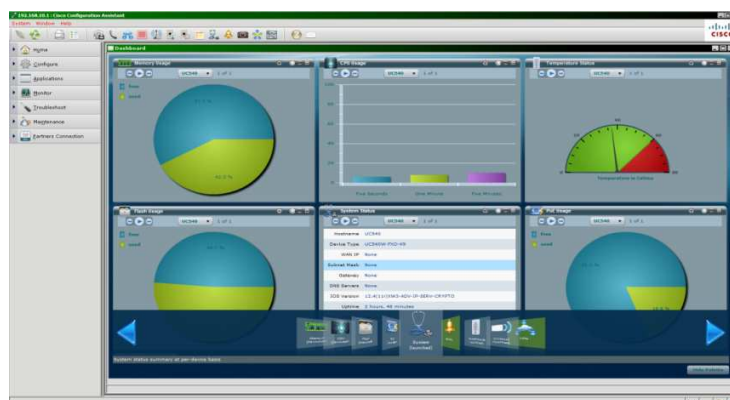


Cisco Small Business Pro

Smart Business Communication System

Technical Enablement Labs



Lab 3

VPN Configuration

Introduction..... 3

Information Required..... 3

Configuration..... 3

 VPN Client..... 3

 VPN Server..... 4

 Server Settings 4

 User Accounts 5

 Network Access..... 5

Verify..... 6

Introduction

This lab is also something that should be done in a staging environment. It is the opportunity for you to enter configuration data you collected during your site survey/customer questionnaire.

For this stage/phase of the UC540 lifecycle, you will want to configure the built in VPN Server on the UC540, so it may be accessed via EZVPN Clients connecting from a non collocated location. This is especially important for ongoing remote maintenance and configuration of the system you will want to have later.

In this lab, you will:

- Build the VPN Server and enter Credentials for access
- Assign the DHCP IP Addresses to be offered to remote VPN clients
- Set up split tunneling so that remote client traffic that comes to the UC540 is only for the UC540

Information Required

For this configuration you will need to have:

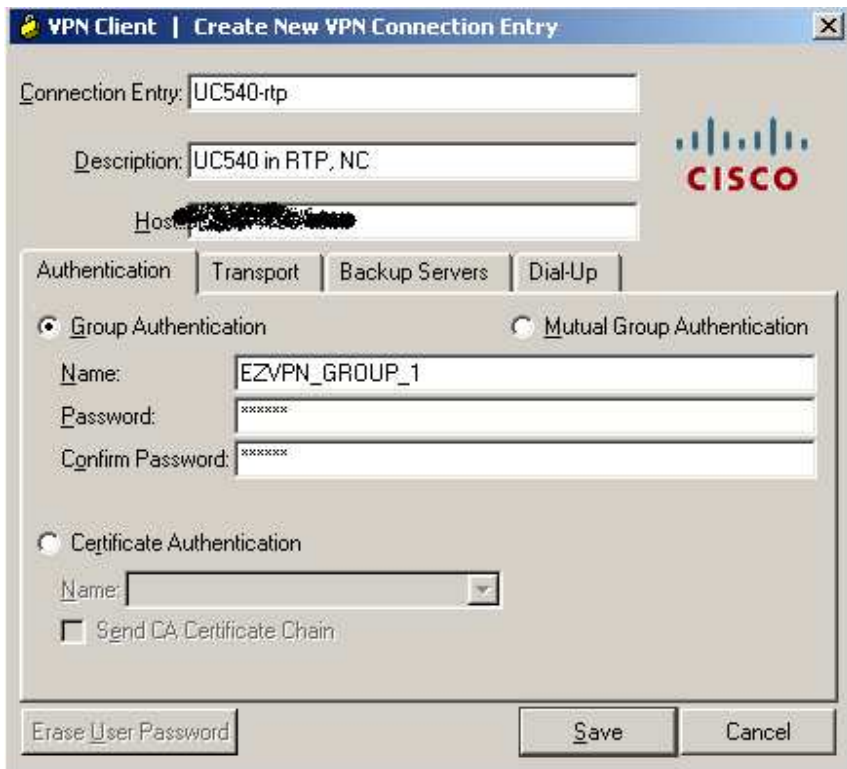
- The Shared Secret which will be used on both the VPN Client and the UC540
- The user name(s) and password(s) for remote clients to use

Configuration

VPN Client

Download the Cisco EZVPN Client to your laptop and configure it to access the UC540.

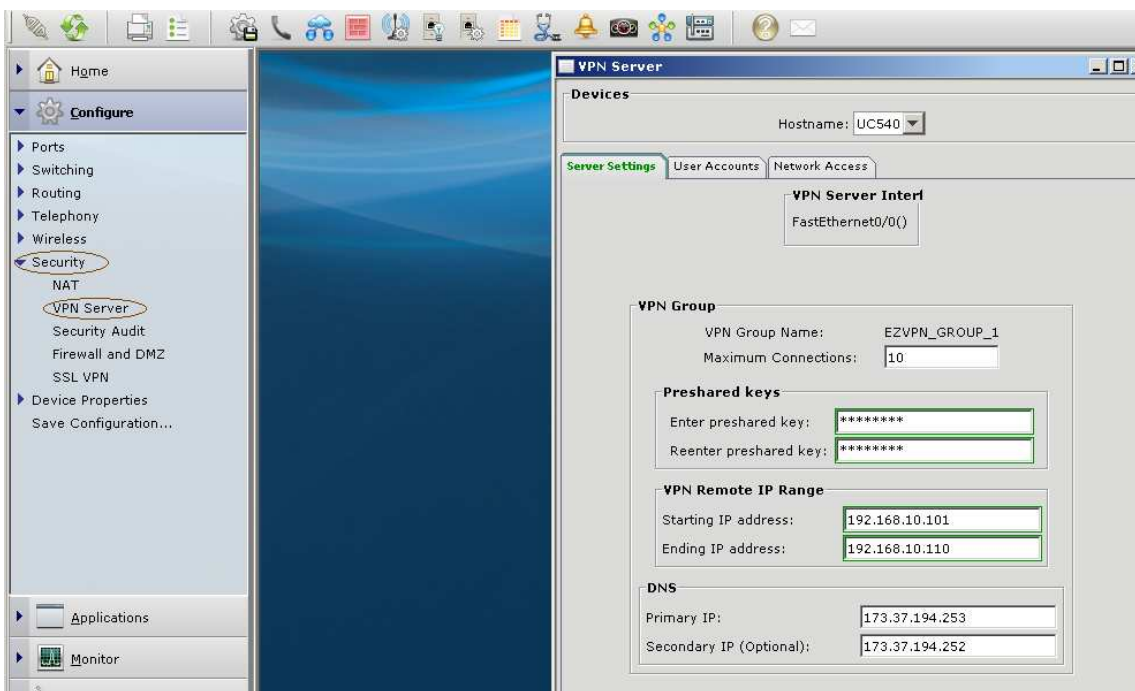
Use the WAN IP of the UC540 FE0/0 or the Host name. Set a Group Name and a Password and Save it.



VPN Server

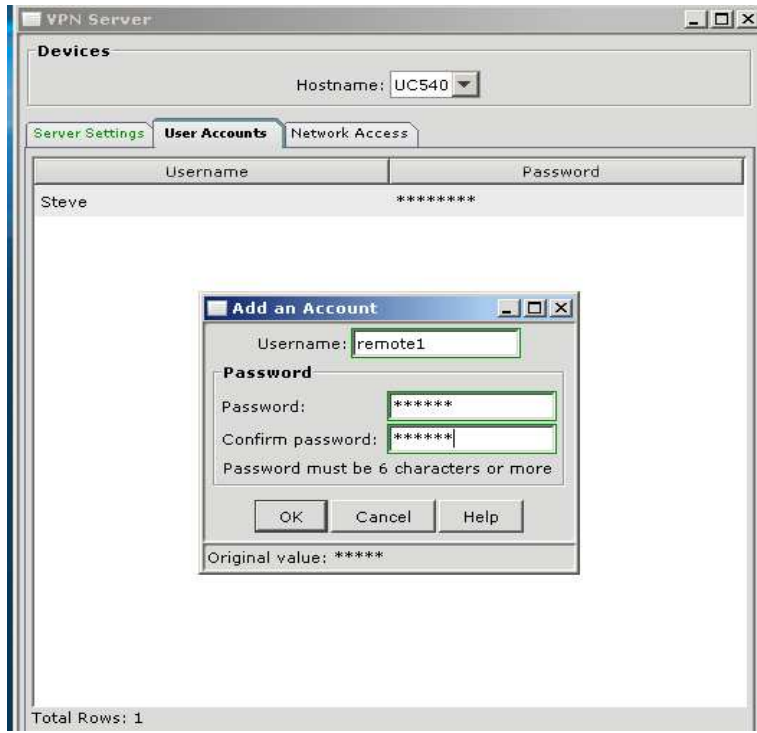
Server Settings

Remember the UC540 supports 10 VPN connections, so consider this when setting the max connections. If you have 2 multisites and 4 Teleworkers, you would set this to 4, and assign the IP Pool accordingly as well. In this case, we assume we have no multisite or remote teleworkers.



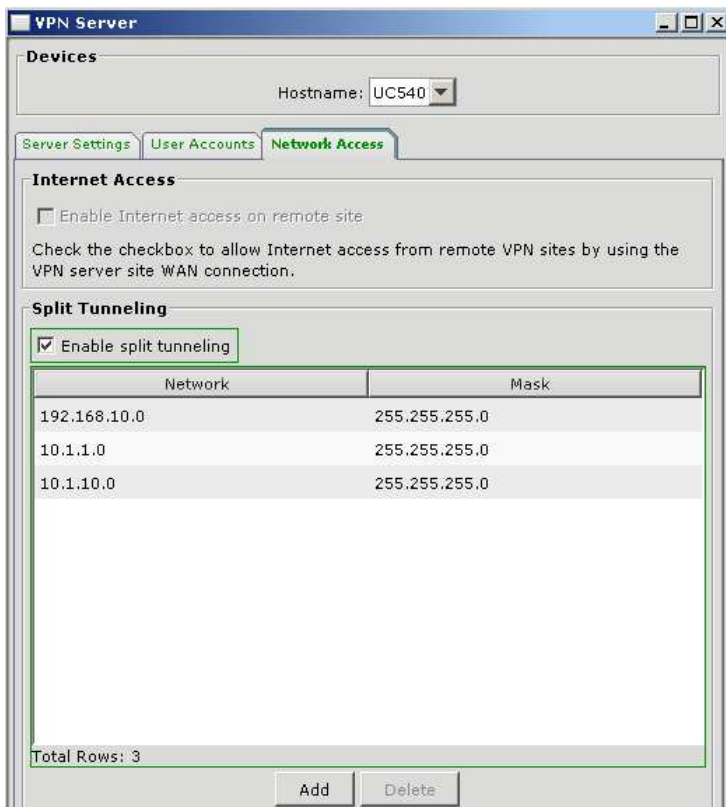
User Accounts

Click on User Account Tab and notice the Admin User is already visible. Don't change that or you will lock yourself out of the UC540. Add the users you want to access from remote.



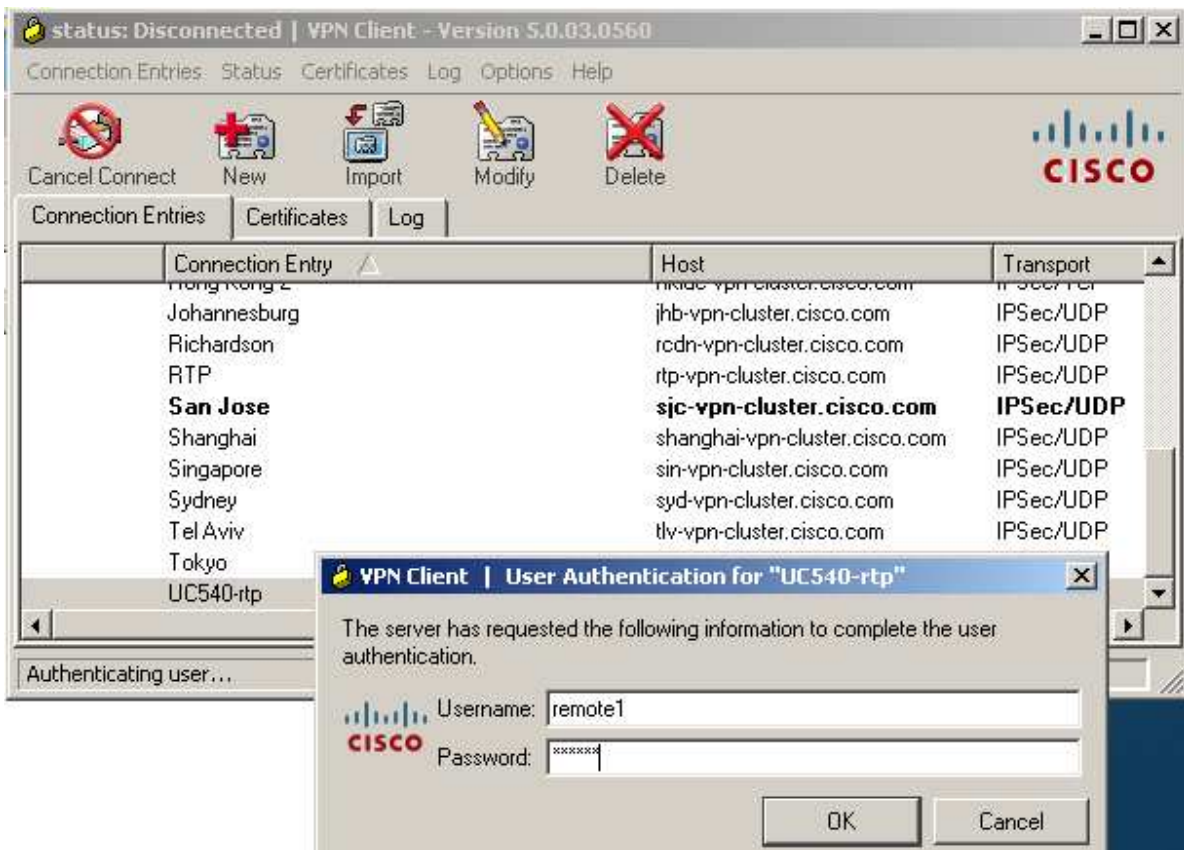
Network Access

Click on Network Access Tab and set Split Tunneling (best practice for bandwidth conservation) for the networks you want to access inside the IPsec tunnel, namely the data VLAN, the CME and the CUE.

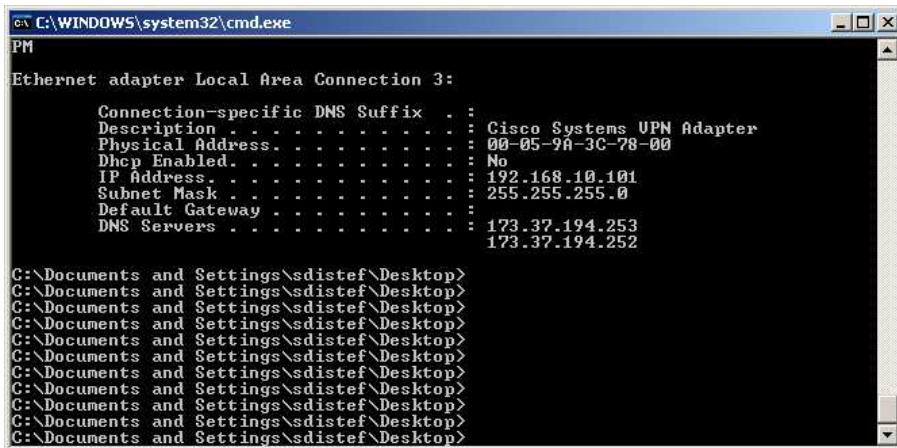


Verify

Connect a notebook or desktop PC running the Cisco VPN Client to an external network and confirm you can connect to the UC540.



Boom, your in!



Now open CCA and check the dashboard to see your connection.

Cisco Small Business Pro Configuration Assistant: Dashboard

Memory Usage

UC540 1 of 1

free: 55.3%
used: 44.5%

CPU Usage

ESW-520-24P 1 of 2

Flash Usage

UC540 1 of 1

free: 48.7%
used: 51.3%

PoE Usage

ESW-520-24P 1 of 2

free: 100.0%

System Status

UC540 1 of 1

Hostname: UC540
Device Type: UC540W-FXO-K9
WAN IP: 173.37.196.131
Subnet Mask: 255.255.255.240

Event Alerts

Type	Description
Informational	Usage activity data sent.

Primary events dialog

Temperature Status

ESW-520-24P 1 of 2

Temperature in Celsius: 40

Voicemail Status

UC540 1 of 1

CUE Software Version: 7.0.3
Used: 13.75%
Used (minutes): 264.0 Available (minutes): 19

User ID	Extension	Type	Size (mi)

VPN Status

UC540 1 of 1

Total number of clients: 1

Public I	VPN IP Address	Status
173.37.	192.168.10.101	UP-ACTIVE