IPSec VPN Guide

Opengear to Check Point **R75.40** Gateway

This is a guide on how to create an IPSec VPN tunnel from an Opengear 3G device to a Check Point **R75.40** Gateway running on 'Gaia' operating system using X.509 certif icates for authentication.

Aim: to provide a secure, reliable, out-of-band console solution for connecting to
branch Cisco devices.

www.opengear.com
www.checkpoint.com

In this document:

Background on how IPSec works:

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

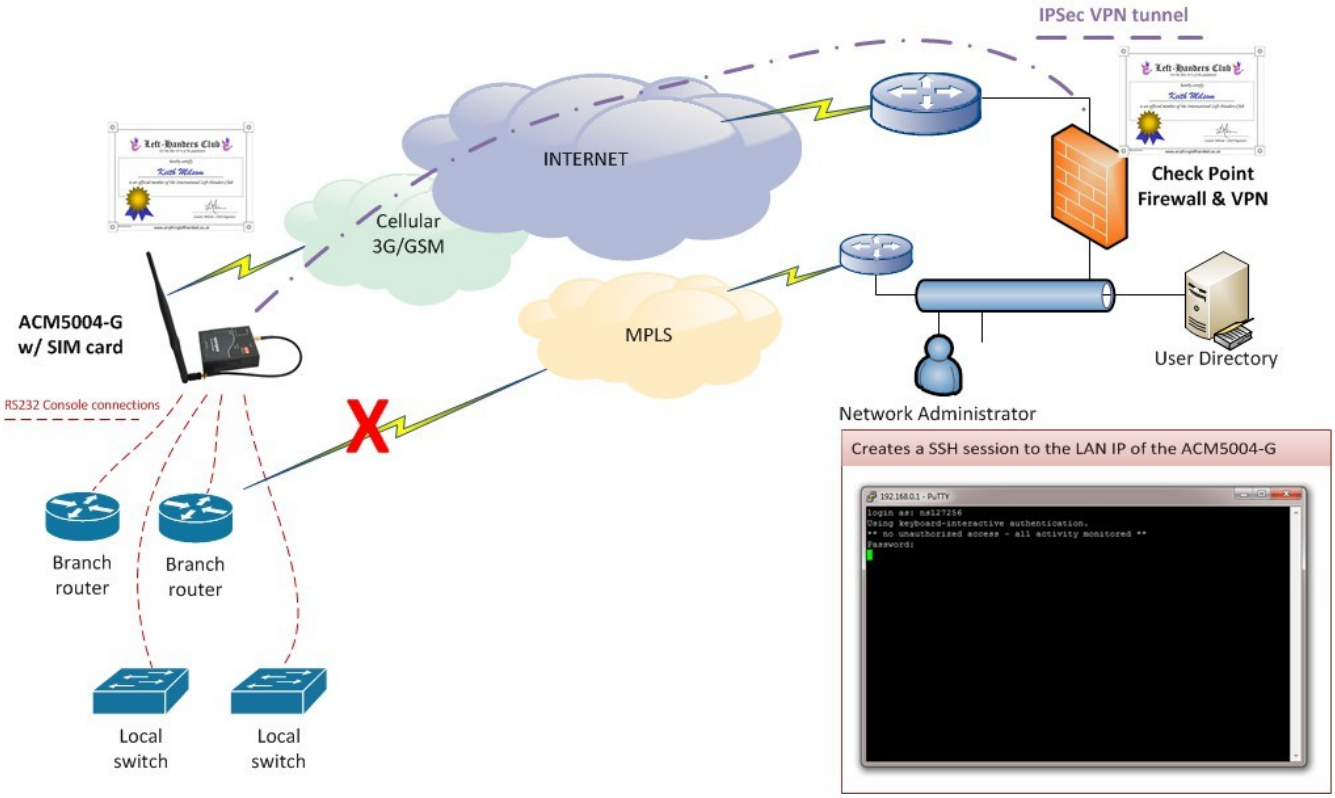
Acknowledgements:

Thanks to **Network Surety** for providing the content for this guide.

1. Network Configuration

The Opengear ACM5004-G has a built-in 3G cellular modem which is used to connect to the Internet. This link may be used to provide out-of-band access to devices at a remote site should their main connection (e.g. MPLS) go down. The ACM supports IPSec VPNs which can be used to provide secure connectivity across the 3G link.

The following diagram illustrates the network connectivity:



• The ACM gets a dynamic (private) IP address from the cellular provider and this is NAT-ed through an arbitrary registered IP address on the Internet .

• The ACM is not patched in to the LAN of the branch office.

• Branch switches and routers requiring console access are connected to the

serial ports of the ACM .

• The IPSec VPN is created using X.509 certificates for mutual authentication and to establish the tunnel .

• Out-of-band access to branch office routers and switches (e.g. in the event of the MPLS being down) is allowed through an SSH connection across the VPN to the LAN of the ACM .

- SSH directly to the required console port (e.g. ssh to port 3002 connects to port 2)
- Authenticate to the ACM using RADIUS (or any other remote authentication method)

Things to note:

• The X.509 certificates are issued by the Check Point CA (ICA):

- ACM certificate
- Gateway certificate
- Root CA certificate for the ICA
- For security purposes the "root" account on the ACM should be configured to use a strong password – to be used in emergencies when remote authentication fails.

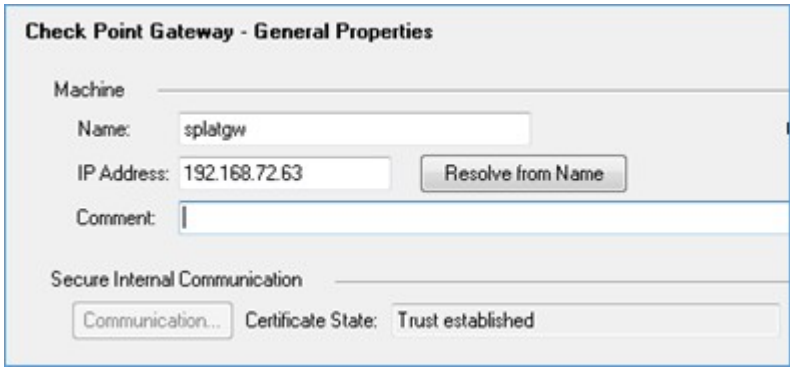
The ACM connects to the Internet via its 3G cellular modem. Once connected it then brings up an IPSec tunnel to the Check Point gateway.

1. Configure the cellular modem on the Opengear and make sure it can connect .
2. Ensure the IP address of the Network Interface of the Opengear is 192.168.0.12.

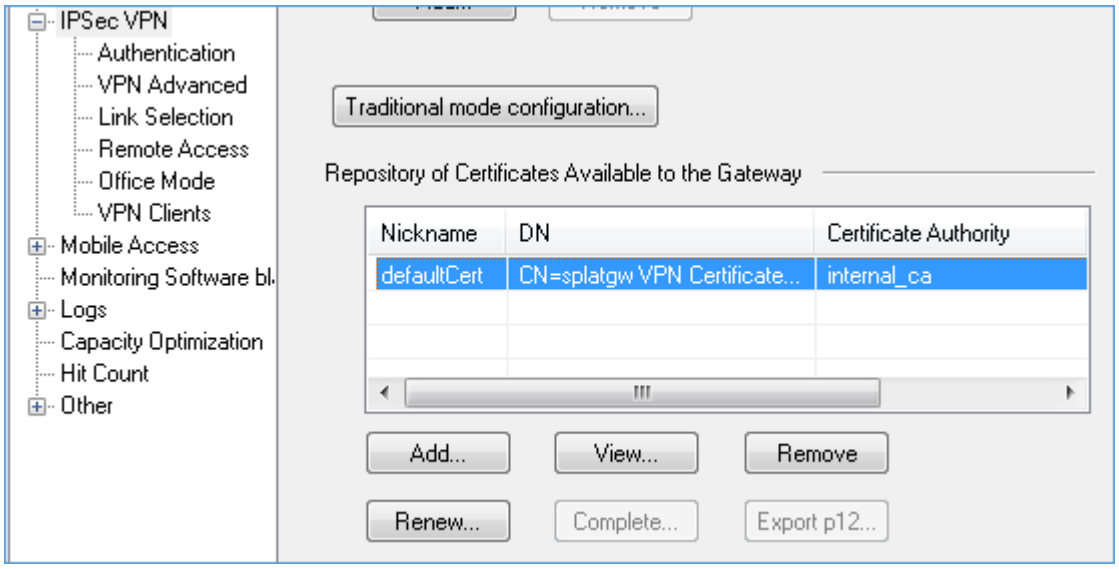
Check Point Certificate Configuration

By default the Check Point may be using an address from an interface that it is not using to connect the VPN. For example the Check Point may be setup to use the Internal Interface address in its certificate details when the External Interface may be preferred. In that case follow this procedure to Gateway Object and IPSec VPN certificate.

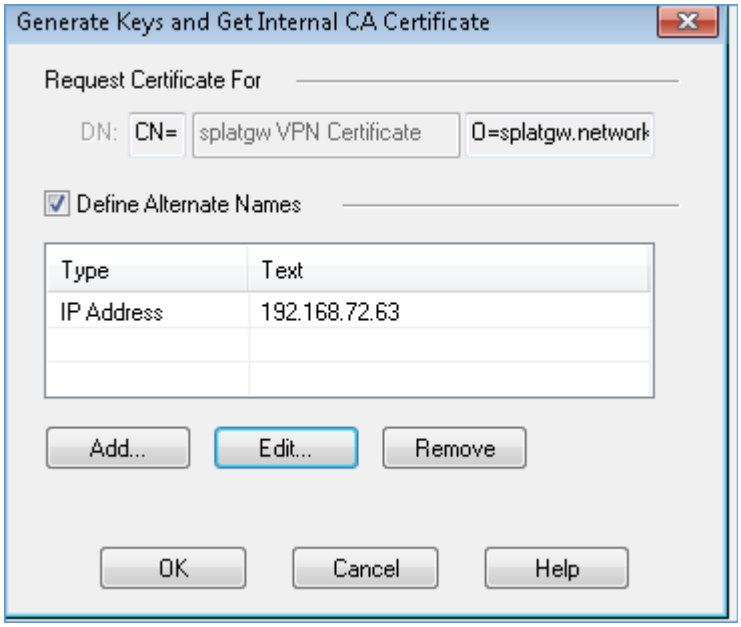
1. Change the IP Field in the Check Point General Properties to the appropriate interfaces IP.



2. Navigate to the IPSec VPN and renew the **defaultCert**.



3. Either Edit the existing IP SAN or add a new IP SAN with the preferred IP Address i.e. External Public IP



4. Save and install the Policy on the Check Point GW

Generating SSL Certificates

1. Create a Certificate Signing Request (CSR) on the ACM via the web UI or via the console
2. Upload the CSR to the ICA Management tool
3. Approve (sign) the CSR
4. Copy the newly issued certif icate and the root CA certif icate to the ACM

Create CSR via console:

```
# cd /var/tmp
# openssl req -out ACM.csr -new -newkey rsa:1024 -nodes -keyout ACM-
private.key
Generating a 1024 bit RSA private key
.......++++++
..............++++++
unable to write 'random state'
writing new private key to 'ACM-private.key'
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:Utah
Locality Name (eg, city) []:Sandy
Organization Name (eg, company) []:Opengear
Organizational Unit Name (eg, section) []:Development
Common Name (eg, YOUR name) []:acm5004-g
Email Address []:support@opengear.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

```
# cat ACM.csr
```

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB1zCCAUACAQAwgZYxCzAJBgNVBAYTAkFVMRMwEQYDVQQIEwpRdWVlbnNsYW5k
MRAwDgYDVQQHEwdUb293b25nMREwDwYDVQQKEwhPcGVuZ2VhcjEUMBIGA1UECxML
RGV2ZWxvcG1lbnQxEjAQBgNVBAMTCWFjbTUwMDQtZzEjMCEGCSqGSIb3DQEJARYU
c3VwcG9ydEBvcGVuZ2Vhci5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
AKl0ip3KfaOesM7e1LFx4lHjkSX89xoi9GUmpK1cfDYi60TtSsx6nKMg8+kVMmxR
B9HhsnGVogLRV2/RMnp/AM0i5nqzfQ3Pv8PfEUu6MDLVZmVHyE1ufGjh9bc98eAh
YaP78qD9/2uLzbMUBkiQyOnv+H30b9P9e8Fiqx2lVyDvAgMBAAGgADANBgkqhkiG
9w0BAQUFAAOBgQAUDr1j26eUSu20ioCKHjNBJWrizeoitBxAA9HFGOccu5bBlkit
r8ICtGSDDFR7VZyoULL9b/iZm6mF4SbD1PUFVECE+/cLKo/Mee73QV2hKciGe9jt
e5MMNBaBMq0svrZKqJcZAtMAjCpJhvTHQ3BAXlqdGmUOzcOrS41bTLVGog==
-----END CERTIFICATE REQUEST-----
```

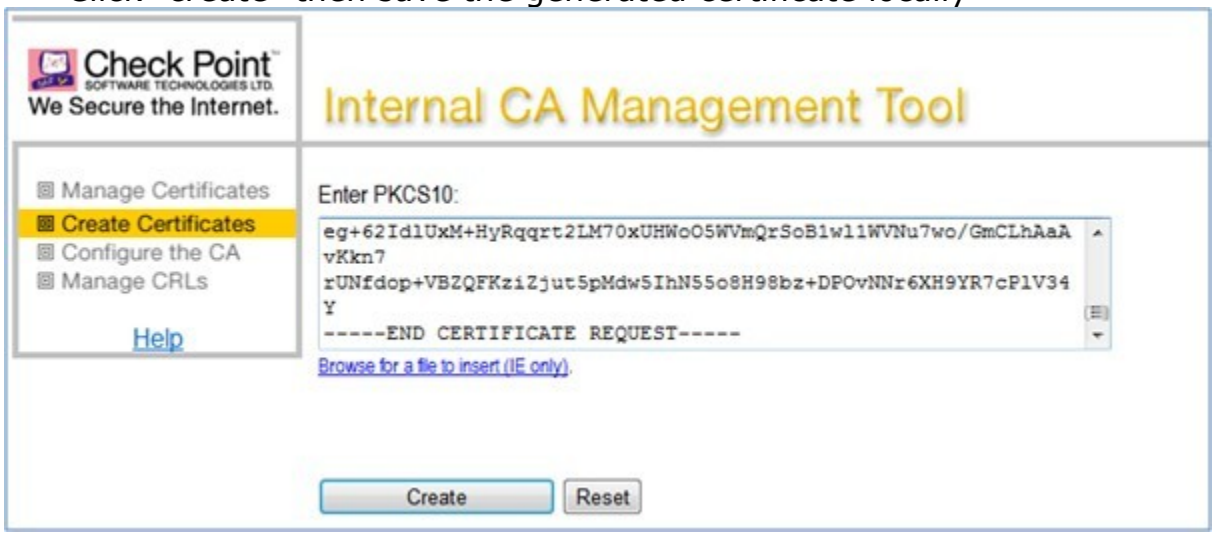
Submit the CSR to the Check Point ICA Management tool in PKCS#10 format:

- The ICA Management tool is disabled by default, to enable it follow the instructions as per the following Check Point Support article: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk39915

- Navigate to the ICA Management tool @ https://<management_server_name_or_IP_address>:18265/

- Upload the CSR from the ACM

- Click "create" then save the generated certificate locally



• SCP the certificate (.cer file in DER format) to /var/tmp on the ACM, then covert it to PEM format using the following OpenSSL command:

```
openssl x509 -inform der -in mgmt96f49329.cer -out ACM-cert.pem
```

• Using the Check Point SmartDashboard export a copy of the ICA root certificate, Navigate to **OPSEC** tab → **Servers** → **Trusted CAs** and select **internal_ca.** Right click on **internal_ca** and select **Edit ..., c**lick on **Local Security Management Server** tab and click **Save As...** Transfer that file to the Opengear **/etc/config/CheckPoint-cert.pem** (No file format change is required)

• Place all three files in /etc/config:

```
ACM-private.key
ACM-cert.pem
CheckPoint-cacert.pem
```

Openswan IPsec does a sweep of the /etc/config/ directory to find valid certificates. During authentication Openswan matches the ICA root CA certif icate to the one used to sign the Check Point Gateway certificate using its distinguished name.

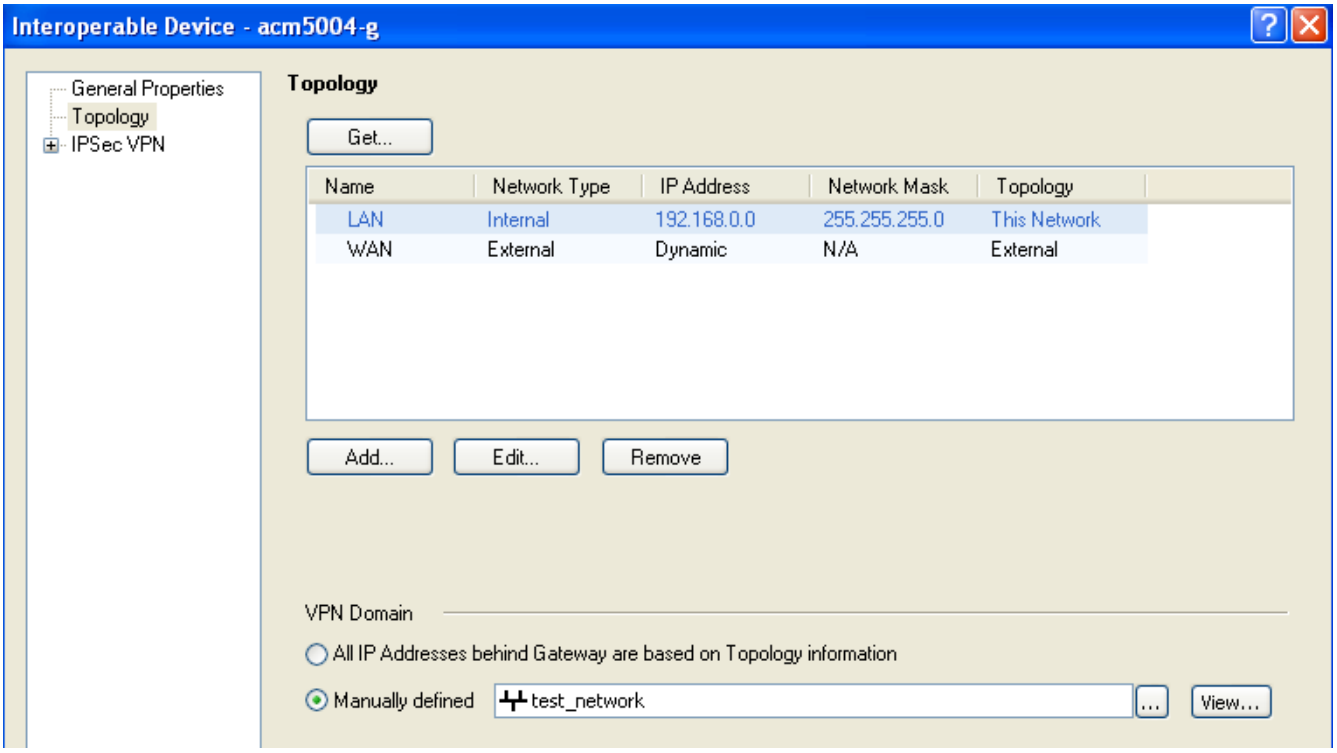
3. Configuring The Check Point Side

Create a new interoperable device from the Smart Dashboard:

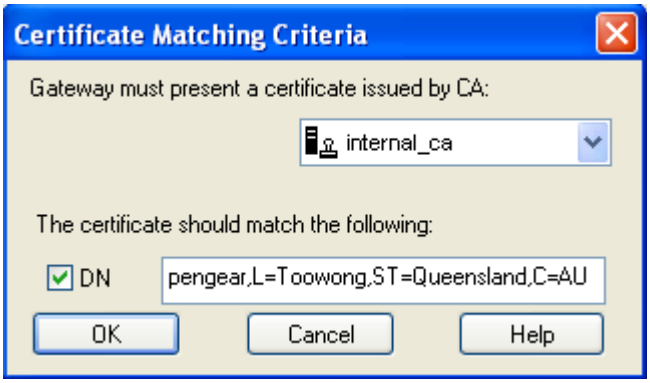
- **Manage → Network Objects → New → Interoperable Device**
- Select **dynamic address**

- Under "Topology" add LAN network information and WAN interface (latter as dynamic IP)

- Assign the Branch LAN network as the "VPN Domain"



- Under “IPSec VPN” define the matching criteria as per the generated certif icate for the ACM



Create a new “star” IPSec VPN Community:

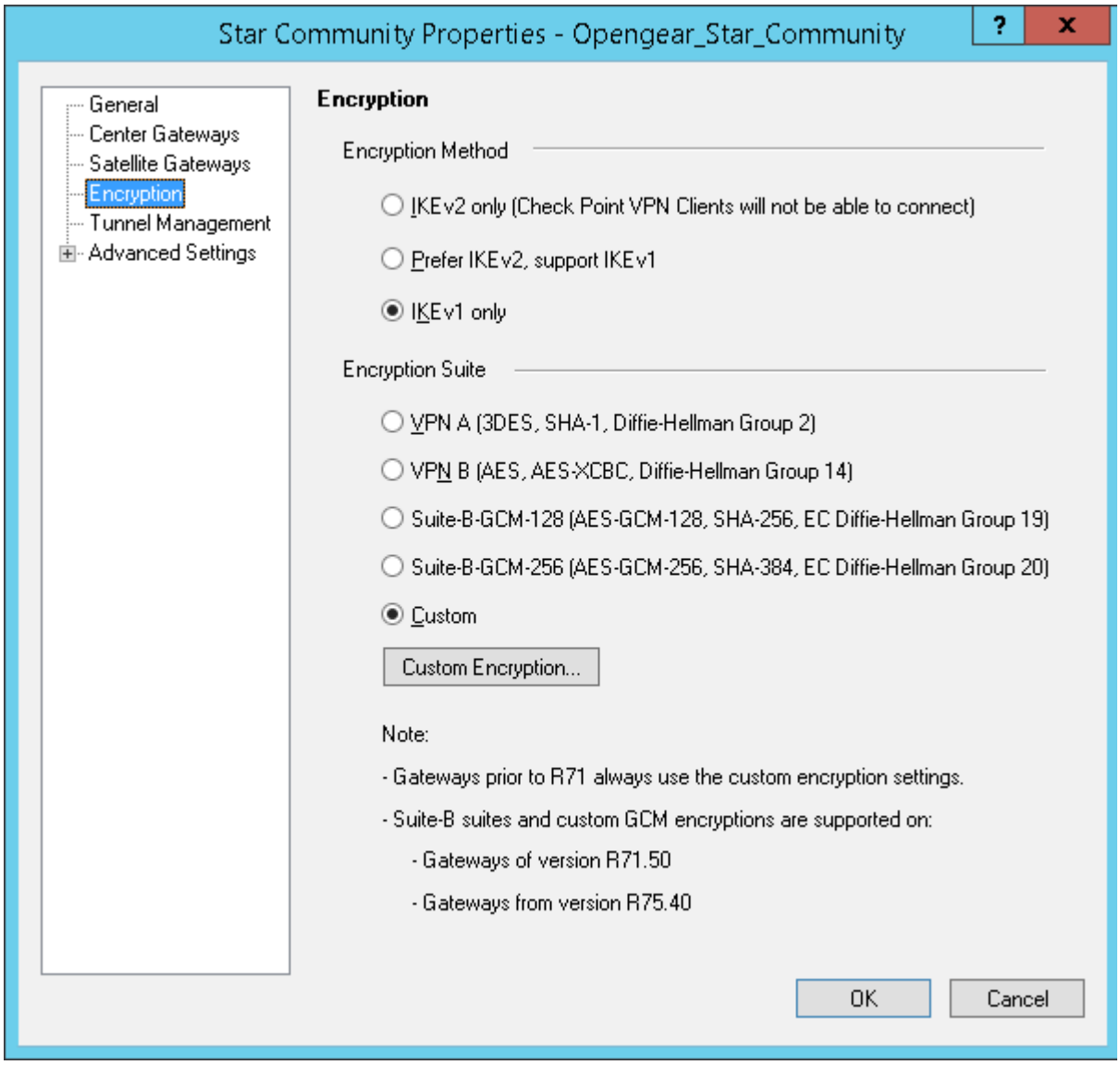
• Set the Check Point gateway as the central gateway

• Set the ACM interoperable device as the satellite gateway.

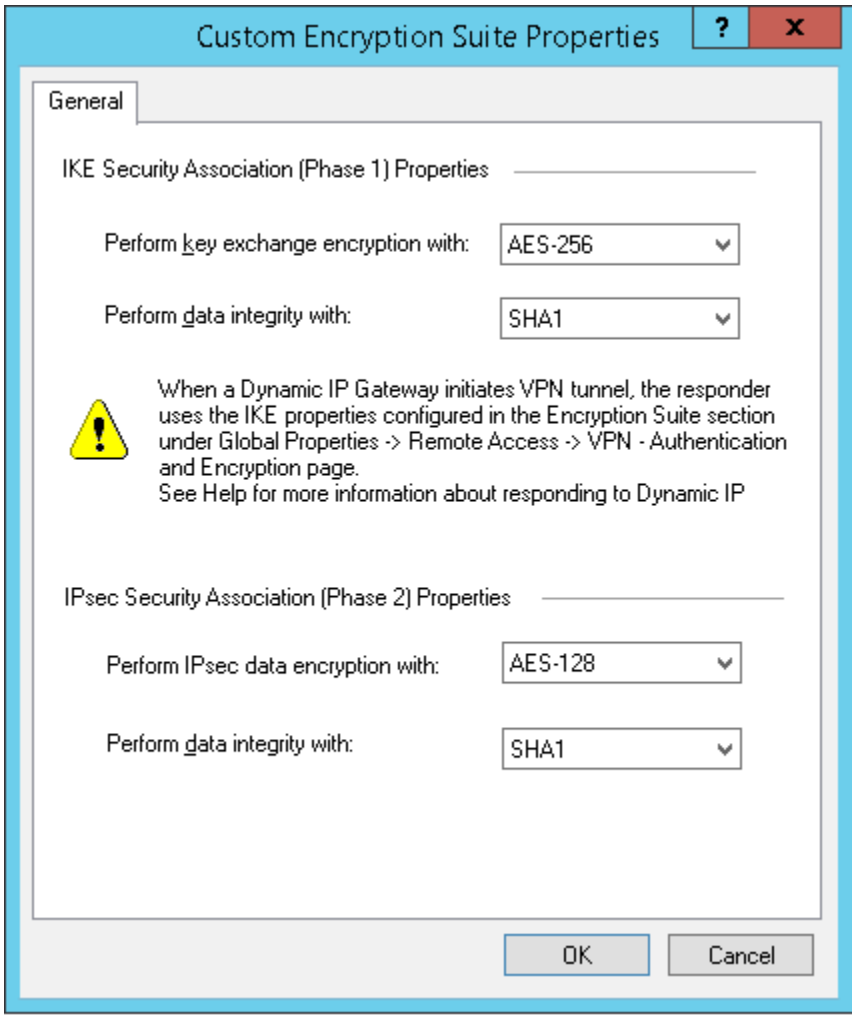
• Add IKE and IKE_NAT_TRAVERSAL to the VPN community excluded services.

• **Note:** for Dynamic IP VPN gateways, the IKE and IPSec encryption methods and supported suites are defined in **Global Properties → Remote Access → VPN Authentication**

• Select **Encryption** and set **Encryption Method** to **IKEv1 only** and **Encryption Suite** to **Custom**



• Click on **Custom Encryption...** and make sure **IKE Security Association (Phase 1)** is set to use **AES-256** and **SHA1**, **IPSec Security Association (Phase 2)** should be set to **AES-128** and **SHA1,** click on **OK**.



Create the rules in the security policy to allow the requisite services in the correct directions:

- ICMP in both directions
- RADIUS and RADIUS Accounting services from Branch to Head Office (for authentication)
- SSH, SSH over high TCP ports and HTTPS from Head Office to Branch

ACM Branch VPN - Inbound	test_network	internal_lan	opengear_test	icmp-proto NEW-RADIUS NEW-RADIUS-A	accept	Log
ACM Branch VPN - Outbound	internal_lan	test_network	opengear_test	icmp-proto ssh https tcp-high-ports	accept	Log

4. Configuring the Opengear Side

In this example:

- The authentication method uses X.509 certificates
- The Opengear device is an ACM5004-G with private network address 192.168.0.1
- The Check Point gateway is on the private subnet 192.168.72.0

Prerequisites:

- Ensure that the ACM is running the correct firmware version (3.6.x or higher)
- Ensure that the cellular link is active and working

Create a new IPSec VPN:

- Navigate to **Serial & Network → IPSec VPN →** click **Add**
- Enter the details as listed in the table, there is a screenshot on the following page

Edit IPSec Tunnel	
Tunnel Name	opengear_to_checkpoint
Initiate Tunnel	Yes

Security	
Authentication Method	RSA digital signatures
Left Public Key	leave blank
Right Public Key	leave blank
Authentication Protocol	ESP
Aggressive Mode	No
IKE Proposal (Phase 1)	Negotiable
Perfect Forward Secrecy	No
Left ID	Leave blank
Right ID	WAN address of the Checkpoint Gateway
Left Address	leave blank
Right Address	WAN address of the Checkpoint Gateway
Networking	
Left Subnet	192.168.0.0/24
Right Subnet	192.168.72.0/24

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

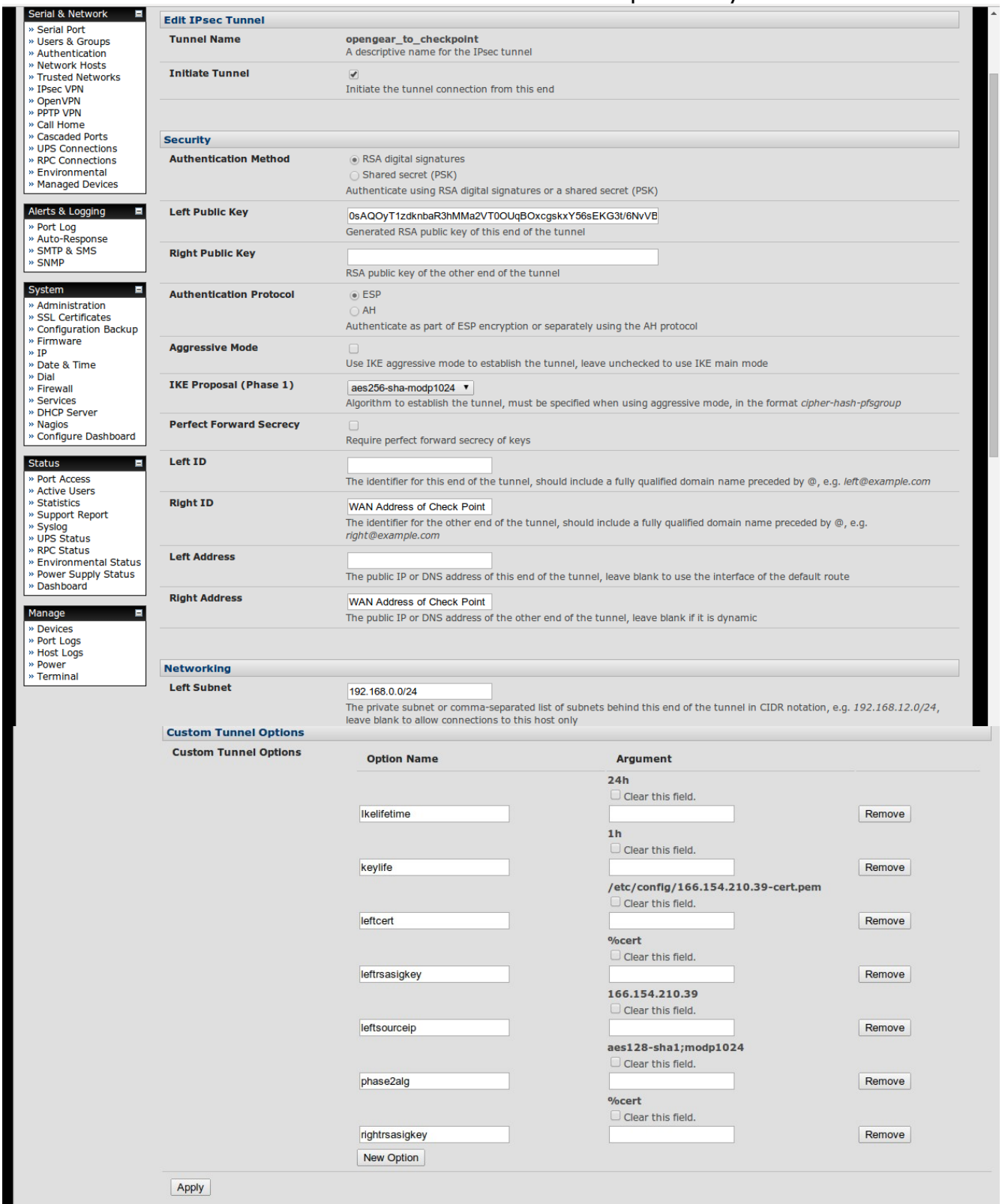
• Replace Right Subnet with the private network address of the Check Point gateway.

Screenshot of Opengear settings:

Custom Tunnel Options	
Ikelifetime	24h
keylife	1h
leftcert	/etc/config/ACM-cert.pem
leftrsasigkey	%cert

leftsourceip	192.168.0.1
phase2alg	aes128-sha1;modp1024
rightrsasigkey	%cert

- The custom IPSec must be added to ensure interoperability with Check Point.



• Click **Apply**

• To make sure the correct RSA key is used login to the Opengear command line and create the file **/etc/config/scripts/config-post-ipsec**

```
#!/bin/sh
echo ": RSA ACM-private.key \"\"" > /etc/config/ipsec.config.secrets
```

Ensure that the script is executable:

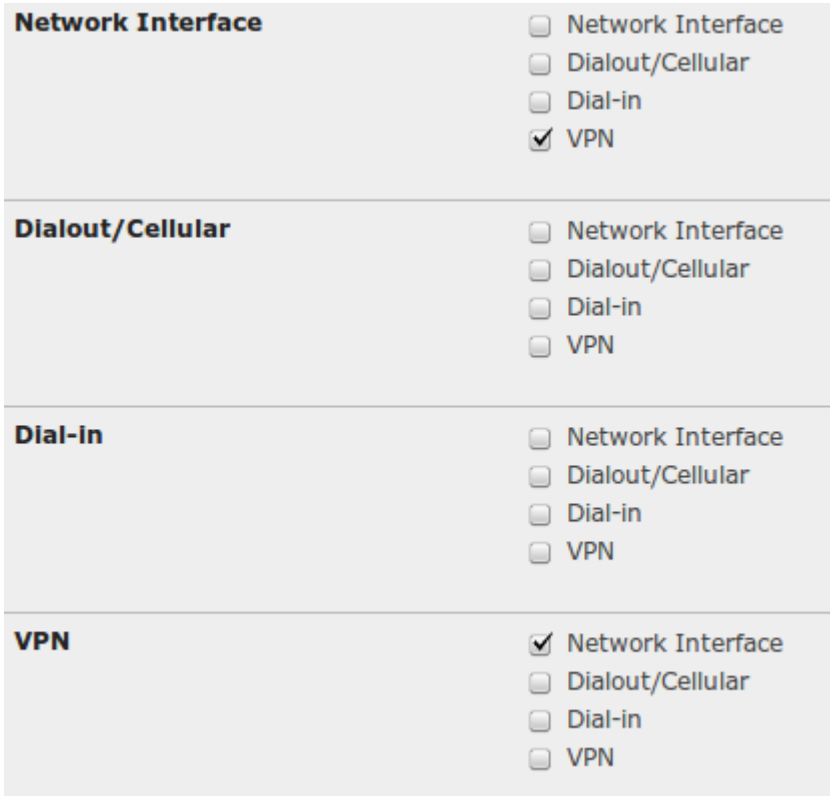
```
# chmod +x /etc/config/scripts/config-post-ipsec
# ls -l /etc/config/scripts/config-post-ipsec
-rwxr-xr-x  1 root     root        66 Sep 12 16:03 config-post-ipsec
```

Traffic Forwarding:

• Navigate to **System → Firewall → Forwarding and Masquerading**

• Tick Network Interface to VPN

• Tick VPN to Network Interface



5. Configure Auto-Response

Since the Check Point gateway does not support Dead Peer Detection (DPD), we need an alternative method to ensure the VPN tunnel is kept UP and available. We can achieve this through the Opengear Auto-Response functionality.

Create a script in /etc/config/scripts called “restart-tunnel” (you may need to create a scripts folder).

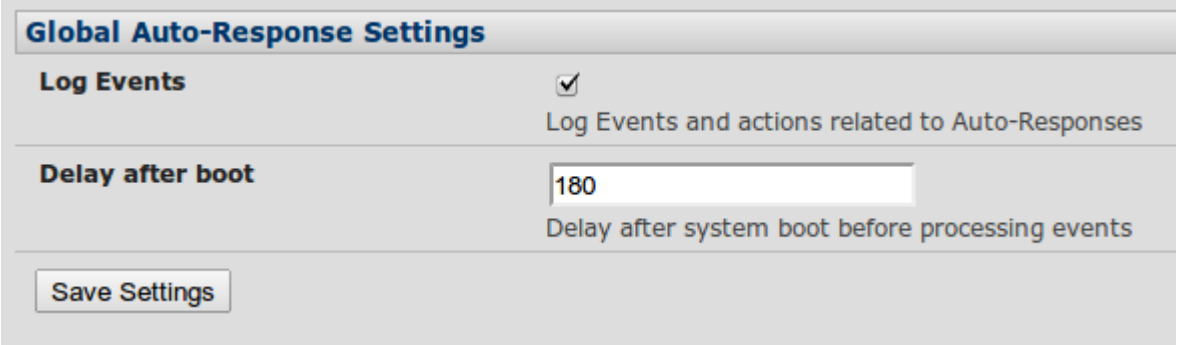
/etc/config/scripts/restart-tunnel:

```
#!/bin/bash
/bin/ipsec auto --down "$1"
/bin/ipsec auto --up "$1"
```

Ensure that the script is executable:

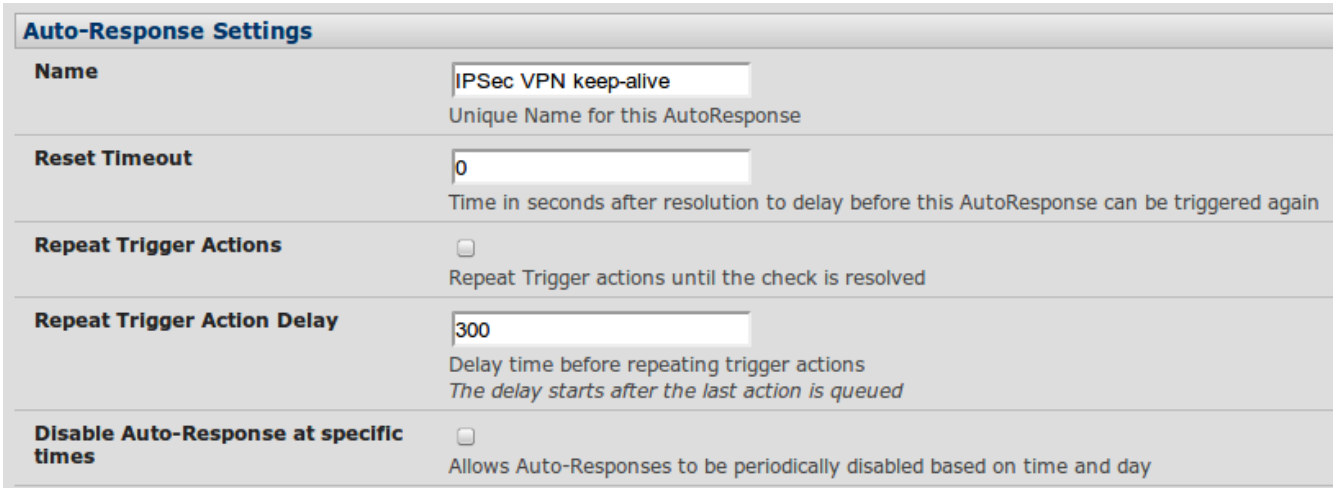
```
# chmod +x /etc/config/scripts/restart-tunnel
# ls -l /etc/config/scripts/restart-tunnel
-rwxr-xr-x  1 root     root         66 Sep 12 16:03 restart-tunnel
```

- Navigate to **Alerts & Logging → Auto-Response**
- Change the global setting to be a 180 second delay after boot
- Enable Log Events

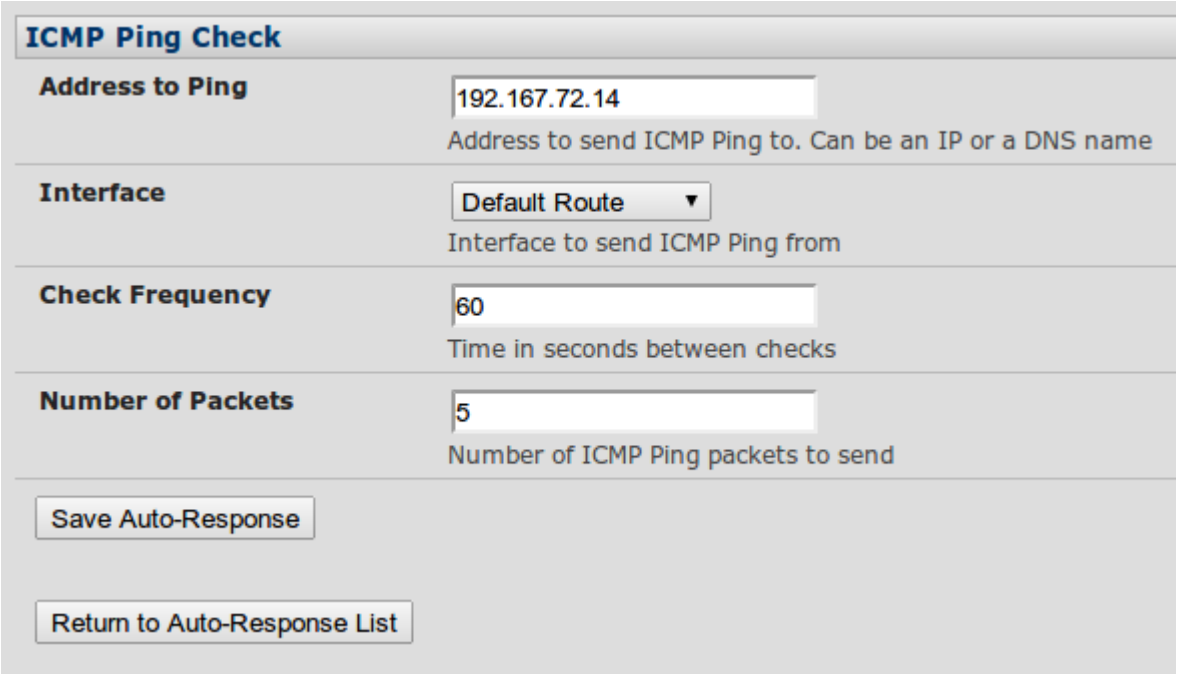


- Save settings

- **Create a new auto-response** as follows:
  - Name – arbitrary name e.g. "IPSec VPN keep-alive"
  - Keep remaining defaults

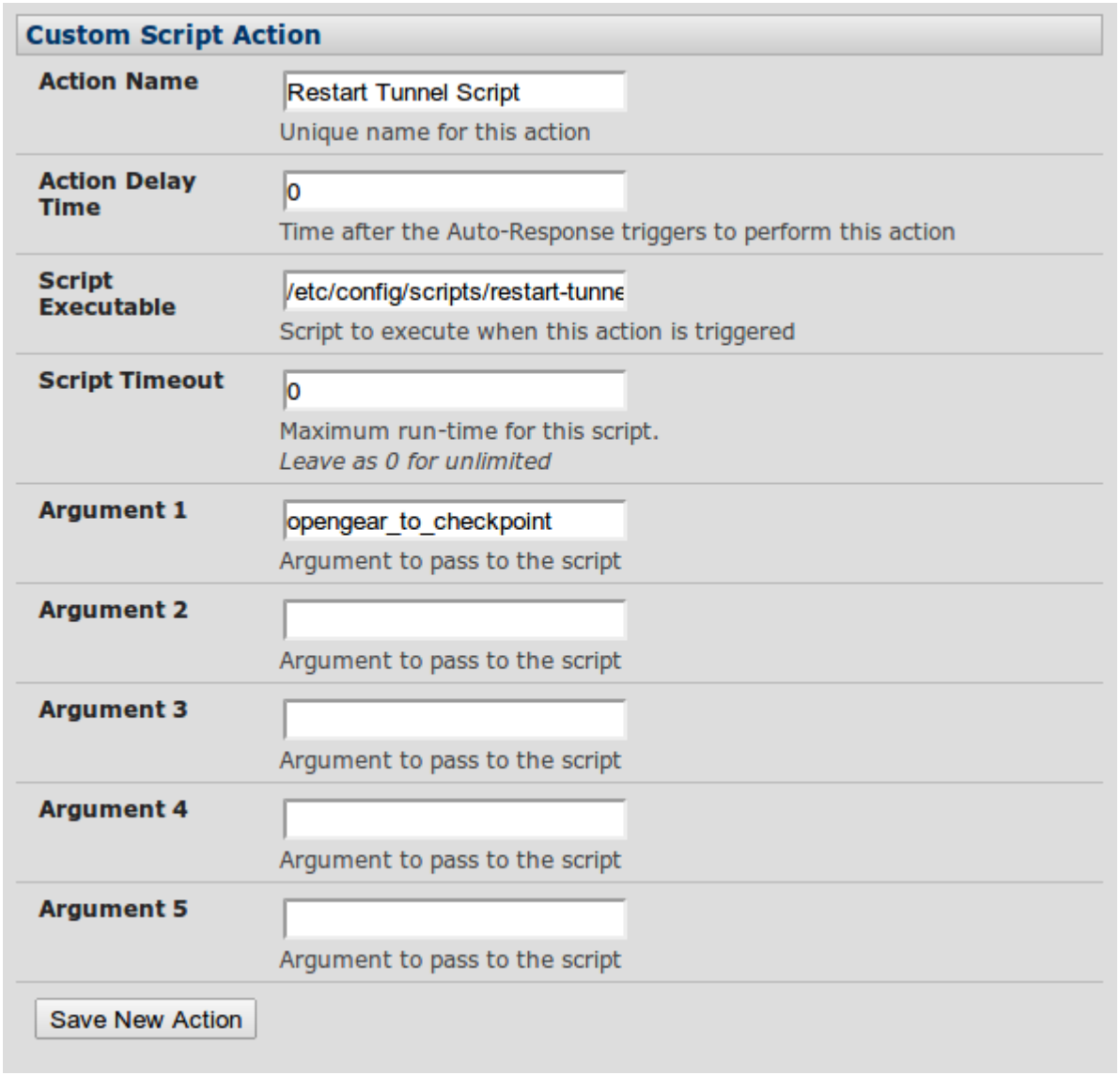


Check Condition ICMP Ping	
Address to ping	selected host in head office e.g. 192.167.72.14
Interface	default route



- **Trigger Actions** Run Custom Script

Custom Script Action	
Action Name	arbitrary name
Script Executable	/etc/config/scripts/restart-tunnel
Argument 1	opengear_to_checkpoint (the exact name of the IPSec VPN tunnel as configured on Opengear)



• Save Changes

6. Summary

You should now have a working IPSec VPN between the ACM and the Check Point gateway. Your network administrators and operators will be able to connect

securely to the ACM serial ports (through this VPN) by creating an SSH connection directly through to **BranchACM_LAN_IP_address:300x** where 'x' is the required console port. They will authenticate using the configured remote authentication e.g. RADIUS.

7. Notes on Opengear IPSec VPN Configuration

• Only on: ACM500x, ACM550x and IM42xx

• 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 or VCMS 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 ACM5004-G 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