VPN Access with IPSec tunnels

6300-CX, 6310-DX, 6330-MX, and 6350-SR

VPN Access with IPSec tunnels

Skill level: ***Expert*** (requires knowledge of IPSec tunnel setup)

Goal

To build an IPSec tunnel through the 63xx device's WAN internet connection, and use that IPSec tunnel to access endpoints inside a VPN.

Setup

For this setup, the 63xx series device will need an active WAN internet connection (cellular for the 6300-series, cellular or Ethernet for the 635x-SR series).

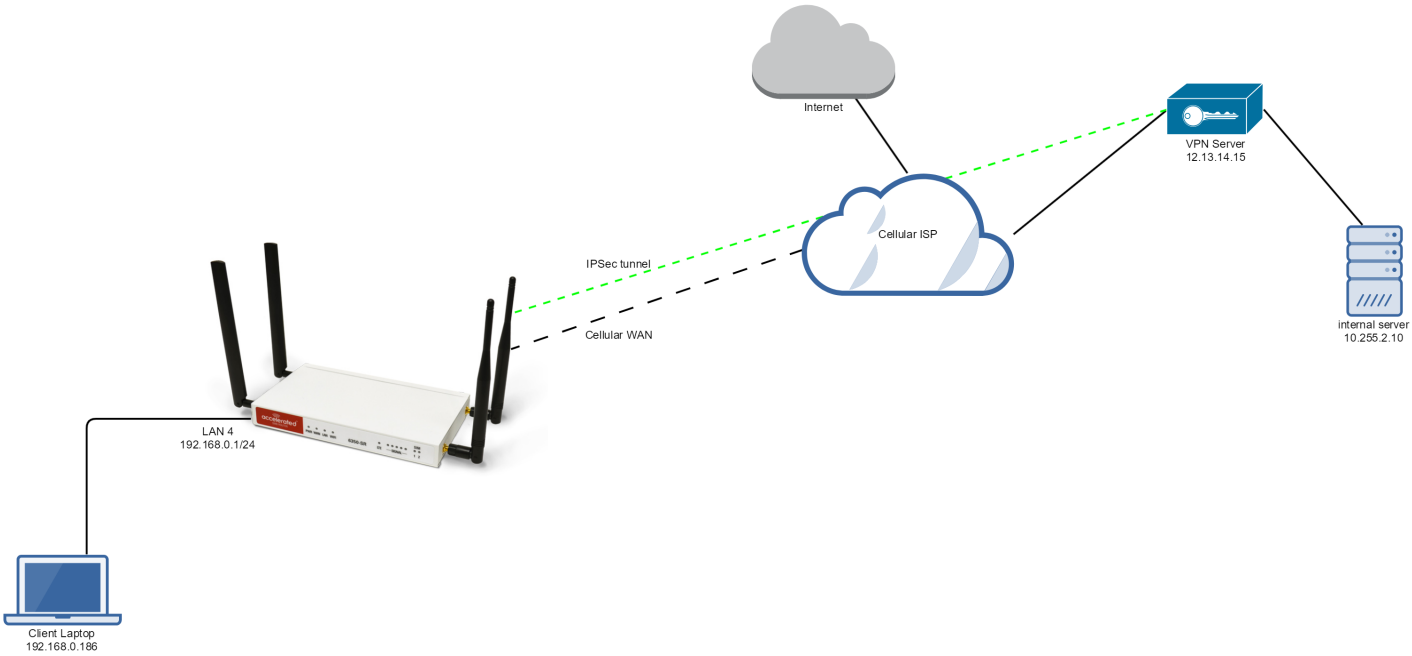
You will also need to know the IPSec credentials and settings needed to build a tunnel to the IPSec endpoint.

NOTE: the 63xx series of devices support building IPSec tunnels to the following endpoints:

- SonicWall routers
- strongswan IPSec servers
- OpenVPN IPSec servers
- other 63xx series devices. See the site-to-site tunnel article for an example.

Sample

The sample configuration below shows a 6350-SR building a tunnel to a VPN server at 12.13.14.15 through it's cellular modem. The client laptop connected to the LAN Ethernet port of the 6350-SR can then use that IPSec tunnel to access any IP address in the 10.255.0.0/16 range behind the IPSec server. Any traffic not destined for 10.255.0.0/16 will instead go through the cellular modem straight to the Internet.



Sample Configuration

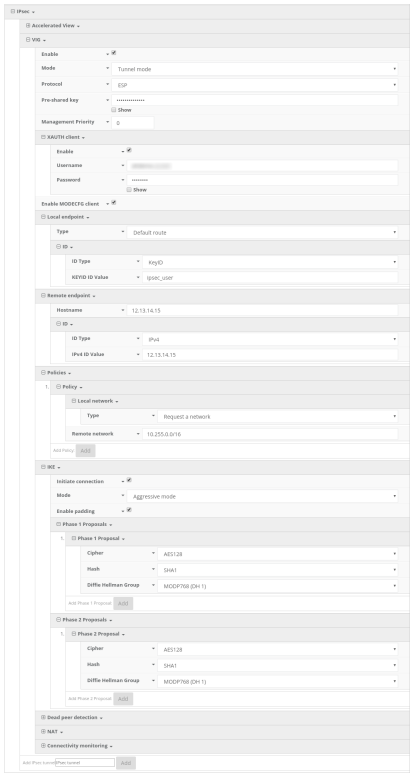
Open the configuration profile for the 6350-SR. Under ***IPSec***, create a new entry titled ***Tunnel***, and add your IPSec settings to the new entry. The following settings reflect the sample setup in the diagram above.

1. Enter in the PSK into the ***Pre-shared key***.
2. (o*ptional*) In ***XAUTH client***, check the ***Enable*** box and enter in the account, username, and password.
3. Check the ***Enable MODECFG client*** box.
4. Change ***Local endpoint -> ID -> ID type*** to ***KeyID***
5. Set the local ID in ***Local endpoint -> ID -> KEYID ID Value***
6. *(optional)* Set ***Local endpoint -> type*** to ***Interface***,and set ***Local endpoint -> Interface*** to ***Modem.*** This configures the 63xx-series device to only build the tunnel through the cellular modem WAN interface. Leaving ***Local endpoint -> type*** to ***Interface*** as ***Default route*** will allow the tunnel to be built through any available WAN interface.
7. Change ***Remote endpoint -> ID -> ID type*** to ***IPv4***
8. Set the IP address of the IPSec server in ***Remote endpoint -> Hostname*** and ***Remote endpoint -> ID -> IPv4 ID Value***. In the example, this is 12.13.14.15
9. Set ***IKE -> Mode*** to ***Aggressive mode***.
10. Set ***IKE -> Phase 1 Proposals*** and ***IKE -> Phase 2 Proposals*** to match the IKE settings required by the IPSec server. In this example, both proposals are set to AES128, SHA1, MOD768.

Under ***Policies***, click ***Add*** to create a new policy, and enter the following settings:

1. Set ***Policy -> Local network -> Type*** to ***Request a network.***
2. Set ***Policy -> Remote network*** to the IPv4 network you wish to access through the tunnel. In the sample, this is 10.255.0.0/16

   (alternative) If you would instead like to have all outbound traffic go through this tunnel, set ***Policy -> Remote network*** to ***0.0.0.0/0***


IPsec
Accelerated View
VTI
Enable
Mode
Tunnel mode
Protocol
ESP
Pre-shared key
Show
Management Priority
0
XAUTH client
Enable
Username
Password
Show
Enable MODECFG client
Local endpoint
Type
Default route
ID
ID Type
KeyID
KEYID ID Value
ipsec_user
Remote endpoint
Hostname
12.13.14.15
ID
ID Type
IPv4
IPv4 ID Value
12.13.14.15
Policies
1
Policy
Local network
Type
Request a network
Remote network
10.255.0.0/16
Add Policy
Add
IKE
Initiate connection
Mode
Aggressive mode
Enable padding
Phase 1 Proposals
1
Phase 1 Proposal
Cipher
AES128
Hash
SHA1
Diffie Hellman Group
MODP768 (DH 1)
Add Phase 1 Proposal
Add
Phase 2 Proposals
1
Phase 2 Proposal
Cipher
AES128
Hash
SHA1
Diffie Hellman Group
MODP768 (DH 1)
Add Phase 2 Proposal
Add
Dead peer detection
NAT
Connectivity monitoring
Add IPsec tunnel
IPsec tunnel
Add