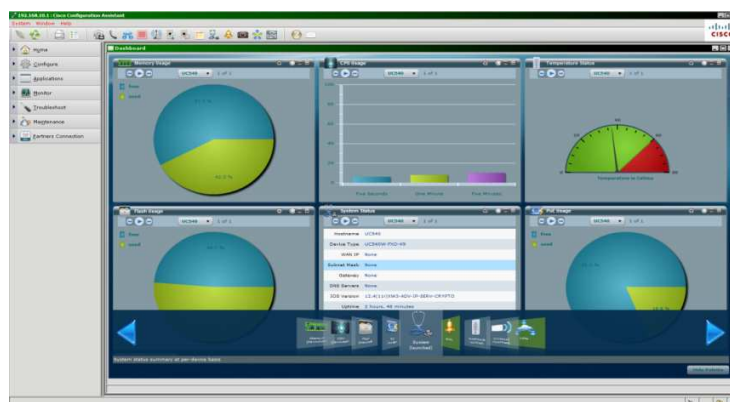


Cisco Small Business Pro

Smart Business Communication System

Technical Enablement Labs



Lab 6

SA500 In front of the UC500

Introduction..... 3

Information Required..... 3

Configuration..... 3

 Disable FW on UC500..... 3

 Delete VPN Server..... 4

 Modify UC500 WAN 5

 SA500 WAN 6

 Static Routes to UC500..... 6

 SIP ALG 7

 PING verify..... 7

 SIP UA Registration 8

 Test Calls & Trace..... 8

 SA500 Pass through Configuration: 11

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:

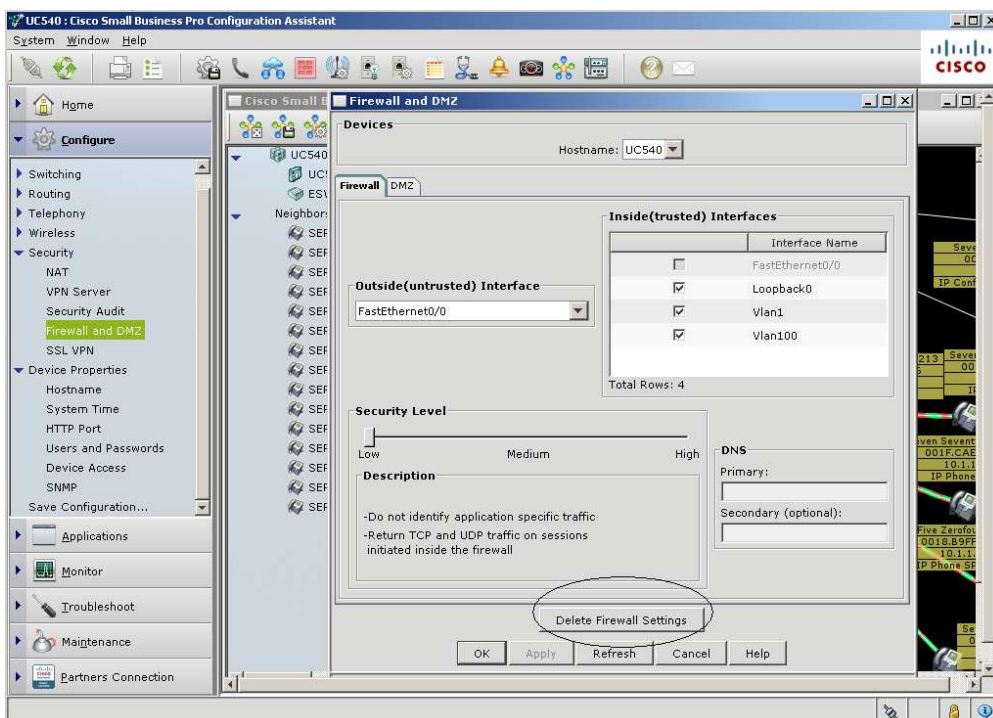
- SIP Trunk SP WAN termination
- Administrative access to the UC540 via CCA and SA500 access via its built in Web GUI (cisco/cisco default on 192.168.75.1)

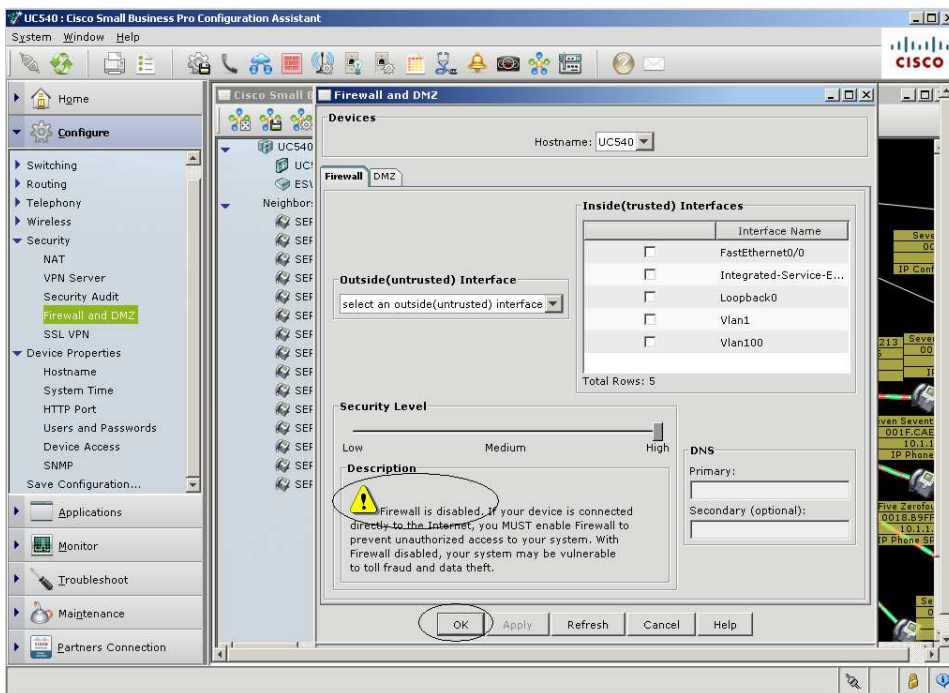
Information Required

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

Configuration

Disable FW on UC500

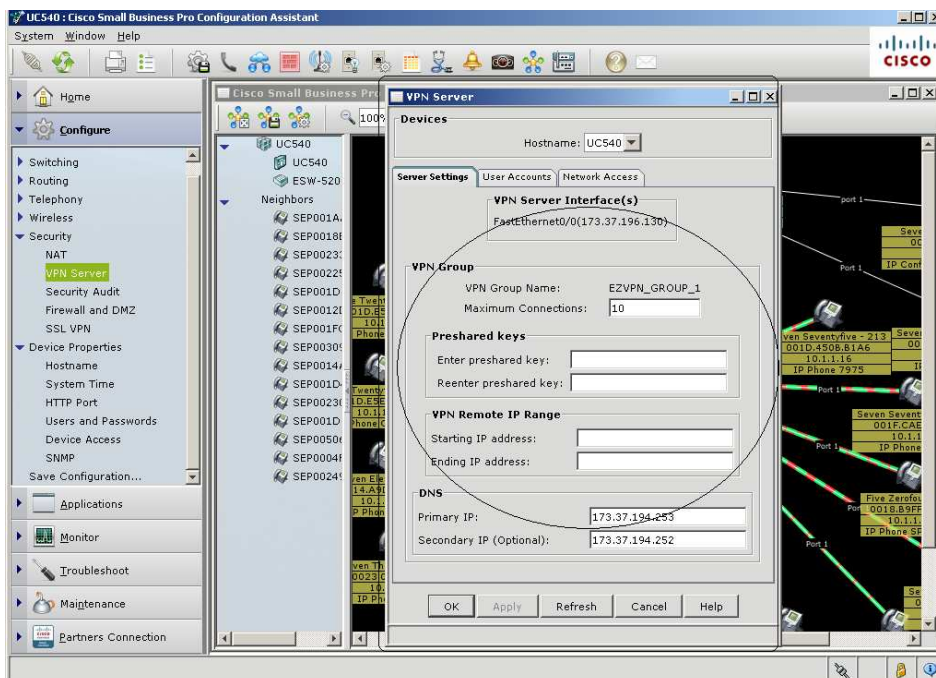




Delete VPN Server

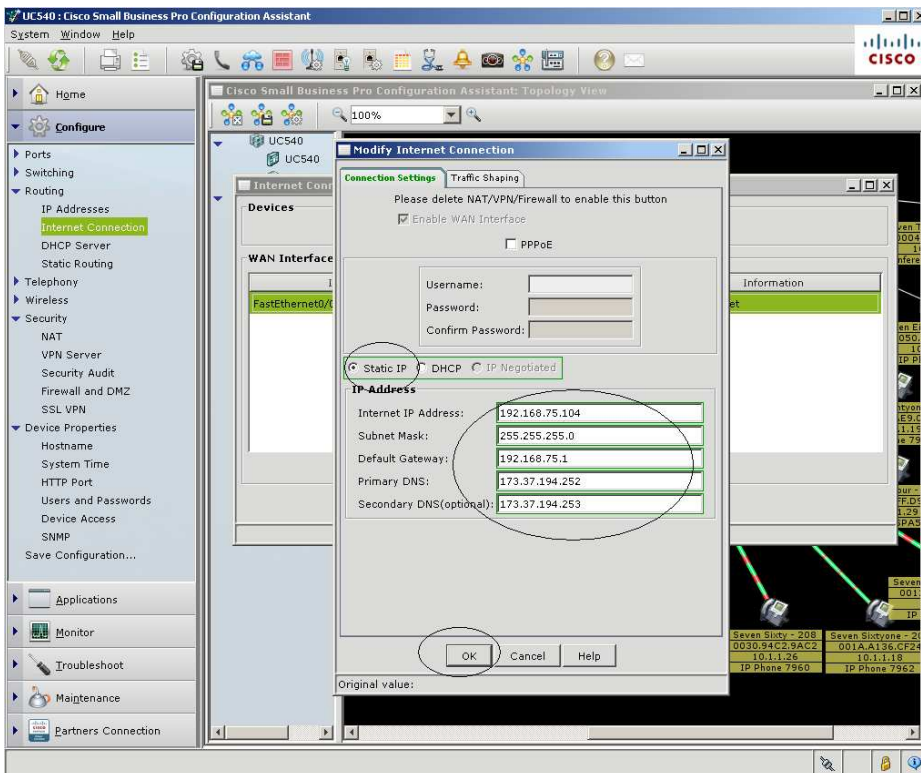
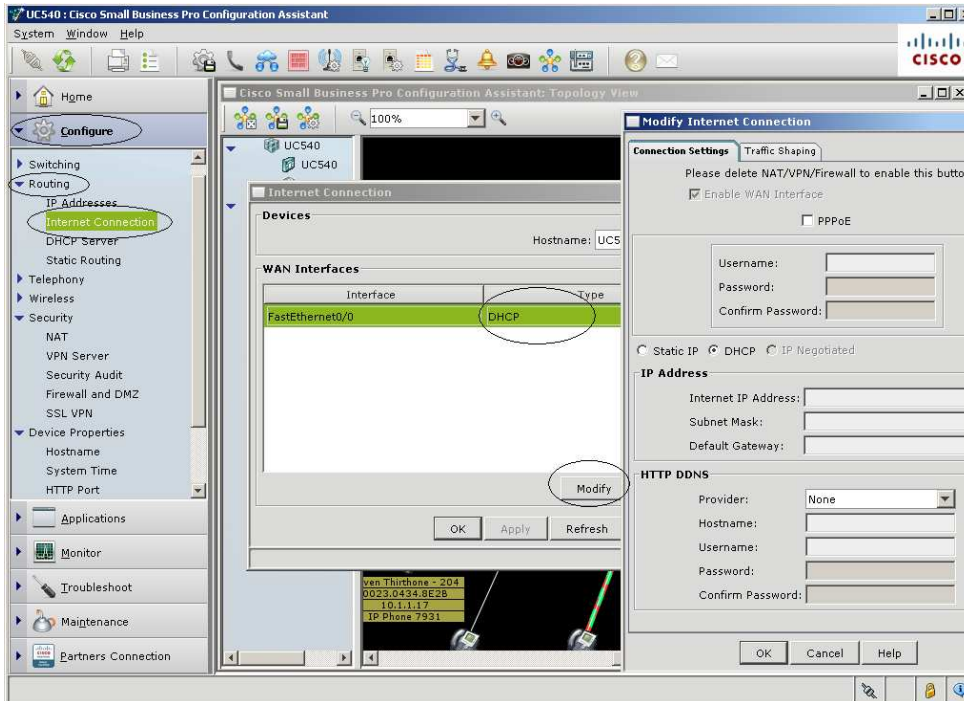
Next Delete the VPN Server if created, since in the next step we will change the FE0/0 WAN IP of the UC500. If the VPN Server is existing, it would have to be deleted first.

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.

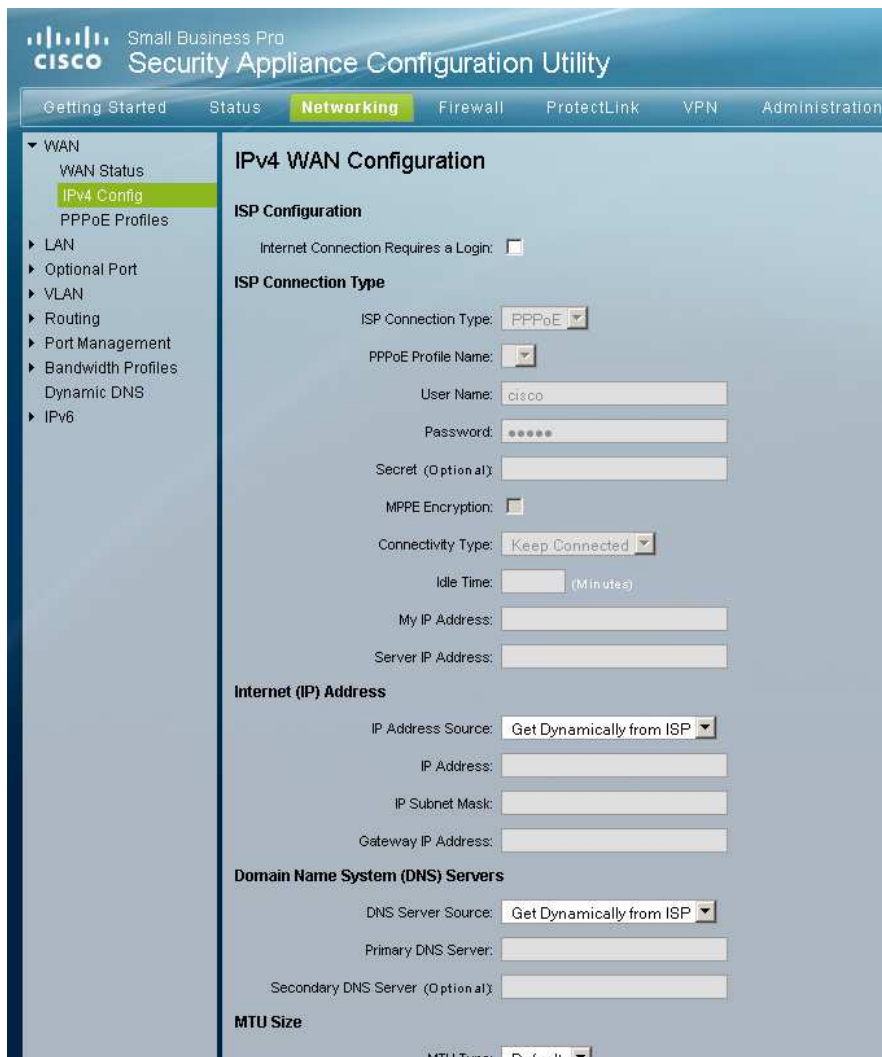


SA500 WAN

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.



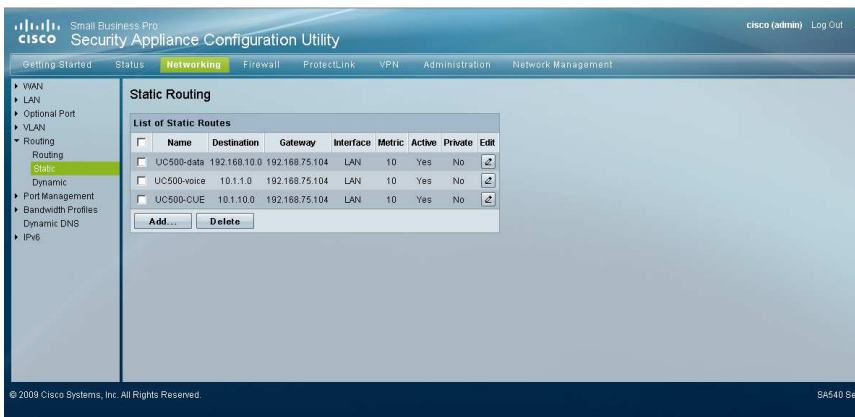
The screenshot displays the Cisco Security Appliance Configuration Utility interface. The top navigation bar includes 'Getting Started', 'Status', 'Networking' (highlighted), 'Firewall', 'ProtectLink', 'VPN', and 'Administration'. The left sidebar shows a tree view with 'WAN' expanded, containing 'WAN Status', 'IPv4 Config' (highlighted), and 'PPPoE Profiles'. Below this are other categories like LAN, Optional Port, VLAN, Routing, Port Management, Bandwidth Profiles, Dynamic DNS, and IPv6.

The main content area is titled 'IPv4 WAN Configuration' and is divided into several sections:

- ISP Configuration:** Includes a checkbox for 'Internet Connection Requires a Login'.
- ISP Connection Type:** Features a dropdown menu set to 'PPPoE', a 'PPPoE Profile Name' dropdown, 'User Name' (text field with 'cisco'), 'Password' (masked field), 'Secret (Optional)' (text field), 'MPPE Encryption' checkbox, 'Connectivity Type' dropdown set to 'Keep Connected', 'Idle Time' (text field with '(Minutes)'), 'My IP Address' (text field), and 'Server IP Address' (text field).
- Internet (IP) Address:** Includes 'IP Address Source' dropdown set to 'Get Dynamically from ISP', 'IP Address' (text field), 'IP Subnet Mask' (text field), and 'Gateway IP Address' (text field).
- Domain Name System (DNS) Servers:** Includes 'DNS Server Source' dropdown set to 'Get Dynamically from ISP', 'Primary DNS Server' (text field), and 'Secondary DNS Server (Optional)' (text field).
- MTU Size:** Includes 'MTU Type' dropdown set to 'Default'.

Static Routes to UC500

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



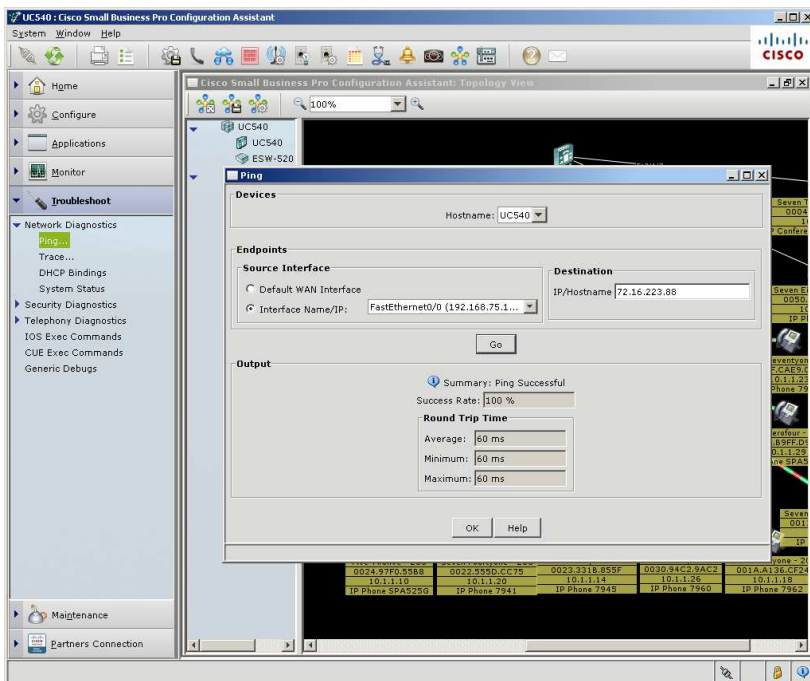
SIP ALG

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)

The screenshot shows the Cisco Small Business Pro Configuration Assistant interface. The left-hand navigation pane is expanded to 'Monitor' > 'Reports' > 'Telephony' > 'SIP Trunk Status'. The main window displays the following information:

- SIP Service:** SIP Service is up.
- SIP Register:** A table showing registration details for three DIDs. The 'yes' status for each is circled in red.
- SIP Status:** SIP User Agent Status is ENABLED for both UDP and TCP. SIP User Agent for TLS over TCP is also ENABLED.
- SIP Timers:** SIP UA Timer Values (in milliseconds) are listed: trying 500, expires 180000, connect 100, disconnect 500, prack 500, rellxx 500, notify 500, update 500, refer 500, register 500, info 500, options 500.
- SIP Statistics:** A detailed log of SIP response statistics, including informational, success, and client error counts.

DID	Registration Status	Port	Count
6783979422	yes	20041	239
6783979423	yes	20040	230
6783979426	yes	20016	132

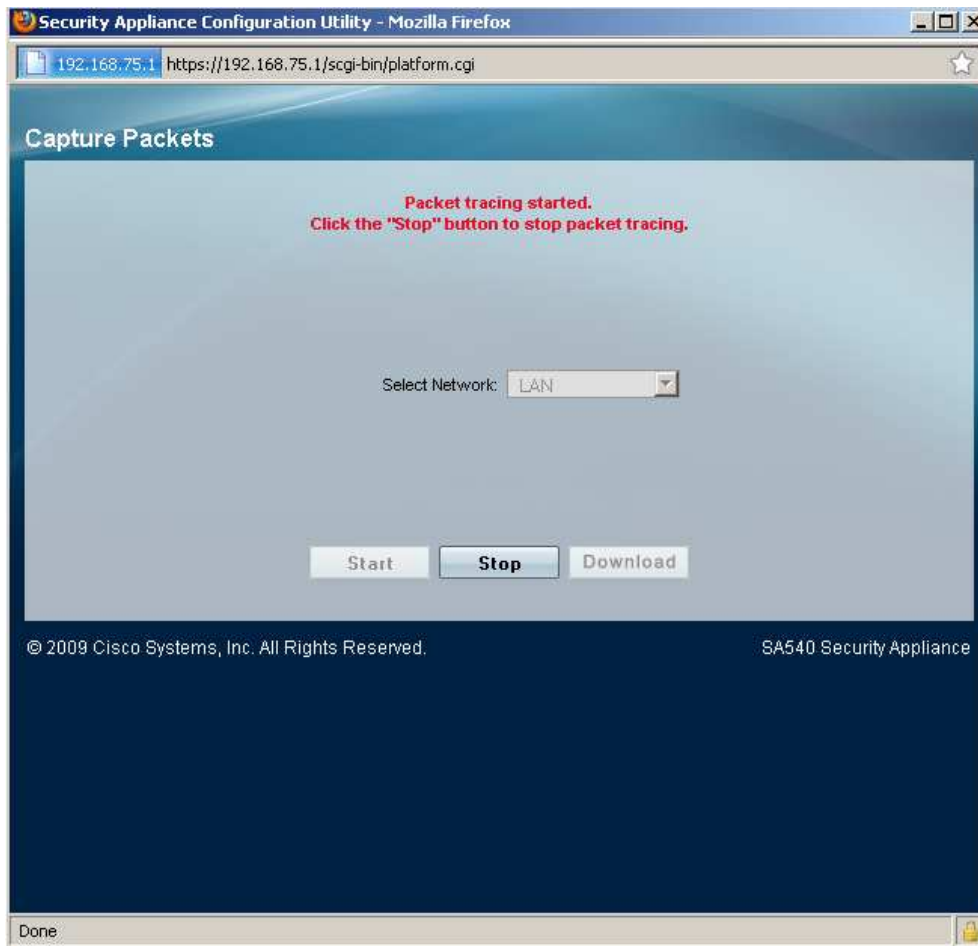
Test Calls & Trace

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

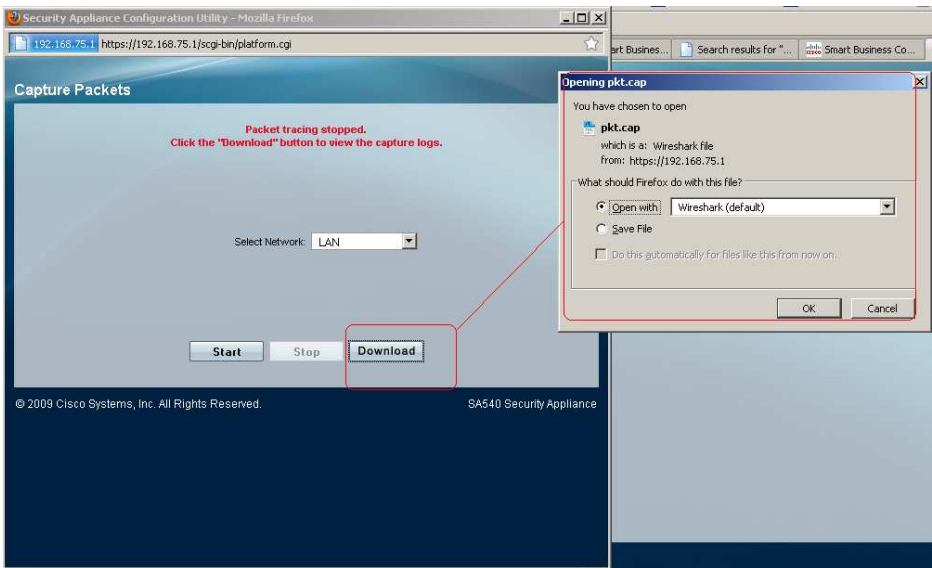
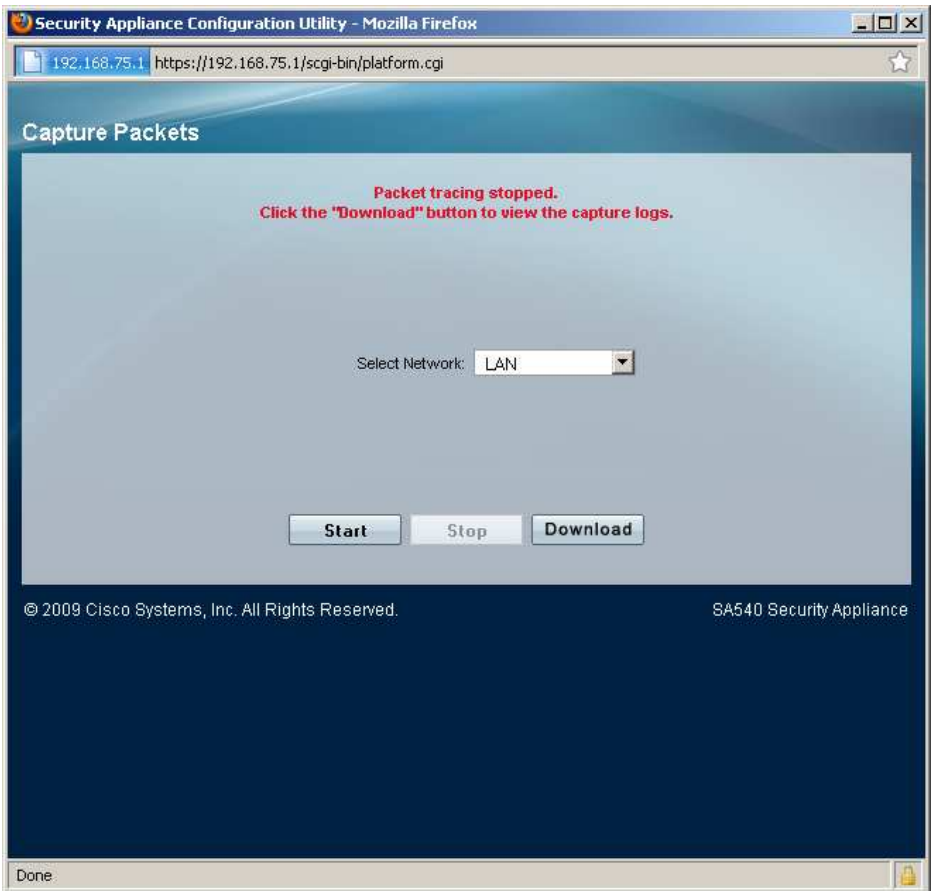
Trace some calls and read the traces into Wireshark if you have any issues.



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



No. -	Time	Source	Destination	Protocol	Info
173	18:14:43.835311	72.16.223.88	192.168.75.104	SIP/SDP	Request: INVITE sip:6783979426@192.168.75.104:5060
174	18:14:43.883035	192.168.75.104	72.16.223.88	SIP	Status: 100 Trying
175	18:14:43.883961	192.168.75.104	72.16.223.88	SIP	Status: 180 Ringing
176	18:14:43.963698	72.16.223.88	192.168.75.104	SIP	Request: PRACK sip:6783979426@192.168.75.104:5060
177	18:14:43.967554	192.168.75.104	72.16.223.88	SIP	Status: 200 OK
178	18:14:45.637704	192.168.75.104	72.16.223.88	SIP/SDP	Status: 200 OK, with session description
179	18:14:45.717191	72.16.223.88	192.168.75.104	SIP	Request: ACK sip:6783979426@192.168.75.104:5060
184	18:14:46.103001	192.168.75.104	72.16.223.88	SIP	Request: BYE sip:9196021572@72.16.223.88:5060;trans
185	18:14:47.765310	72.16.223.88	192.168.75.104	SIP	Status: 200 OK

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:

Small Business Pro
cisco Security Appliance Configuration Utility

Getting Started Status Networking **Firewall** ProtectLink VPN Administration Network Management

Firewall
 Default Outbound
 Policy
IPv4 Rules
 IPv6 Rules
 Services
 Schedules
 Attacks
 Content Filtering
 MAC Filtering
 Port Triggering
 Session Settings
 SIP

IPv4 Firewall Rules

List of Available Firewall Rules

<input type="checkbox"/>	Status	From Zone	To Zone	Service	Action	Source Hosts	Destination Hosts	Local Server	Internet Destination	Log	Edit
<input type="checkbox"/>	Enabled	WAN	LAN	IPSEC-UDP-ENCAP	ALLOW always	Any		192.168.75.104	WAN1	Always	↗
<input type="checkbox"/>	Enabled	WAN	LAN	IKE	ALLOW always	Any		192.168.75.104	WAN1	Always	↗

Add... **Enable** **Disable** **Delete**

Small Business Pro
cisco Security Appliance Configuration Utility

Getting Started Status Networking Firewall ProtectLink **VPN** Administration Network Management

IPSec
 VPN Wizard
 Basic Settings
 Defaults
 IKE Policies
 VPN Policies
 IPSec Users
Passthrough
 SSL VPN Server
 SSL VPN Client
 VeriSign ID Protection

Passthrough

IPSec VPN Passthrough

IPSec
 PPTP
 L2TP

Apply **Reset**

