IPsec VPN Guide

Opengear to Opengear

> This is a guide on how to create an IPsec VPN tunnel between two Opengear devices. In the first example both Opengear devices are on the same network. In the second example one of the Opengear devices is connected to the Internet via 3G. Both examples use RSA authentication.

In this document:

Background on how IPsec works:

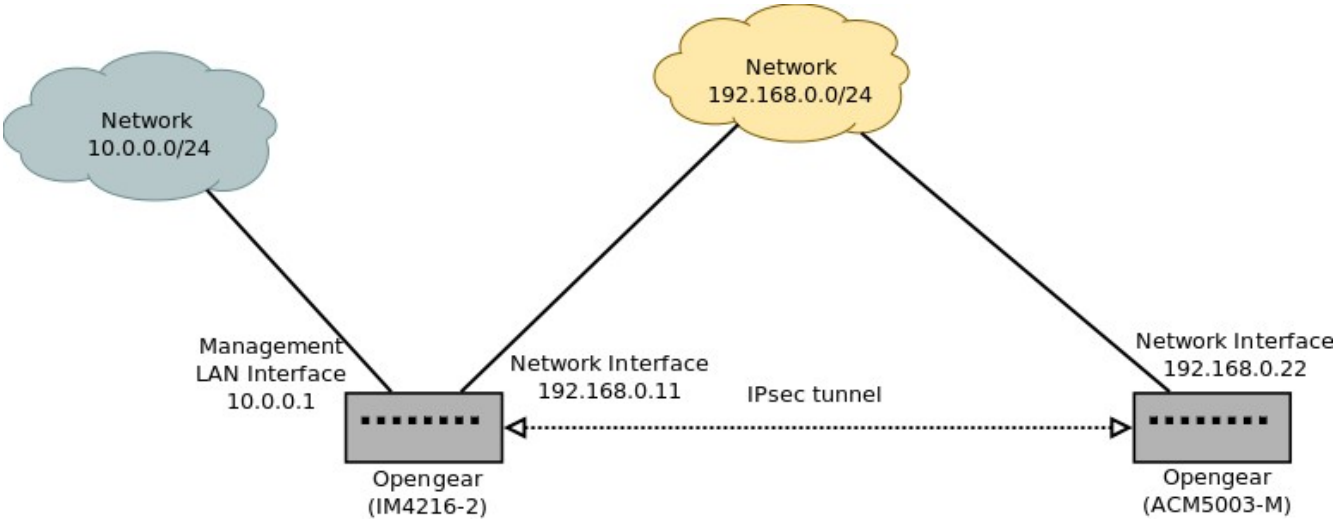
> http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=6

Scenario: using two Opengear devices to create an IPsec VPN between two secure networks over an insecure network (such as the Internet). A workstation on either network would be able to securely manage any network host on the VPN.

1. Opengear to Opengear on Same Network

1. Opengear device: IM4216-2
   Network Interface: 192.168.0.11
   Management LAN Interface: 10.0.0.1
2. Opengear device: ACM5003-M
   Network Interface: 192.168.0.22

This example creates an IPsec VPN tunnel between two subnets on a local network. The IM4216-2 is acting as a gateway for the 10.0.0.0/24 network and is connecting to a single host – ACM5003-M. Both Opengear devices are on the 192.168.0.0/24 network.



In web UI for both devices: **Serial & Network** → **IPsec VPN**, click **Add**

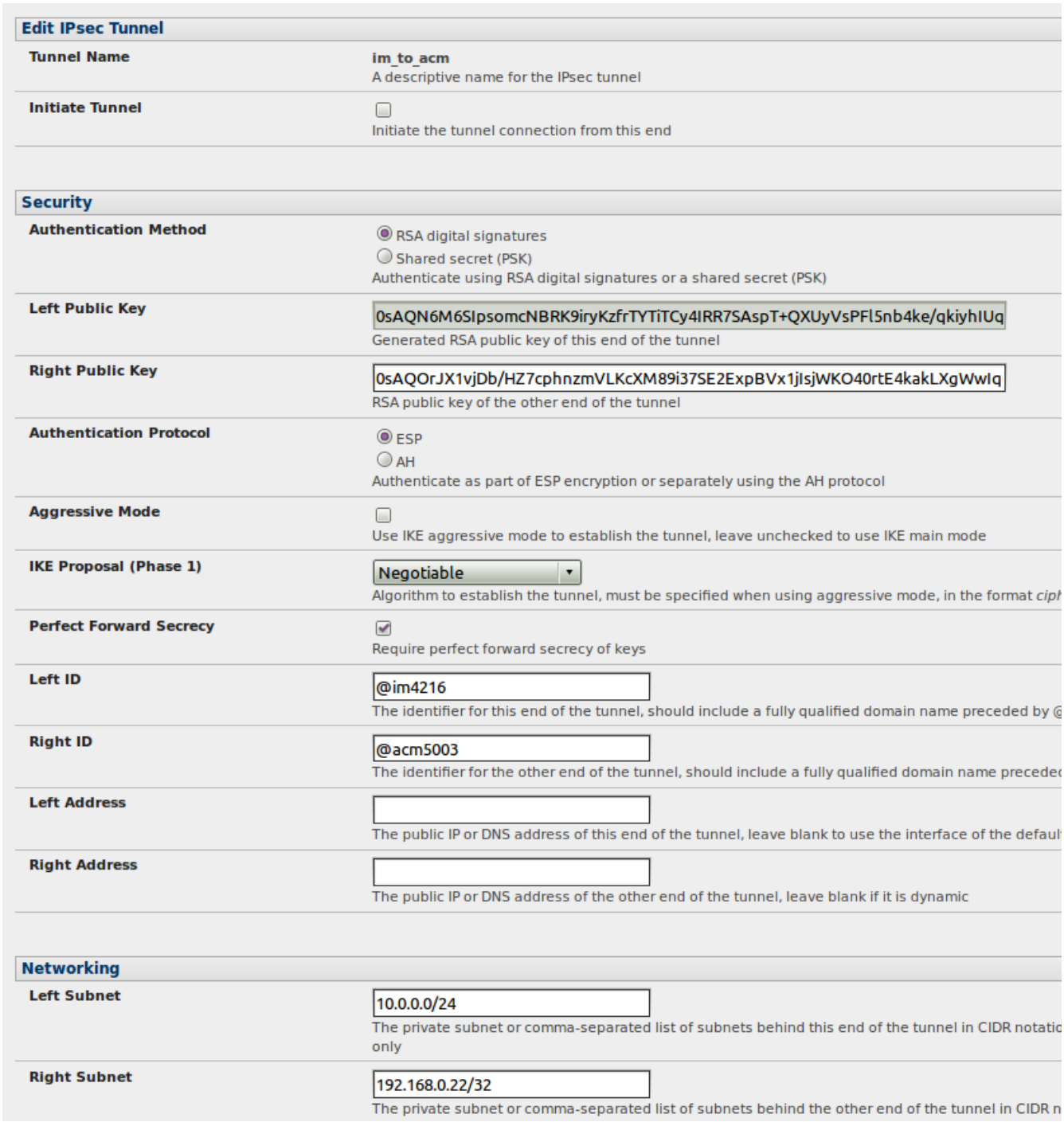
Enter the following:

Field	IM4216-2	ACM5003-M
Tunnel Name	im_to_acm	acm_to_im
Initiate Tunnel	No	Yes
Authentication Method	RSA	RSA
Left Public Key	[generate keys]	[generate keys]
Right Public Key	Copy and paste from 'Left Public Key' of ACM5003	Copy and paste from 'Left Public Key' of IM4216
Authentication Protocol	ESP	ESP
Aggressive Mode	Leave unchecked	Leave unchecked
IKE Proposal	Negotiable	Negotiable
Perfect Forward Secrecy	Check	Check
Left ID	im4216@opengear.com	acm5003@opengear.com
Right ID	acm5003@opengear.com	im4216@opengear.com
Left Address	*leave blank*	*leave blank*
Right Address	*leave blank*	192.168.0.11
Left Subnet	10.0.0.0/24	192.168.0.22/32
Right Subnet	192.168.0.22/32	10.0.0.0/24

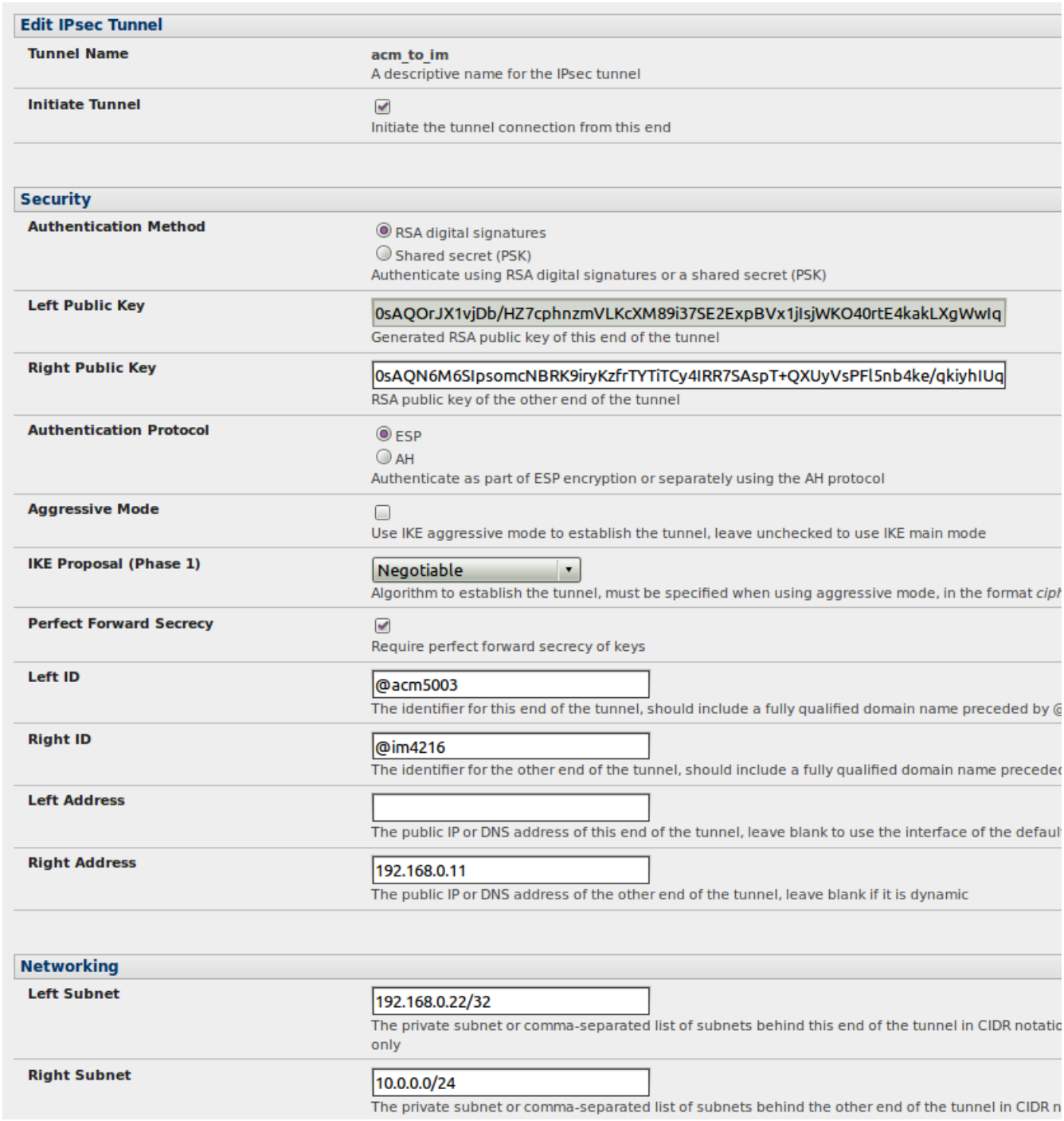
“IPsec SA established tunnel mode” should be visible in the Syslog:

```
<84>Dec  3 19:50:25 pluto[6210]: "im_to_acm/1x1"[1] 192.168.250.4 #2:
STATE_QUICK_R2: IPsec SA established tunnel mode {ESP=>0xd36f30de
<0x1698a1bd xfrm=AES_128-HMAC_SHA1 NATOA=none NATD=none DPD=none}
```

IM4216-2 IPsec VPN Configuration



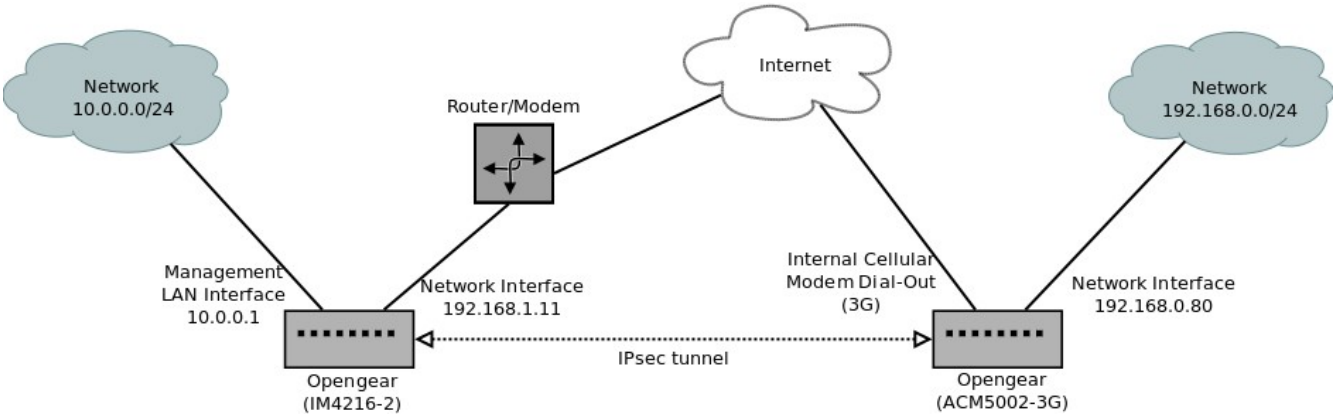
ACM5003-M IPsec VPN Configuration



2. Opengear to Opengear via Internet (3G and ADSL2+)

1. Opengear device: IM4216-2
   Network Interface: 192.168.1.11
   Management LAN Interface: 10.0.0.1
2. Opengear device: ACM5002-3G
   Internal Cellular Modem: opengeartest.dyndns.org
   Network Interface: 192.168.0.80

This example creates an IPsec VPN tunnel between two subnets via the Internet. The IM4216-2 is acting as a VPN gateway for the 10.0.0.0/24 network and the ACM5002-3G is acting as a VPN gateway for the 192.168.0.0/24 network.



In web UI for both devices: **Serial & Network** → **IPsec VPN**, click **Add**

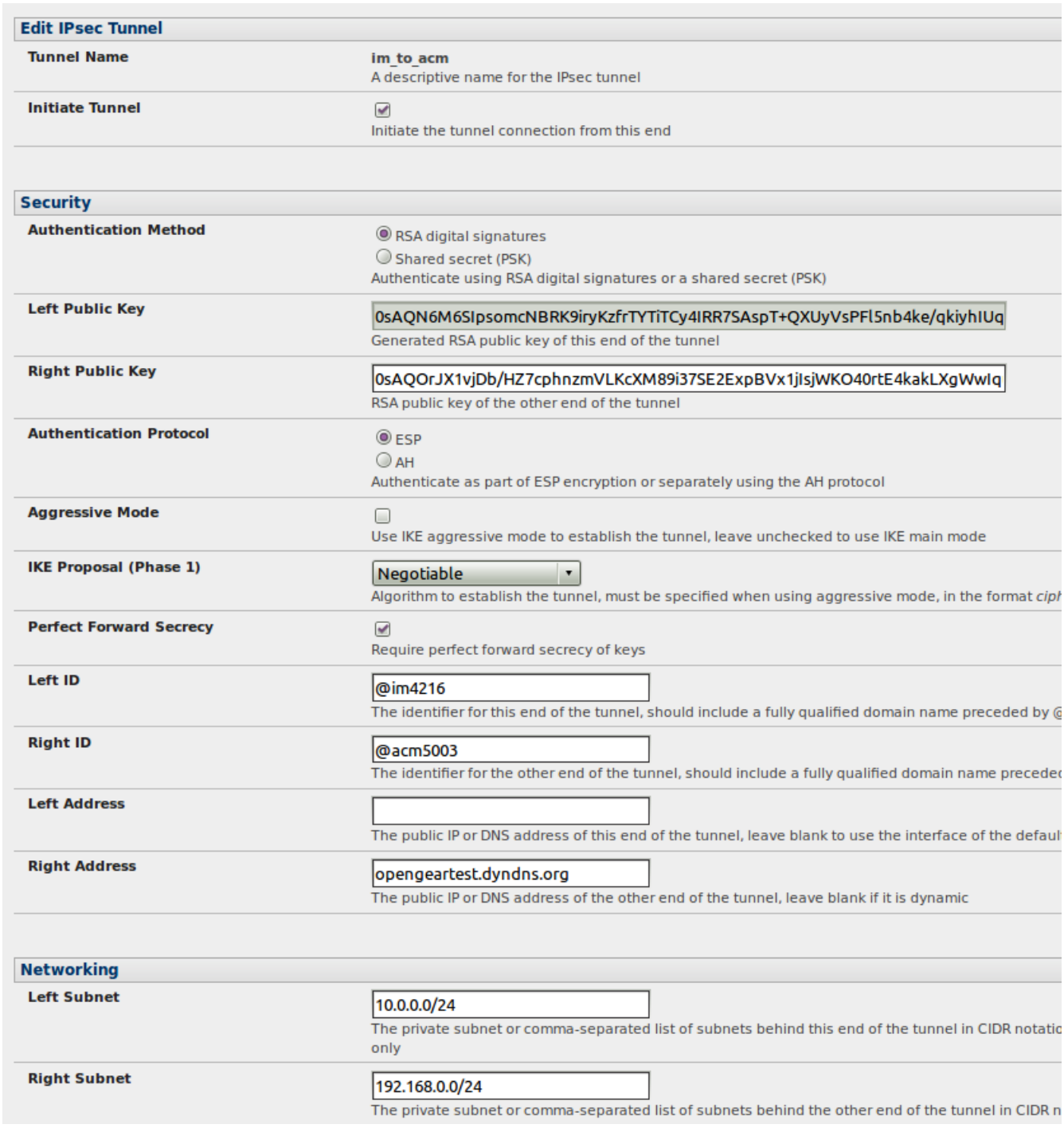
Enter the following:

Field	IM4216-2	ACM5002-3G
Tunnel Name	im_to_acm	acm_to_im
Initiate Tunnel	Yes	No
Authentication Method	RSA	RSA
Left Public Key	[generate keys]	[generate keys]
Right Public Key	Copy and paste from 'Left Public Key' of ACM5003	Copy and paste from 'Left Public Key' of IM4216
Authentication Protocol	ESP	ESP
Aggressive Mode	Leave unchecked	Leave unchecked
IKE Proposal	Negotiable	Negotiable
Perfect Forward Secrecy	Check	Check
Left ID	@im4216	@acm5002
Right ID	@acm5002	@im4216
Left Address	*leave blank*	*leave blank*
Right Address	opengeartest.dyndns.org	*leave blank*
Left Subnet	10.0.0.0/24	192.168.0.0/24
Right Subnet	192.168.0.0/24	10.0.0.0/24

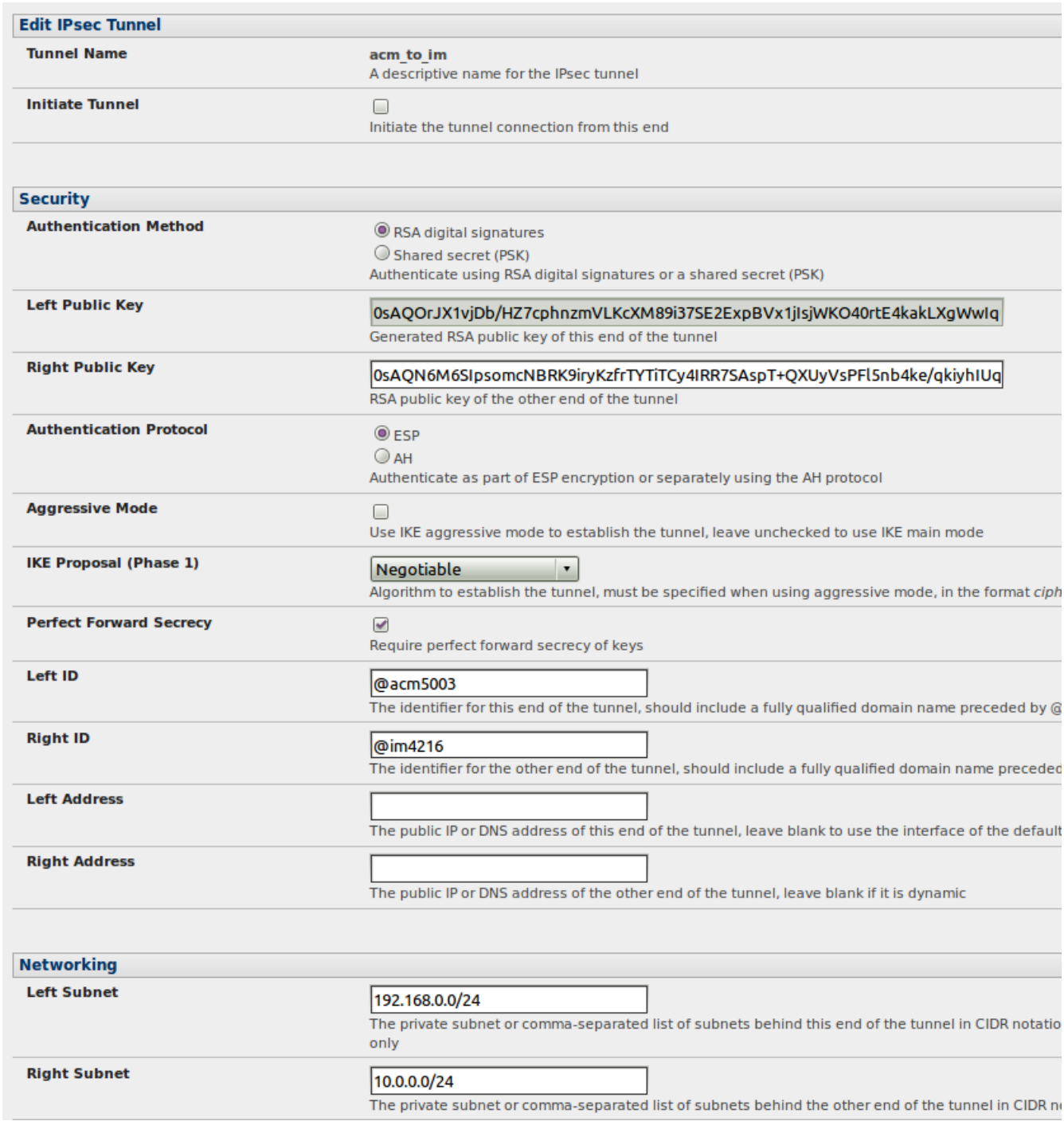
“IPsec SA established tunnel mode” should be visible in the Syslog:

```
<84>Apr  4 19:47:22 pluto[2458]: "im_to_acm" #4: STATE_QUICK_R2: IPsec SA
established tunnel mode {ESP=>0x1222ddfc <0x9c361881 xfrm=AES_128-HMAC_SHA1
NATOA=none NATD=none DPD=none}
```

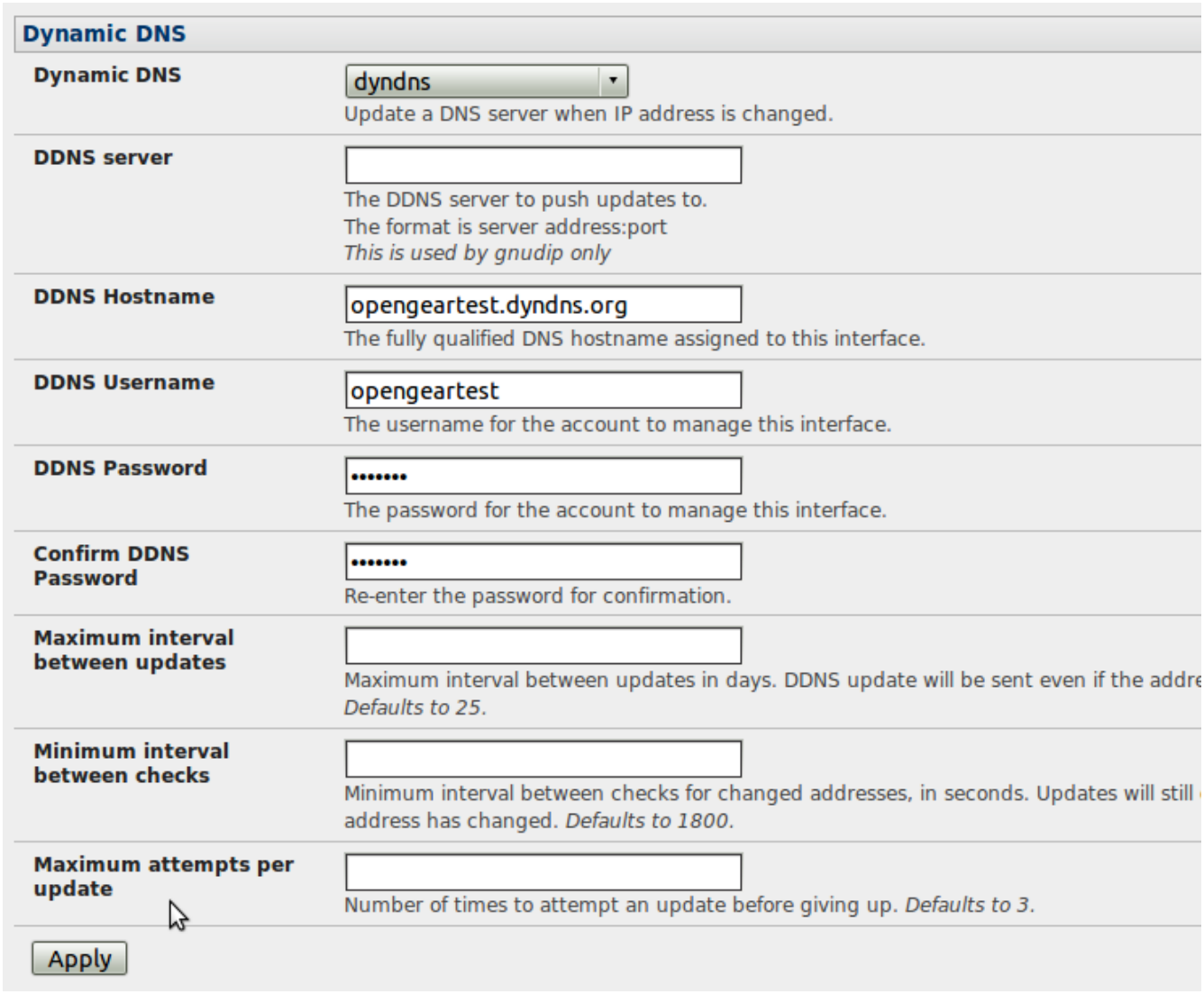
IM4216-2 IPsec VPN Configuration



ACM5002-3G IPsec VPN Configuration



3. Example Using Dynamic DNS



4. 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