

IPsec VPN Guide

Opengear to Cisco ASA Appliance

This is a guide on how to create an IPsec VPN tunnel from an Opengear 3G device to a Cisco ASA.

In this document:

1. Network Configuration
2. Configuring the Opengear Side
3. Configuring the Cisco ASA Side
4. Example Using Dynamic DNS
5. Notes on Opengear IPsec VPN Configuration

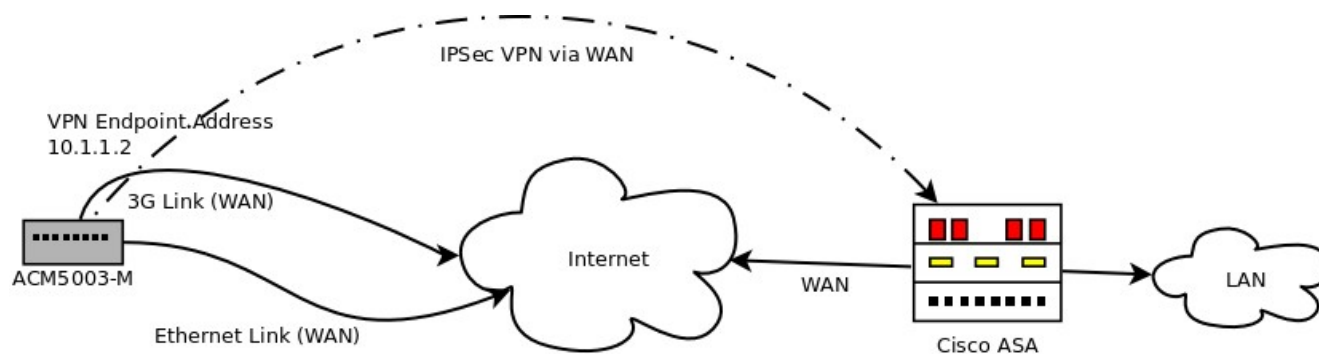
Background on how IPsec works:

<http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=6>

1. Network Configuration

The Opegear ACM5003-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.

1. Configure the cellular modem on the Opegear and make sure it can connect .
2. Setup failover from the Network interface to the cellular modem .

2. Configuring the Opengear Side

1. Go to the Web UI, from the navigation menu under **Serial & Network** select **IPsec VPN**, click **Add**
2. Enter the details as listed in the table, there is a screenshot on the following page

In this example:

- The authentication method is Pre Shared Key (PSK)
- The Opengear device is an ACM5002-3G with private network address 10.1.1.2
- The Cisco ASA is on the private subnet 192.168.1.0

Field	Opengear Device
Tunnel Name	opengear_to_cisco
Initiate Tunnel	Yes
Authentication Method	PSK
Shared Secret (PSK)	default
Authentication Protocol	ESP
Aggressive Mode	Yes
IKE Proposal	3des-sha-modp1024
Left ID	@opengear
Right ID	@cisco_asa
Left Address	<i>leave blank</i>
Right Address	<i>WAN address of the Cisco ASA</i>
Left Subnet	10.1.1.2/32
Right Subnet	192.168.1.0/24

Replace Left Subnet with the private network address of the Opengear device.

Replace Right Subnet with the private network address of the Cisco ASA.

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

Screenshot of Opengear settings:

Add IPsec Tunnel	
Tunnel Name	<input type="text" value="opengear_to_cisco"/> A descriptive name for the IPsec tunnel
Initiate Tunnel	<input checked="" type="checkbox"/> Initiate the tunnel connection from this end
Security	
Authentication Method	<input type="radio"/> RSA digital signatures <input checked="" type="radio"/> Shared secret (PSK) Authenticate using RSA digital signatures or a shared secret (PSK)
Shared Secret (PSK)	<input type="text" value="default"/> A passphrase, must match the passphrase configured at the other end of the tunnel
Authentication Protocol	<input checked="" type="radio"/> ESP <input type="radio"/> AH Authenticate as part of ESP encryption or separately using the AH protocol
Aggressive Mode	<input checked="" type="checkbox"/> Use IKE aggressive mode to establish the tunnel, leave unchecked to use IKE main mode
IKE Proposal (Phase 1)	<input type="text" value="3des-sha-modp1024"/> Algorithm to establish the tunnel, must be specified when using aggressive mode, in the format <i>crypt</i>
Perfect Forward Secrecy	<input checked="" type="checkbox"/> Require perfect forward secrecy of keys
Left ID	<input type="text" value="@opengear"/> The identifier for this end of the tunnel, should include a fully qualified domain name preceded by @
Right ID	<input type="text" value="@cisco"/> The identifier for the other end of the tunnel, should include a fully qualified domain name preceded by @
Left Address	<input type="text"/> The public IP or DNS address of this end of the tunnel, leave blank to use the interface of the default gateway
Right Address	<input type="text" value="WAN address of the Cisco ASA"/> The public IP or DNS address of the other end of the tunnel, leave blank if it is dynamic
Networking	
Left Subnet	<input type="text" value="10.1.1.2/32"/> The private subnet or comma-separated list of subnets behind this end of the tunnel in CIDR notation
Right Subnet	<input type="text" value="192.168.1.0/24"/> The private subnet or comma-separated list of subnets behind the other end of the tunnel in CIDR notation

3. Configuring the Cisco ASA Side

Cisco introduction to IPsec:

http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094203.shtml

This configuration uses a dynamic mapping (needed for dynamic endpoints).

The usual use case is to provide an alias on eth0 of the Opengear to provide an unchanging private address to access the device on. Under System → IP add an alias for the interface that will be used to create the VPN tunnel eg the Network Interface:

IP Settings: Network	
Configuration Method	<input type="radio"/> DHCP <input type="radio"/> Static The mechanism to acquire IP settings.
IP Address	<input type="text"/> A statically assigned IP address.
Subnet Mask	<input type="text"/> A statically assigned network mask.
Gateway	<input type="text"/> A statically assigned gateway.
Primary DNS	<input type="text"/> A statically assigned primary name server.
Secondary DNS	<input type="text"/> A statically assigned secondary name server.
Media	<input type="button" value="Auto"/> ▾ The Ethernet media type.
DHCP Server	Disabled Configure a DHCP server for this interface.
IP Alias	<input type="text" value="10.1.1.2"/> Secondary address or comma-separated list of addresses i

- The dynamic-map settings act as a template, matching incoming connections that come in.
- This requires aggressive mode on the client.

ASA 8.4

```
crypto ipsec ikev1 transform-set fwConfigTset esp-3des esp-sha-hmac
crypto dynamic-map fwConfigDynMap 222 set pfs
crypto dynamic-map fwConfigDynMap 222 set ikev1 transform-set fwConfigTset
crypto map fwConfigMapToDyn 223 ipsec-isakmp dynamic fwConfigDynMap
crypto map fwConfigMapToDyn interface internet
crypto ikev1 enable internet
crypto ikev1 policy 222
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400

tunnel-group acmbrisbane type ipsec-l2l
tunnel-group acmbrisbane ipsec-attributes
  ikev1 pre-shared-key *****
tunnel-group acmtoowong type ipsec-l2l
tunnel-group acmtoowong ipsec-attributes
  ikev1 pre-shared-key *****
```

On the Cisco, you need to be careful about NAT (8.2 on does auto NAT which won't show up in config). Use show nat to see if its NATting stuff.

IOS 12.4

```
crypto isakmp policy 10
  encryption 3des
  hash sha
  authentication pre-share
  group 2
  lifetime 86400

crypto isakmp key default hostname acm-kensdesk

crypto ipsec transform-set acm-transforms esp-3des esp-sha-hmac
crypto dynamic-map acm-dyn-map 101
  set transform-set acm-transforms
  set pfs group2
crypto map acm-stat-map 101 ipsec-isakmp dynamic acm-dyn-map

interface FastEthernet 0
  crypto map acm-stat-map
```

Once the tunnel is working make sure you change the PSK passphrase at both ends to something secret (currently set to *default*).

“IPsec SA established tunnel mode” should be visible in the Syslog on the Opengear:

```
<84>Apr  5 23:01:56 pluto[7357]: "opengear_to_cisco"[1] 150.101.188.49 #2:  
STATE_QUICK_R2: IPsec SA established tunnel mode {ESP=>0x06c91a10  
<0x9c53c62c xfrm=AES_256-HMAC_MD5 NATOA=none NATD=none DPD=none}
```

4. Debugging

Debugging on Cisco

- debug icmp trace
 - Shows any NATting occurring when pinging to the otherside of the tunnel
- debug crypto isakmp 10
 - Shows the IPsec packets - the different stages, and actually gives you error messages that mean something (like the openswan kernel info)
- show crypto ipsec sa
 - Shows the current security associations
- show nat
 - Shows any natting that is occurring - first try pinging the remote site with debug icmp trace turned on to see if natting is occurring - show nat will show you what is configured. If the cisco needs to provide nat then there needs to be an exemption for the vpn traffic.

Debugging on Opendgear

- ipsec setup --restart / --stop
 - Stops or restarts the vpn connections
- ipsec auto --status
 - Shows you the current status of the tunnel, and shows what openswan thinks the routed networks are

5. Notes on Opengear IPsec VPN Configuration

- Only on: ACM500x, IM42xx, IMG4xxx and KCS
- Establishes a VPN connection between console servers at remote sites and a VPN gateway (e.g.: CISCO router) on central office network. Remote console server can be accessed with CMS6000 on central network.
- Uses Openswan to configure a VPN allowing multiple access to console servers
- In **Authentication Protocol** select the authentication protocol to be used. Either authenticate as part of *ESP* (Encapsulating Security Payload) encryption or separately using the *AH* (Authentication Header) protocol.
- Enter a **Left ID** and **Right ID**. This is the identifier that the Local host/gateway and remote host/gateway use for IPsec negotiation and authentication. Each ID must include an '@' and can include a fully qualified domain name preceded by '@' (e.g. *left@example.com*)
- Enter the public IP or DNS address of this Opengear VPN gateway (or if not an ACM5004G enter the address of the gateway device connecting it to the Internet) as the **Left Address**. You can leave this blank to use the interface of the default route
- In **Right Address** enter the public IP or DNS address of the remote end of the tunnel (only if the remote end has a static or dyndns address). Otherwise leave this blank
- If the Opengear VPN gateway is serving as a VPN gateway to a local subnet (e.g. the *console server* has a Management LAN configured) enter the private subnet details in **Left Subnet**.
- Use the CIDR notation (where the IP address number is followed by a slash and the number of 'one' bits in the binary notation of the netmask). For example 192.168.0.0/24 indicates an IP address where the first 24 bits are used as the network address. This is the same as 255.255.255.0. If the VPN access is only to the console server itself and to its attached serial console devices then leave **Left Subnet** blank
- If there is a VPN gateway at the remote end, enter the private subnet details in **Right Subnet**. Again use the CIDR notation and leave blank if there is only a remote host
- Select **Initiate Tunnel** if the tunnel connection is to be initiated from the Left console server end. This can only be initiated from the VPN gateway (Left) if the remote end was configured with a static (or dyndns) IP address