Mediant 1000 MSBG

IPSec Tunnel to Cisco router

Overview

This document explains how to configure an IPSec tunnel connection between the Mediant 1000 MSBG and a Cisco router. The connection is encrypted with the industry-standard AES cipher.

The first part of this document explains how to create a simple tunnel, where each network consists of one subnet. The second part explains how to extend this model to route multiple subnets over the same encrypted link.

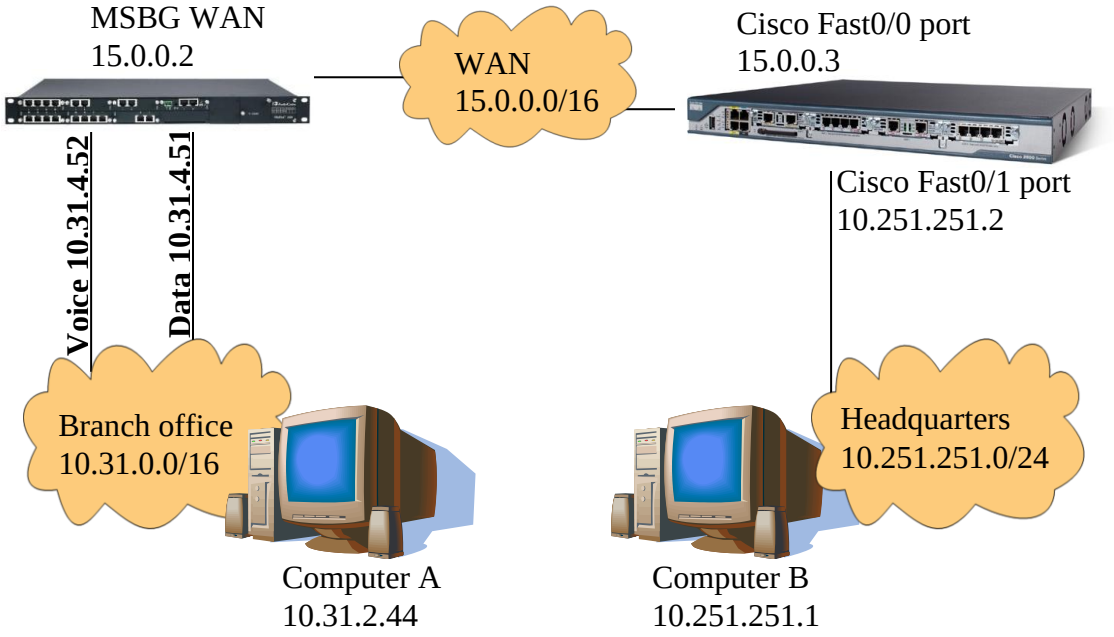
Setup

For the purpose of creating this document, we used a Cisco 2801 router running IOS 12.4 software, and a Mediant 1000 MSBG running software version 5.8.

Our network consisted of three networks, as follows:

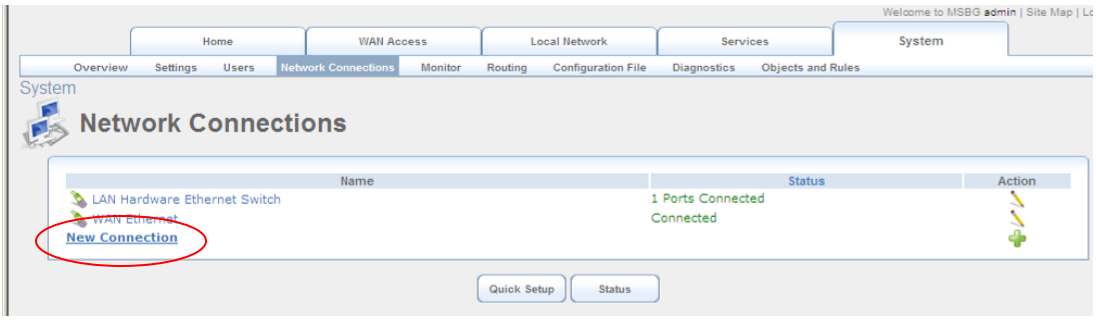
Headquarters network: 10.251.251.xx
WAN network: 15.0.xx.xx
Branch office network: 10.31.xx.xx

The MSBG connects the branch office to the WAN, while the Cisco router connects the headquarters network to the WAN.



MSBG configuration screenshots

To configure the IPSec tunnel, navigate to the MSBG's web interface and click on "Data Home". New connections are added using the "System" main tab; click on "Network Connections" and select "New Connection".

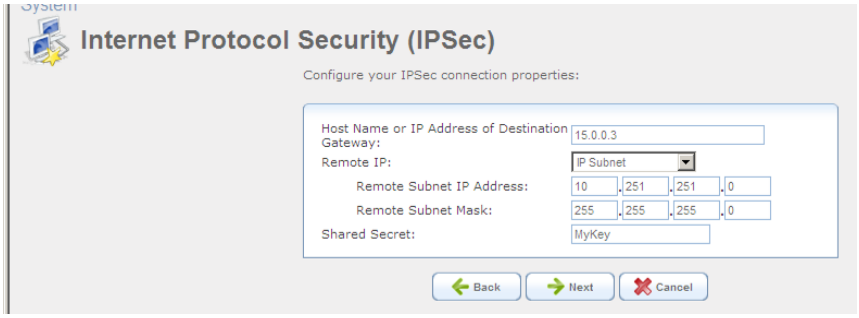


The network connection wizard appears; choose "Connect to a Virtual Private Network over the Internet" and click Next.

Select "VPN Client or Point-to-Point" and click Next.

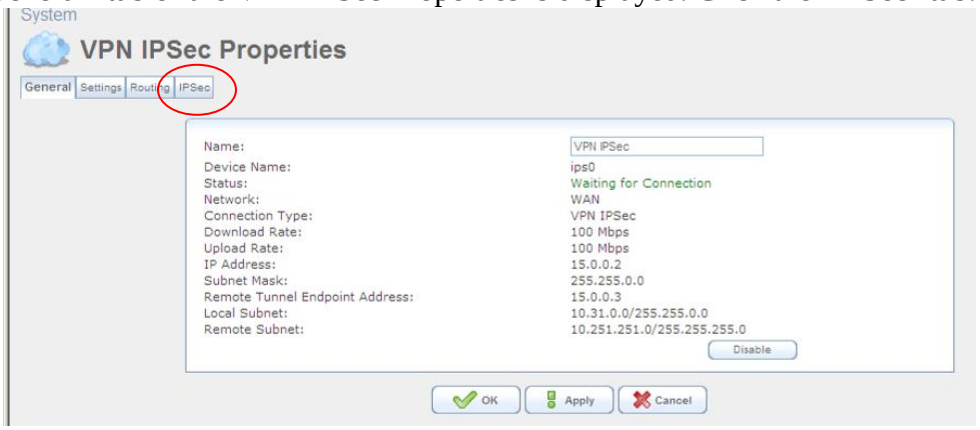
Select "Internet Protocol Security (IPSec)" and click Next.

In the following dialog, fill in the IP address of the Cisco router's WAN interface (in our case, 15.0.0.3). In "Remote IP", select the option "IP Subnet" and fill in the network information for the headquarters network (in our case, 10.251.251.0 with subnet mask 255.255.255.0). Type in a shared secret to be used for the connection, and click Next.

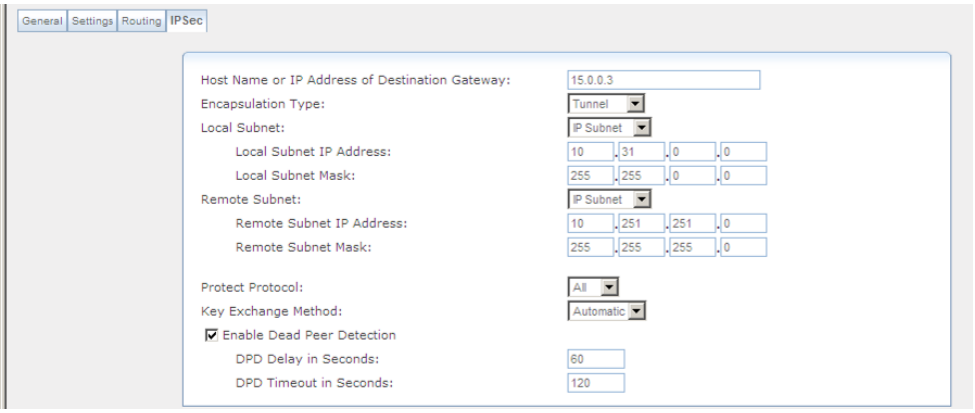


To complete defining the IPSec connection, check the option "Edit the Newly Created Connection" and click Finish.

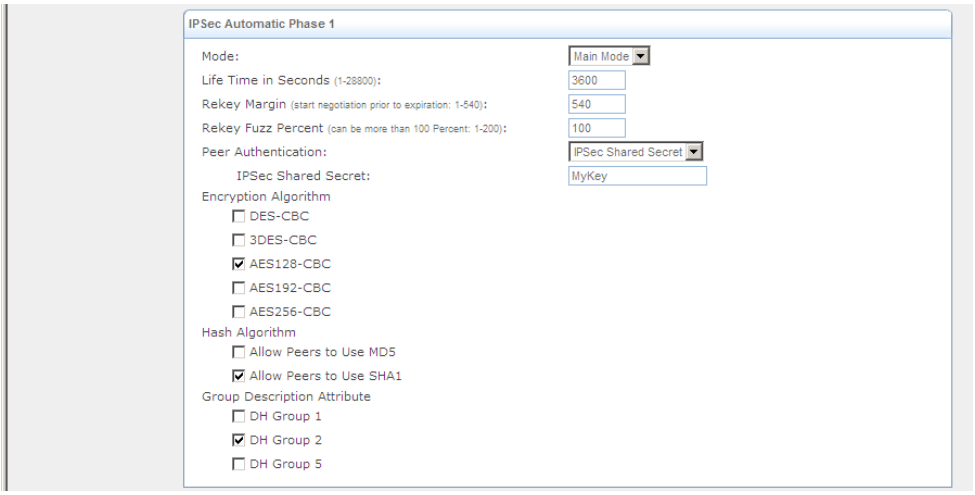
The "General" tab of the VPN IPSec Properties is displayed. Click the "IPSec" tab.



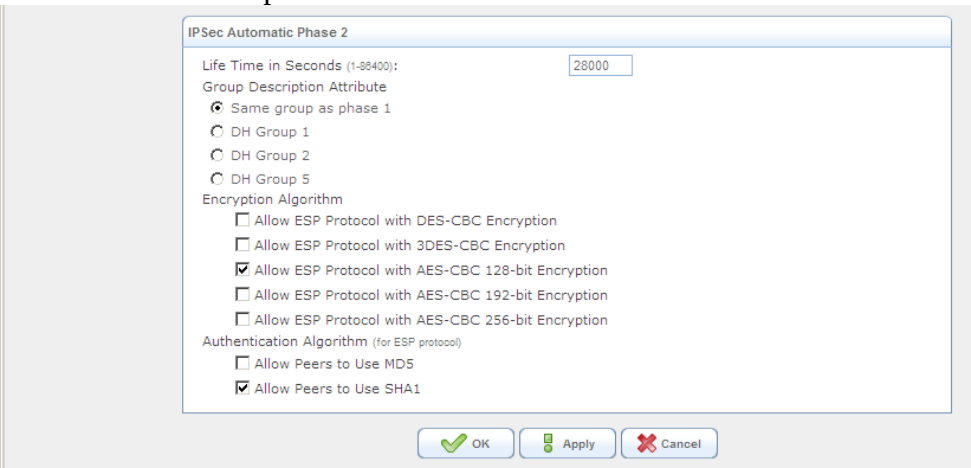
The "IPSec" tab of the VPN IPSec Connection is now displayed. Verify the desired settings and scroll down to "IPSec Automatic Phase 1".



Verify the IPSec shared secret, check the options for encryption algorithm AES128-CBC, hash algorithm SHA1, DH group 2. Uncheck all other options, and scroll down to "IPSec Automatic Phase 2".



Check the options for encryption algorithm AES-CBC 128-bit, authentication algorithm SHA1. Uncheck the other options and click OK.



Configuration of the MSBG is now complete.

Cisco router configuration

Configuration of the Cisco router is done over a serial connection. In our setup, port FastEthernet0/0 was connected to the WAN and port FastEthernet0/1 was connected to the headquarters LAN. Following is a summary of the configuration:

```
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
  lifetime 3600

crypto isakmp key MyKey address 15.0.0.2
crypto ipsec transform-set TR-AES esp-aes esp-sha-hmac

crypto map CM 100 ipsec-isakmp
  set peer 15.0.0.2
  set transform-set TR-AES
  match address 2110

interface FastEthernet0/0
  ip address 15.0.0.3 255.255.0.0
  crypto map CM

interface FastEthernet0/1
  ip address 10.251.251.2 255.255.255.0

access-list 2110 permit ip 10.251.251.0 0.0.0.255 any

ip route 10.31.0.0 255.255.0.0 15.0.0.2
```

Notes regarding the Cisco configuration:

- Access list 2110 defines the IP addresses which should be encrypted. This setting must match the MSBG's setting of "Remote Subnet".
- An IP route is defined to the branch office LAN (in our case 10.31.0.0/16) with the gateway address set to the MSBG's WAN interface (in our case 15.0.0.2). This setting must match the MSBG's setting of "Local Subnet".
- The IKE peer address is the MSBG's WAN interface address (15.0.0.2). Note that this address appears twice: in the crypto map definition and in the crypto isakmp key definition.

PC configuration

Computer A and Computer B should be configured such that the local router interface is the default gateway.
For Computer A, the default gateway should be set to 10.31.4.51 (MSBG data interface).
For Computer B, the default gateway should be set to 10.251.251.2 (Fast0/1 interface).

Verifying the configuration

Once the configuration is defined on both MSBG and Cisco router, initiate a ping from Computer A to Computer B:

```
C:\>ping 10.251.251.1

Pinging 10.251.251.1 with 32 bytes of data:

Reply from 10.251.251.1: bytes=32 time=1ms TTL=64
Reply from 10.251.251.1: bytes=32 time<1ms TTL=64
Reply from 10.251.251.1: bytes=32 time<1ms TTL=64
```

Note that IPSec/IKE set-up takes a short while, therefore the first few packets may be dropped. Once the connection is up, all traffic between Computer A and Computer B flows through the tunnel.

Important notes:

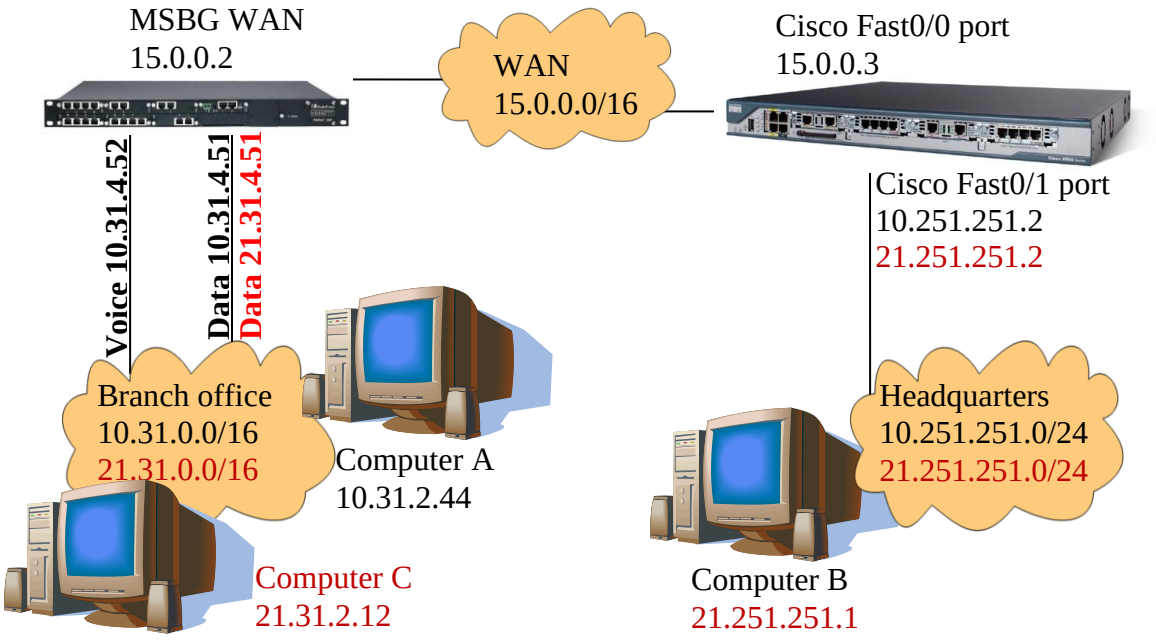
- A network sniffer on the WAN interface will show the ping packets are encrypted (protocol type ESP).
- It is not possible to ping the remote network from the router. The MSBG's Diagnostics page can be used to ping the Cisco router, but not the private network behind it; the Cisco CLI can be used to ping the MSBG, but not the private network behind it. The reason is that IPSec routers are "invisible" to users of the secure network.
- Ping from Computer A to the Cisco router's Fast0/0 interface (15.0.0.3) will work but will not be encrypted.
- Ping from Computer B to the MSBG's WAN interface (15.0.0.2) will not work.

Multiple Subnets

In this section, a more complex network topology is demonstrated. Both the branch office and headquarters now have multiple subnets in their network:

Headquarters network: 10.251.251.xx **and 21.251.251.xx**
WAN network: 15.0.xx.xx
Branch office network: 10.31.xx.xx **and 21.31.xx.xx**

We connected the subnets over the same physical link; further separation is possible through the use of VLANs (which are outside the scope of this document) or using additional routers.



Since IPSec does not support multiple subnets in one tunnel, we will define a GRE tunnel from the MSBG to a loopback address on the Cisco router. The entire GRE payload will be encrypted using the same IPSec link.

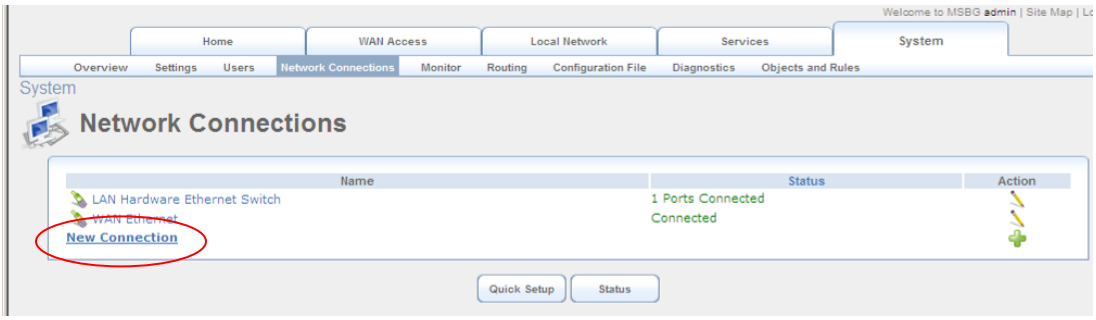
MSBG configuration screenshots - multiple subnets

(Note: differences from the single-subnet example are marked in red)

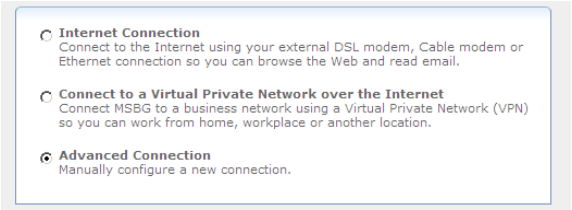
To configure the IPSec tunnel, navigate to the MSBG's web interface and click on "Data Home". New connections are added using the "System" main tab; click on "Network Connections".

If you previously configured an IPSec tunnel for a single subnet, remove it using the red "X" on the right.

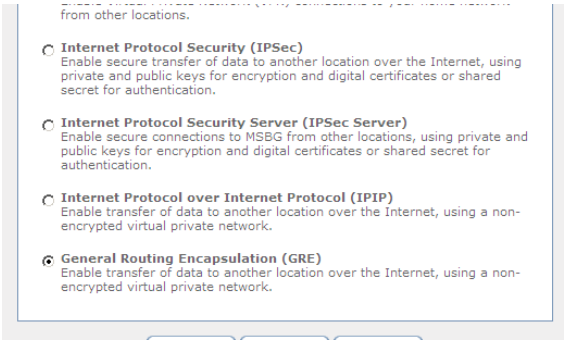
Select "New Connection" to define the new tunnel.



The network connection wizard appears; choose "Advanced Connection" and click Next.

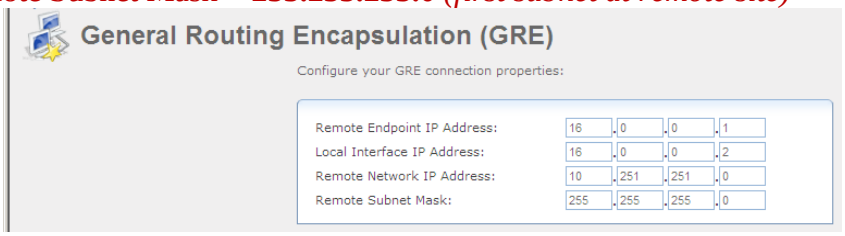


Select "GRE connection" from the list and click Next.

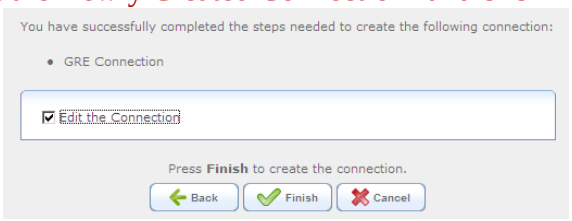


In the following dialog, fill in the following addresses:

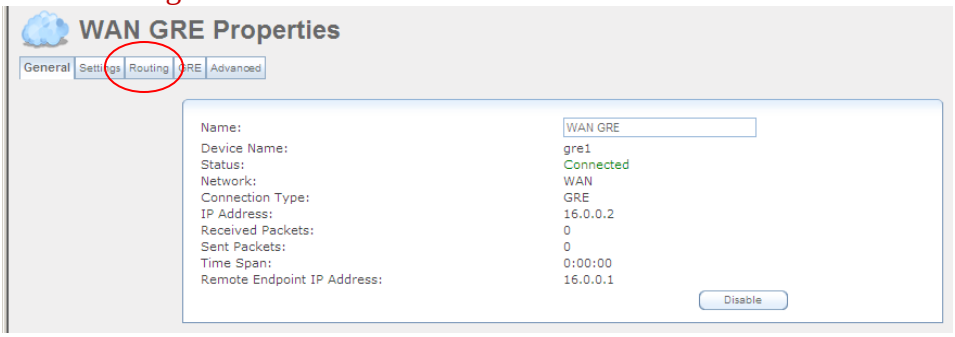
Remote Endpoint IP Address = **15.0.0.3** *(the WAN address of the Cisco router)*
Local Interface IP Address = **16.0.0.2** *(a virtual IP address, to be used later)*
Remote Network IP Address = **10.251.251.0** *(first subnet at remote site)*
Remote Subnet Mask = **255.255.255.0** *(first subnet at remote site)*



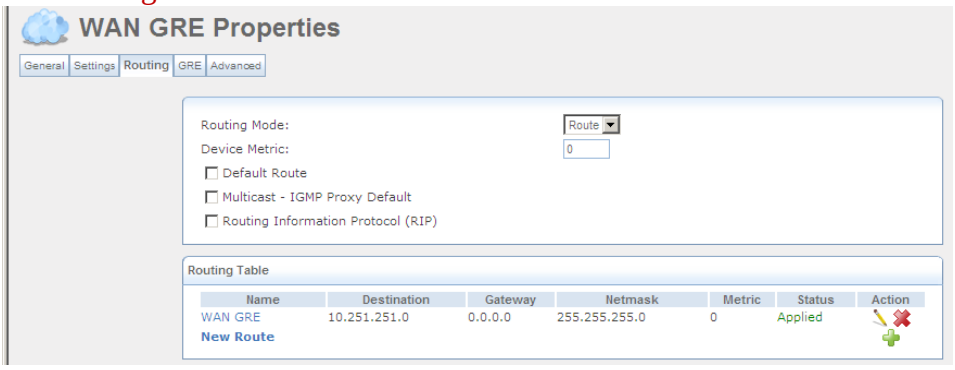
Click Next.
Check the option "Edit the Newly Created Connection" and click Finish.



The following page displays the connection properties for the WAN GRE connection.
Click on the "Routing" tab.

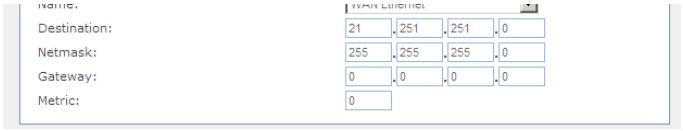


Change the Routing Mode to "Route".

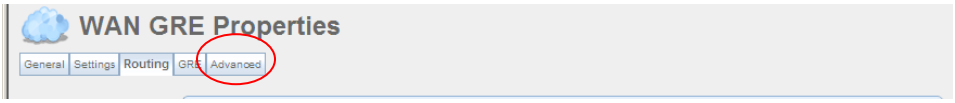


Add a new route by clicking on "New Route" at the bottom.
Fill in the second remote subnet information as follows:

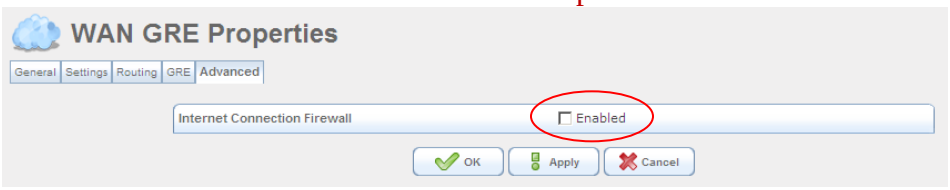
Name = **WAN GRE**
Destination = **21.251.251.0**
Netmask = **255.255.255.0**



Click OK to return to the GRE properties page.
Click on the "Advanced" tab.

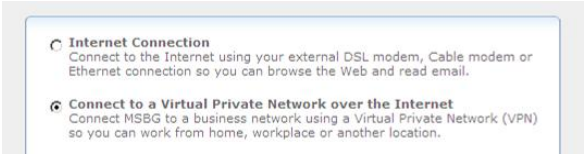


Uncheck "Internet Connection Firewall" to allow all packets from this interface.



Click OK to return to the Network Connections page.

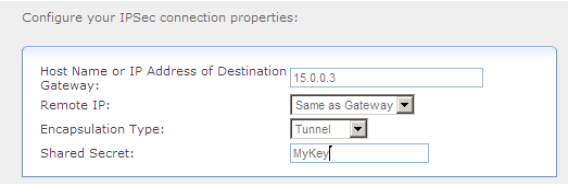
Press "New Connection" to add the IPSec tunnel.
The network connection wizard appears; choose "Connect to a Virtual Private Network over the Internet" and click Next.



Select "VPN Client or Point-to-Point" and click Next.

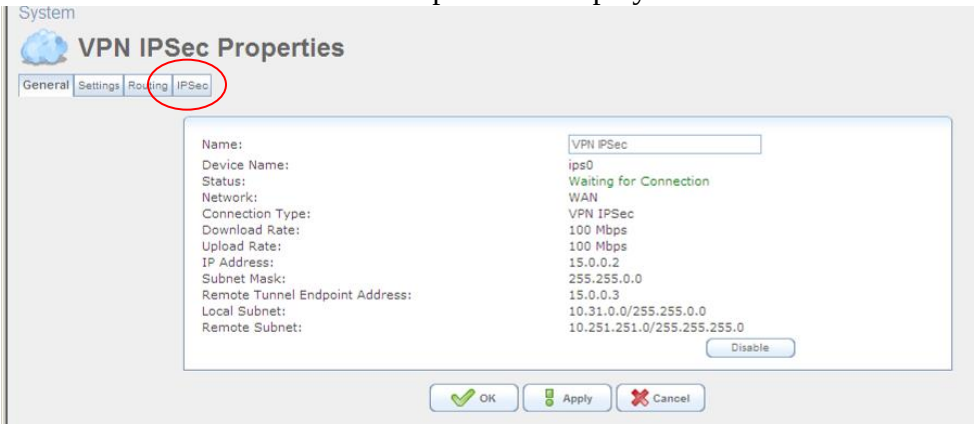
Select "Internet Protocol Security (IPSec)" and click Next.

In the following dialog, fill in the IP address of the Cisco router's WAN interface (in our case, **15.0.0.3**). In "Remote IP", select the option "Same as gateway". Type in a shared secret to be used for the connection, and click Next.

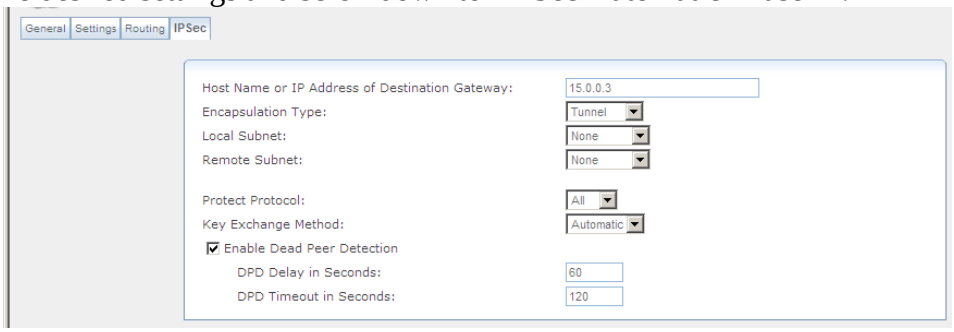


To complete defining the IPSec connection, check the option "Edit the Newly Created Connection" and click Finish.

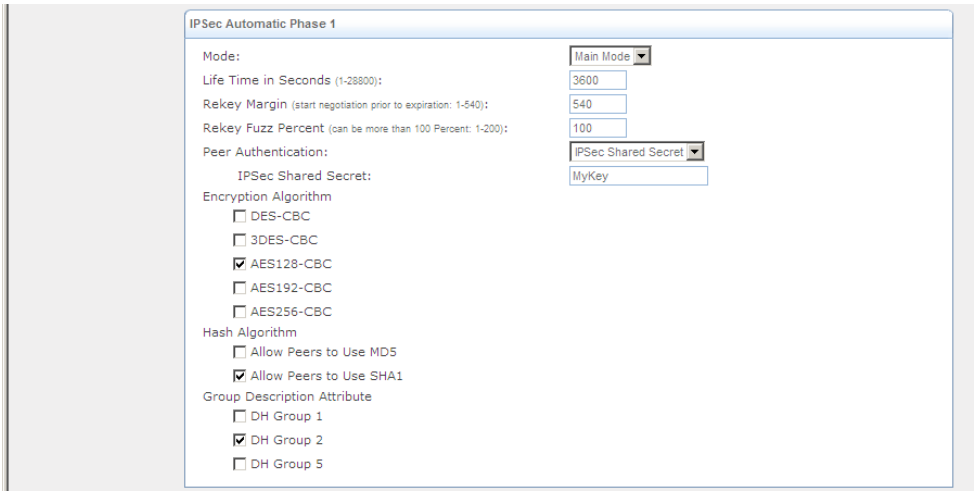
The "General" tab of the VPN IPSec Properties is displayed. Click the "IPSec" tab.



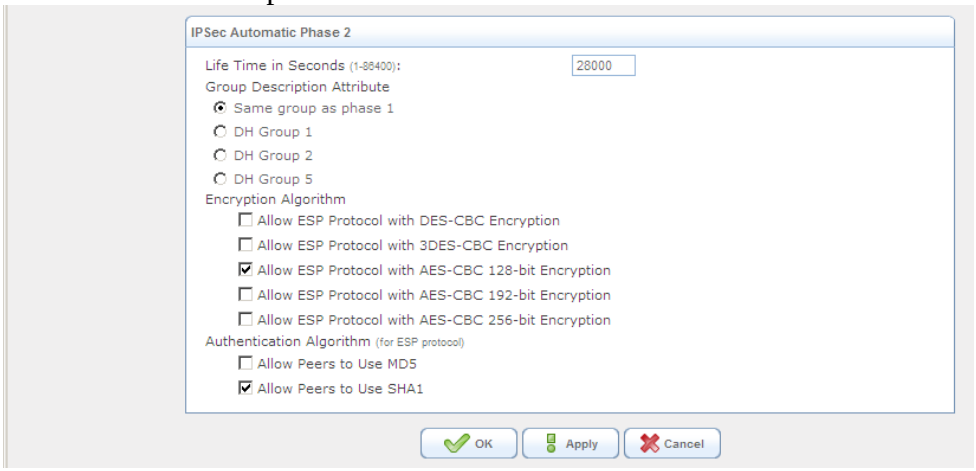
The "IPSec" tab of the VPN IPSec Connection is now displayed.
Set the "Local Subnet" option to "**None**".
Verify the desired settings and scroll down to "IPSec Automatic Phase 1".



Verify the IPSec shared secret, check the options for encryption algorithm AES128-CBC, hash algorithm SHA1, DH group 2. Uncheck all other options, and scroll down to "IPSec Automatic Phase 2".



Check the options for encryption algorithm AES-CBC 128-bit, authentication algorithm SHA1. Uncheck the other options and click OK.



Configuration of the MSBG is now complete.

Cisco router configuration - multiple subnets

Following is a summary of the configuration used:

```
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
  lifetime 3600

crypto isakmp key MyKey address 15.0.0.2
crypto ipsec transform-set TR-AES esp-aes esp-sha-hmac

crypto map CM 100 ipsec-isakmp
  set peer 15.0.0.2
  set transform-set TR-AES
  match address 2110

interface FastEthernet0/0
  ip address 15.0.0.3 255.255.0.0
  crypto map CM

interface FastEthernet0/1
  ip address 10.251.251.2 255.255.255.0
  ip address 21.251.251.2 255.255.255.0 secondary

access-list 2110 permit ip host 15.0.0.3 host 15.0.0.2

interface Tunnel1082
  ip address 16.0.0.1 255.255.255.252
  tunnel source 15.0.0.3
  tunnel destination 15.0.0.2

ip route 10.31.0.0 255.255.0.0 Tunnel1082 16.0.0.2
ip route 21.31.0.0 255.255.0.0 Tunnel1082 16.0.0.2
```

Notes regarding the Cisco configuration:

- Access list 2110 defines the IP addresses which should be encrypted.
- Two IP routes are defined to the branch office LAN with the gateway address set to the MSBG's GRE interface (in our case 16.0.0.2). This setting must match the MSBG's setting of GRE local address.