SA500 series router

How to connect Client to Gateway (Mac)

This article will explain how to connect a Mac to an SA500 series router for remote access using IPSec VPN connection.

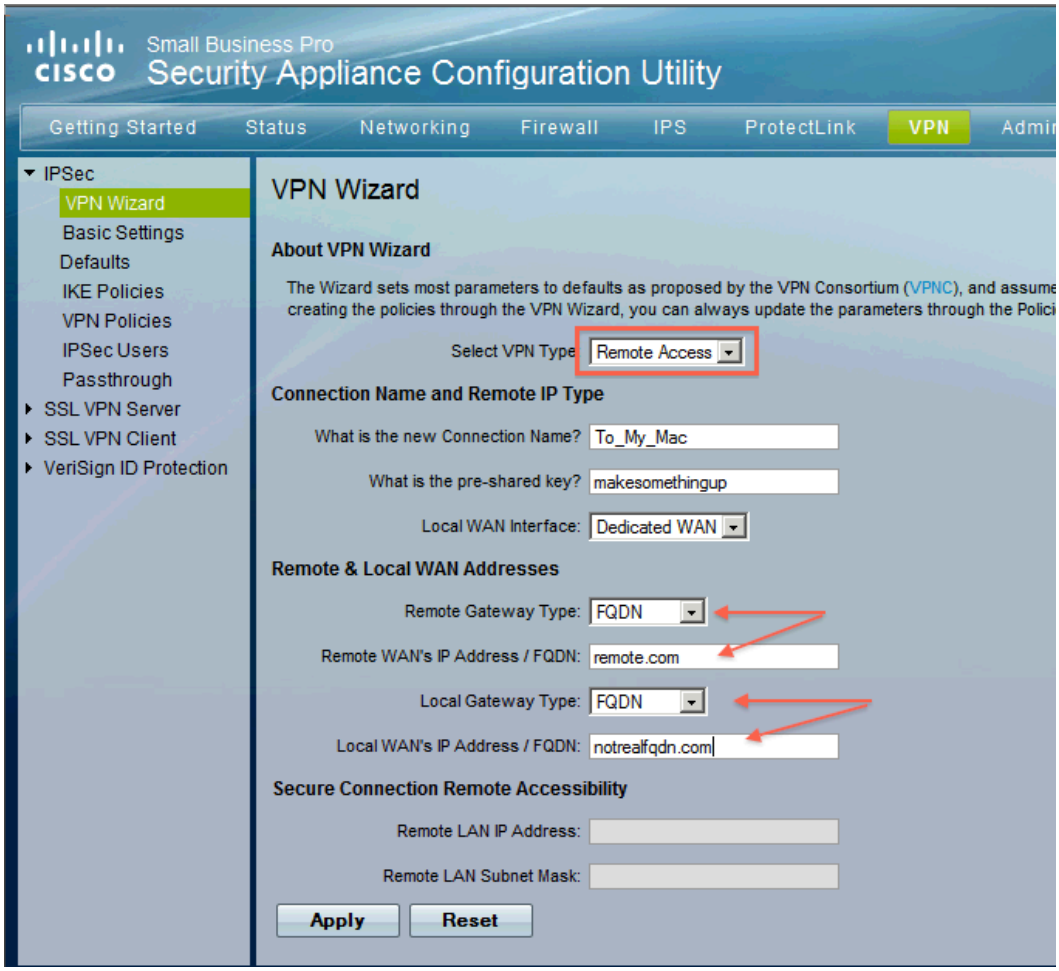
This article will not cover how to configure the connection when multiple subnets exist at the remote site, or how to implement “XAuth” for connection authentication.

Pre-requisites:

1. Internet connection
2. Access to the SA500 series router for initial configuration
3. Knowledge of your network IP requirements (WAN and LAN)
4. For Mac client; installation of “IPSecuritas” – you can download this application from here

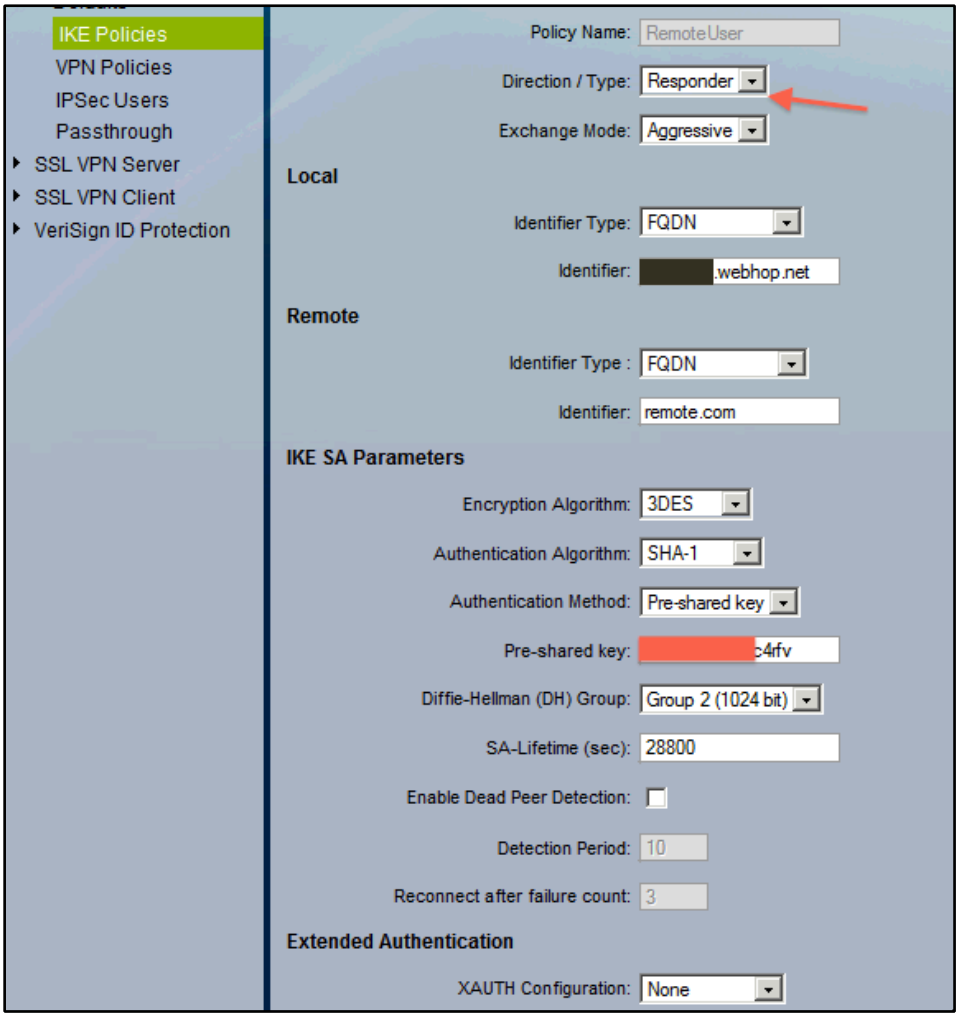
Configuration:

1. Log into the SA router and navigate to “VPN > IPSec > VPN Wizard”



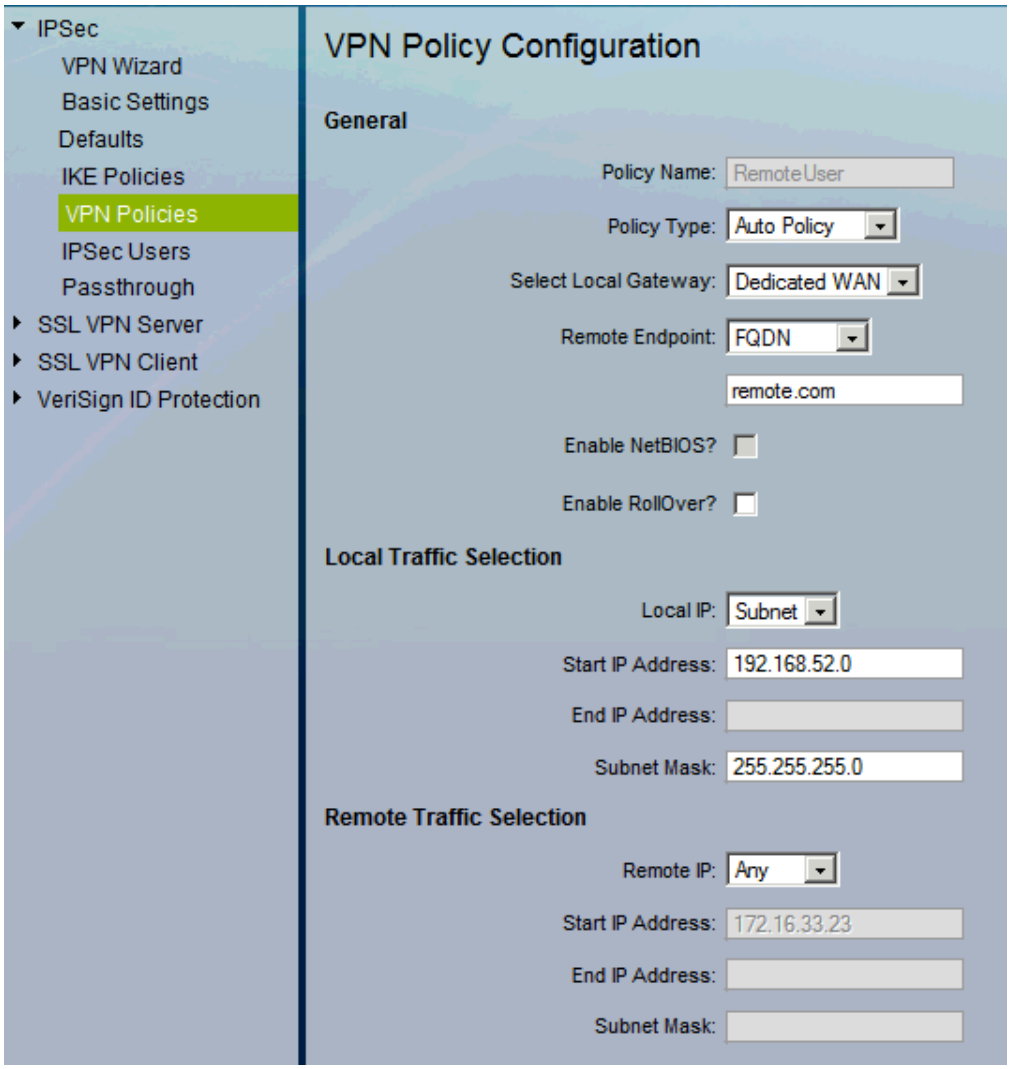
2. VPN Type: “Remote Access”

3. Give the connection a name (This is just a Tag and has no value to the tunnel)
4. Enter a “Pre-Shared” key; the longer the key the better but stay above 8 characters
5. Select the Wan interface, if multiple are configured. Remember if Aliases are being used, select the appropriate IP for the tunnel
6. This is the confusing part; for the Remote and Local WAN addresses just leave them as FQDN and the remote leave as “remote.com” or make something up keeping the FQDN structure (example: myfakedomain.com). If you have a domain name accessible from the WAN specify your domain in Local field as it will make it easier for your users
7. Go ahead and “Apply” settings
8. Now navigate to “IKE Policy” and make sure the settings are like this:



9. Direction / Type should be set to “Responder” and if FQDN was specified Exchange mode should be set to “Aggressive”
10. Take note of all the IKE SA Parameters, as we will need those later. Also if “XAuth” is to be used, you will configure it here (we will not cover XAuth).

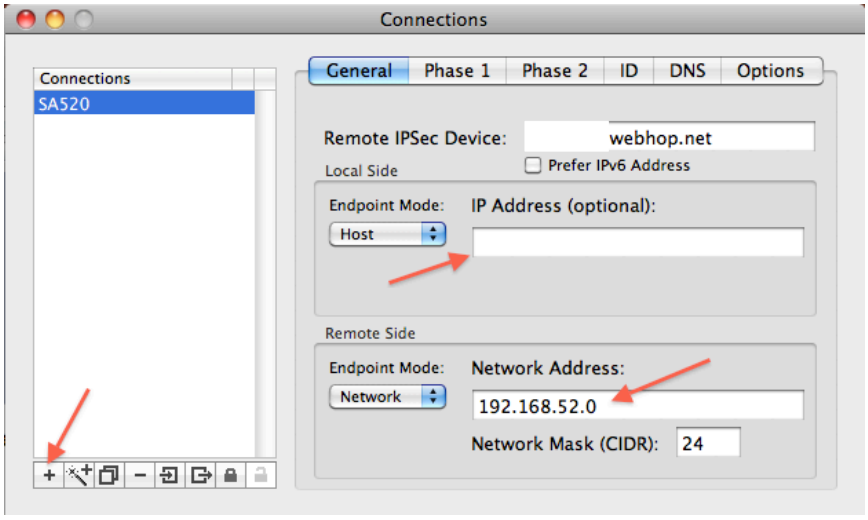
11. Now navigate to “VPN Policy” and adjust local IP information as needed, but make sure to leave “Remote IP” set to “Any”



If changes were made, click Apply and head over to the Mac

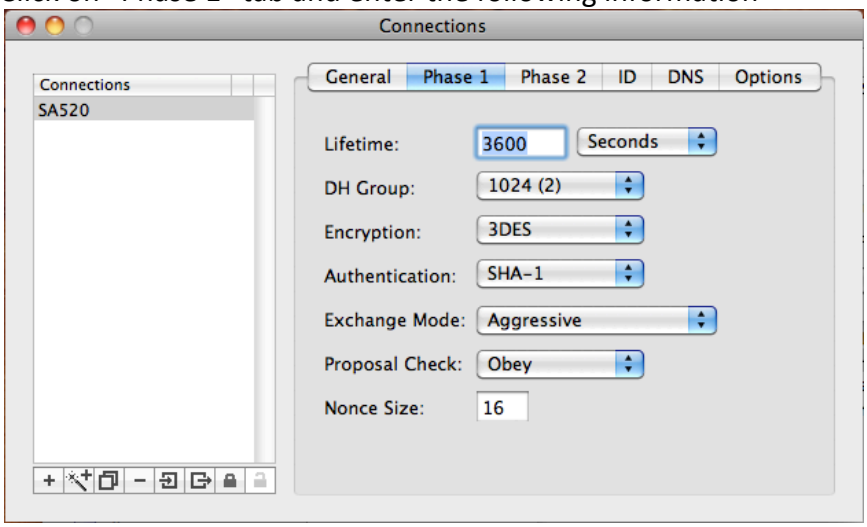
NOTE:
Make sure you have read and understood the “Read Me” file included with the IPSecuritas download and your software is installed.

1. Open IPSecuritas application
2. Press “Command + e” to edit your connections. In our case to create a new connection
3. With the edit window open, click on the plus and give your connection a name



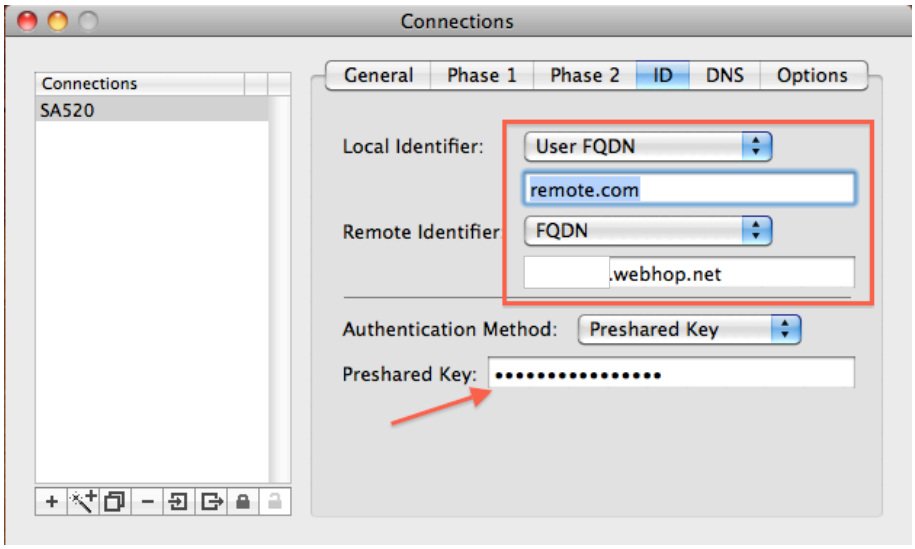
Enter the IP address or FQDN of your site (this does not have to match what we specified earlier on the SA’s local WAN) and the network you are trying to access.

4. Click on “Phase 1” tab and enter the following information



*Because in my tunnel I chose to use the FQDN of my site, I need to use “Aggressive” for my exchange mode. If you chose IP, leave Exchange Mode as main. The lifetime is specified in seconds on the SA, and default is 3600 for Phase 1 and 28800 for Phase 2.

5. Go to Phase 2, change the Lifetime to 28800, ensure PFS group is 2 (1024) and clean up the Encryption and Authentication selections by limiting to what we are using; 3DES and SHA1 (HMAC-SHA1)
6. Now go to ID tab (pay attention because this where it gets confusing)



The ID is an optional setting that may be used for tunnel authentication. We are using this option to tell the router who we are by proving our authenticity using these identifiers. Even though we chose FQDN, the tunnel will not attempt to resolve these names, because as stated they are used for "ID".
Now enter the Pre-shared key you chose. If you want to configure a remote DNS server or domain continue to step 7. Otherwise you may close this window and start the IPSec tunnel from the IPSecuritas window

7. Under DNS tab just enter the appropriate information for your domain and that is it. This window is self explanatory

If you have problems or you are not able to make the connection work no matter how many times you read this, please feel free to post at https://www.myciscocommunity.com and I will do my best to answer posts.

Enjoy!