Cisco Small Business

Smart Business Communication System

Technical Enablement Lab

Configuring Teleworkers on UC 500 using CCA 3.0

2/08/2011

(minor update for MTP on 4/7)

Contents

Introduction

Considering a Teleworker phone can connect to the host UC 500 as if it was local (VPN connection), it is much more appealing and easier to manage than a multisite deployment where Call Control, AA and Voicemail, Directories, not to mention management is all handled separately.

In a multisite you can get extension dialing among sites with some feature interaction (limited) and Data VLAN sharing among the multisite mesh.

With the teleworker solution, you have everything integrated because the remote phones are effectively connected to the host UC 500.

Make sure you procure the appropriate number of licenses for the host UC 500 since any registered phone (local or remote) will decrement the total count by 1.

Reference the platform reference guide for UC540 and UC560 and see we can support 10 and 20 (respectively) remote Teleworker connections. These can be any combination of the following:

- individual SPA525G or G2 phones using SSL VPN
- individual CIPC Soft phones using PC connected with Cisco EZ_VPN client
- individual Teleworker routers (like the SR520) with up to 5 phones behind each

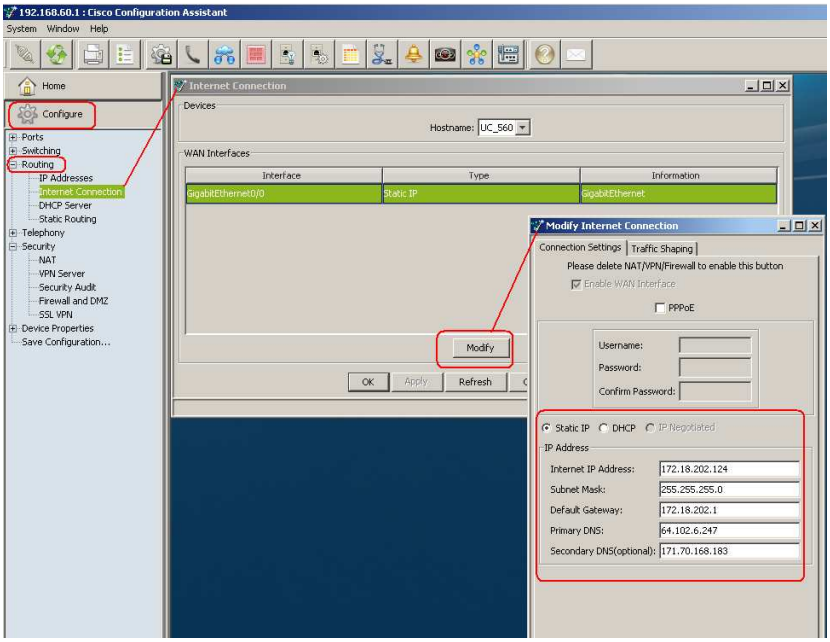
In this lab, I will create an SR520 as a remote Teleworker router and connect it to the UC560 all using CCA 3.0.

After the CCA configuration, we will have to discuss several options to work around an IOS NAT interaction with Cisco IP phones running SCCP version 17 or later (CSCte70727), which basically make them unusable behind the remote teleworker router due to this bug, unless you do one of the following:

- Downgrade the Phone FW to get SCCP version prior to 17
- Use phones that support an earlier version of SCCP even with their latest SWP phone load (i.e. SPA500 series).
- Configure some OOB CLI until a CCA 3.1 enhancement (CSCtj82336) is implemented to work around the IOS bug.

UC 560 Configuration

WAN Interconnect

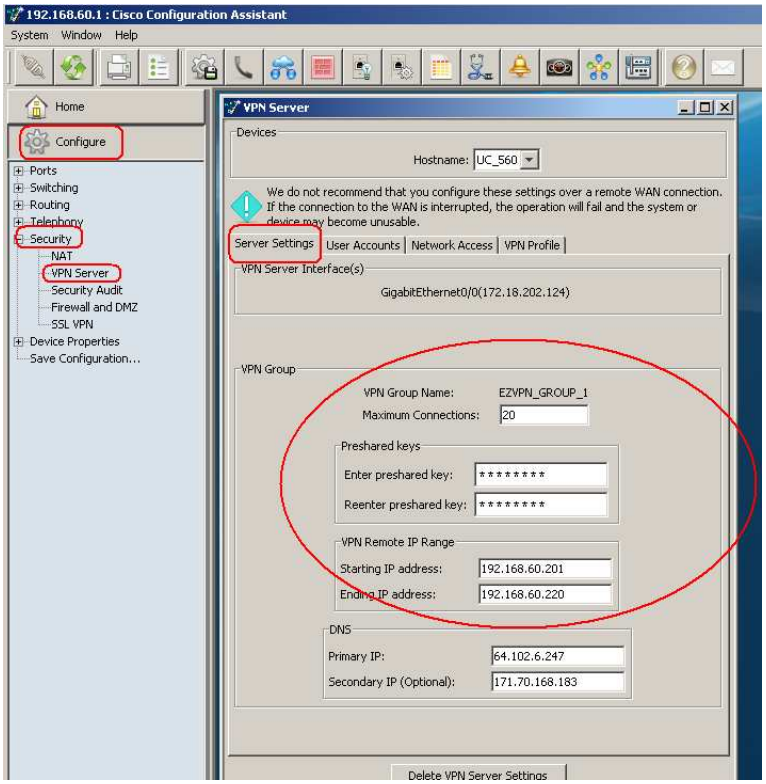


VPN Server

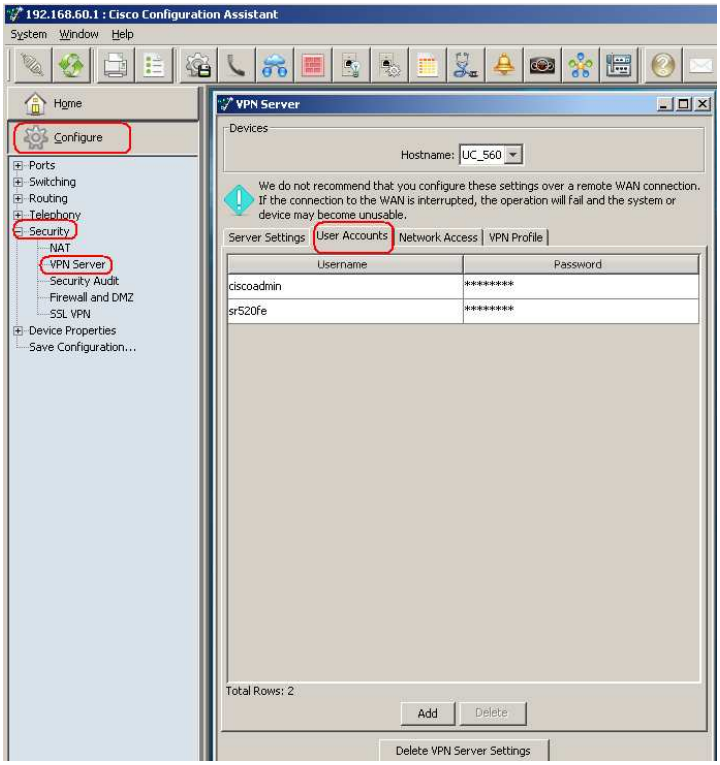
Create the VPN Server on the UC 500 for the maximum number of remote users that will be accessing the system using IPsec VPN tunnels (EZ_VPN is used for UC 500 teleworkers) and enter the shared secret (preshared key). Mine is cisco123 and don't use that ☺

Assign the DHCP Address pool you want to be leased to remote Teleworker routers.

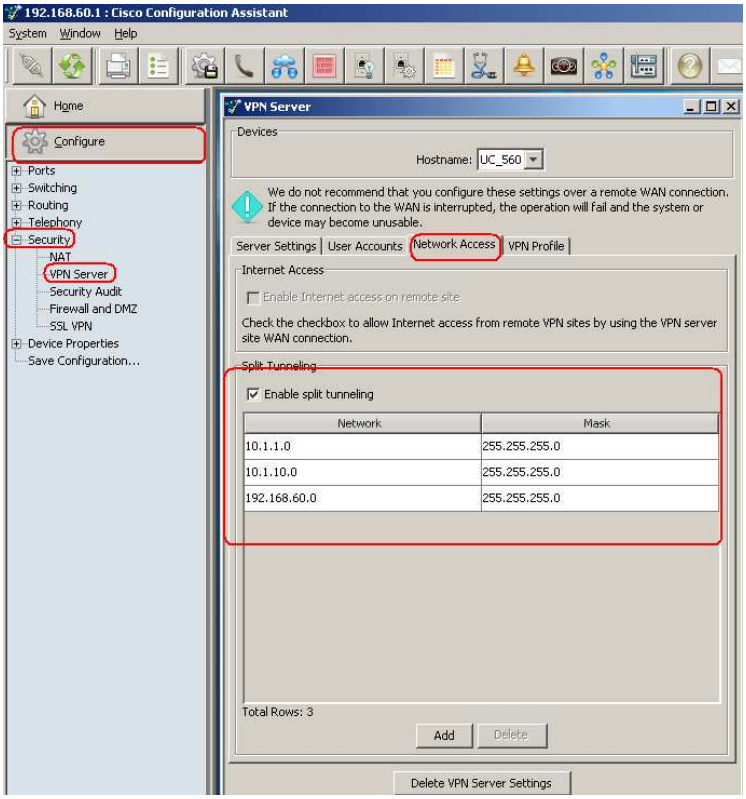
The DNS should be prefilled based on your UC 500 configuration (mine are lab DNSs that wont work in the real public internet).



Create the Teleworker User Accounts (my password is ciscosb).



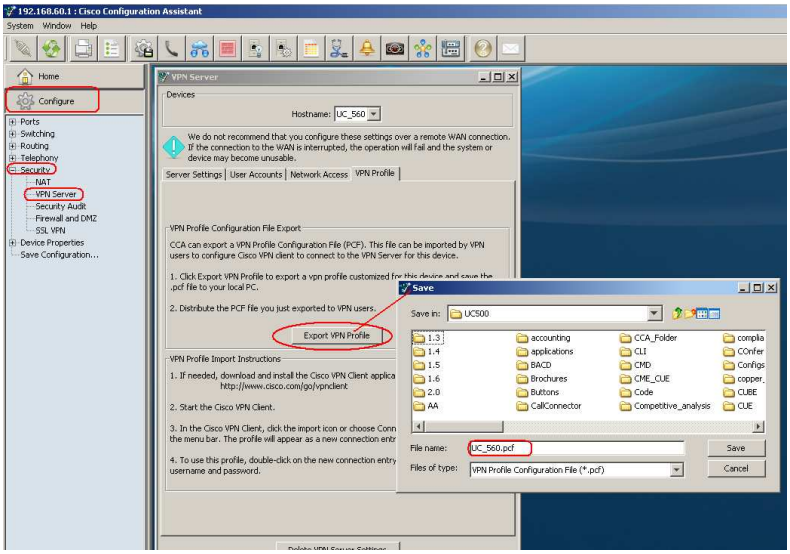
Enable Split tunneling to preserve bandwidth. Specify your Data & Voice VLAN and your CUE network IPs so ACLs are created correctly in the IOS Firewall.



APPLY this configuration.

See Appendix A for the CLI shown in the CCA post view window.

You may export the VPN Profile, but in this scenario it is not needed.



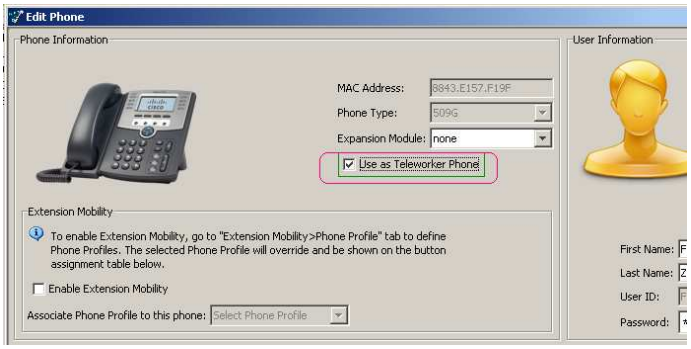
Phone Configuration

In the Telephony> Voice> Users and extensions tab, select each user that will be at the remote site and check the box for “use as Teleworker Phone. When Use as teleworker phone is checked, Media Termination Point (MTP) is configured on the phone so that Cisco Unified CME terminates the media stream. The MTP setting

causes the UC500 to act as a proxy. Media packets are forwarded to other IP phones with the IP address of the UC500 in the source address field. MTP is typically used in remote teleworker phone deployments.

When this option is unchecked, MTP is not configured on the phone.

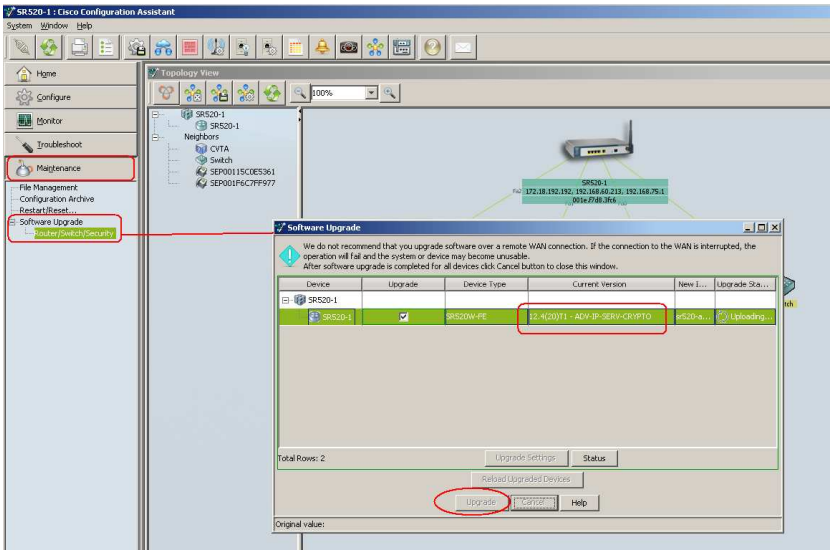
The Use as teleworker phone checkbox is not displayed for Cisco IP Communicator (CIPC) softphones, since MTP is always configured for CIPC softphones.



SR520 Configuration

SW Upgrade

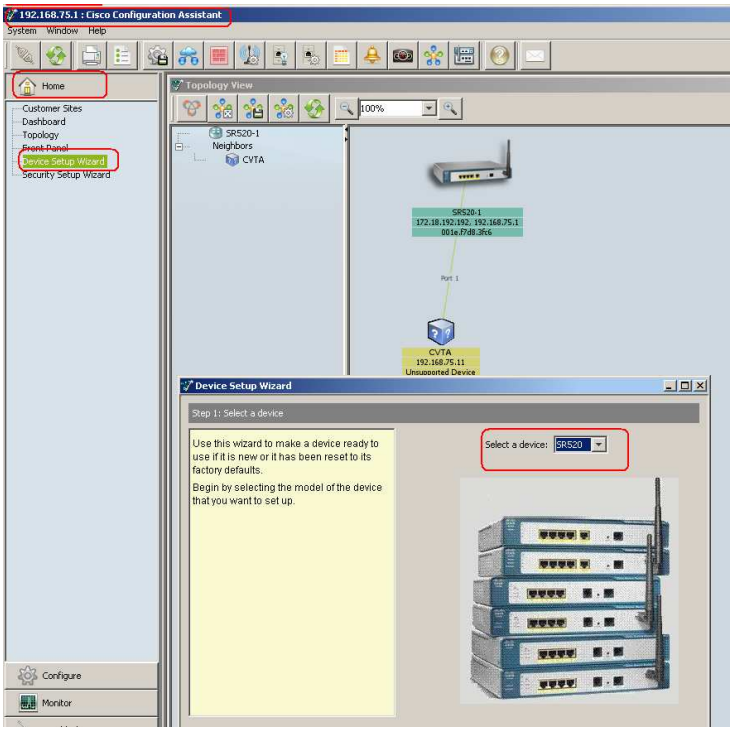
Upgrade to the latest IOS for the Cisco 500 series router (SR520) using CCA.



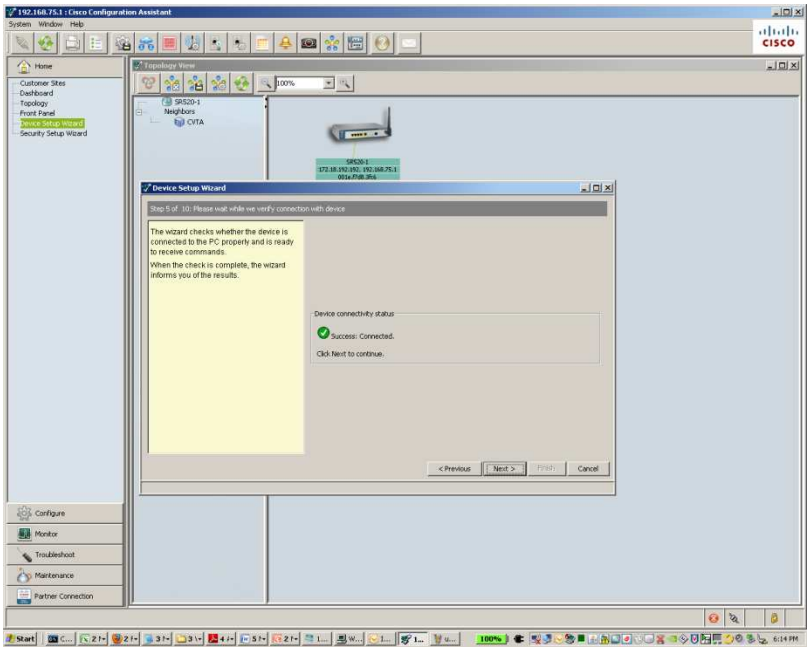
Connect to the SR520 with an Ethernet cable from your PC to one of the FE LAN ports (0,1,2 or 3).

SR520 Wizard

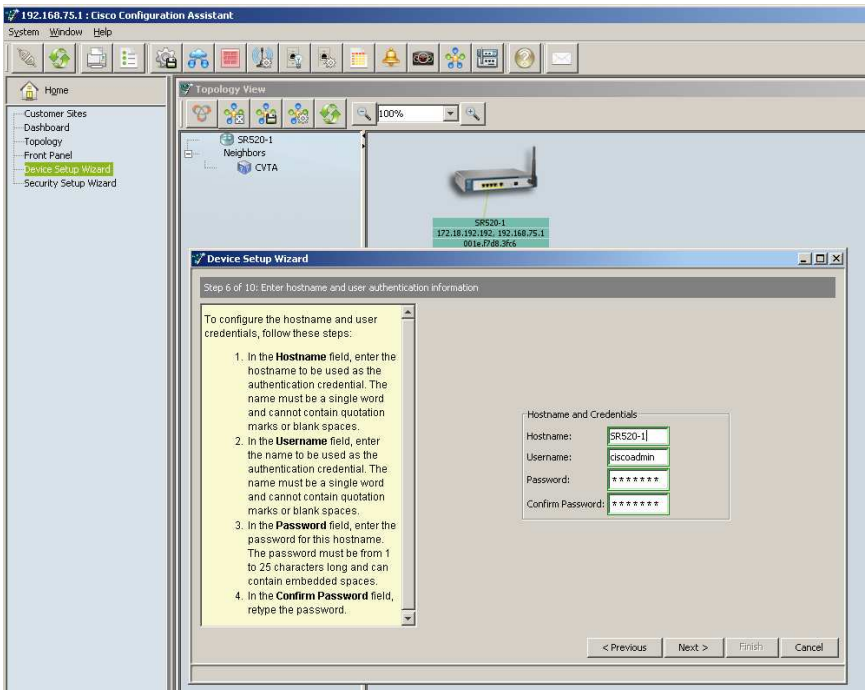
Launch CCA and connect to an IP Address, open the HOME Device Wizards and select the SR520:



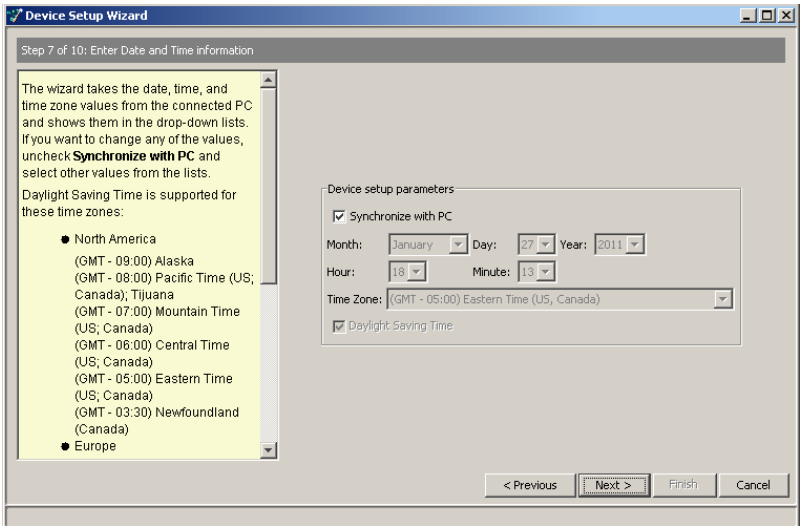
Click Next past steps 2 & 3 which basically tell you to not have the SR520 connected to anything else at this point. Step 4 prompts for username and password. Then you should see this. If you get a connection error, you are connecting from a CCA SITE (not supported for the wizard):



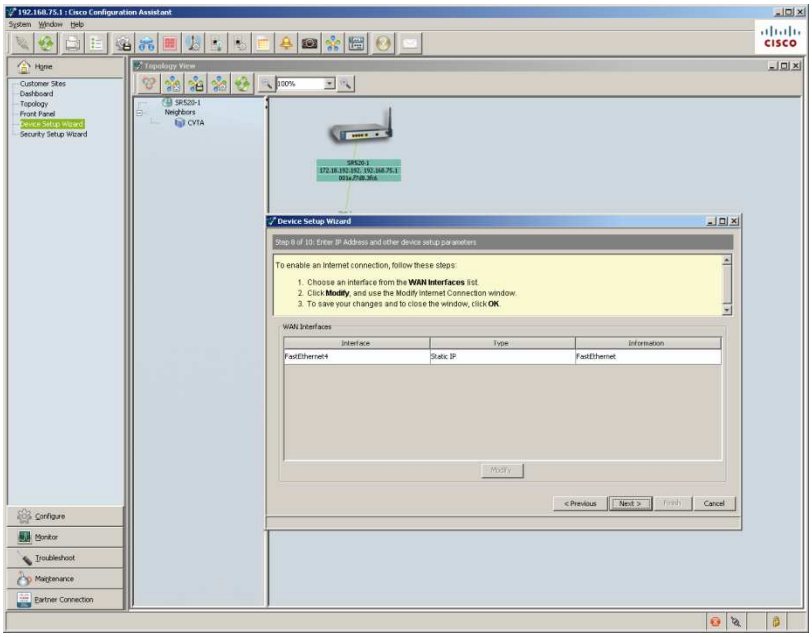
Next step I enter the hostname and credentials (I used ciscoadmin/ciscosb):

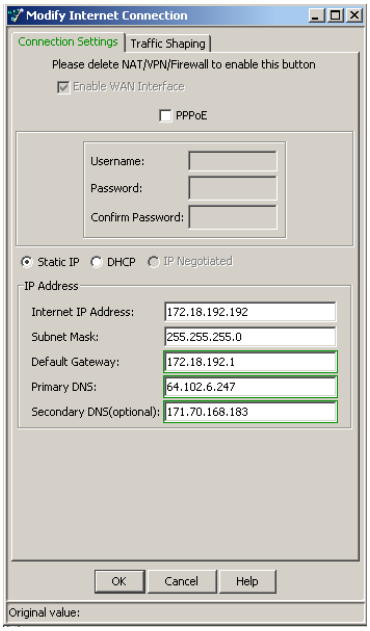


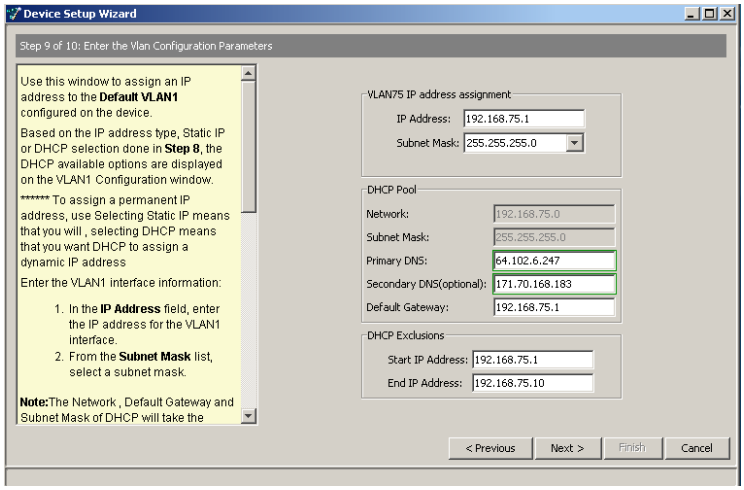
Since we have no WAN, Synch to PC at this point is fabulous darling.

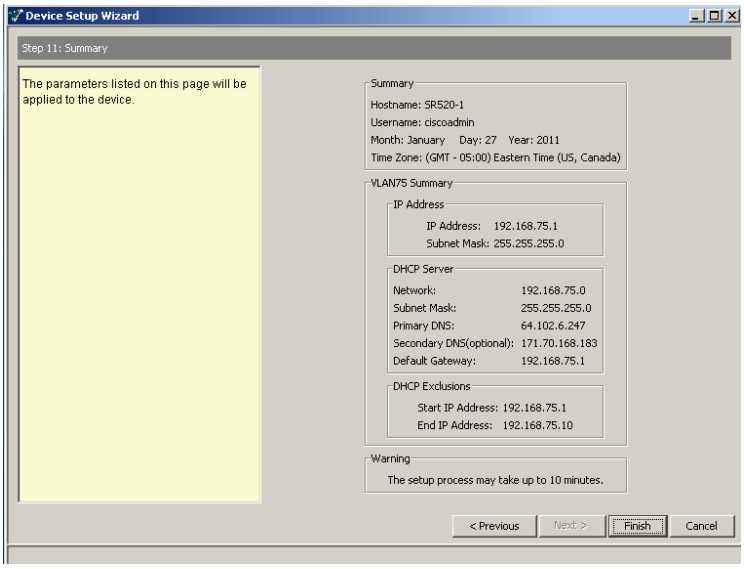


Next Modify the WAN. This screen takes a minute to react when you highlight it and click modify.

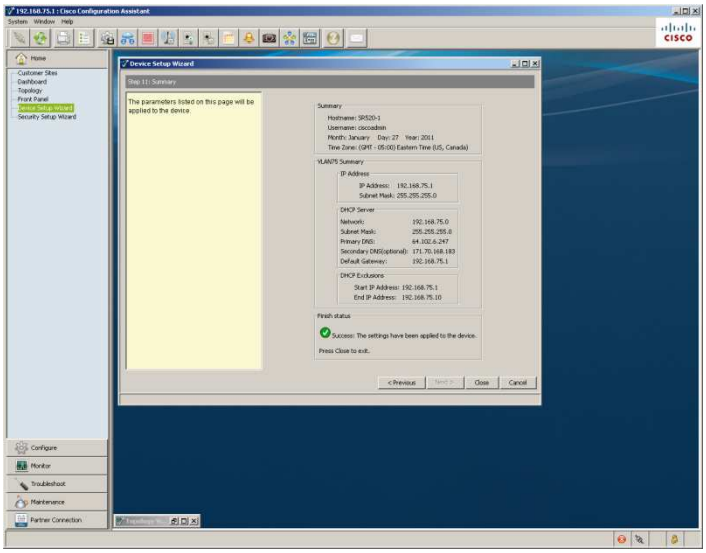

192.168.75.1 : Cisco Configuration Assistant
Device Setup Wizard
To enable an Internet connection, follow these steps:
1. Choose an interface from the WAN Interfaces list.
2. Click Modify, and use the Modify Internet Connection window.
3. To save your changes and to close the window, click OK.
WAN Interfaces
Interface
Type
Information
FastEthernet4
Static IP
FastEthernet
Modify
< Previous
Next >
Finish
Cancel
Configure
Monitor
Troubleshoot
Maintenance
Partner Connection


Modify Internet Connection
Connection Settings
Traffic Shaping
Please delete NAT/VPN/Firewall to enable this button
Enable WAN Interface
PPPoE
Username:
Password:
Confirm Password:
Static IP
DHCP
IP Negotiated
IP Address
Internet IP Address: 172.18.192.192
Subnet Mask: 255.255.255.0
Default Gateway: 172.18.192.1
Primary DNS: 64.102.6.247
Secondary DNS(optional): 171.70.168.183
OK
Cancel
Help
Original value:

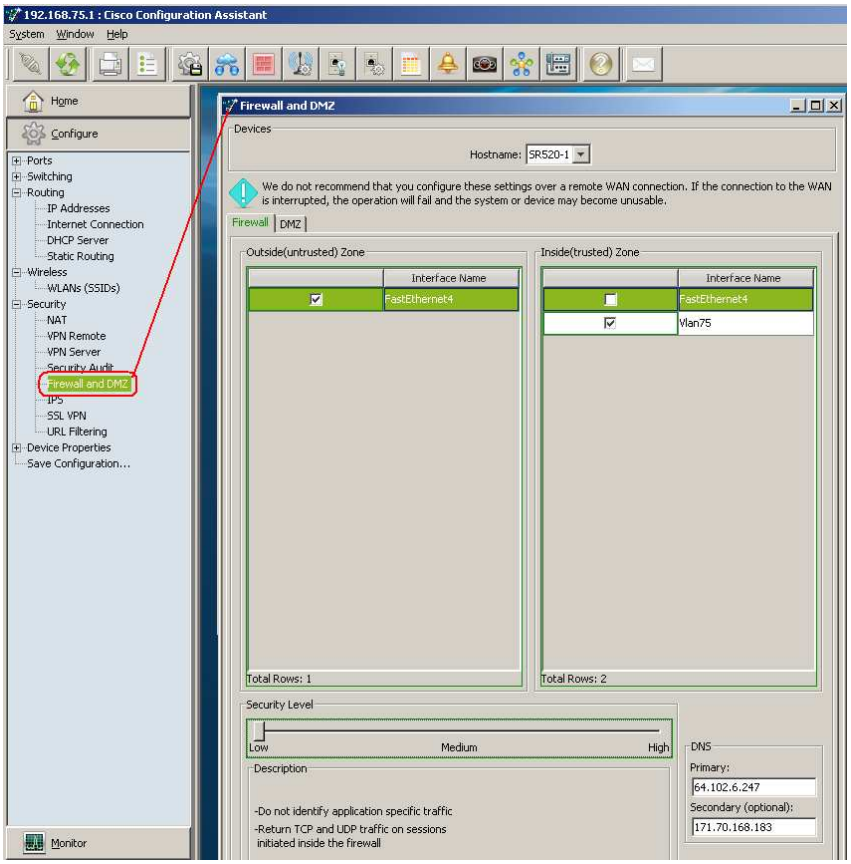

Device Setup Wizard
Step 9 of 10: Enter the Vlan Configuration Parameters
Use this window to assign an IP address to the Default VLAN1 configured on the device.
Based on the IP address type, Static IP or DHCP selection done in Step 8, the DHCP available options are displayed on the VLAN1 Configuration window.
****** To assign a permanent IP address, use Selecting Static IP means that you will , selecting DHCP means that you want DHCP to assign a dynamic IP address
Enter the VLAN1 interface information:
1. In the IP Address field, enter the IP address for the VLAN1 interface.
2. From the Subnet Mask list, select a subnet mask.
Note:The Network , Default Gateway and Subnet Mask of DHCP will take the
VLAN75 IP address assignment
IP Address: 192.168.75.1
Subnet Mask: 255.255.255.0
DHCP Pool
Network: 192.168.75.0
Subnet Mask: 255.255.255.0
Primary DNS: 64.102.6.247
Secondary DNS(optional): 171.70.168.183
Default Gateway: 192.168.75.1
DHCP Exclusions
Start IP Address: 192.168.75.1
End IP Address: 192.168.75.10
< Previous
Next >
Finish
Cancel



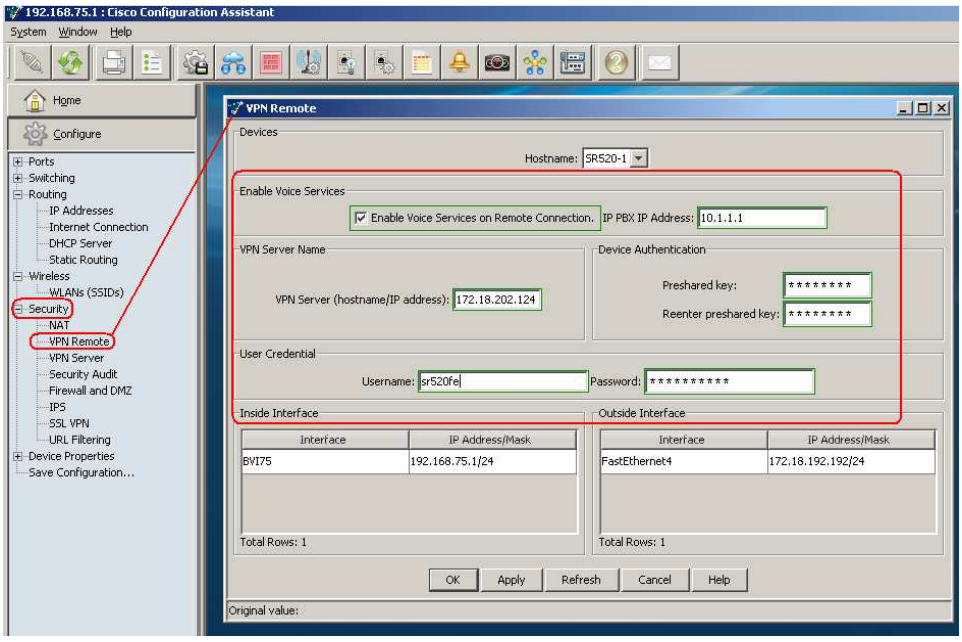
When you see the click OK to reconnect, you may click it:



Make sure your Firewall is recognized by CCA and set it accordingly:



OK, now the other half of the IPsec VPN. Remember my UC560 IP address, the user/pass (sr520/ciscosb) I entered in its VPN Server config and the Shared secret (cisco123). Enable voice and apply.



After applying, release / renew you PC IP address and then SAVE the CCA SR520 config using CCA SAVE ICON!!!

DO NOT power off the SR520 until you do this.

Operation

Plug in a few phones at this point:

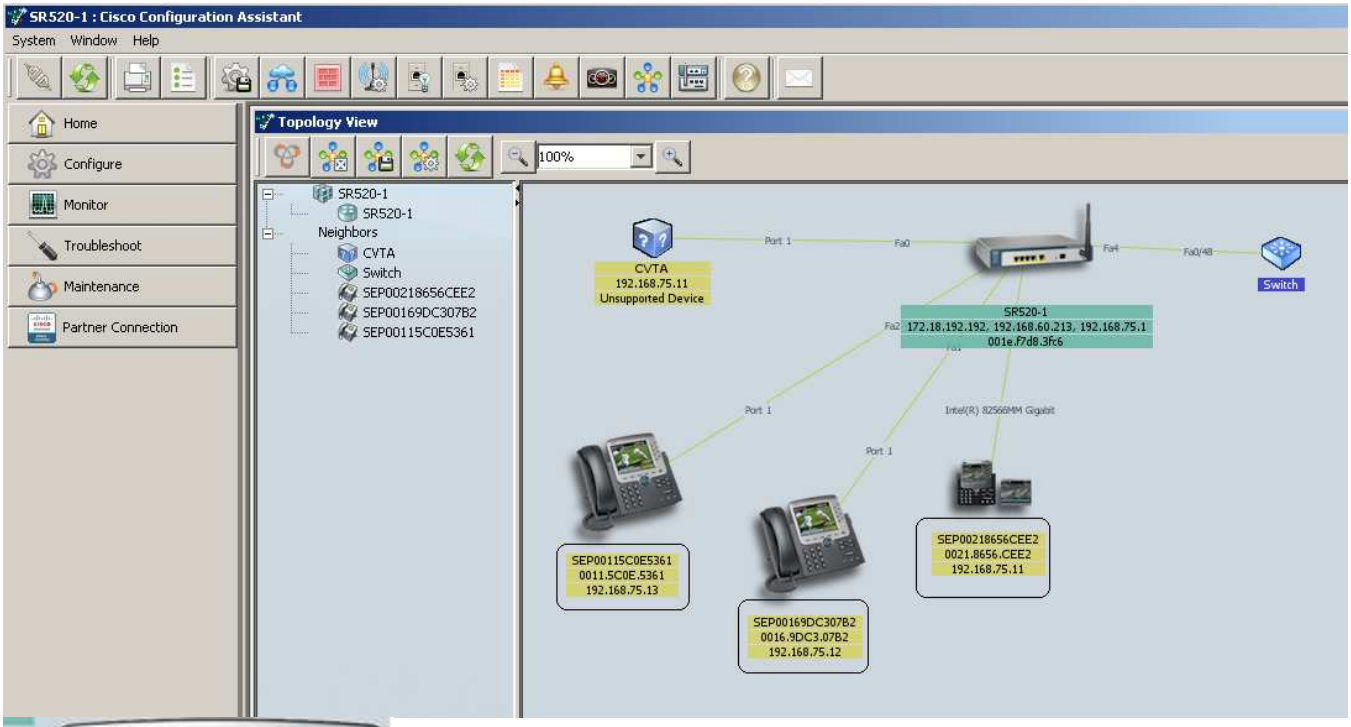
1) A phone plugged into the SR520 FE0,1,2 or 3 (with power brick)
2) A phone plugged into a Cisco SB Switch (SG-300), which is plugged into the SR520 LAN 0,1,2 or 3.
3) A CIPC Soft phone on a PC behind the SR520

Remember since CCA 3.0 disables auto ephone-dn assignment, I am connecting 3 examples of configuration options.

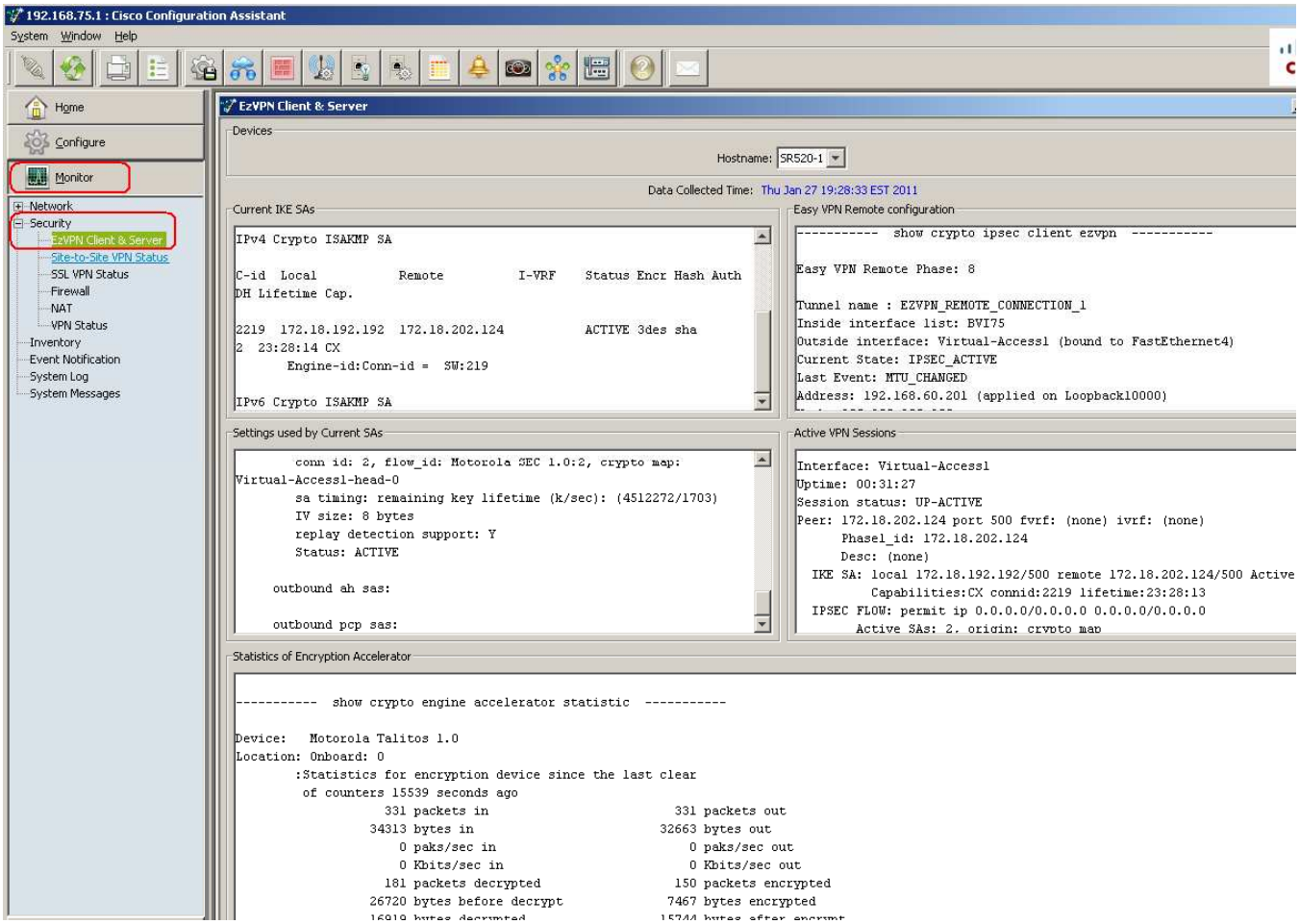
1) Take a phone already configured at the host and connect it at the SR520 (recognized and inherits config)
2) Connect a phones for the first time at the SR520 (must configure with CCA on the UC560)
3) Connect a Soft Phone from a PC connected to the SR520 for the first time (same as #2)

Notes:

1) The Cisco SG-300 8 port switch is perfect for this. Next quarter it will support CDP and then CCA topology can discover it. But this is really OK, because the Users/Extensions/Voicemail/<all features> are not configured here. They are configured with CCA 3.0 on the host UC560 (I will show later). SO this is correct.
2) The 2 phones that are new, will not show extensions and will not have dial tone. This is normal at this point.


SR520-1 : Cisco Configuration Assistant
System Window Help
Home
Configure
Monitor
Troubleshoot
Maintenance
Partner Connection
Topology View
100%
SR520-1
SR520-1
Neighbors
CVTA
Switch
SEP00218656CEE2
SEP00169DC307B2
SEP00115C0E5361
CVTA
192.168.75.11
Unsupported Device
Port 1
Fa0
Fa4
Fa0/48
Switch
SR520-1
Fa2
172.18.192.192, 192.168.60.213, 192.168.75.1
001e.f7d8.3fc6
Fa1
Port 1
Intel(R) 82566MM Gigabit
Port 1
SEP00115C0E5361
0011.5C0E.5361
192.168.75.13
SEP00169DC307B2
0016.9DC3.07B2
192.168.75.12
SEP00218656CEE2
0021.8656.CEE2
192.168.75.11

Monitor



Work Around

OK so now we make some calls and realize we have no audio from phones running SCCP Version 17.

Analysis of the output of 'debug ip udp', showed the RTP stream being built for the remote without the proper IP (CME:2000---->0.0.0.0:0). CME wasn't getting the right destination address via SCCP on the phones with SCCP v17.

There are a few possible workarounds:

- Only Use Cisco 79xx phones with SCCP versions prior to 17 (this means downgrading phone FW; not recommended)
- Only use SPA500 series phones at the remote since they don't use the SCCP version 17 even with the latest phone load.
- Change the VPN from Client mode to Network Extension mode and manually adjust ACL for NAT bypass.

We have already filed an enhancement request with CCA 3.1 (CSCtj82336) to add support for network-extension mode and NAT bypass in CCA until IOS NAT will support it with 15.1(3)T as per CSCte70727

Using the OOB CLI and will cause CCA to not recognize the Firewall or Remote VPN GUI menus so the workaround should be done last and should not be done if you are not specialized to manage your system with CLI.

A simple CLI command to check to see the version of phone FW and SCCP version:

UC560# show ephone registered

```
ephone-13[12] Mac:0011.5C0E.5361 TCP socket:[26] activeLine:0 whisperLine:0 REGISTERED in SCCP
ver 17/17 max_streams=5 mediaActive:0 whisper_mediaActive:0 startMedia:0 offhook:0 ringing:0
reset:0 reset_sent:0 paging 0 debug:0 caps:8 privacy:1 IP:192.168.60.213 * 22895 7970  keepalive
77 max_line 8 available_line 7 button 1: cw:1 ccw:(0 0 0 0 0 0 0 0)
  dn 23 number 214 CH1   IDLE         CH2   IDLE         CH3   IDLE         CH4   IDLE
CH5   IDLE         CH6   IDLE         CH7   IDLE         CH8   IDLE
button 2: cw:1 ccw:(0)
  dn 597 number DBA214  auto dial DBA CH1   IDLE
button 3: cw:1 ccw:(0 0 0 0 0 0 0 0)
  dn 60 number 251 CH1   IDLE         CH2   IDLE         CH3   IDLE         CH4   IDLE
CH5   IDLE         CH6   IDLE         CH7   IDLE         CH8   IDLE         shared
privacy button is enabled
Preferred Codec: g711ulaw
Lpcor Type: none Username: SevenSeventy Password: 123456
```

VPN CLI Workaround

These are the following configuration changes supported by SBSC (STAC)to get it to work. This configuration changes would be on the remote SR520 router and considers the remote phones are configured as 'Teleworker Phone' in CCA of the host, and split tunneling is enabled on the host VPN server.

From:

```
crypto ipsec client ezvpn EZVPN_REMOTE_CONNECTION_1
 connect auto
 group EZVPN_GROUP_1 key cisco123
 mode client
 peer 172.18.202.124
 virtual-interface 2
 username sr520fe password ciscosb
 xauth userid mode local
!
```

To:

```
crypto ipsec client ezvpn EZVPN_REMOTE_CONNECTION_1
 mode network-extension
```

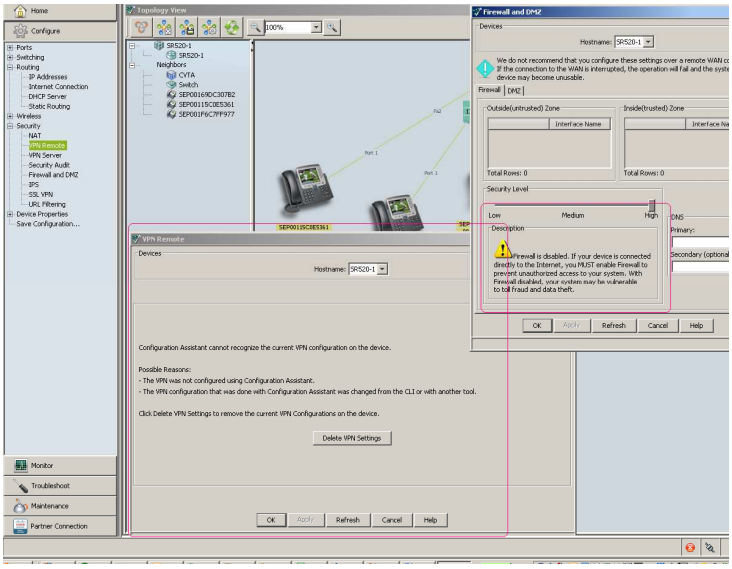
from:

```
ip nat inside source list 1 interface FastEthernet4 overload

access-list 1 remark SDM_ACL Category=2
access-list 1 permit 192.168.75.0 0.0.0.255
```

replace with:

```
ip nat inside source list 110 interface FastEthernet4 overload

  access-list 110 remark SDM_ACL
  access-list 110 deny ip 192.168.75.0 0.0.0.255 10.1.1.0 0.0.0.255
  access-list 110 deny ip 192.168.75.0 0.0.0.255 10.1.10.0 0.0.0.255
  access-list 110 permit ip 192.168.75.0 0.0.0.255 any
```

Resulting CCA GUI for SR520:



Appendix A

POST CLI View for VPN Server Configuration

ip local pool FOXTROT_TEST_LOCAL_POOL1 192.168.60.201 192.168.60.220
no ip local pool FOXTROT_TEST_LOCAL_POOL1

aaa authorization network Foxtrot_sdm_easyvpn_group_ml_1 local
aaa authentication login Foxtrot_sdm_easyvpn_xauth_ml_1 local

access-list 105 remark SDM_ACL Category=4
access-list 105 permit ip 10.1.1.0 0.0.0.255 any
access-list 105 permit ip 10.1.10.0 0.0.0.255 any
access-list 105 permit ip 192.168.60.0 0.0.0.255 any
no access-list 104
access-list 104 remark auto generated by SDM firewall configuration##NO_ACES_15##
access-list 104 remark SDM_ACL Category=1
access-list 104 permit udp any host 172.18.202.124 eq non500-isakmp
access-list 104 permit udp any host 172.18.202.124 eq isakmp
access-list 104 permit esp any host 172.18.202.124
access-list 104 permit ahp any host 172.18.202.124
access-list 104 deny ip 192.168.60.0 0.0.0.255 any
access-list 104 deny ip 10.1.10.0 0.0.0.3 any
access-list 104 deny ip 10.1.1.0 0.0.0.255 any
access-list 104 permit udp host 64.102.6.247 eq domain any
access-list 104 permit udp host 171.70.168.183 eq domain any
access-list 104 permit icmp any host 172.18.202.124 echo-reply
access-list 104 permit icmp any host 172.18.202.124 time-exceeded
access-list 104 permit icmp any host 172.18.202.124 unreachable
access-list 104 deny ip 10.0.0.0 0.255.255.255 any
access-list 104 deny ip 172.16.0.0 0.15.255.255 any
access-list 104 deny ip 192.168.0.0 0.0.255.255 any
access-list 104 deny ip 127.0.0.0 0.255.255.255 any
access-list 104 deny ip host 255.255.255.255 any

```
access-list 104 deny ip host 0.0.0.0 any
access-list 104 deny ip any any log
no access-list 103
access-list 103 remark auto generated by SDM firewall configuration##NO_ACES_8##
access-list 103 remark SDM_ACL Category=1
access-list 103 permit udp any host 10.1.10.2 eq non500-isakmp
access-list 103 permit udp any host 10.1.10.2 eq isakmp
access-list 103 permit esp any host 10.1.10.2
access-list 103 permit ahp any host 10.1.10.2
access-list 103 permit tcp 10.1.1.0 0.0.0.255 eq 2000 any
access-list 103 permit udp 10.1.1.0 0.0.0.255 eq 2000 any
access-list 103 deny ip 172.18.202.0 0.0.0.255 any
access-list 103 deny ip 192.168.60.0 0.0.0.255 any
access-list 103 deny ip 10.1.1.0 0.0.0.255 any
access-list 103 deny ip host 255.255.255.255 any
access-list 103 deny ip 127.0.0.0 0.255.255.255 any
access-list 103 permit ip any any
no access-list 102
access-list 102 remark auto generated by SDM firewall configuration##NO_ACES_8##
access-list 102 remark SDM_ACL Category=1
access-list 102 permit udp any host 10.1.1.1 eq non500-isakmp
access-list 102 permit udp any host 10.1.1.1 eq isakmp
access-list 102 permit esp any host 10.1.1.1
access-list 102 permit ahp any host 10.1.1.1
access-list 102 permit tcp 10.1.10.0 0.0.0.3 any eq 2000
access-list 102 permit udp 10.1.10.0 0.0.0.3 any eq 2000
access-list 102 deny ip 172.18.202.0 0.0.0.255 any
access-list 102 deny ip 192.168.60.0 0.0.0.255 any
access-list 102 deny ip 10.1.10.0 0.0.0.3 any
access-list 102 deny ip host 255.255.255.255 any
access-list 102 deny ip 127.0.0.0 0.255.255.255 any
access-list 102 permit ip any any
no access-list 101
access-list 101 remark auto generated by SDM firewall configuration##NO_ACES_6##
access-list 101 remark SDM_ACL Category=1
access-list 101 permit udp any host 192.168.60.1 eq non500-isakmp
access-list 101 permit udp any host 192.168.60.1 eq isakmp
access-list 101 permit esp any host 192.168.60.1
access-list 101 permit ahp any host 192.168.60.1
access-list 101 deny ip 172.18.202.0 0.0.0.255 any
access-list 101 deny ip 10.1.10.0 0.0.0.3 any
access-list 101 deny ip 10.1.1.0 0.0.0.255 any
access-list 101 deny ip host 255.255.255.255 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 permit ip any any
ip local pool SDM_POOL_1 192.168.60.201 192.168.60.220
crypto ipsec transform-set ESP-3DES-SHA esp-sha-hmac esp-3des
 mode tunnel
 exit
crypto isakmp profile sdm-ike-profile-1
 isakmp authorization list Foxtrot_sdm_easyvpn_group_ml_1
 client authentication list Foxtrot_sdm_easyvpn_xauth_ml_1
 match identity group EZVPN_GROUP_1
 client configuration address respond
```

```
 exit
crypto ipsec profile SDM_Profile1
 set transform-set ESP-3DES-SHA
 set isakmp-profile sdm-ike-profile-1
 exit
interface Virtual-Template1 type tunnel
 exit
default interface Virtual-Template1
interface Virtual-Template1 type tunnel
 no shutdown
 ip unnumbered Vlan1
 tunnel protection ipsec profile SDM_Profile1
 tunnel mode ipsec ipv4
 exit
crypto isakmp client configuration group EZVPN_GROUP_1
 key 0 cisco123
 pool SDM_POOL_1
 acl 105
 dns 64.102.6.247 171.70.168.183
 save-password
 max-users 20
 exit
show running-config | include banner
exit
crypto isakmp policy 1
 authentication pre-share
 encr 3des
 hash sha
 group 2
 lifetime 86400
 exit
crypto isakmp profile sdm-ike-profile-1
 virtual-template 1
 exit
crypto isakmp xauth timeout 15
username sr520fe privilege 1 secret 0 ciscosb
sh run | include 105
```