Opengear to Cisco IPSec Guide

Opengear to Cisco ASA Appliance/ Cisco 1700 series router

This is a guide on how to create an IPsec VPN tunnel from an Opengear device to a Cisco ASA appliance and 1700 series router.

In this document:

Background on how IPsec works:

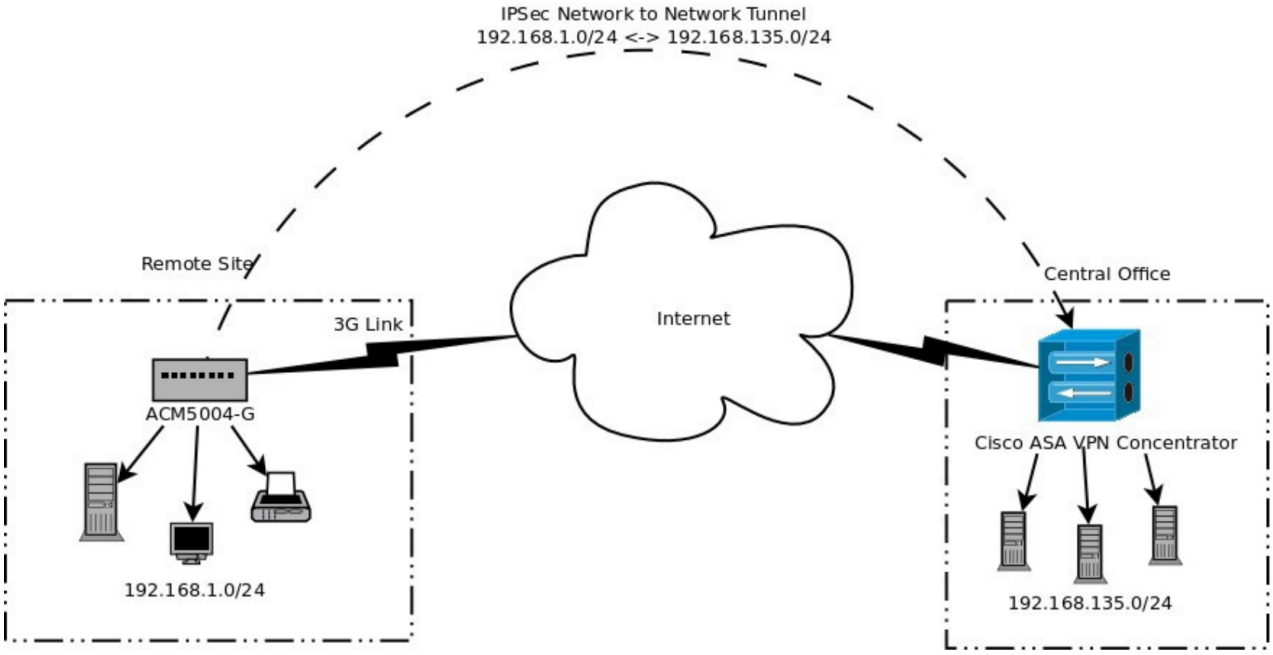
http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=6

1. Network Configuration

Some Opengear console servers come equipped with a built-in cellular modem, which can be used as the console server's primary or secondary link to the Internet.

Many low-end cellular plans do not provide publicly accessible IP addresses so the console server is not IP accessible from other sites over the Internet. One way to allow such connectivity is to use a VPN. The Opengear ACM and IM products support IPSec VPNs. Regardless of how the Opengear console server connects to the internet, an IPSec VPN can provide a way to maintain a secure connection to the remote console server and, if it exists, the private network it resides in.

The following diagram illustrates a typical setup for this solution (showing an Opengear ACM5004-G as an example):



The ACM5004-G at the remote site has its Ethernet address set to be on the 192.168.1.0/24 subnet. It can either act as a gateway for that network, or simply be a member of the network. It is configured to initiate the IPSec connection.
Please note that if the ACM is not the gateway, you must add a route to the router responsible for the network to forward traffic for the central office (192.168.135.0/24) via

the ACM.

The Central Office Cisco is configured to accept dynamic connections from the ACM (and possibly other branch offices).

2. Cisco Configuration

2.1 Cisco ASA Configuration

The following configuration excerpts give the required configuration settings for the Cisco ASA to accept IPSec connections from the Opengear.

```
access-list allow_vpn extended permit ip 192.168.135.0 255.255.255.0 192.168.1.0
255.255.255.0
access-list allow_vpn extended permit ip 192.168.1.0 255.255.255.0 192.168.135.0
255.255.255.0

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 dynamic-map fwConfigDynMap 222 set reverse-route
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 28800

tunnel-group opengearremotesite type ipsec-l2l
tunnel-group opengearremotesite ipsec-attributes
  ikev1 pre-shared-key *****
  isakmp keepalive threshold 300 retry 2
```

The configuration contains a number of statements:

- The *access-list* statements permit traffic between the central office network and the remote site. ***NOTE:*** you need to change these to suit ***your*** remote and local subnets.
- The *crypto ipsec ikev1 transform-set* statement defines the cryptographic transforms that the

IPSec connection will use. In this case, 3DES encryption has been chosen with SHA as the hashing algorithm

- The *crypto dynamic-map* statements:
  - enable Perfect Forward Security
  - set the transform-set to be the one defined in the previous statements
  - enable Reverse-route injection which configures the Cisco device to add the network provided by the Opengear into its route table when the Opengear connects.
- The *crypto map* statements:
  - enable the use of the dynamic-map defined previously
  - enable the use of they dynamic-map on the *internet* interface of the Cisco device. ***NOTE:*** "*internet*" is the name of the interface on the Cisco device and needs to be changed to suit the configuration of the Cisco device.
- The *crypto ikev1 enable* statement enables IPSec on the *internet* interface.
- The *crypto ikev1 policy* statements:
  - set the authentication method to Pre-Shared-Key
  - set the authentication algorithm to 3DES
  - set the hash algorithm to SHA
  - set the Dffie Hellman group to 2 (MODP1024)
  - sets the IKE lifetime to 8 hours (28800 seconds)
- The *tunnel-group* statements set the attributes for each individual connection. The name of the *tunnel-group* (in this example, *opengearremotesite*) corresponds to the left-id of the Opengear device. Also:
  - sets the pre-shared-key. Replace the ***** with your chosen pre-shared-key (this key is to be the same as that to be entered into the Opengear device)

2.2 Cisco 1700 Configuration

The following configuration excerpts give the required configuration settings for a Cisco 1721 to accept IPSec connections from the Opengear.

```
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
  lifetime 28800

crypto isakmp key ***** hostname opengearremotesite
crypto isakmp keepalive 300 3

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
  reverse-route

crypto map acm-stat-map 101 ipsec-isakmp dynamic acm-dyn-map

interface FastEthernet0
crypto map acm-stat-map

ip access-list extended remote-site-vpn
  permit ip 192.168.135.0 0.0.0.255 192.168.1.0 0.0.0.255
  permit ip 192.168.1.0 0.0.0.255 192.168.135.0 0.0.0.255
```

This is similar to the ASA but note the different syntax required. Also note that there are no tunnel groups and settings that affect tunnels are global.

Make sure to change the subnets in the *ip access-list* to suit your remote and local subnets. Also replace '*****' with your preshared key.

3. Configuring the Opengear Side

For these examples, the Opengear must be able to route to the Cisco device. It doesn't matter if the tunnel connection to the Cisco device is made via the Opengear's network interface or via an always-up cell modem connection. However, on the Opengear, forwarding needs to be setup between the VPN interface and the interface which is on the **Left Subnet** (the Left Subnet from the Opengear's perspective is the Opengear remote site's private network – 192.168.1.0/24 in the examples used so far).

Configuration and Forwarding Examples:

- **Scenario 1**. The Opengear is connecting to the Cisco device via an always-up cell modem connection. The Network interface of the Opengear is on the left subnet. Forwarding needs to be enabled between the VPN interface and the Network interface.

- **Scenario 2**. The Opengear is connecting to the Cisco device via the Network interface. The Management LAN interface of the Opengear is on the left subnet. Forwarding needs to be enabled between the VPN interface and the Management LAN interface.

Also note that other devices on the left subnet need to add the tunneling Opengear device as the route to the right subnet located at the Cisco end of the tunnel. This would already be the case if the Opengear device is the left subnet's default gateway.

To configure the Opengear device:

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. Note that custom options need to be added.

In this example:

- The Cisco ASA or 1700 is on a private subnet 192.168.135.0/24
- The Opengear is on a private subnet 192.168.1.0/24 and has an address of 192.168.1.50 on that subnet.

Field	Opengear Device
Tunnel Name	opengear_to_cisco (rename this to suit your configuration)
Initiate Tunnel	yes (checked)
Authentication Method	Shared Secret (PSK)
Shared Secret (PSK)	*Enter your pre-shared-secret – this should be the same as what you set in the tunnel-group configuration on the Cisco device*
Authentication Protocol	ESP
Aggressive Mode	yes (checked)
IKE Proposal	3des-sha-modp1024
Perfect Forward Security	Yes
Left ID	@opengearremotesite
Right ID	*leave blank*
Left Address	*leave blank*
Right Address	*WAN address of the Cisco device*
Left Subnet	192.168.1.0/24
Right Subnet	192.168.135.0/24
Custom Options	
leftsourceip	192.168.1.50 *(Adjust this to the be address the Opengear device has on the left subnet)*
ikelifetime	8h
salifetime	1h
forceencaps	yes
dpddelay	60
dpdtimeout	120
dpdaction	restart

Replace *Left Subnet* with the private network address of the Opengear device.
Replace *Right Subnet* with the private network address of the Cisco device.
Make sure you click “Apply” once you have entered all the required details.

Custom options are used to aid debugging and inter-operability with the Cisco device.

- The *leftsourceip=x.x.x.x* option sets the source IP for traffic originating on the Opengear which will traverse the tunnel. This allows tunnel testing using the *ping* comand locally on the Opengear.
- The *ikelifetime=8h* option sets the lifetime for the Phase 1 Security Associations (ISAKMP SA) to 8 hours. This corresponds to the *lifetime 28800* entries on the Cisco configurations.
- The *salifetime=1h* option sets the lifetime for Phase 2 Security Associations (IPSec SA) to 1 hour. This corresponds to the Cisco default of 3600 seconds.
- The *forceencaps=yes* option instructs the IPSec implementation on the Opengear to UDP encapsulate the IPSec traffic. This works around an interoperability problem between Openswan (the IPSec implementation used by the Opengear) and the Cisco devices. This also helps with firewall traversal issues.
- The *dpddelay=60* option is part of the Dead Peer Detection (DPD) functionality. It sets the delay (in seconds) between DPD keepalives that are sent to the remote end.
- The *dpdtimeout=120* option is also part of the DPD functionality. It sets the length of time (in seconds) the connection can be idle without hearing either a keepalive poll from the remote end or an acknowledgement from the remote end to a keepalive sent from this end. After this period has elapsed with no response and no traffic the peer is declared dead.
- The *dpdaction=restart* option determines the action to be performed when the DPD enabled peer is declared dead, the restart option means the the SA will immediately be renegotiated.

Screenshot of Opengear settings:

4. Checking if the Tunnel is Up

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

```
<84>Jun  5 20:50:15 pluto[9997]: "opengear_to_cisco/1x1" #2: STATE_QUICK_I2: sent QI2, IPsec SA established tunnel mode {ESP/NAT=>0x36f27b4f <0x2bc2cd9c xfrm=3DES_0-HMAC_SHA1 NATOA=none NATD=x.x.x.x:4500 DPD=enabled}
```

NOTE: x.x.x.x will be the WAN address of the Cisco device.

5. Debugging

Debugging on Cisco

- debug icmp trace
  - Shows any NATting occuring 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 occuring - first try pinging the remote site with debug icmp trace turned on to see if natting is occuring - 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 Opengear

- 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