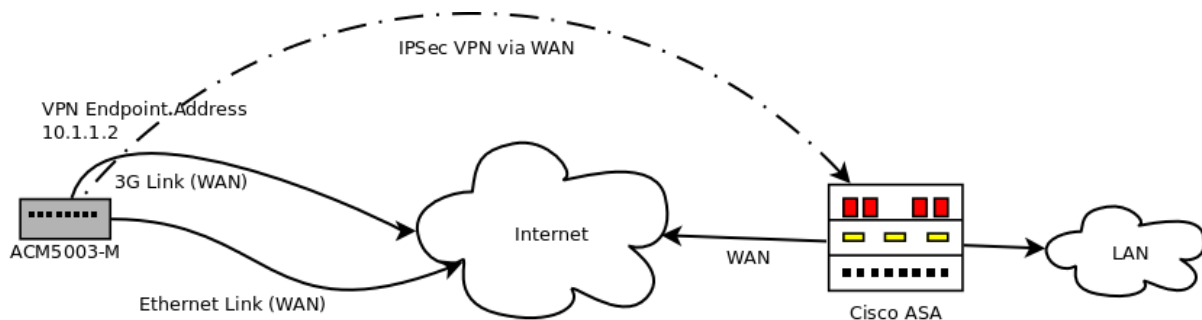


Application Note

Opengear 3G IPSec connection to Cisco ASA Appliance

The Opengear ACM 5003-G has a built-in 3G cellular modem, which can be used as a primary or secondary link to the Internet. Many low-end 3G cellular plans do not provide publicly accessible IP addresses so the ACM is not IP accessible from remote sites over the Internet. One way to allow such connectivity is using a VPN. The ACM supports IPSec VPNs which can be used to provide a secure connection back to the ACM over whichever link is currently in use.

The following diagram illustrates a typical setup for this solution:



The ACM can connect to the Internet via its Ethernet link or a 3G link. Once connected it then brings up an IPSec tunnel to the Cisco ASA Appliance. The ASA is configured so that any requests for 10.1.1.2 are forwarded over the tunnel to the ACM. This means that the ACM has a consistent address regardless of whether it uses Ethernet or 3G to connect.

Opengear Configuration

Step 1

Configure the cellular modem, and make sure it can connect
Setup failover from the Network interface to the cellular modem

Step 2

Create a script *ipsecupdown* in */etc/config/scripts* (you may need to create this directory)

Add the following to the file

```
#!/bin/bash
/sbin/ifconfig ipsec0:0 10.1.1.2 netmask 255.255.255.255 up
```

Note: 10.1.1.2 should be changed to what you want your VPN Endpoint IP to be

Then, type `chmod +x /etc/config/scripts/ipsecupdown` to make it executable.

Step 3

Configure the IPSec tunnel:

- set the right address as the WAN address of the Cisco ASA
- set the right subnet as the LAN network of the Cisco ASA
- set the leftid to a unique name for the ACM (for example *@acmbrisbane*) and
- set the left subnet to the VPN Endpoint IP (i.e. 10.1.1.2/32)

Step 4

Add the following to `/etc/config/ipsec.config.conf`

```
aggrmode=yes
ike=3des-sha-modp1024
leftupdown="/etc/config/scripts/ipsecupdown"
```

Type `ipsec setup --restart`

Verify that you can *ping* through the tunnel to the VPN Endpoint IP from the LAN of the Cisco ASA

Step 5

We now need to protect our changes to the IPsec configuration to make sure that if the IPsec configurator gets run, we don't lose our configs:

Once you have a working tunnel, copy `ipsec.config.conf` to `/etc/config/ipsec.config.conf.backup`

Create a file `/etc/config/scripts/config-post-ipsec`

Add the following to the script

```
#!/bin/bash
cp /etc/config/ipsec.config.conf.backup /etc/config/ipsec/config.conf
ipsec setup --restart
```

Now, after this, try forcing the device to failover to 3G. Once the 3G link comes up you should still be able to access the device via the VPN Endpoint IP.

Cisco ASA Configuration

The following is the relevant parts of a `config` dump of a Cisco ASA configured to allow the ACM to connect in via a dynamic address, and to route any traffic destined for the VPN Endpoint IP from the LAN of the Cisco ASA over the tunnel

The configuration assumes the following

- The LAN network of the Cisco ASA is 192.168.1.0/24
- The preshared key for the tunnel is 123456789
- The VPN Endpoint IP for the ACM is 10.1.1.2

```
access-list 122 extended permit ip 192.168.1.0 255.255.255.0 10.1.1.2
255.255.255.255
crypto ipsec transform-set fwConfigTset esp-3des esp-sha-hmac crypto dynamic-map
fwConfigDynMap 222 match address 122
crypto dynamic-map fwConfigDynMap 222 set pfs crypto dynamic-map fwConfigDynMap
222 set transform-set fwConfigTset
crypto map fwConfigMapToDyn 223 ipsec-isakmp dynamic fwConfigDynMap
crypto map fwConfigMapToDyn interface outside
crypto isakmp enable outside
crypto isakmp policy 222
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

tunnel-group acmbrisbane type ipsec-l2l
tunnel-group acmbrisbane ipsec-attributes
pre-shared-key 123456789
```