No
Policy: Inherit Tunnel Network List Below
Network List: Inherit Just-10
Intercept DHCP Configuration Message from Microsoft Clients

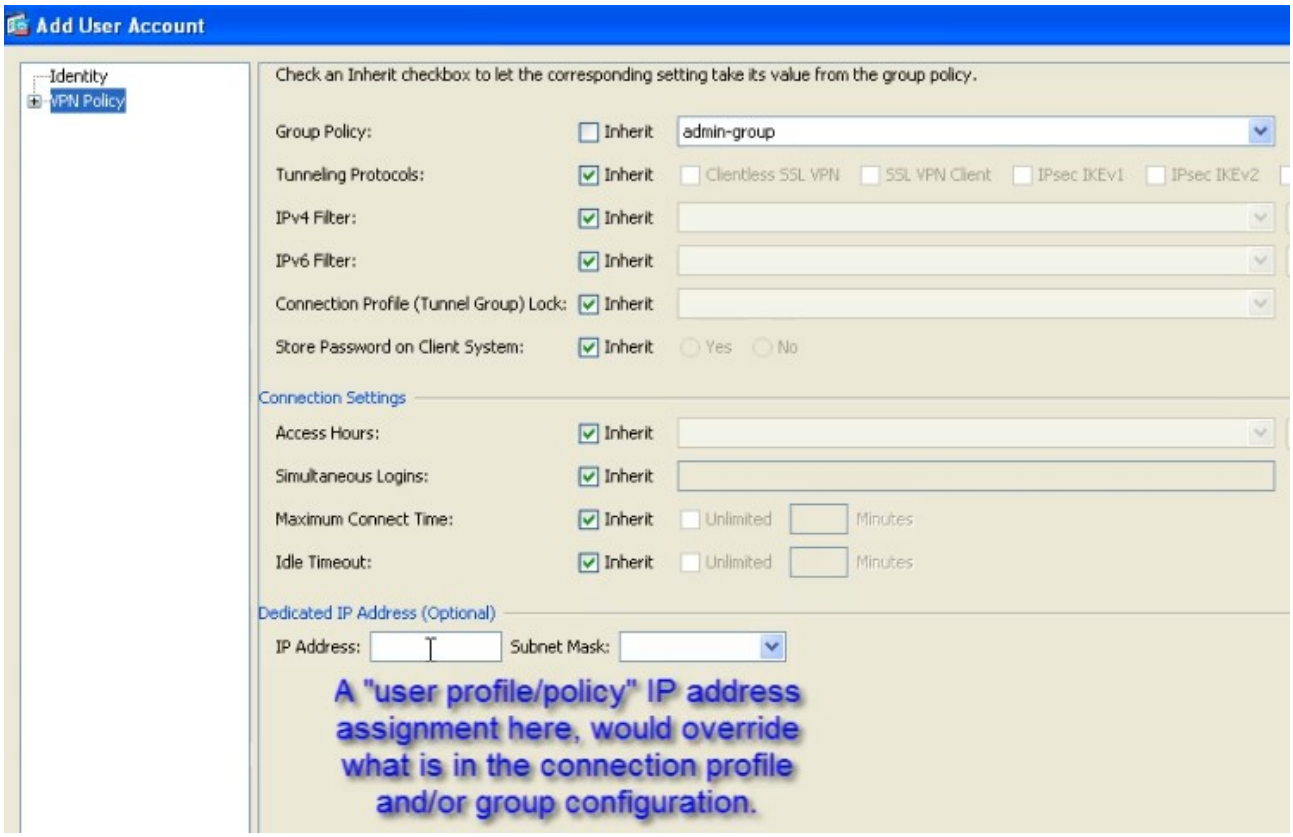

Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
Remote Access VPN
Introduction
Network (Client) Acce
AnyConnect Conn
AnyConnect Cust
AnyConnect Clien
AnyConnect Clien
Dynamic Access P
Group Policies
IPsec(IKEv1) Con
Secure Mobility So
Address Assignme
Advanced
Clientless SSL VPN Ac
AAA/Local Users
Host Scan Image
ACL Manager
Standard ACL
Extended ACL
Add
Edit
Delete
No
Address
Action
Description
Just-10
1
inside-network/24
Permit

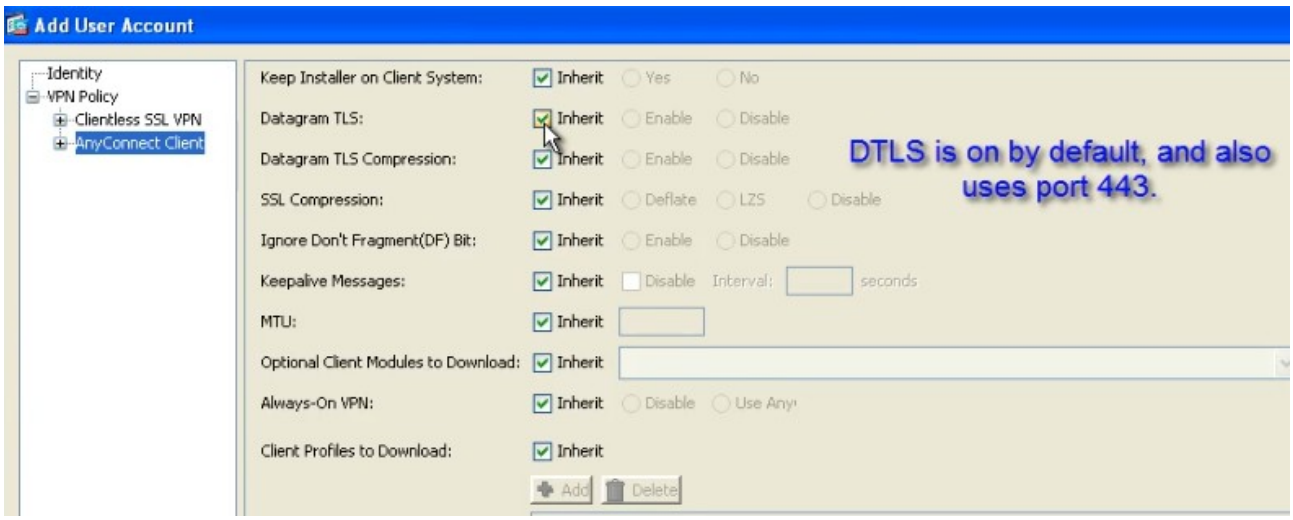

Preview CLI Commands
The following CLI commands are generated based on the changes yo
ASA, click Send. To not send the commands and continue making char
ip local pool 10-pool 10.0.0.51-10.0.0.100 mask 255.255.255.0
group-policy admin-group internal
group-policy admin-group attributes
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Just-10
address-pools value 10-pool
exit


Add AnyConnect Connection Profile
View
Tools
Wizards
Window
Help
Home
Configuration
Monitoring
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced
Device Setup
Basic
Advanced
Name:
admin-con-profile
Aliases:
admin-con-profile-alias
Authentication
Method:
AAA
Certificate
Both
AAA Server Group:
LOCAL
Manage
Use LOCAL if Server Group fails
Client Address Assignment
DHCP Servers:
None
DHCP Link
DHCP Subnet
Client Address Pools:
10-pool
Select
Client IPv6 Address Pools:
IPv6 address pool is only supported for SSL.
Default Group Policy
Group Policy:
admin-group
(Following fields are attributes of the group policy selected above.)
Enable SSL VPN client protocol
Enable IPsec(IKEv2) client protocol
DNS Servers:
10.0.0.40
WINS Servers:
Domain Name:
CBTNuggets.com

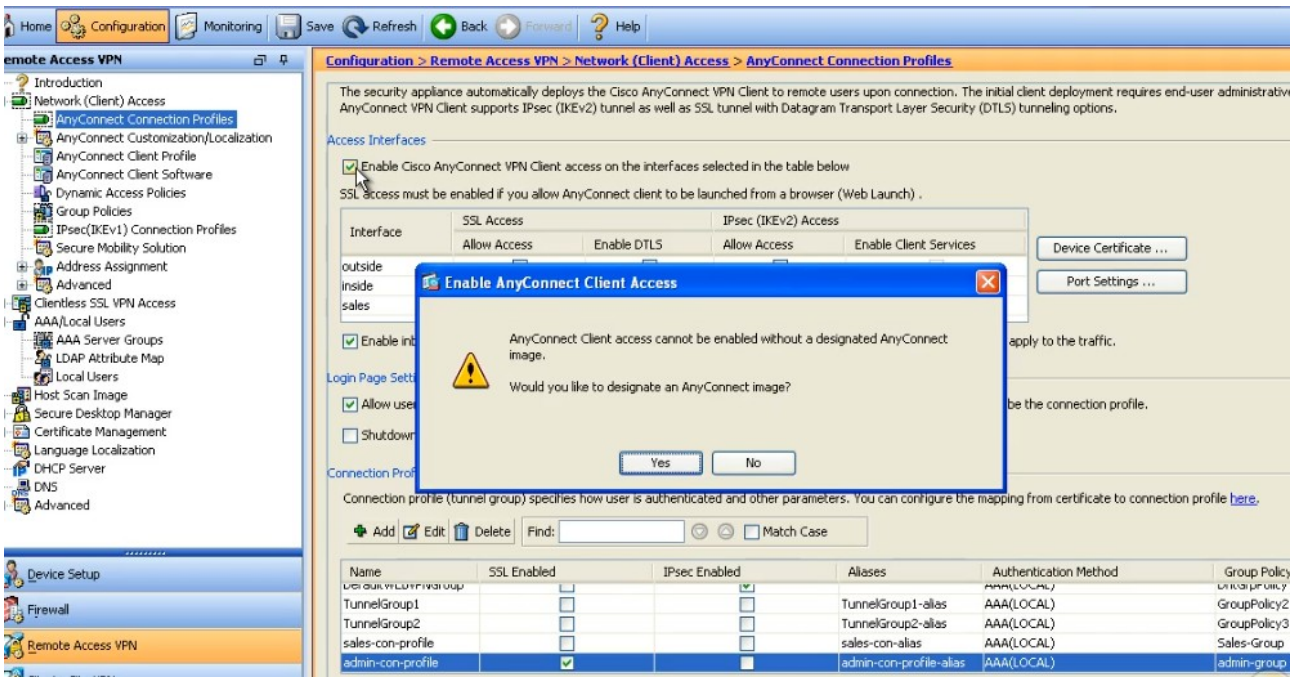

Preview CLI Commands
The following CLI commands are generated based on the char
ASA, click Send. To not send the commands and continue maki
group-policy admin-group attributes
vpn-tunnel-protocol ssl-client
dns-server value 10.0.0.40
wins-server none
default-domain value CBTNuggets.com
exit
tunnel-group admin-con-profile type remote-access
tunnel-group admin-con-profile general-attributes
default-group-policy admin-group
address-pool 10-pool
tunnel-group admin-con-profile webvpn-attributes
group-alias admin-con-profile-alias enable

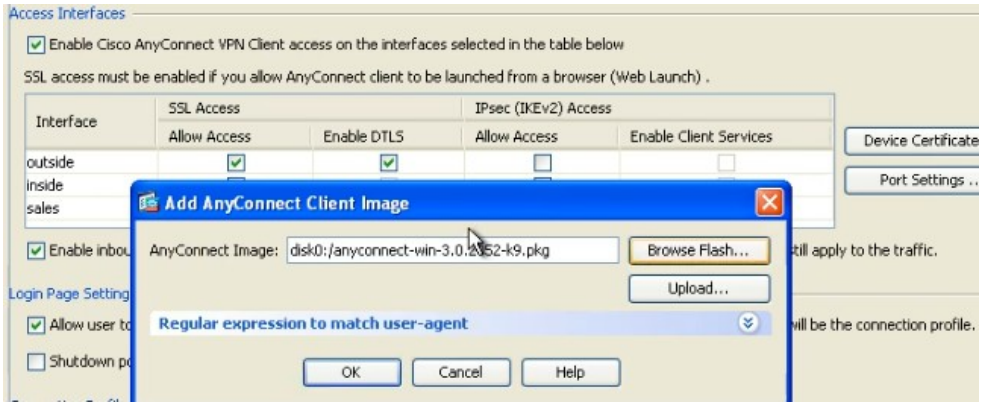

View
Tools
Wizards
Configuration
Introduction
Network (Client) Access
AnyConnect Connec
AnyConnect Custom
AnyConnect Client P
AnyConnect Client S
Dynamic Access Poli
Group Policies
IPsec(IKEv1) Conne
Secure Mobility Solu
Address Assignment
Advanced
Clientless SSL VPN Acces
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
Local Users
Host Scan Image
Secure Desktop Manage
Certificate Management
Add User Account
Identity
VPN Policy
Username:
admin-user
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:
15
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.

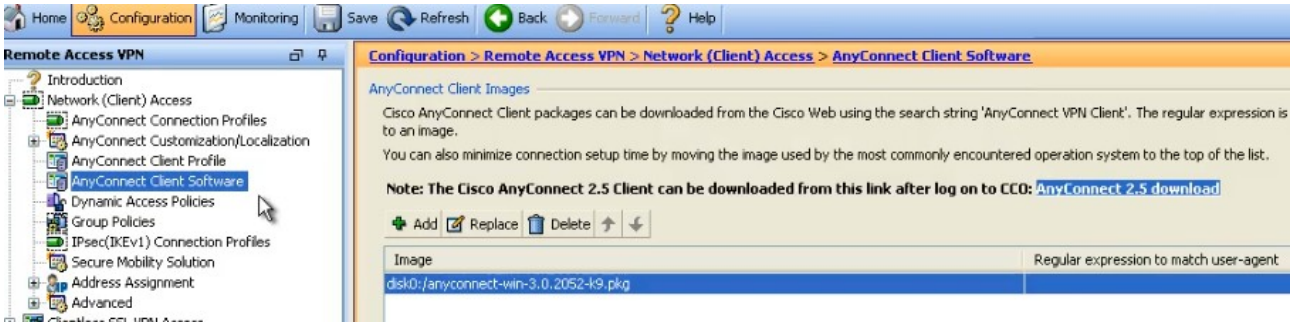

Add User Account
Identity
VPN Policy
Check an Inherit checkbox to let the corresponding setting take its value from the group policy.
Group Policy:
Inherit
admin-group
Tunneling Protocols:
Inherit
Clientless SSL VPN
SSL VPN Client
IPsec IKEv1
IPsec IKEv2
IPv4 Filter:
Inherit
IPv6 Filter:
Inherit
Connection Profile (Tunnel Group) Lock:
Inherit
Store Password on Client System:
Inherit
Yes
No
Connection Settings
Access Hours:
Inherit
Simultaneous Logins:
Inherit
Maximum Connect Time:
Inherit
Unlimited
Minutes
Idle Timeout:
Inherit
Unlimited
Minutes
Dedicated IP Address (Optional)
IP Address:
Subnet Mask:
A "user profile/policy" IP address assignment here, would override what is in the connection profile and/or group configuration.


Add User Account
Identity
VPN Policy
Clientless SSL VPN
AnyConnect Client
Keep Installer on Client System:
Datagram TLS:
Datagram TLS Compression:
SSL Compression:
Ignore Don't Fragment(DF) Bit:
Keepalive Messages:
MTU:
Optional Client Modules to Download:
Always-On VPN:
Client Profiles to Download:
Inherit
Yes
No
Enable
Disable
Deflate
LZS
Interval:
seconds
Add
Delete
DTLS is on by default, and also uses port 443.

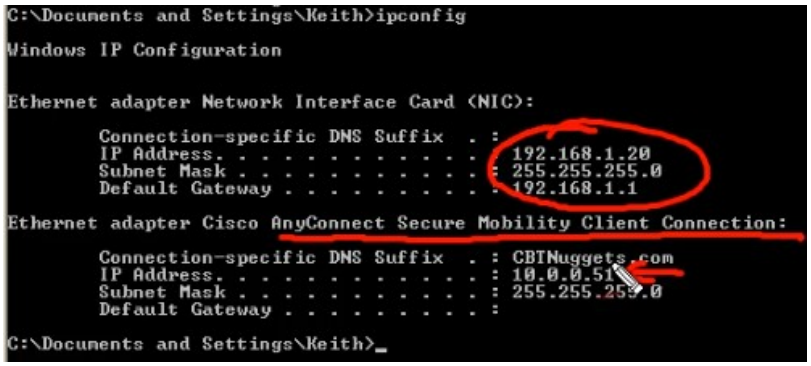

Preview CLI Commands
The following CLI commands are generated based on the changes you made in ASDM
ASA, click Send. To not send the commands and continue making changes in ASDM, cl
username admin-user password f3UhLvUj1QsXsuK7 encrypted privilege 15
username admin-user attributes
vpn-group-policy admin-group
exit

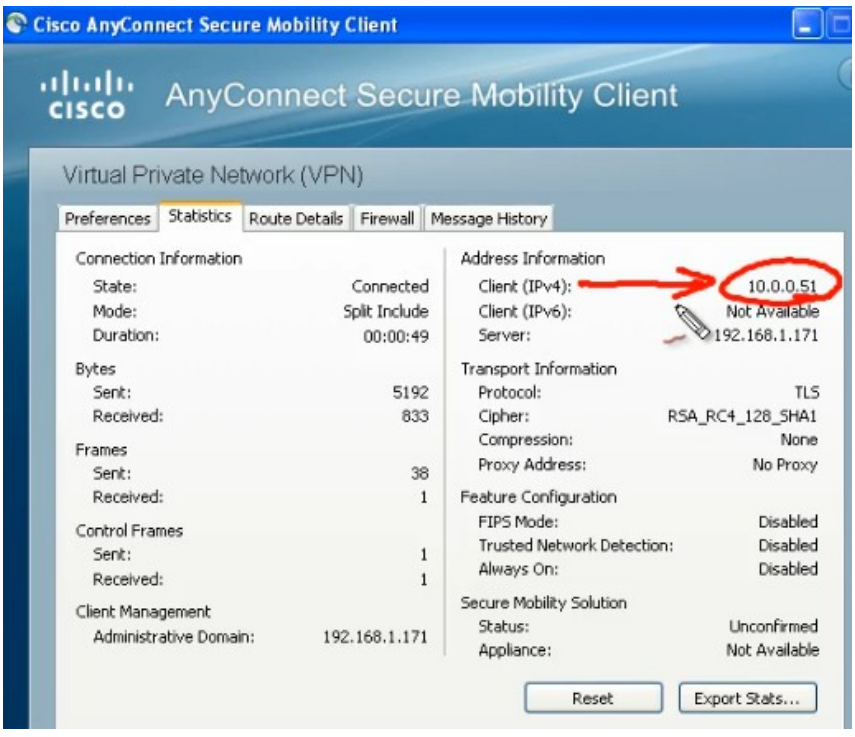

Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
AAA Server Groups
LDAP Attribute Map
Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
DHCP Server
DNS
Advanced
Device Setup
Firewall
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
AnyConnect VPN Client supports IPsec (IKEv2) tunnel as well as SSL tunnel with Datagram Transport Layer Security (DTLS) tunneling options.
Access Interfaces
Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below
SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .
Interface
SSL Access
Allow Access
Enable DTLS
IPsec (IKEv2) Access
Allow Access
Enable Client Services
outside
inside
sales
Device Certificate ...
Port Settings ...
Enable AnyConnect Client Access
AnyConnect Client access cannot be enabled without a designated AnyConnect image.
Would you like to designate an AnyConnect image?
Yes
No
Login Page Setting
Allow user
Shutdown
Connection Profiles
Connection profile (tunnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.
Add
Edit
Delete
Find:
Match Case
Name
SSL Enabled
IPsec Enabled
Aliases
Authentication Method
Group Policy
TunnelGroup1
TunnelGroup1-alias
AAA(LOCAL)
GroupPolicy2
TunnelGroup2
TunnelGroup2-alias
AAA(LOCAL)
GroupPolicy3
sales-con-profile
sales-con-alias
AAA(LOCAL)
Sales-Group
admin-con-profile
admin-con-profile-alias
AAA(LOCAL)
admin-group

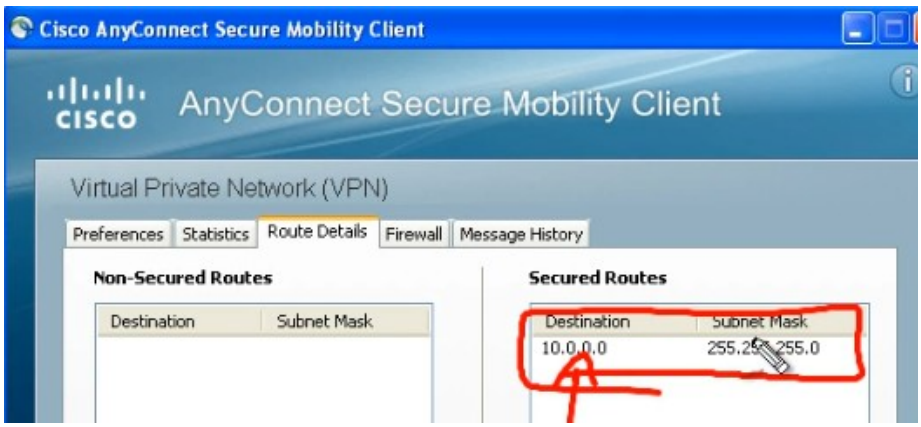

Access Interfaces
Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below
SSL access must be enabled if you allow AnyConnect client to be launched from a browser (Web Launch) .
Interface
SSL Access
Allow Access
Enable DTLS
IPsec (IKEv2) Access
Allow Access
Enable Client Services
outside
inside
sales
Device Certificate
Port Settings ...
Add AnyConnect Client Image
AnyConnect Image:
disk0:/anyconnect-win-3.0.2052-k9.pkg
Browse Flash...
Upload...
Regular expression to match user-agent
OK
Cancel
Help

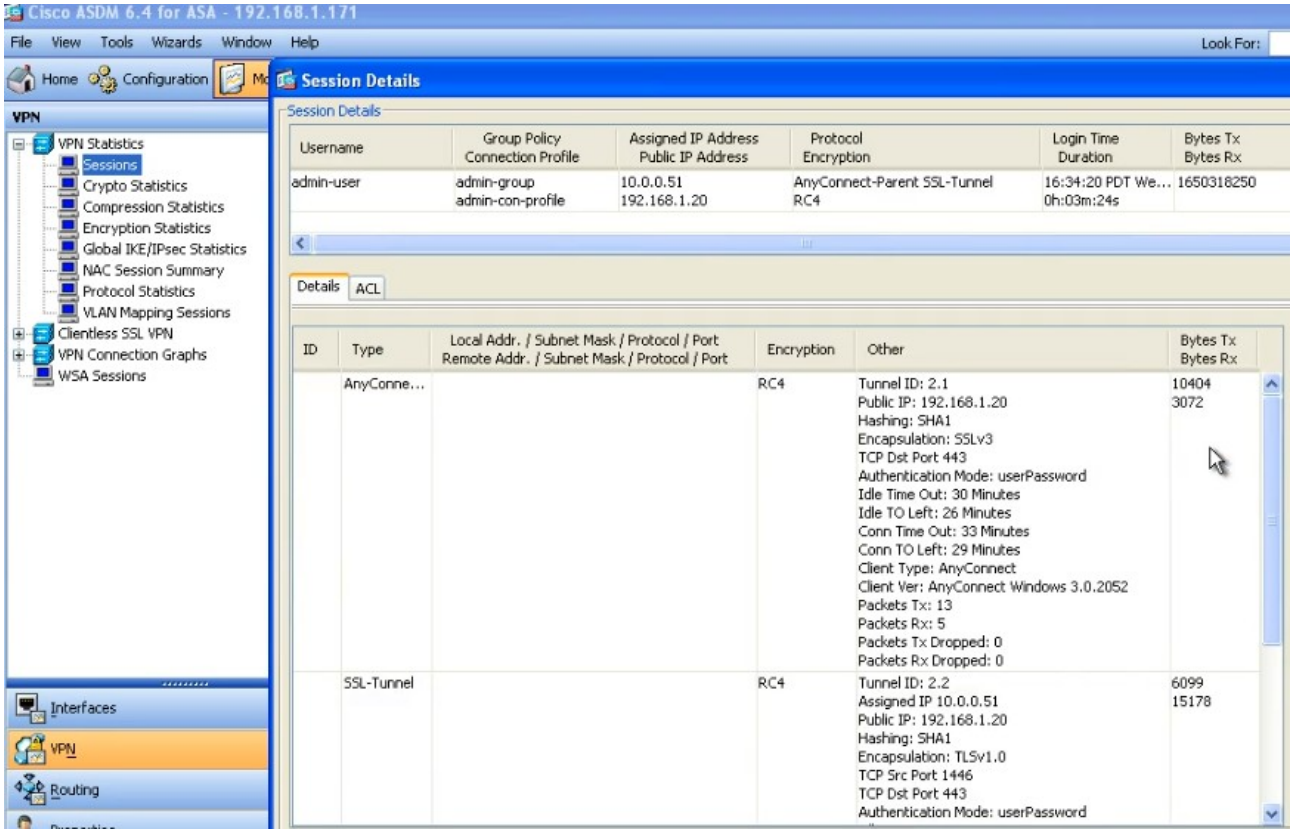

Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software
AnyConnect Client Images
Cisco AnyConnect Client packages can be downloaded from the Cisco Web using the search string 'AnyConnect VPN Client'. The regular expression is to an image.
You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.
Note: The Cisco AnyConnect 2.5 Client can be downloaded from this link after log on to CCO: AnyConnect 2.5 download
Add
Replace
Delete
Image
Regular expression to match user-agent
disk0:/anyconnect-win-3.0.2052-k9.pkg


Cisco AnyConnect | ASA1.CBTNuggets.com
Please enter your username and password.
Group:
admin-con-profile-alias
Username:
admin-user
Password:
OK
Cancel
cisco
AnyConnect
Secure Mobility Client
VPN: Please enter your username and password.
ASA1.CBTNuggets.com
Connect
Advanced...


C:\Documents and Settings\Keith>ipconfig
Windows IP Configuration
Ethernet adapter Network Interface Card (NIC):
Connection-specific DNS Suffix . :
IP Address. . . . . : 192.168.1.20
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
Ethernet adapter Cisco AnyConnect Secure Mobility Client Connection:
Connection-specific DNS Suffix . : CBTNuggets.com
IP Address. . . . . : 10.0.0.51
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
C:\Documents and Settings\Keith>_


Cisco AnyConnect Secure Mobility Client
cisco
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Preferences
Statistics
Route Details
Firewall
Message History
Connection Information
State: Connected
Mode: Split Include
Duration: 00:00:49
Bytes
Sent: 5192
Received: 833
Frames
Sent: 38
Received: 1
Control Frames
Sent: 1
Received: 1
Client Management
Administrative Domain: 192.168.1.171
Address Information
Client (IPv4): 10.0.0.51
Client (IPv6): Not Available
Server: 192.168.1.171
Transport Information
Protocol: TLS
Cipher: RSA_RC4_128_SHA1
Compression: None
Proxy Address: No Proxy
Feature Configuration
FIPS Mode: Disabled
Trusted Network Detection: Disabled
Always On: Disabled
Secure Mobility Solution
Status: Unconfirmed
Appliance: Not Available
Reset
Export Stats...






```
ASA1# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : admin-user              Index        : 2
Assigned IP  : 10.0.0.51               Public IP    : 192.168.1.20
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : RC4                     Hashing      : SHA1
Bytes Tx     : 16503                   Bytes Rx     : 18766
Group Policy : admin-group             Tunnel Group : admin-con-profile
Login Time   : 16:34:20 PDT Wed Oct 10 2012
Duration     : 0h:04m:21s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                     VLAN         : none

ASA1#
```