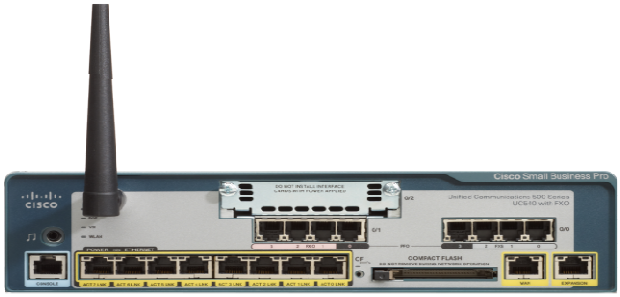
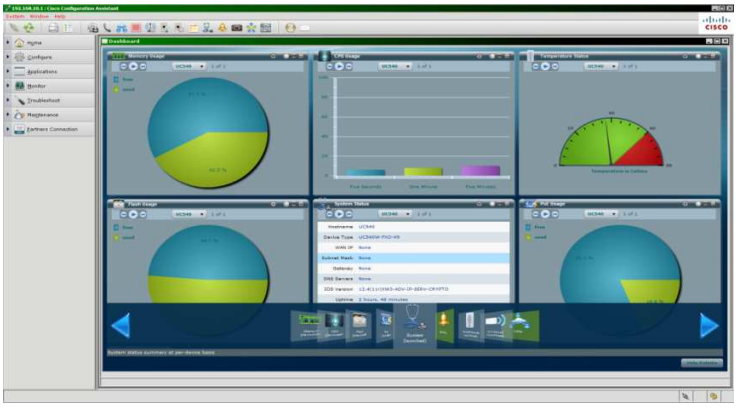
Cisco Small Business Pro

Smart Business Communication System

Technical Enablement Labs





Lab 6

SA500 In front of the UC500

Introduction

If the customer desires advanced security and Web threat Protection / EMAIL Spam Filtering / Web Reputation filtering in front of the UC540, or wants to use some of the additional features of the Security Appliance 500 series (SA 500), you may place the SA500 in front of the UC500.

In this case you will assign the UC500 a WAN address that is from the SA500 data VLAN (192.168.75.0/24 default) and plug your WAN termination connection into the WAN port of the SA 500. Connect the UC500 FE0/0 into one of the LAN ports of the SA 500 and make the changes detailed in this document.

In this lab, you will:

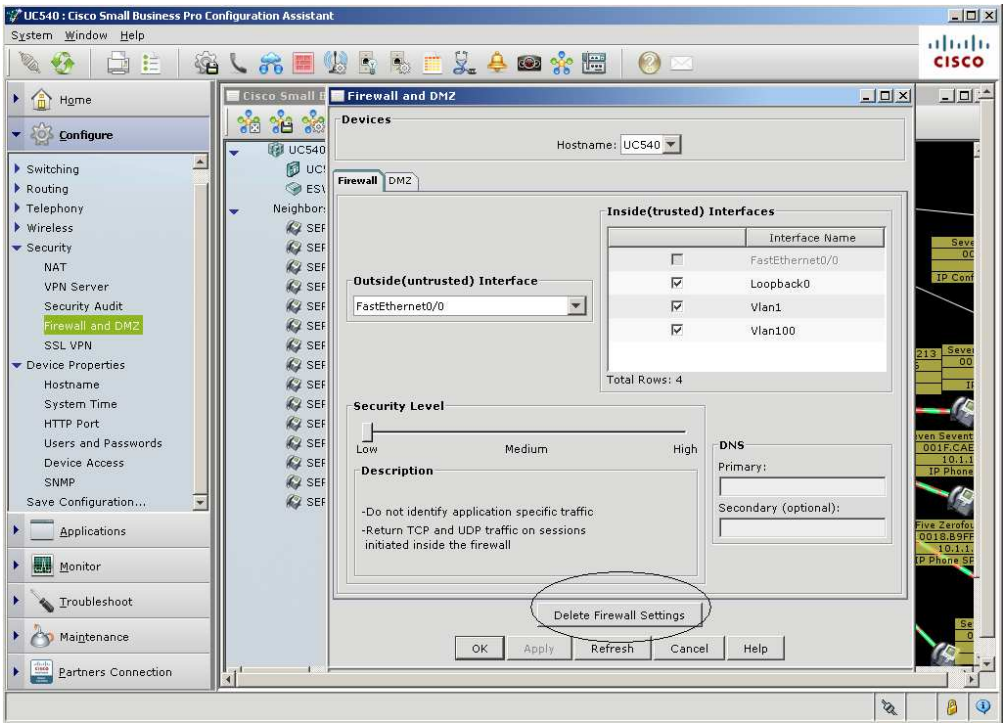
- SIP Trunk SP WAN termination
- Administrative access to the UC540 via CCA and SA500 access via its built in Web GUI (cisco/cisco default on 192.168.75.1)

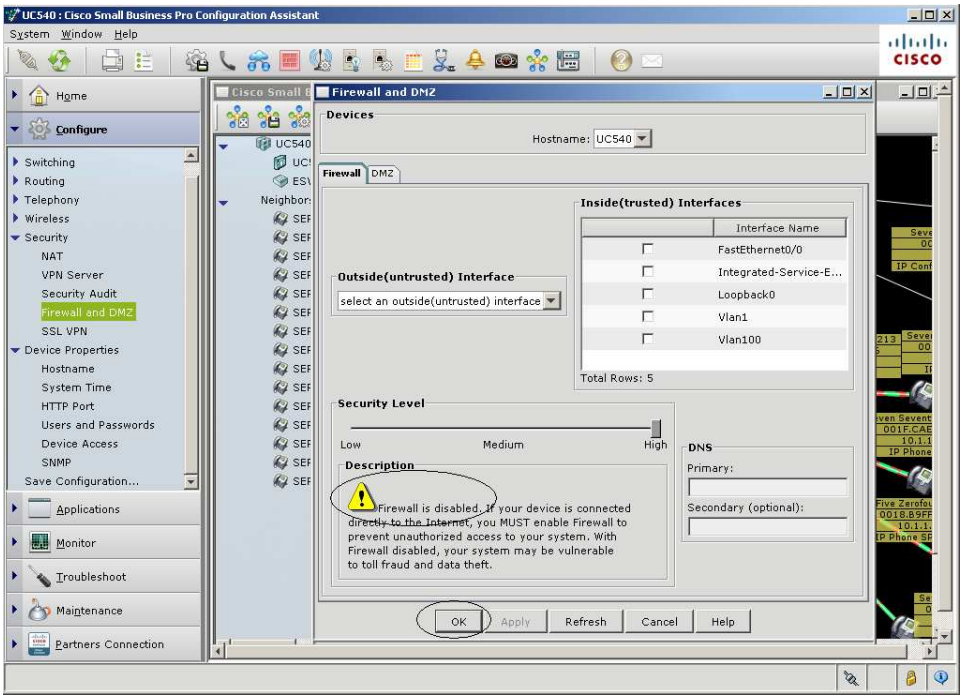
Information Required

No special information is required as the SIP Trunk has already been configured on the UC540.

Configuration

Disable FW on UC500

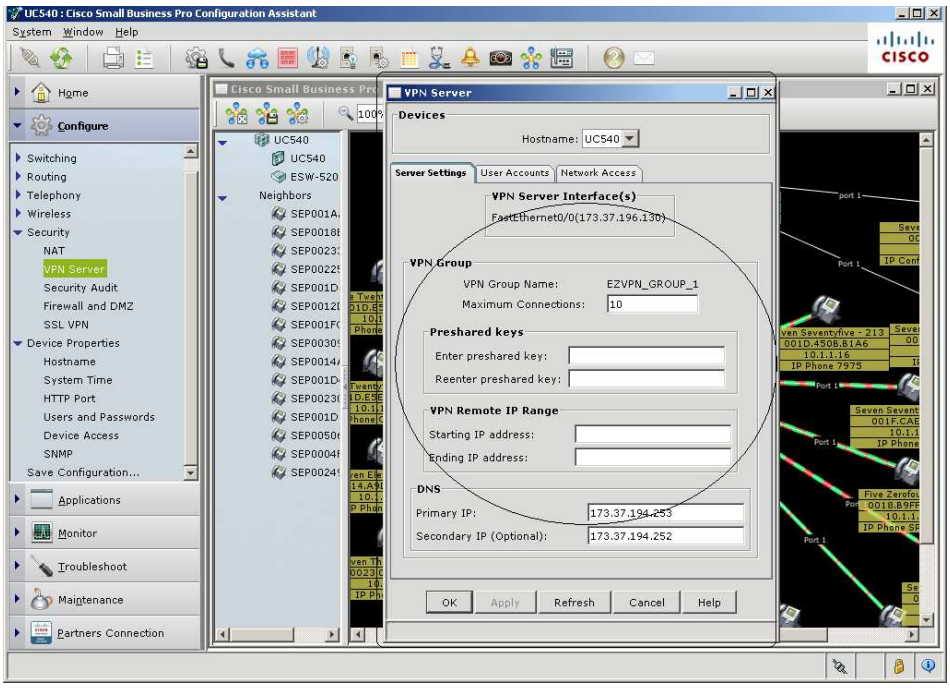




Delete VPN Server

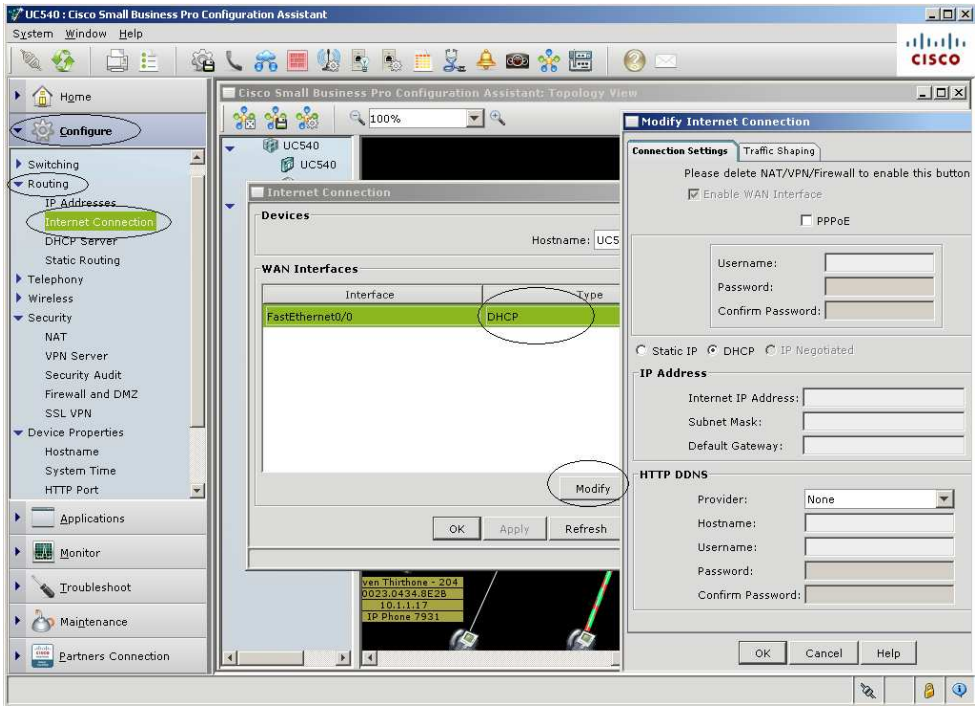
Next Delete the VPN Server if created, since in the next step we will change the FE0/0 WAN IP of the UC500. If the VPN Server is existing, it would have to be deleted first.

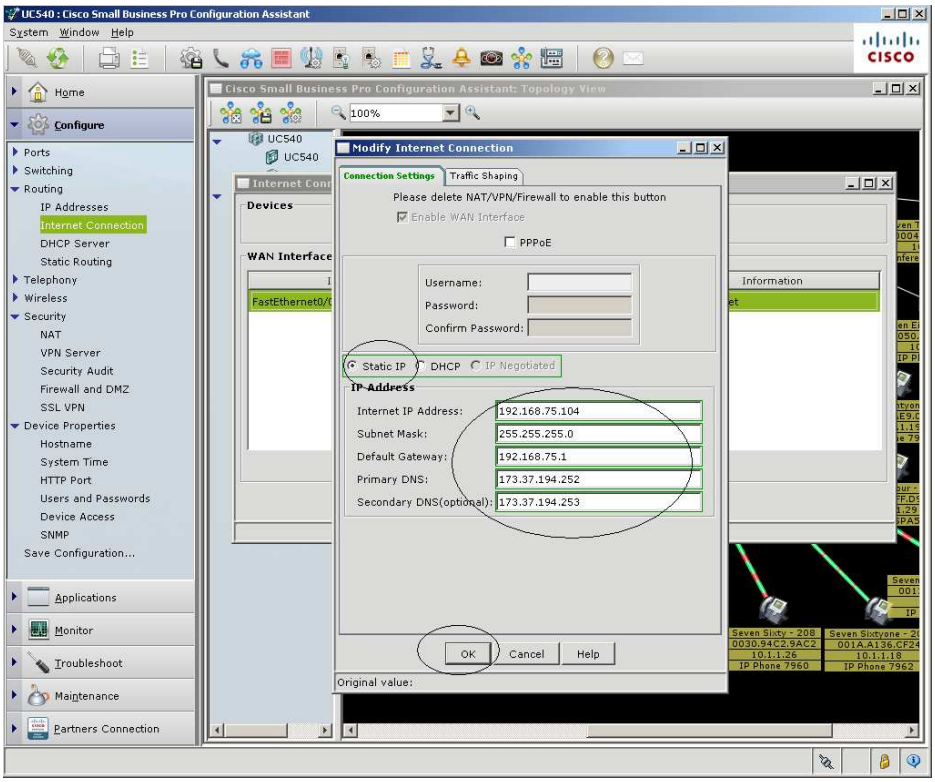
If you don't have it configured yet, or after you delete it, it should look like this…



Modify UC500 WAN

Now we can modify the WAN interface of the UC500. Use a static IP in the SA500 Data Subnet that will be reliable and consistent, since you will later map static routes to this address.



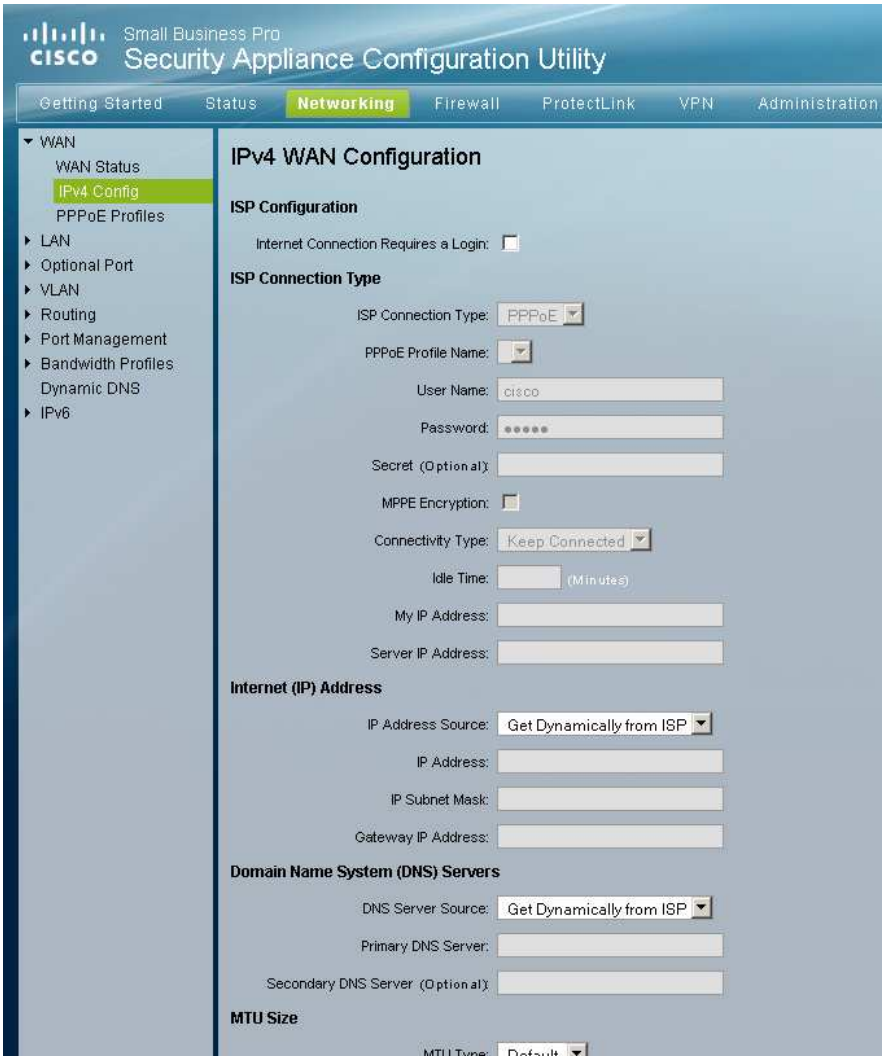


SA500 WAN

Now Lets configure the SA500.

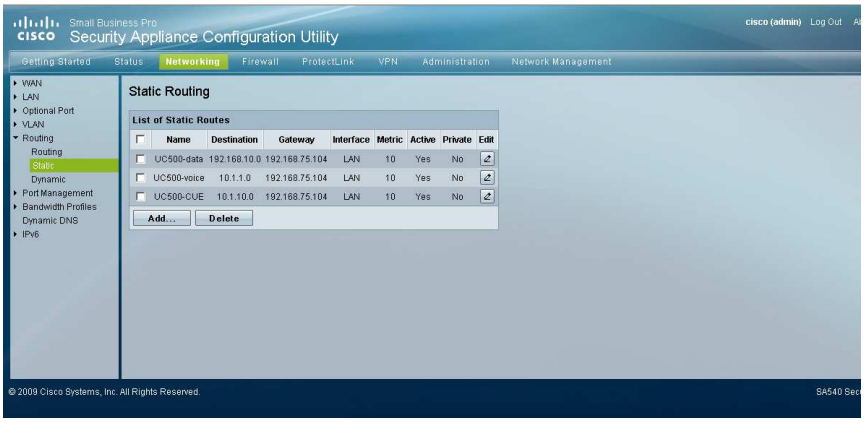
The WAN Interface must be set to what the SIP Trunk SP requires (Static, DHCP, etc).

Mine is a test Account so it's DHCP.



Static Routes to UC500

Now set up some Route to push the traffic for data and voice to the subnets of UC500.

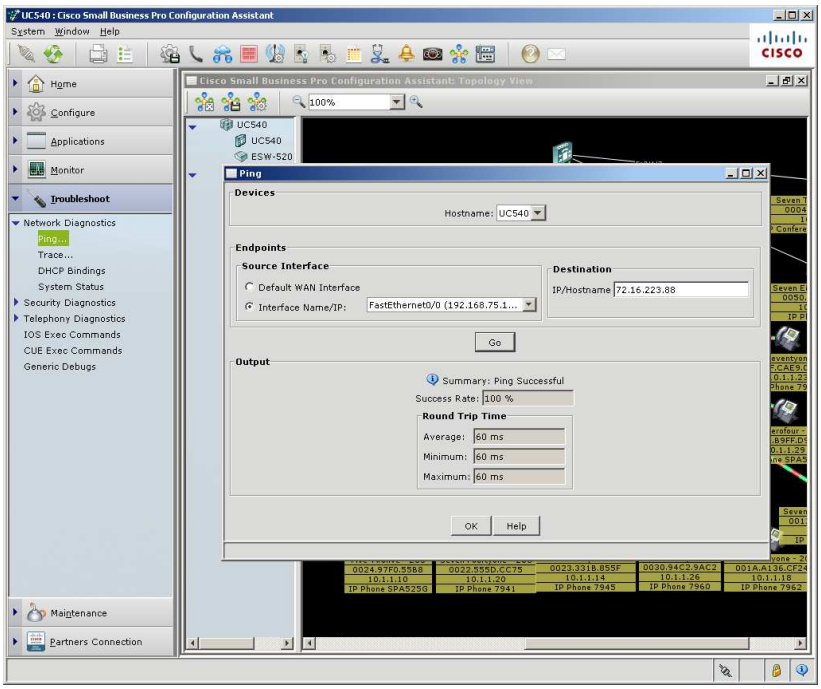


SIP ALG

Now make sure the SIP ALG is enabled:

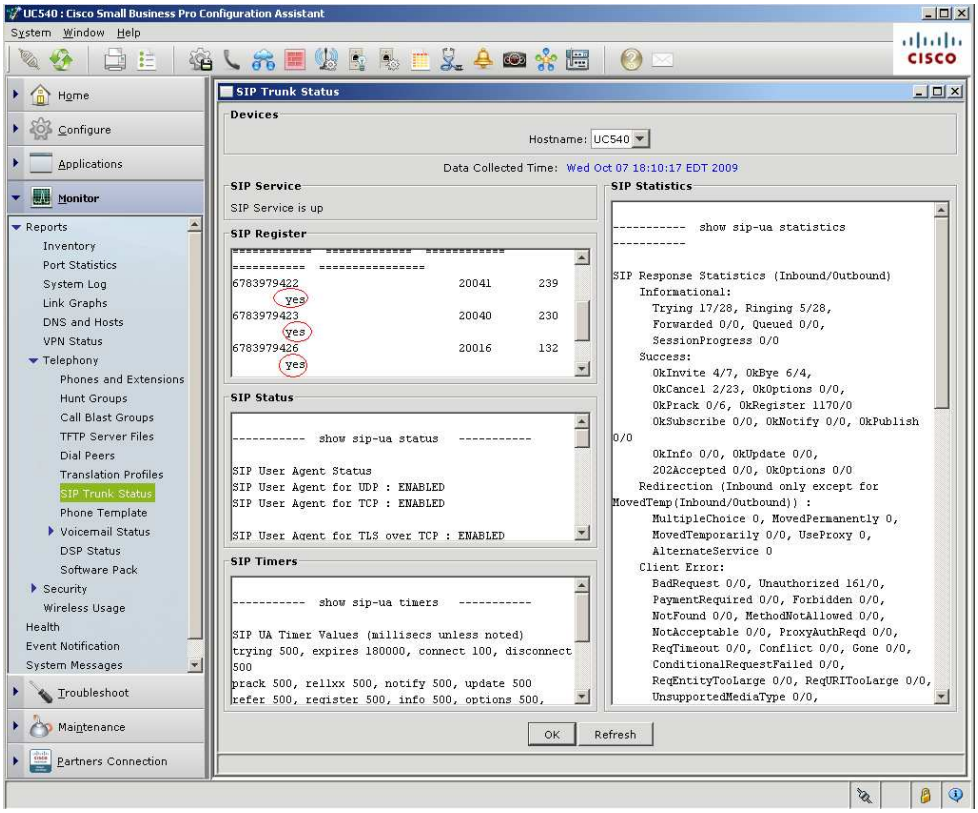
PING verify

"Ping" the SIP-Proxy (either FQDN or IP) for your SIP trunk SP from CCA Troubleshooting: Network Diagnostics.



SIP UA Registration

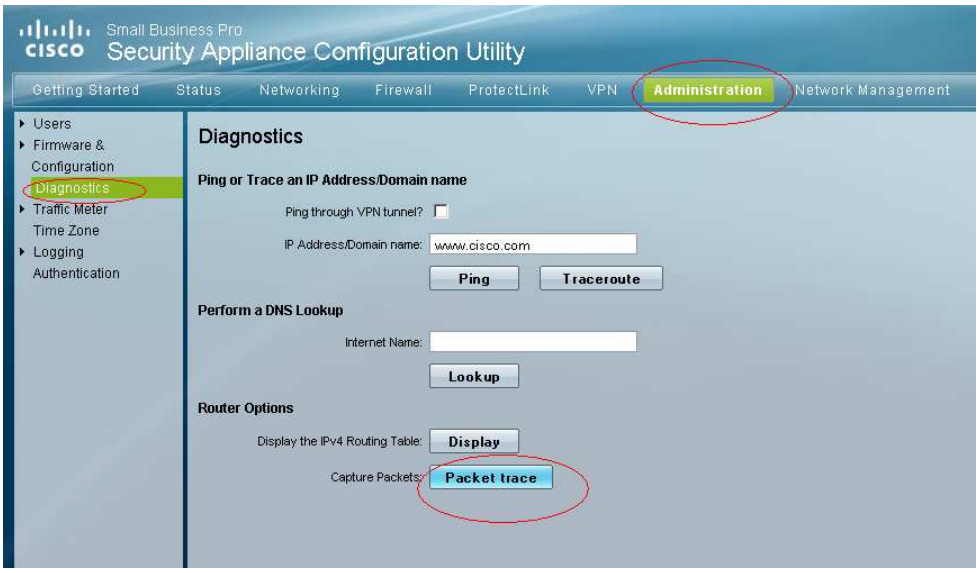
Now check the SIP UA registration (your DIDs)



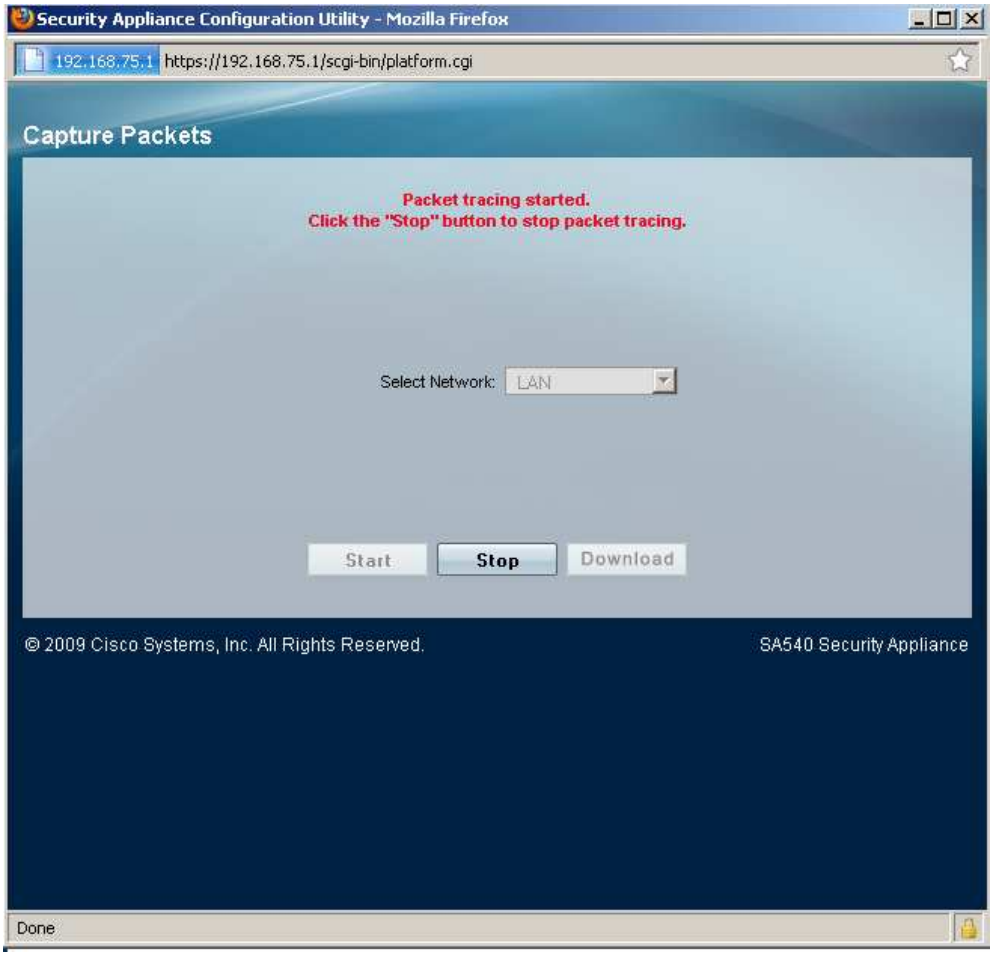
Test Calls & Trace

Make some calls (Egress and Ingress) and verify they work.

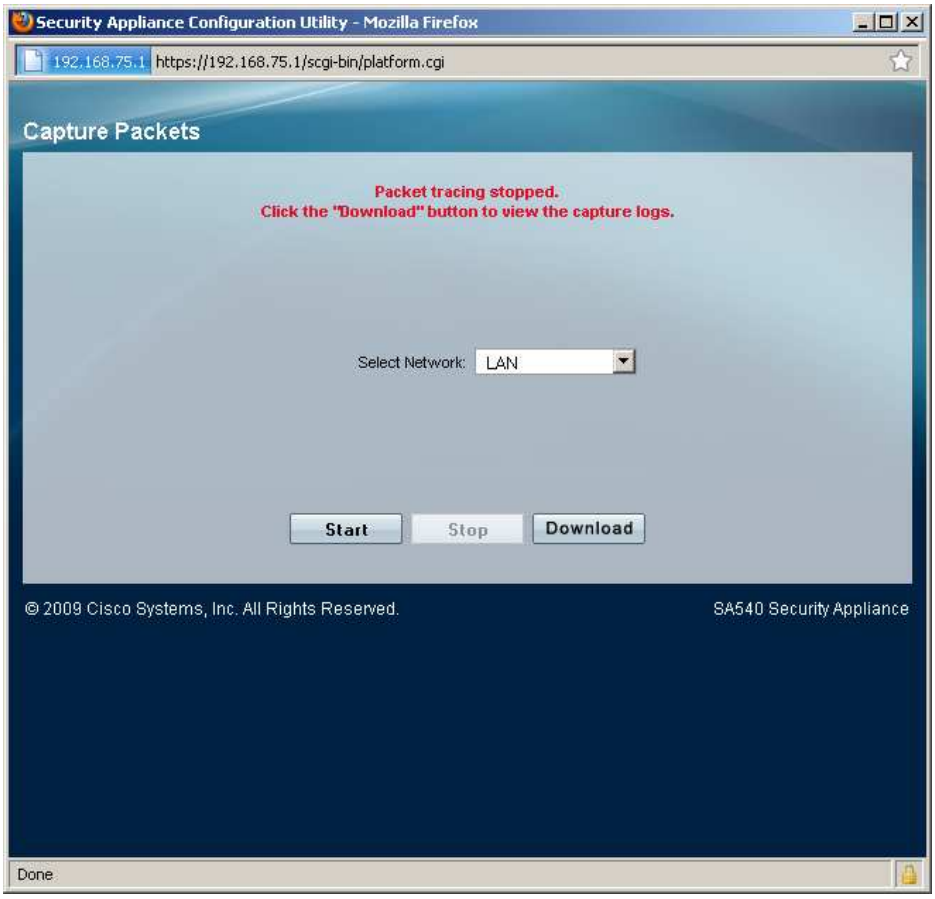
Trace some calls and read the traces into Wireshark if you have any issues.

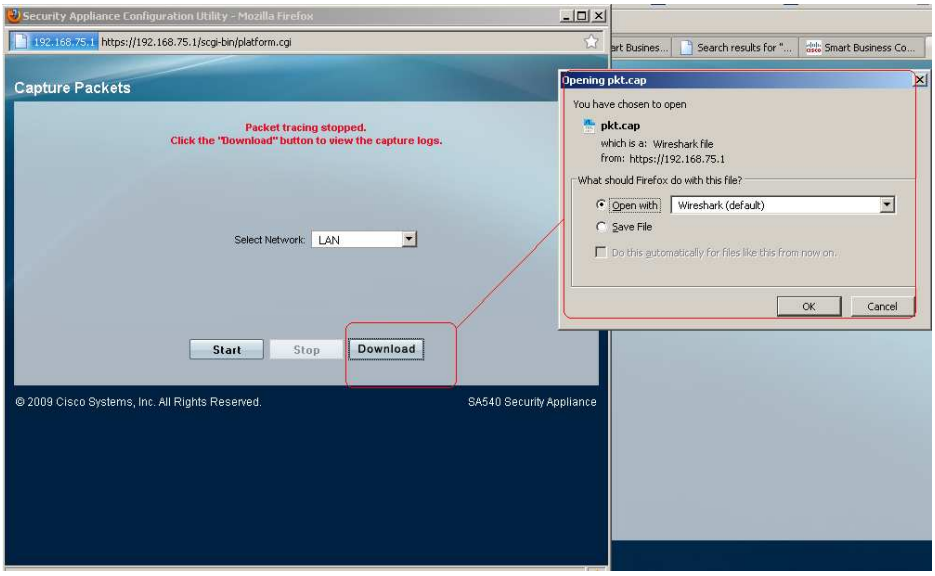


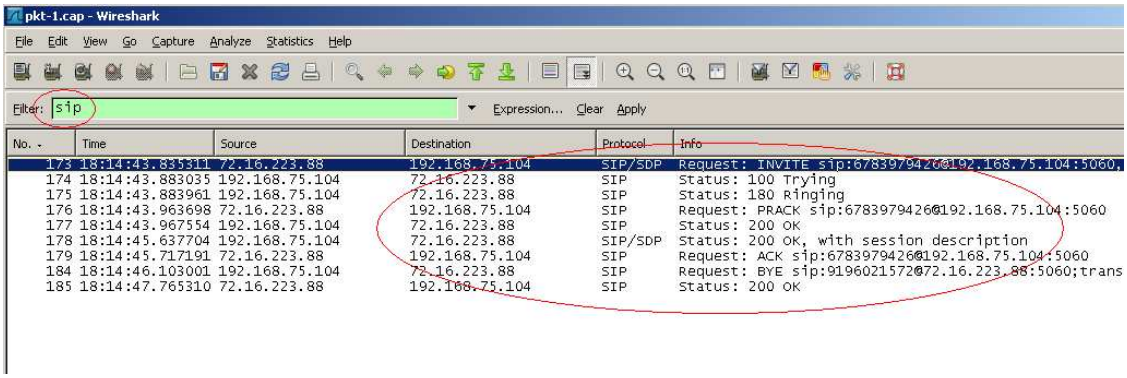
After clicking on packet Trace, you can make calls (in this case a call into one of the UC540 DIDs)



Stop the trace when you hang up the call


Security Appliance Configuration Utility - Mozilla Firefox
192.168.75.1
https://192.168.75.1/scgi-bin/platform.cgi
Capture Packets
Packet tracing stopped.
Click the "Download" button to view the capture logs.
Select Network:
LAN
Start
Stop
Download
© 2009 Cisco Systems, Inc. All Rights Reserved.
SA540 Security Appliance
Done


Security Appliance Configuration Utility - Mozilla Firefox
https://192.168.75.1/scgi-bin/platform.cgi
Capture Packets
Packet tracing stopped.
Click the "Download" button to view the capture logs.
Select Network:
LAN
Start
Stop
Download
© 2009 Cisco Systems, Inc. All Rights Reserved.
SA540 Security Appliance
Search results for "...
Smart Business Co...
Opening pkt.cap
You have chosen to open
pkt.cap
which is a: Wireshark file
from: https://192.168.75.1
What should Firefox do with this file?
Open with
Wireshark (default)
Save File
Do this automatically for files like this from now on.
OK
Cancel



We are done and the customer is happy to have advanced security protecting his UC500 ☺

Now you may use the built in SSL VPN server for the SA500 for remote access (VPN) to the UC500, or the Greenbow or QuickVPN IPSec Client.

Another option is to pass through VPN Traffic to the UC500 (in which case you rebuild the EZVPN server on the UC500) and use the Cisco EZVPN IPSec Client if you wish.

SA500 Pass through Configuration: