

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.

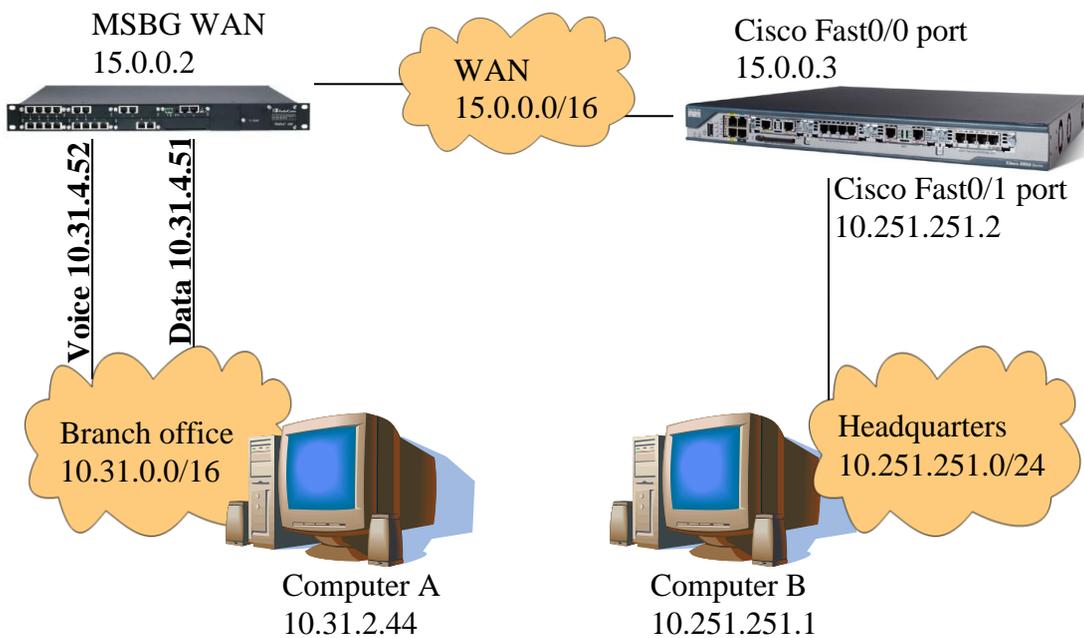
Our network consisted of three networks, as follows:

Headquarters network: 10.251.251.xx

WAN network: 15.0.xx.xx

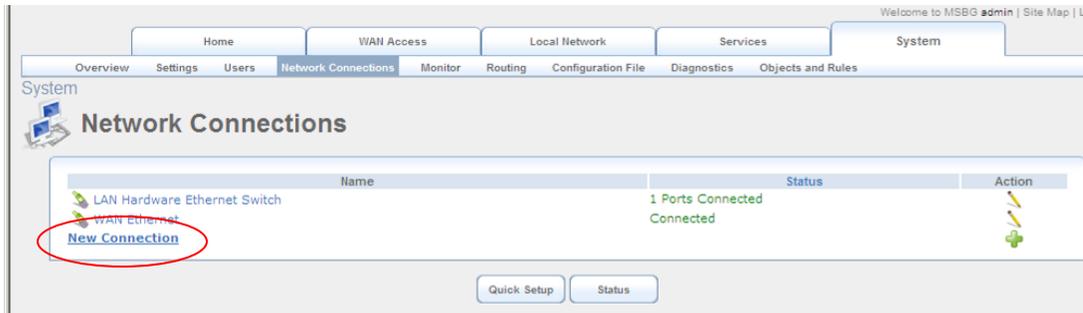
Branch office network: 10.31.xx.xx

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.



System
Internet Protocol Security (IPSec)
Configure your IPSec connection properties:

Host Name or IP Address of Destination: 15.0.0.3
Gateway:
Remote IP: IP Subnet
Remote Subnet IP Address: 10.255.255.0
Remote Subnet Mask: 255.255.255.0
Shared Secret: MyKey

Back Next Cancel

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



System
Connection Summary
You have successfully completed the steps needed to create the following connection:

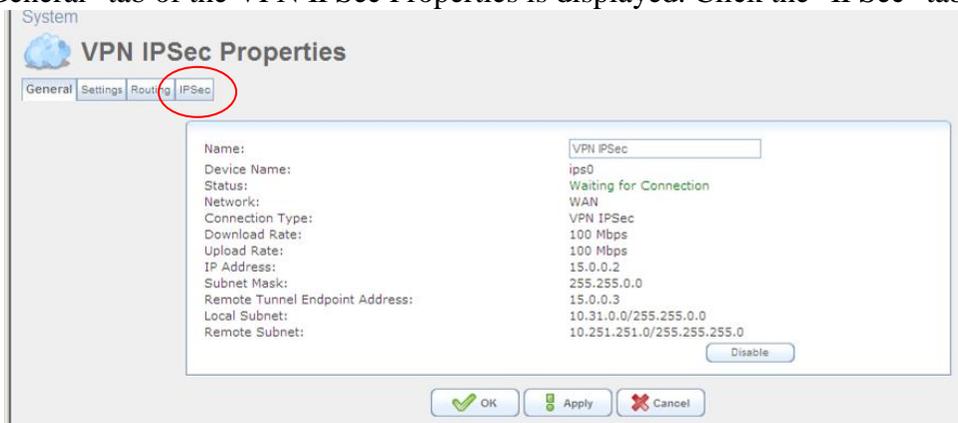
- IPSec connection with 15.0.0.3

Edit the Newly Created Connection

Press **Finish** to create the connection.

Back Finish Cancel

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



System
VPN IPSec Properties

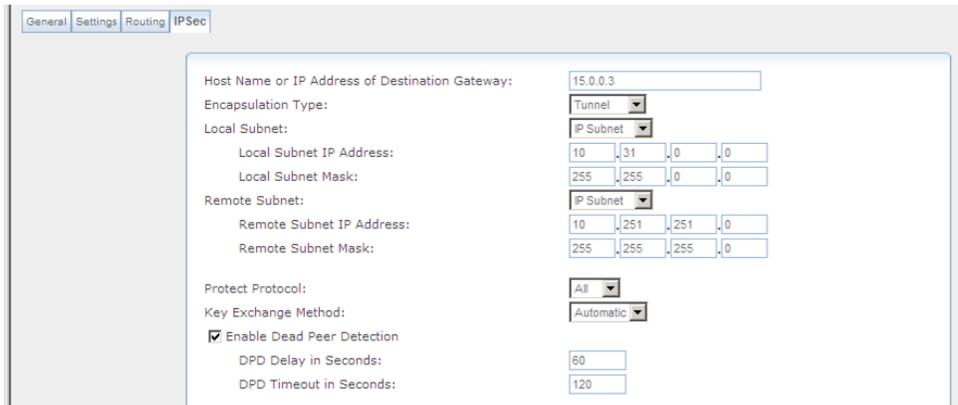
General Settings Routing **IPSec**

Name: VPN IPSec
Device Name: ips0
Status: Waiting for Connection
Network: WAN
Connection Type: VPN IPSec
Download Rate: 100 Mbps
Upload Rate: 100 Mbps
IP Address: 15.0.0.2
Subnet Mask: 255.255.0.0
Remote Tunnel Endpoint Address: 15.0.0.3
Local Subnet: 10.31.0.0/255.255.0.0
Remote Subnet: 10.251.251.0/255.255.255.0

Disable

OK Apply Cancel

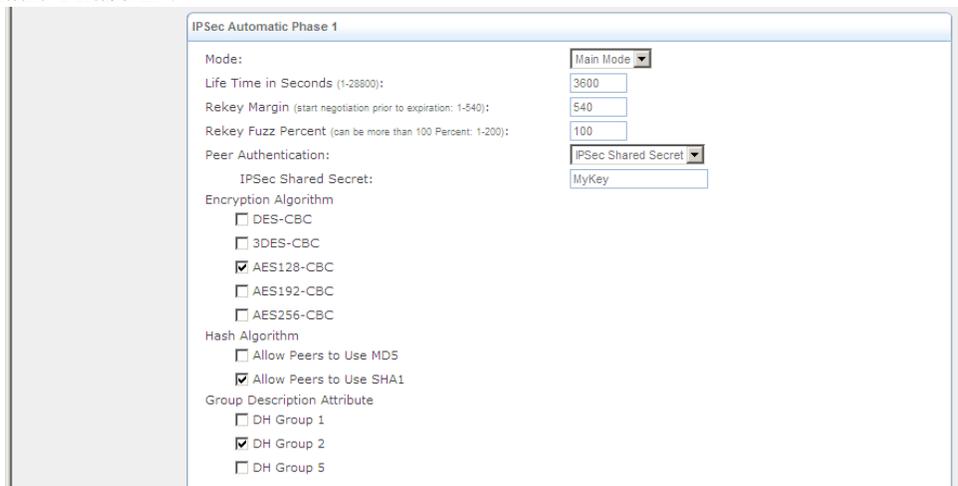
The "IPSec" tab of the VPN IPSec Connection is now displayed. Verify the desired settings and scroll down to "IPSec Automatic Phase 1".



The screenshot shows the "IPSec" configuration tab with the following settings:

- Host Name or IP Address of Destination Gateway: 15.0.0.3
- Encapsulation Type: Tunnel
- Local Subnet:
 - Local Subnet IP Address: 10.31.0.0
 - Local Subnet Mask: 255.255.0.0
- Remote Subnet:
 - Remote Subnet IP Address: 10.251.251.0
 - Remote Subnet Mask: 255.255.255.0
- Protect Protocol: All
- Key Exchange Method: Automatic
- Enable Dead Peer Detection
 - DPD Delay in Seconds: 60
 - DPD Timeout in Seconds: 120

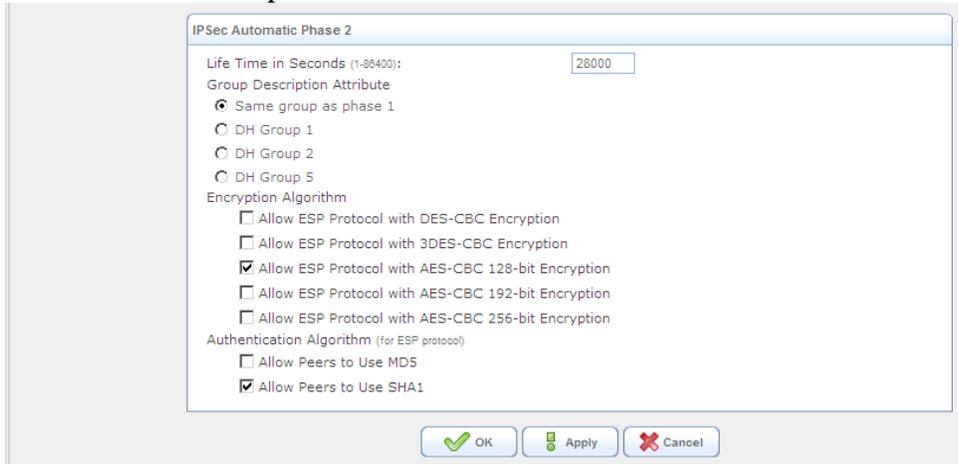
Verify the IPSec shared secret, check the options for encryption algorithm AES128-CBC, hash algorithm SHA1, DH group 2. Uncheck all other options, and scroll down to "IPSec Automatic Phase 2".



The screenshot shows the "IPSec Automatic Phase 1" configuration with the following settings:

- Mode: Main Mode
- Life Time in Seconds (1-28800): 3600
- Rekey Margin (start negotiation prior to expiration: 1-540): 540
- Rekey Fuzz Percent (can be more than 100 Percent: 1-200): 100
- Peer Authentication:
 - IPSec Shared Secret: MyKey
- Encryption Algorithm:
 - DES-CBC
 - 3DES-CBC
 - AES128-CBC
 - AES192-CBC
 - AES256-CBC
- Hash Algorithm:
 - Allow Peers to Use MD5
 - Allow Peers to Use SHA1
- Group Description Attribute:
 - DH Group 1
 - DH Group 2
 - DH Group 5

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



The image shows a configuration dialog box titled "IPSec Automatic Phase 2". It contains the following settings:

- Life Time in Seconds (1-86400): 28000
- Group Description Attribute:
 - Same group as phase 1
 - DH Group 1
 - DH Group 2
 - DH Group 5
- Encryption Algorithm:
 - Allow ESP Protocol with DES-CBC Encryption
 - Allow ESP Protocol with 3DES-CBC Encryption
 - Allow ESP Protocol with AES-CBC 128-bit Encryption
 - Allow ESP Protocol with AES-CBC 192-bit Encryption
 - Allow ESP Protocol with AES-CBC 256-bit Encryption
- Authentication Algorithm (for ESP protocol):
 - Allow Peers to Use MD5
 - Allow Peers to Use SHA1

At the bottom of the dialog box are three buttons: "OK" (with a green checkmark icon), "Apply" (with a green gear icon), and "Cancel" (with a red X icon).

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

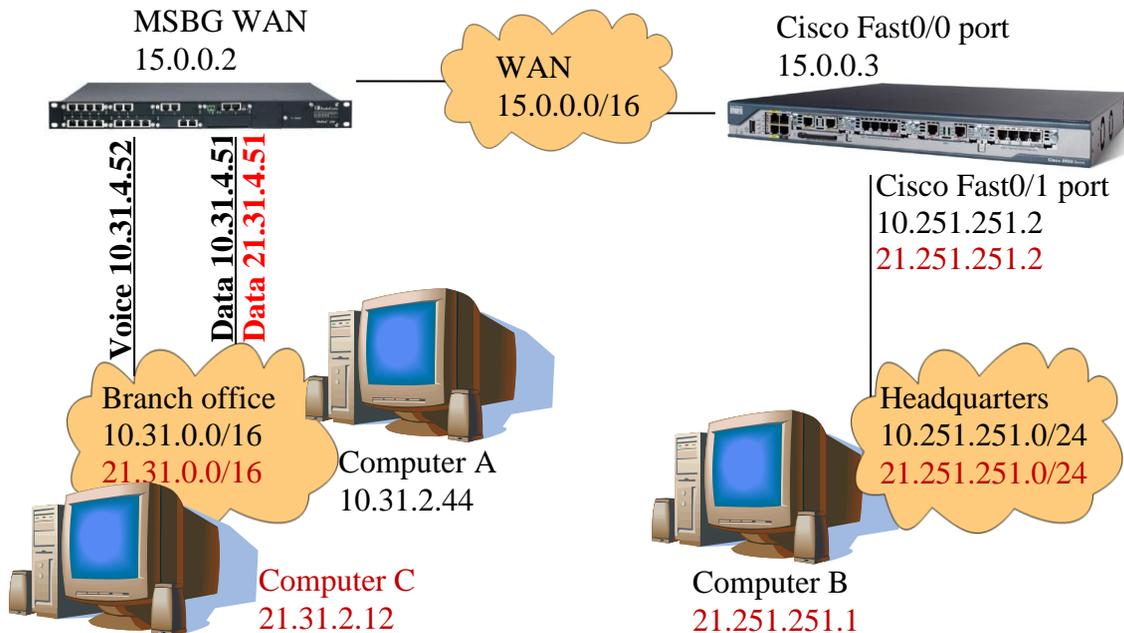
In this section, a more complex network topology is demonstrated. Both the branch office and headquarters now have multiple subnets in their network:

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.

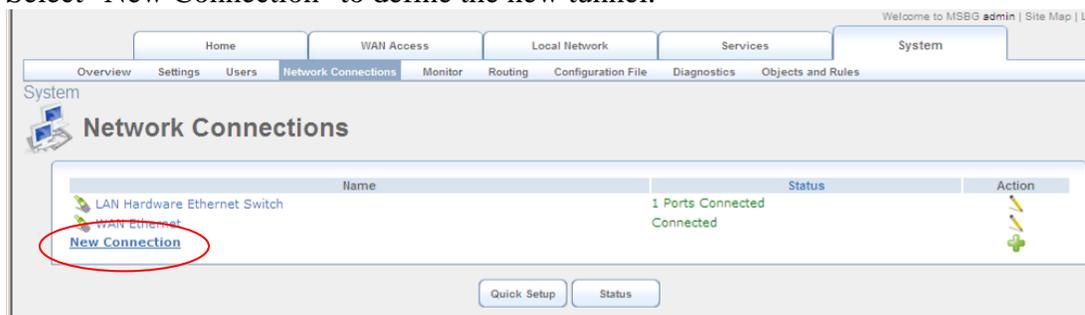
MSBG configuration screenshots - multiple subnets

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

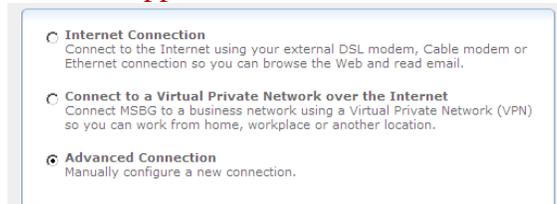
To configure the IPsec tunnel, navigate to the MSBG's web interface and click on "Data Home". New connections are added using the "System" main tab; click on "Network Connections".

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)

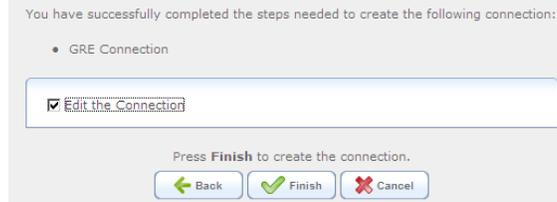


General Routing Encapsulation (GRE)
Configure your GRE connection properties:

Remote Endpoint IP Address:	16	0	0	1
Local Interface IP Address:	16	0	0	2
Remote Network IP Address:	10	251	251	0
Remote Subnet Mask:	255	255	255	0

Click Next.

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



You have successfully completed the steps needed to create the following connection:

- GRE Connection

Edit the Connection

Press **Finish** to create the connection.

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



WAN GRE Properties

General Settings **Routing** GRE Advanced

Name: WAN GRE

Device Name: gre1

Status: **Connected**

Network: WAN

Connection Type: GRE

IP Address: 16.0.0.2

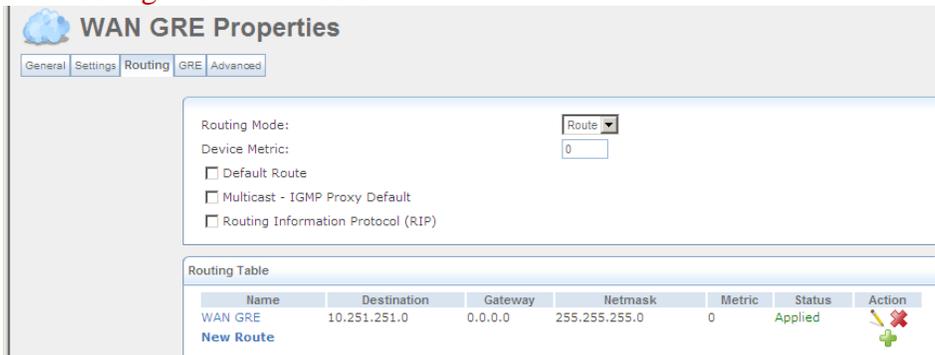
Received Packets: 0

Sent Packets: 0

Time Span: 0:00:00

Remote Endpoint IP Address: 16.0.0.1

Change the Routing Mode to "Route".



WAN GRE Properties

General Settings **Routing** GRE Advanced

Routing Mode: **Route**

Device Metric: 0

Default Route
 Multicast - IGMP Proxy Default
 Routing Information Protocol (RIP)

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
WAN GRE	10.251.251.0	0.0.0.0	255.255.255.0	0	Applied	

[New 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**

Destination:	21	251	251	.0
Netmask:	255	255	255	.0
Gateway:	0	0	0	.0
Metric:	0			

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



The dialog box shows the "Advanced" tab selected, indicated by a red circle around the tab label.

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



The "Internet Connection Firewall" checkbox is unchecked, with a red circle around the checkbox and the word "Enabled".

Click OK to return to the Network Connections page.

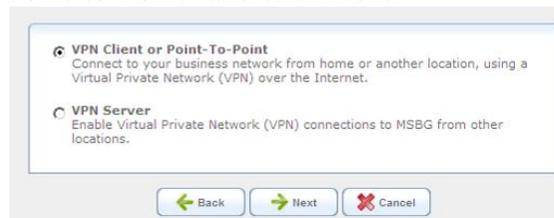
Press "New Connection" to add the IPSec tunnel.

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



The dialog box shows two options: "Internet Connection" and "Connect to a Virtual Private Network over the Internet". The second option is selected with a radio button.

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



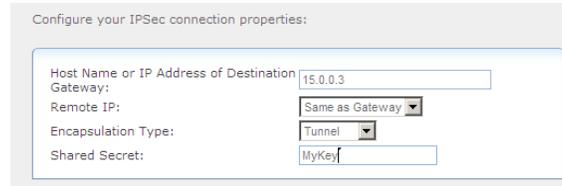
The dialog box shows two options: "VPN Client or Point-To-Point" and "VPN Server". The first option is selected with a radio button.

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



The dialog box shows three options: "Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)", "Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)", and "Internet Protocol Security (IPSec)". The third option is selected with a radio button.

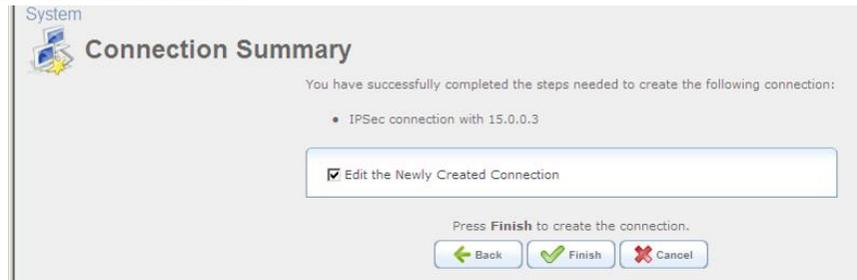
In the following dialog, fill in the IP address of the Cisco router's WAN interface (in our case, **15.0.0.3**). In "Remote IP", **select the option "Same as gateway"**. Type in a shared secret to be used for the connection, and click Next.



Configure your IPSec connection properties:

Host Name or IP Address of Destination Gateway:	15.0.0.3
Remote IP:	Same as Gateway
Encapsulation Type:	Tunnel
Shared Secret:	MyKey

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



System
Connection Summary

You have successfully completed the steps needed to create the following connection:

- IPSec connection with 15.0.0.3

Edit the Newly Created Connection

Press **Finish** to create the connection.

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



System
VPN IPSec Properties

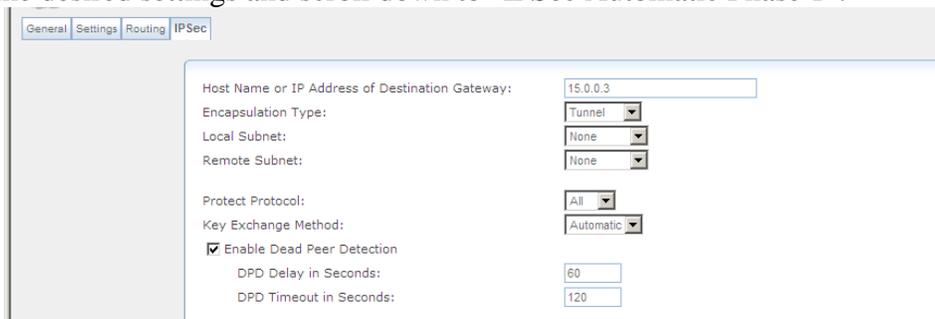
General Settings Routing **IPSec**

Name:	VPN IPSec
Device Name:	ips0
Status:	Waiting for Connection
Network:	WAN
Connection Type:	VPN IPSec
Download Rate:	100 Mbps
Upload Rate:	100 Mbps
IP Address:	15.0.0.2
Subnet Mask:	255.255.0.0
Remote Tunnel Endpoint Address:	15.0.0.3
Local Subnet:	10.31.0.0/255.255.0.0
Remote Subnet:	10.251.251.0/255.255.255.0

The "IPSec" tab of the VPN IPSec Connection is now displayed.

Set the "Local Subnet" option to "None".

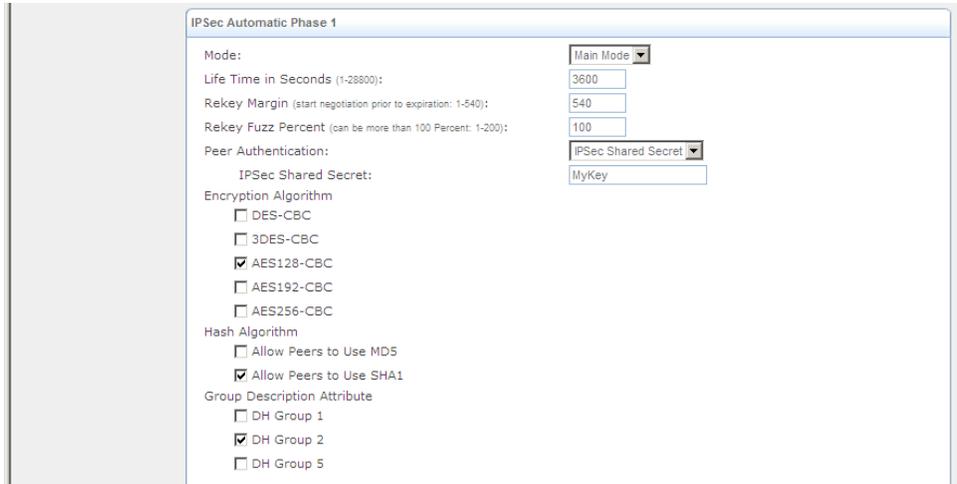
Verify the desired settings and scroll down to "IPSec Automatic Phase 1".



General Settings Routing **IPSec**

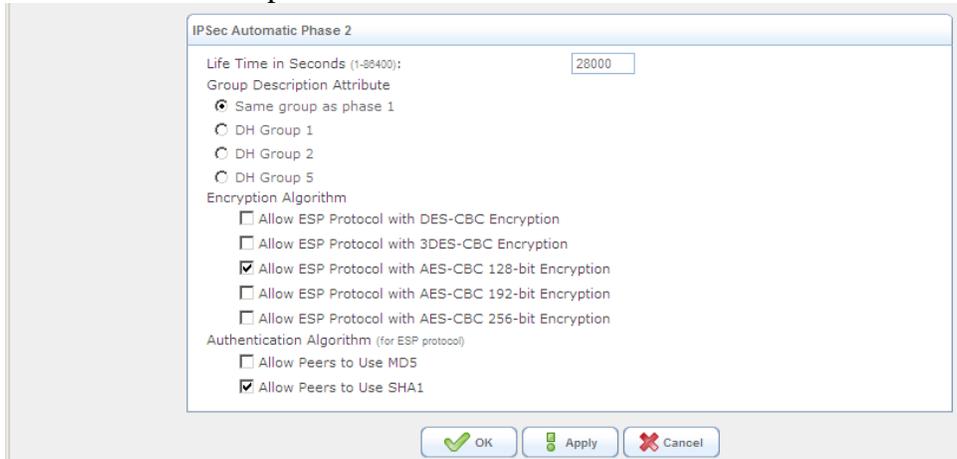
Host Name or IP Address of Destination Gateway:	15.0.0.3
Encapsulation Type:	Tunnel
Local Subnet:	None
Remote Subnet:	None
Protect Protocol:	All
Key Exchange Method:	Automatic
<input checked="" type="checkbox"/> Enable Dead Peer Detection	
DPD Delay in Seconds:	60
DPD Timeout in Seconds:	120

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".



The screenshot shows the "IPsec Automatic Phase 1" configuration window. The "Mode" is set to "Main Mode". The "Life Time in Seconds" is 3600, "Rekey Margin" is 540, and "Rekey Fuzz Percent" is 100. The "Peer Authentication" is set to "IPsec Shared Secret" with the secret "MyKey". Under "Encryption Algorithm", "AES128-CBC" is checked. Under "Hash Algorithm", "Allow Peers to Use SHA1" is checked. Under "Group Description Attribute", "DH Group 2" is checked. All other options are unchecked.

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



The screenshot shows the "IPsec Automatic Phase 2" configuration window. The "Life Time in Seconds" is 28000. Under "Group Description Attribute", "Same group as phase 1" is selected. Under "Encryption Algorithm", "Allow ESP Protocol with AES-CBC 128-bit Encryption" is checked. Under "Authentication Algorithm (for ESP protocol)", "Allow Peers to Use SHA1" is checked. All other options are unchecked. At the bottom, there are "OK", "Apply", and "Cancel" buttons.

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.