

# Tech Tip

## Contivity Secure IP Services Gateway



### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

---

#### Contents

Contents .....	1
Overview .....	1
Sample Configuration .....	2
Setup .....	2
Configuring WS1 .....	2
Configuring WS2 .....	3
Configuring CES.....	3
Configuring network parameters.....	3
Configuring Branch Office connection .....	4
Configuring Branch Office IPSec parameters.....	12
Configuring BCM .....	15
Configuring Interfaces.....	15
Configuring Branch Office tunnel parameters.....	17
Configuring local and remote accessible networks .....	21
Verifying firewall rules .....	24
Enabling IPSec .....	25
Event Log .....	26

#### Overview

This technical tip illustrates a sample IPSec peer-to-peer tunnel configuration between Contivity Secure IP Services Gateway and Business Communication Manager (BCM) using pre-shared key authentication.

# Tech Tip

## Contivity Secure IP Services Gateway

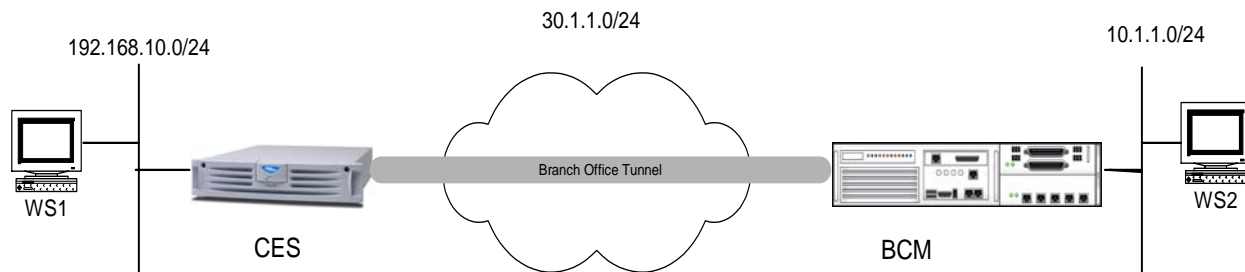


### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

---

#### Sample Configuration

##### Setup



**WS1** – Windows 2000 workstation, IP 192.168.10.11/24;

**WS2** - Windows 2000 workstation, IP 10.1.1.10/24;

**CES** – Contivity Secure IP Services Gateway, code version V04\_85, management IP 192.168.10.1/24, private IP 192.168.10.2/24, public IP 30.1.1.2/24

**BCM** – Business Communication Manager, Private IP (LAN 1) 10.1.1.1/24, public IP (LAN 2) 30.1.1.1/24.

The goal of the configuration is to set up an IPSec peer-to-peer branch office tunnel between a CES and a BCM using 3DES with MD5 integrity and a pre-shared key authentication.

#### Configuring WS1

Configure the IP address (192.168.10.11/24) on the WS1 and the CES private interface (192.168.10.2) as the default gateway:

```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.10.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.2
```

# Tech Tip

## Contivity Secure IP Services Gateway

### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

#### Configuring WS2

Configure the IP address (10.1.1.10/24) on the WS2 and the NG private interface (10.1.1.1) as a default gateway:

```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 10.1.1.10
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 10.1.1.1
```

#### Configuring CES

##### Configuring network parameters

Configure IP address for management (192.268.10.1/24), private (192.168.10.2/24) and public (30.1.1.2/24) interfaces:

The screenshot shows a web browser window titled "192.168.10.1 - Contivity Extranet Switch - Microsoft Internet Explorer". The address bar shows "http://192.168.10.1/manage/manager.htm". The interface has a dark blue header with "LAN Interfaces" and "HELP LOGOFF" buttons. A left sidebar contains a menu with "SYSTEM", "SERVICES", "ROUTING", "QOS", "PROFILES", "SERVERS", "ADMIN", "STATUS", and "HELP". Under "ROUTING", "LAN" is selected. The main content area displays two tables for LAN interfaces.

Interface	Description	State	Type	Actions
Fast Ethernet		Enabled	Private	Configure Statistics

IP Address	Subnet Mask	Interface Filter	Actions
192.168.10.2	255.255.255.0	permit all (Contivity Interface Filter in use)	Edit Delete

Interface	Description	State	Type	Actions
Slot 1 Interface 1		Enabled	Public	Configure Statistics

IP Address	Subnet Mask	Interface Filter	Actions
30.1.1.2	255.255.255.0	permit all (Contivity Interface Filter in use)	Edit Delete

In this configuration CES and BCM are directly connected, if a router is used between CES and BCM a public default gateway must be configured on **Routing→Static Routes** screen by clicking **Add Public Route** and specifying the address of a public default router.

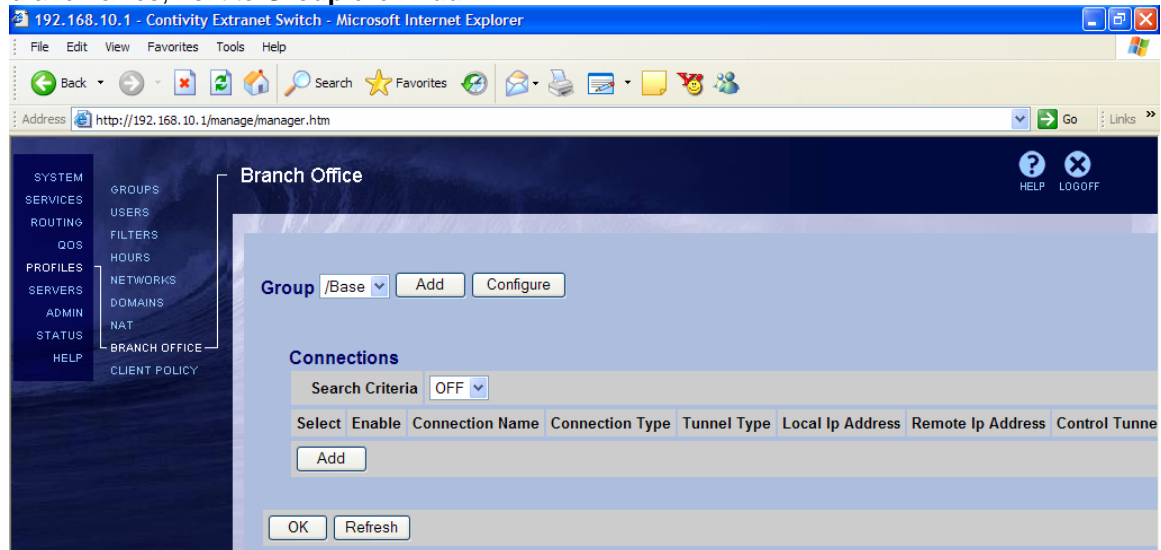
# Tech Tip

## Contivity Secure IP Services Gateway

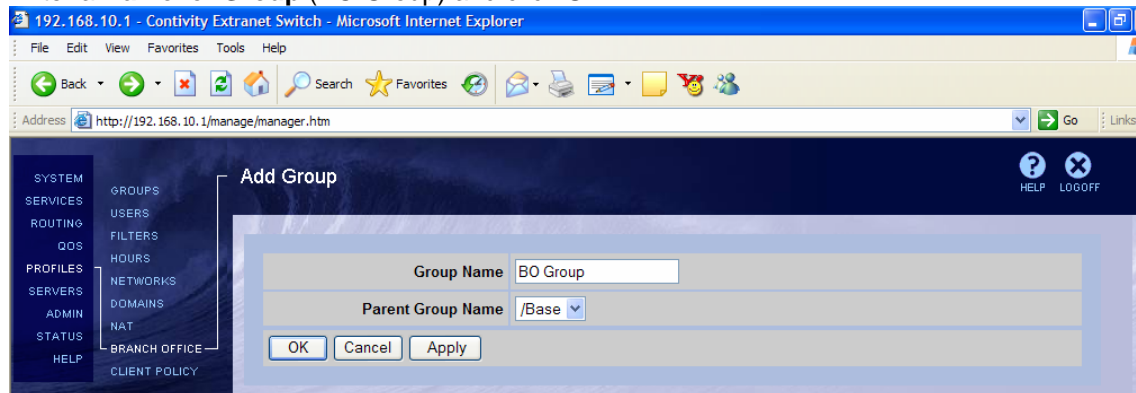
### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

#### Configuring Branch Office connection

Configure the BO connection. Navigate **Profiles → Branch Office**. To add a new group for the branch office, next to **Group** click **Add**:



Enter a **Name** for **Group** (BO Group) and click **OK**:

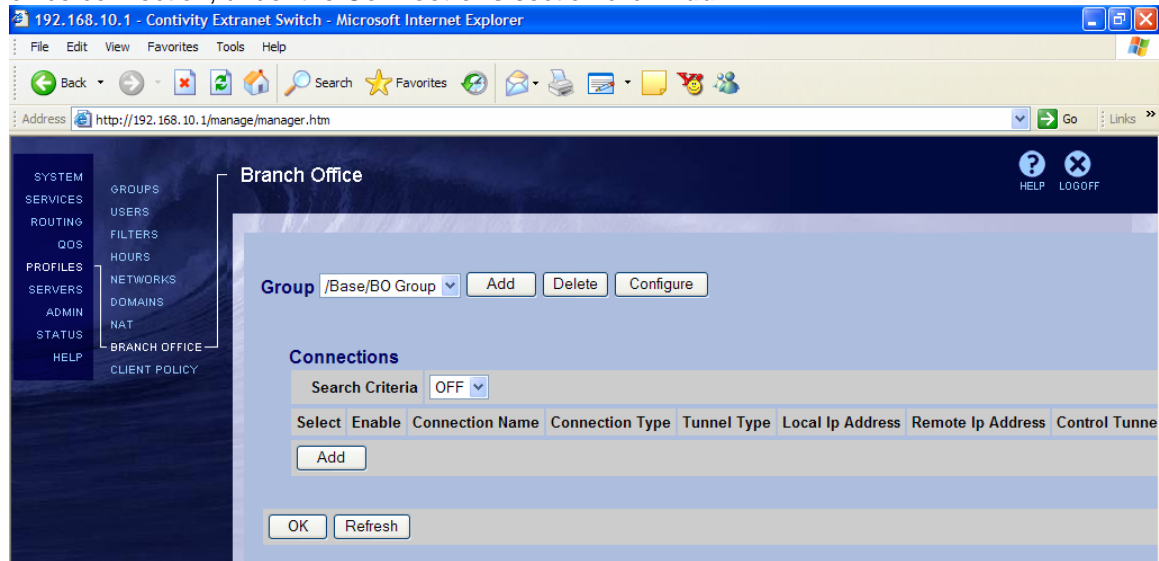


# Tech Tip

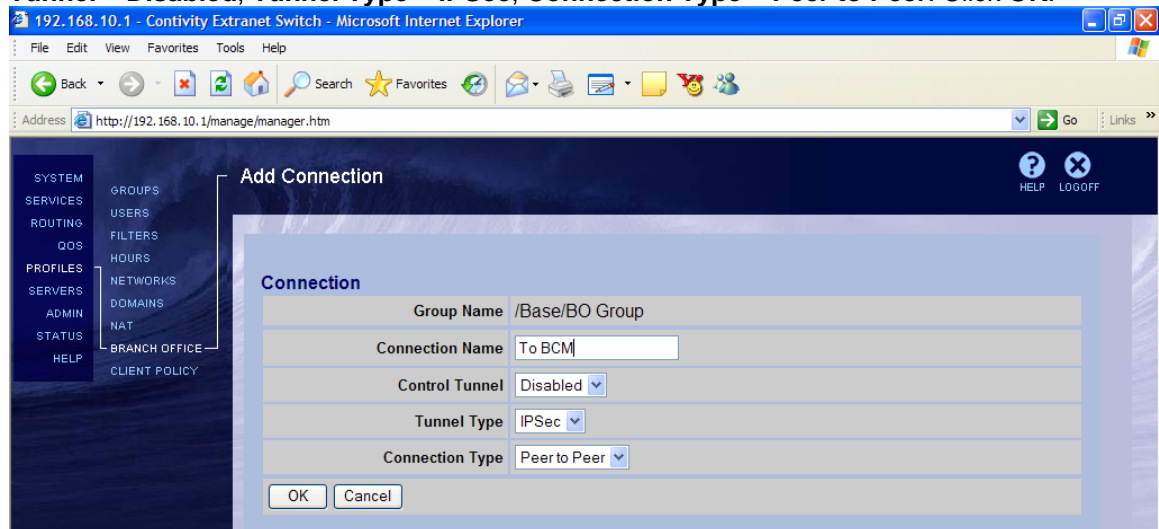
## Contivity Secure IP Services Gateway

### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

From the drop down menu next to **Group**, select the newly created group. To add a new branch office connection, under the **Connections** section click **Add**:



Enter a **Connection Name** (To BCM), leave the rest of the fields to their defaults – **Control Tunnel – Disabled, Tunnel Type – IPSec, Connection Type – Peer to Peer**. Click **OK**:



## Tech Tip

### Contivity Secure IP Services Gateway



## Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

---

The **Connection Configuration** screen appears. Select the **Enable** option:

Connection	
Group Name	/Base/BO Group
Connection Name	To BCM
Control Tunnel	Disabled
Tunnel Type	IPSec
Connection Type	Peer to Peer
Enable	<input checked="" type="checkbox"/>

Select CES public IP address (30.1.1.2) as the **Local Endpoint IP Address**;  
Enter BCM public IP address (30.1.1.1) as the **Remote Endpoint IP Address**:

Endpoints	
Local Ip Address	30.1.1.2
Remote Ip Address	30.1.1.1

Leave the **Filter** at **Permit All**:

Filters	
Filter	permit all

For **Authentication** select the **Text Pre-Shared Key** (selected by default):

Authentication	
Text Pre-Shared Key	<input type="button" value="Text Pre-Shared Key"/>

Enter a **Text Pre-Shared Key** – 12345 in this case:

Authentication	
Text Pre-Shared Key	<input type="button" value="Text Pre-Shared Key"/>
Text Pre-Shared Key	*****
Confirm	*****

# Tech Tip

## Contivity Secure IP Services Gateway

### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

---

Leave **MTU** at the default setting:

<b>MTU</b>	
<b>Tunnel MTU</b>	Enable ▾
<b>MTU Value</b>	1788

No NAT will be used in this example, leave the default **(None)** selection for **NAT**:

<b>NAT</b>	
<b>NAT</b>	(None) ▾

For the **IP Configuration** select **Static**:

<b>IP Configuration</b>	Static ▾
-------------------------	----------

Define local accessible networks. Next to **Local Network** select **Create Local Network**:

<b>Local Networks</b>	
<b>Local Network</b>	(None) ▾ <input type="button" value="Create Local Network"/>

The **Networks** screen appears. Enter the name of the network (local 192.168.10.0) to be created and click **Create**:

192.168.10.1 - Contivity Extranet Switch - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites RSS Feeds

Address http://192.168.10.1/manage/manager.htm Go Links

**Networks**

Return to Connection Configuration

**Current Networks**  
(No networks defined)

Local 192.168.10.0

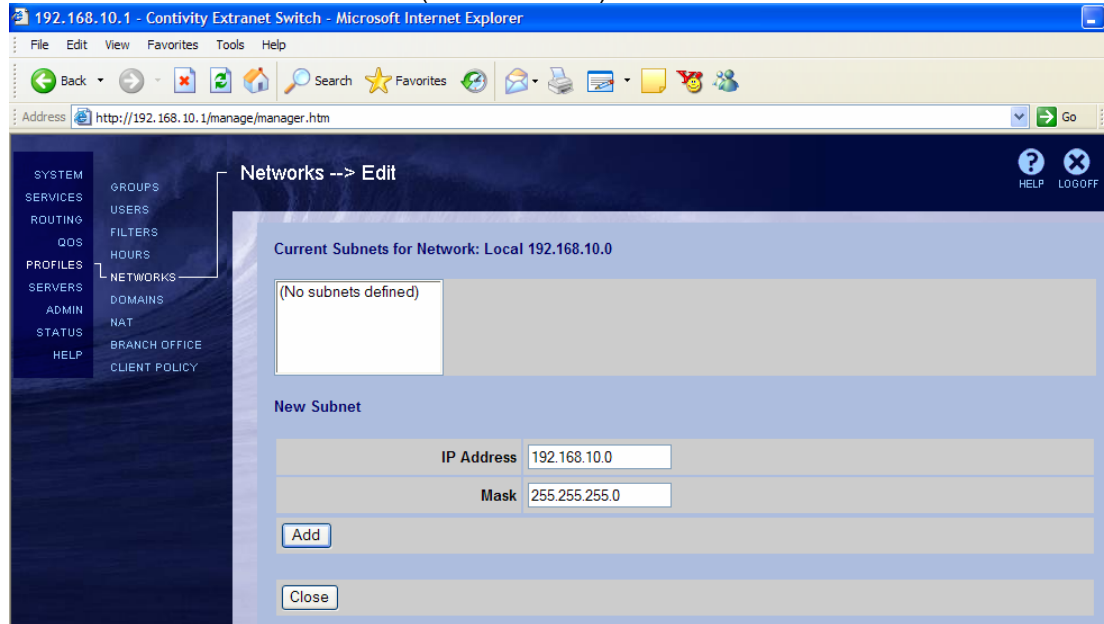
Enter new Network name and press create

# Tech Tip

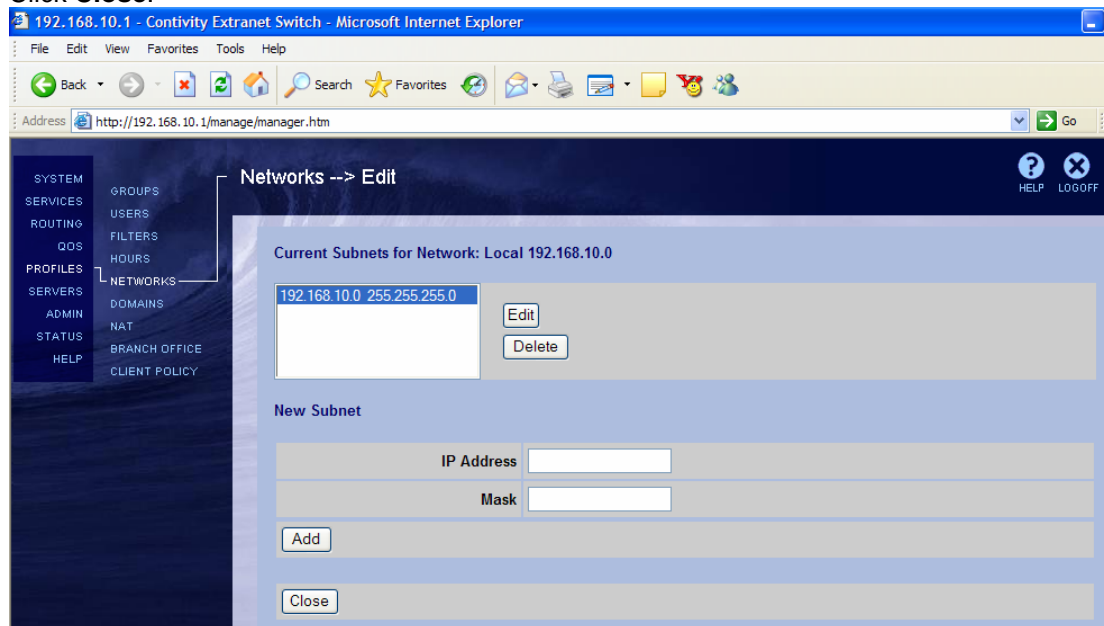
## Contivity Secure IP Services Gateway

### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

Enter the IP address of the **Local Accessible Network** (CES private network, 192.168.10.0), **Mask** associated with the address (255.255.255.0) and click **Add**:



Listed under the **Current Subnets for Network** window is the configured subnet for the network. Click **Close**:



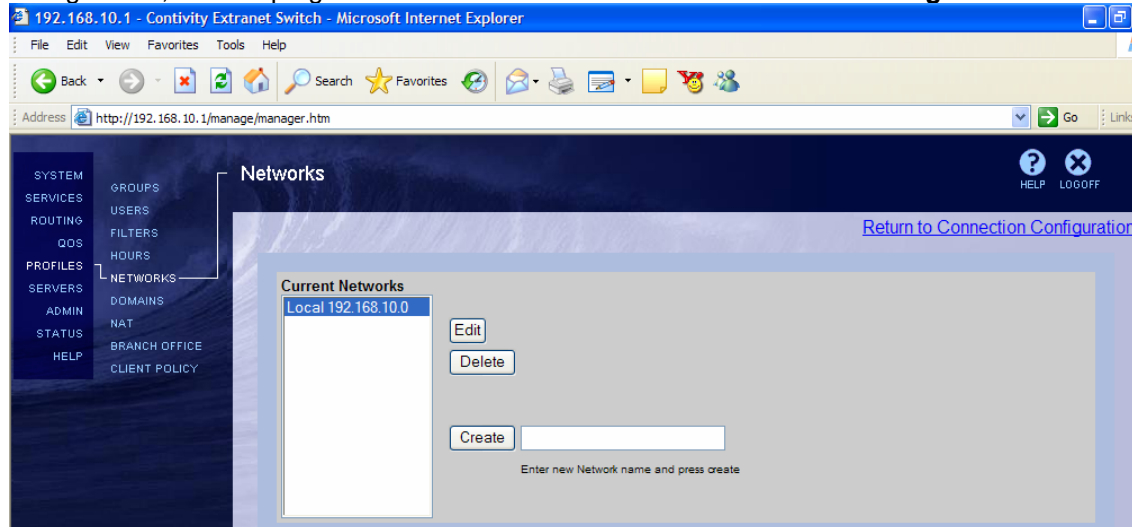


# Tech Tip

## Contivity Secure IP Services Gateway

### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

Listed under the **Current Networks** is the configured network. To return to the branch office configuration, in the top right corner click on the **Return to Connection Configuration** link:



From the drop-down list next to **Local Network** select the **newly configured local network** (local 192.168.10.0):

**Local Networks**

Local Network: (None)

Local 192.168.10.0

(None)

**Remote Networks**

Select	IP Address	IP Mask	Cost	Enabled
<input type="button" value="Add"/>				

Define the remote accessible networks. Under the **Remote Networks** click **Add**:

**Remote Networks**

Select	IP Address	IP Mask	Cost	Enabled
<input type="button" value="Add"/>				

# Tech Tip

## Contivity Secure IP Services Gateway

### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

The **Add Remote Network** screen appears. Enter the **IP Address** of the Remote Network (BCM private network LAN 1 (10.1.1.0), and **Mask** (255.255.255.0). Leave the **Cost** to its default. Select **Enabled** and click **OK**:

192.168.10.1 - Contivity Extranet Switch - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Print Mail News RSS Feeds

Address http://192.168.10.1/manage/manager.htm Go Links

SYSTEM SERVICES ROUTING QOS PROFILES SERVERS ADMIN STATUS HELP

GROUPS USERS FILTERS HOURS NETWORKS DOMAINS NAT BRANCH OFFICE CLIENT POLICY

HELP LOGOFF

### Add Remote Network

**Connection**

Group Name /Base/BO Group

Connection Name To BCM

**Remote Network**

IP Address 10.1.1.0

IP Mask 255.255.255.0

Cost 10

Enabled ☒

OK Cancel Apply

Listed under the **Remote Networks** tab is the configured remote network:

Remote Networks				
Select	IP Address	IP Mask	Cost	Enabled
<input checked="" type="radio"/>	10.1.1.0	255.255.255.0	10	<input checked="" type="checkbox"/>
Add Configure Delete				

# Tech Tip

## Contivity Secure IP Services Gateway



### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

Once all the parameters have been set, at the bottom of the screen click **OK**:

The screenshot shows the 'Connection Configuration' page in the Contivity Extranet Switch management interface. The browser address bar shows 'http://192.168.10.1/manage/manager.htm'. The left sidebar contains a navigation menu with options like SYSTEM, SERVICES, ROUTING, QOS, PROFILES, SERVERS, ADMIN, STATUS, and HELP. The main content area is titled 'Connection Configuration' and includes a 'HELP' and 'LOGOFF' link.

**Connection Configuration**

**Connection**

Group Name	/Base/BO Group
Connection Name	To BCM
Control Tunnel	Disabled
Tunnel Type	IPSec
Connection Type	Peer to Peer
Enable	<input checked="" type="checkbox"/>

**Endpoints**

Local Ip Address	30.1.1.2
Remote Ip Address	30.1.1.1

**Filters**

Filter	permit all
--------	------------

**Authentication** Text Pre-Shared Key

Text Pre-Shared Key	.....	Confirm	.....
---------------------	-------	---------	-------

**MTU Value** 1788

**NAT**

NAT	(None)
-----	--------

**IP Configuration** Static

**Local Networks**

Local Network	IP Address	IP Mask	Cost	Enabled
Local 192.168.1.0	192.168.1.0	255.255.255.0	10	TRUE

**Remote Networks**

Select	IP Address	IP Mask	Cost	Enabled
<input checked="" type="radio"/>	10.1.1.0	255.255.255.0	10	<input checked="" type="checkbox"/>

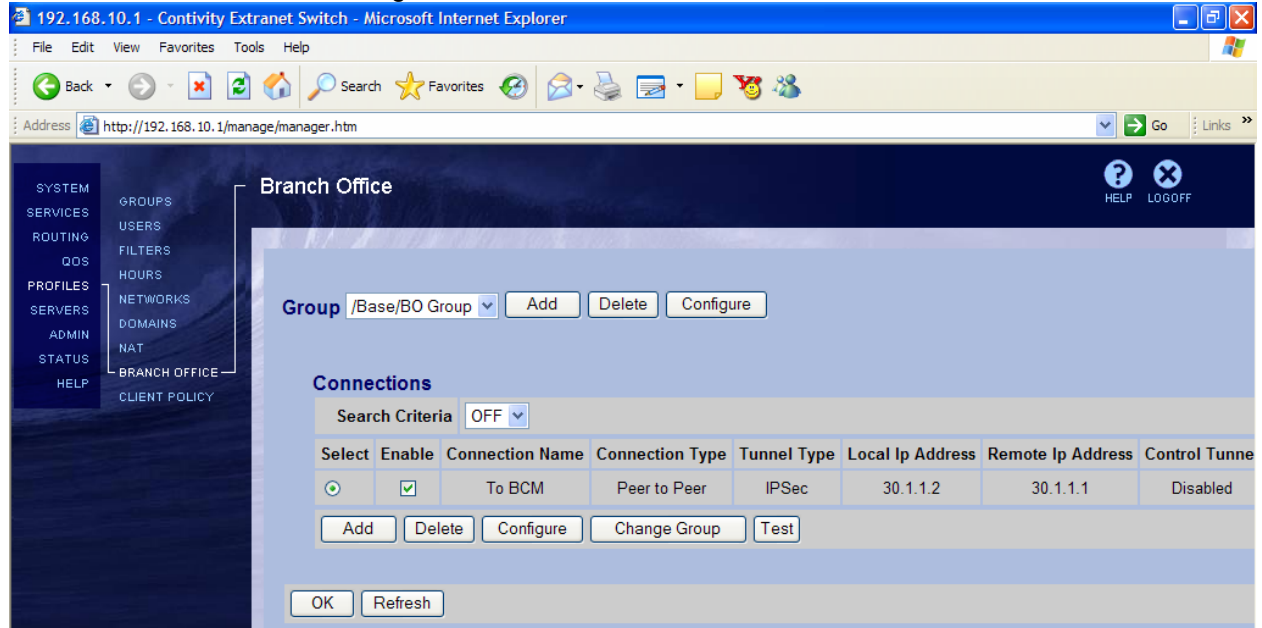
Buttons: Add, Configure, Delete, OK, Cancel, Apply, Refresh

# Tech Tip

## Contivity Secure IP Services Gateway

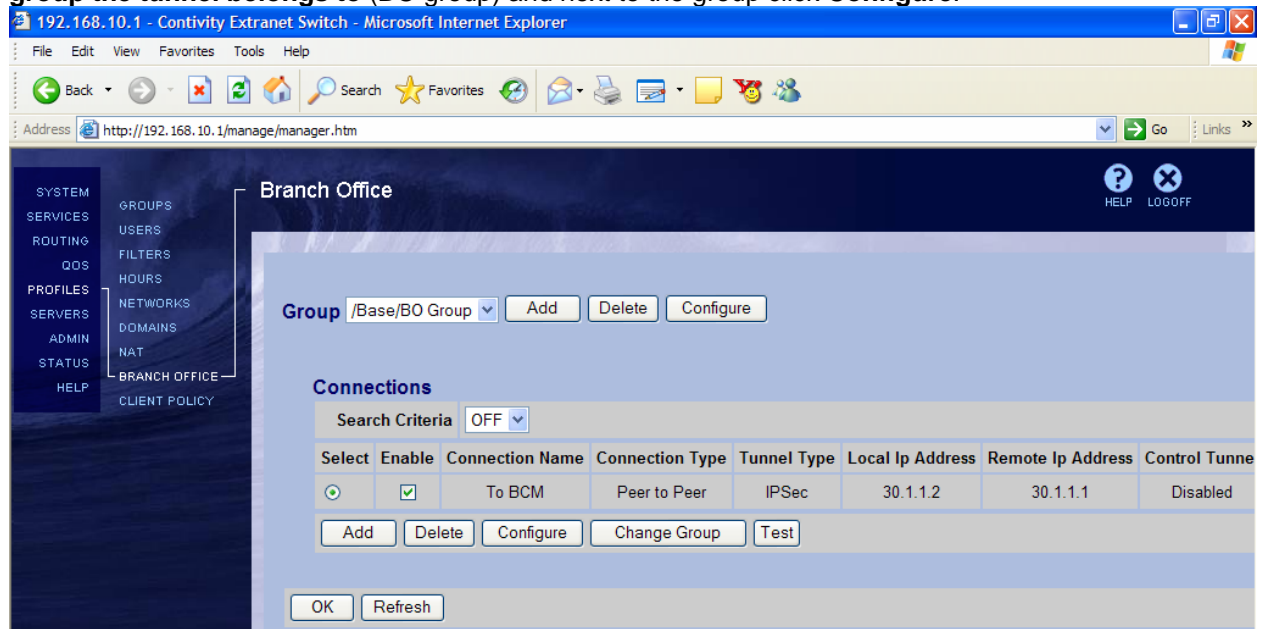
### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

Branch office connection is configured:



### Configuring Branch Office IPSec parameters

Navigate **Profiles → Branch Office** to configure branch office IPSec parameters. Select the **group the tunnel belongs to (BO group)** and next to the group click **Configure**:

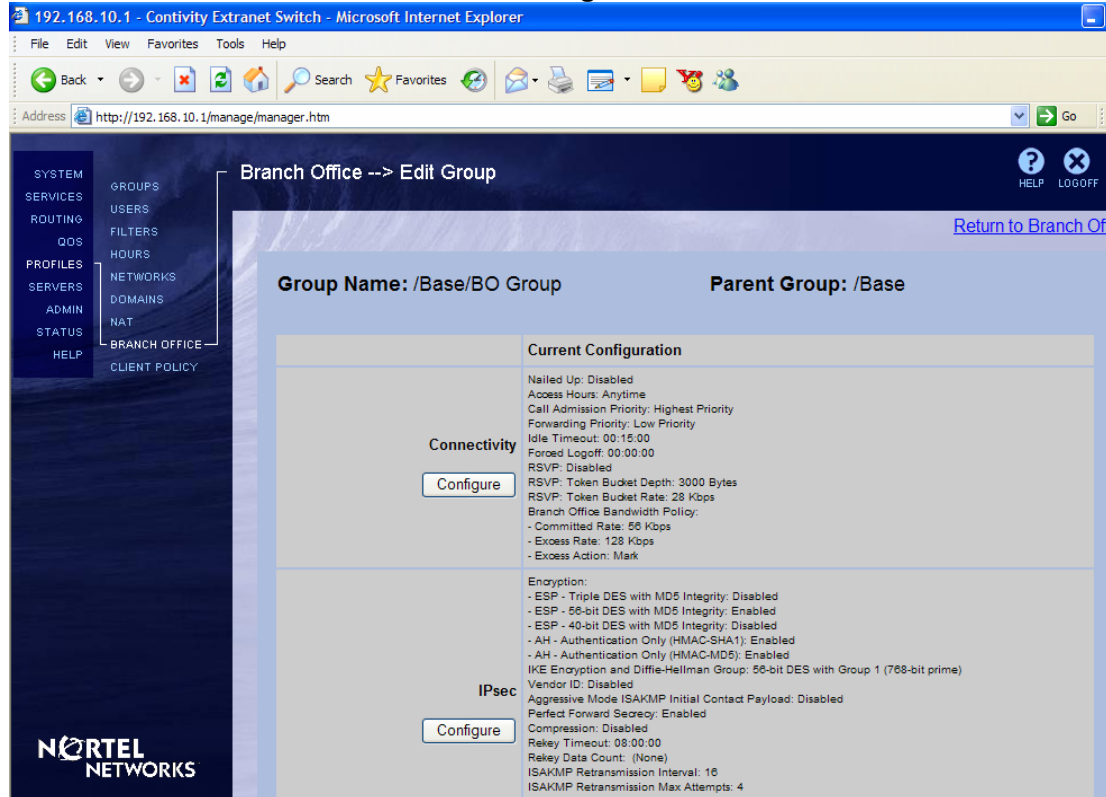


# Tech Tip

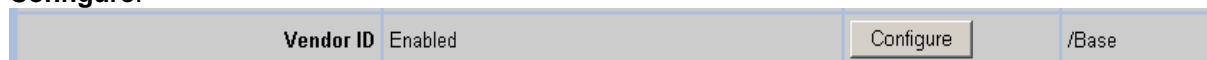
## Contivity Secure IP Services Gateway

### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

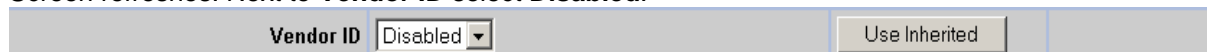
Scroll down to the **IPSec** section and click **Configure**:



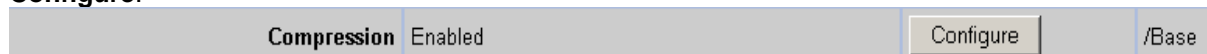
To interoperate with the BCM, **Vendor ID** must be disabled for the group. Next to **Vendor ID** click **Configure**:



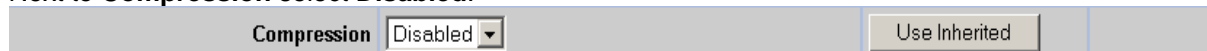
Screen refreshes. Next to **Vendor ID** select **Disabled**:



Compression also needs to be disabled to interoperate with BCM. Next to **Compression** select **Configure**:



Next to **Compression** select **Disabled**:



# Tech Tip

## Contivity Secure IP Services Gateway

### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

Once all the parameters have been set, at the bottom of the screen select **OK**:

192.168.10.1 - Contivity Extranet Switch - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Go Links

Address http://192.168.10.1/manage/manager.htm

SYSTEM SERVICES ROUTING QOS PROFILES SERVERS ADMIN STATUS HELP

GROUPS USERS FILTERS HOURS NETWORKS DOMAINS NAT

BRANCH OFFICE CLIENT POLICY

Branch Office

HELP LOGOFF

IKE Encryption and Diffie-Hellman Group 56-bit DES with Group 1 (768-bit prime)

Vendor ID Disabled

Aggressive Mode ISAKMP Initial Contact Payload Disabled

Perfect Forward Secrecy Enabled

Compression Disabled

Rekey Timeout 08:00:00

Rekey Data Count 0 Kb

ISAKMP Retransmission Interval 16

ISAKMP Retransmission Max Attempts 4 (Range 0 - 10)

Keepalive interval 00:01:00

Keepalive (On-Demand connections) Disabled

Anti Replay Enabled

IPsec DFBit Clear

OK Cancel

The Contivity gateway is now configured.

# Tech Tip

## Contivity Secure IP Services Gateway

### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

---

#### Configuring BCM

##### Configuring Interfaces

Log into the BCM **Unified Manager**. On the navigation Tree, expand the **Resources** key and then the **LAN** key. Click on **LAN 1**. This is the Private Interface. Enter IP 10.1.1.1 with a mask of 255.255.255.0:

<https://10.1.1.1> - Business Communications Manager - Unified Manager - Microsoft Internet Explorer

The screenshot displays the BCM Unified Manager web interface. On the left, a navigation tree under the 'Resources' section shows 'LAN' expanded, with 'LAN1' selected. The main panel is titled '[10.1.1.1] Comprehensive' and contains two tabs: 'LAN Summary' (active) and 'Additional IP Address'. The 'LAN Summary' tab shows the following configuration details:

- IPAddress: 10.1.1.1
- SubNet Mask: 255.255.255.0
- Physical Address: 00-00-50-0E-C2-60
- Description: 10/100 Base T Ethernet NIC
- Version: 4.52
- Speed: 100000000
- Duplex Type: Half Duplex
- Connection Type: Auto Sense (dropdown)
- Status: Up (dropdown)
- Admin Status: Up (dropdown)
- Primary Wins Address: (empty field)
- Secondary Wins Address: (empty field)

The status bar at the bottom of the browser window indicates 'Ready ...'.

# Tech Tip

## Contivity Secure IP Services Gateway

### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

Click on **LAN 2**. This is the Public Interface. Enter IP 30.1.1.1 with a mask of 255.255.255.0:

<https://10.1.1.1> - Business Communications Manager - Unified Manager - Microsoft Internet Explorer

The screenshot displays the Contivity configuration web interface. On the left, a tree view under 'System' shows 'Resources' expanded, with 'LAN' selected and 'LAN2' highlighted. The main panel shows the 'LAN Summary' configuration for LAN2. The IP Address is set to 30.1.1.1, SubNet Mask to 255.255.255.0, and Physical Address to 00-00-50-0E-C2-5E. The Description is '10/100 Base T Ethernet NIC'. Other settings include Version 4.52, Speed 100000000, Duplex Type Half Duplex, Connection Type Auto Sense, Status Up, and Admin Status Up. The Primary and Secondary Wins Address fields are empty.

Field	Value
IPAddress	30.1.1.1 (Format 255.255.255.255)
SubNet Mask	255.255.255.0
Physical Address	00-00-50-0E-C2-5E
Description	10/100 Base T Ethernet NIC
Version	4.52
Speed	100000000
Duplex Type	Half Duplex
Connection Type	Auto Sense
Status	Up
Admin Status	Up
Primary Wins Address	
Secondary Wins Address	



# Tech Tip

## Contivity Secure IP Services Gateway

### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

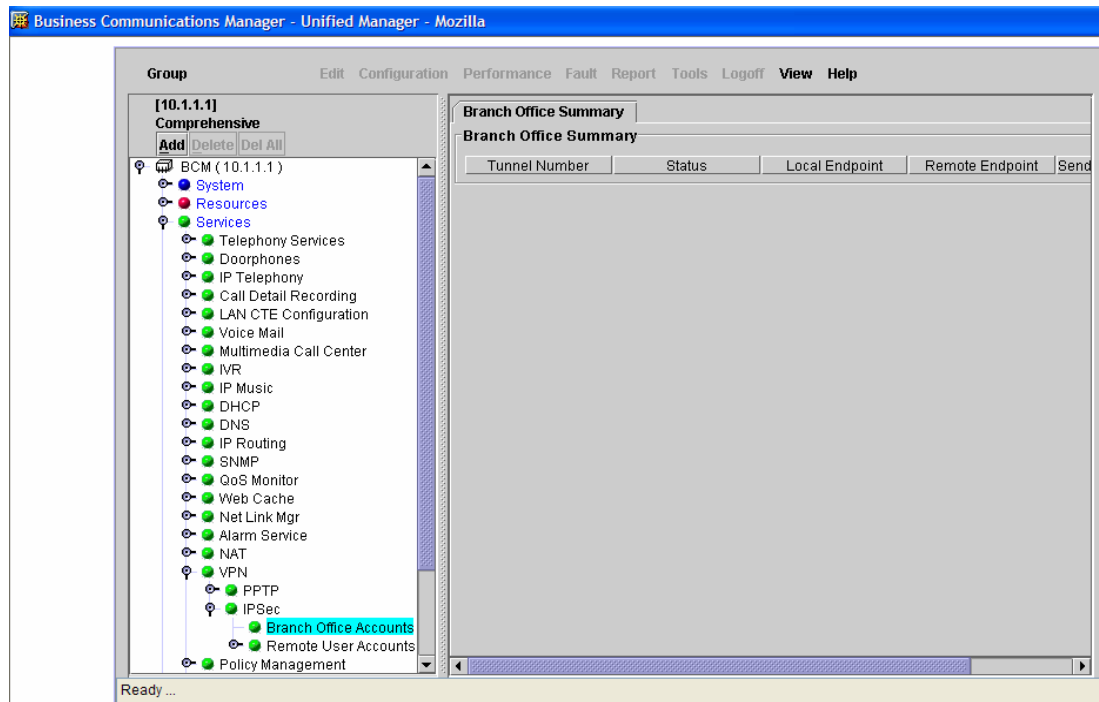
---

#### Configuring Branch Office tunnel parameters

On the navigation tree, expand the **Services** key, expand the **VPN** key, and expand the **IPSec** key.

This will show two options, **Branch Office Accounts** and **Remote User Accounts**.

Click on the **Branch Office Accounts**. This will enable the **'Add'** button under the heading **Comprehensive**.

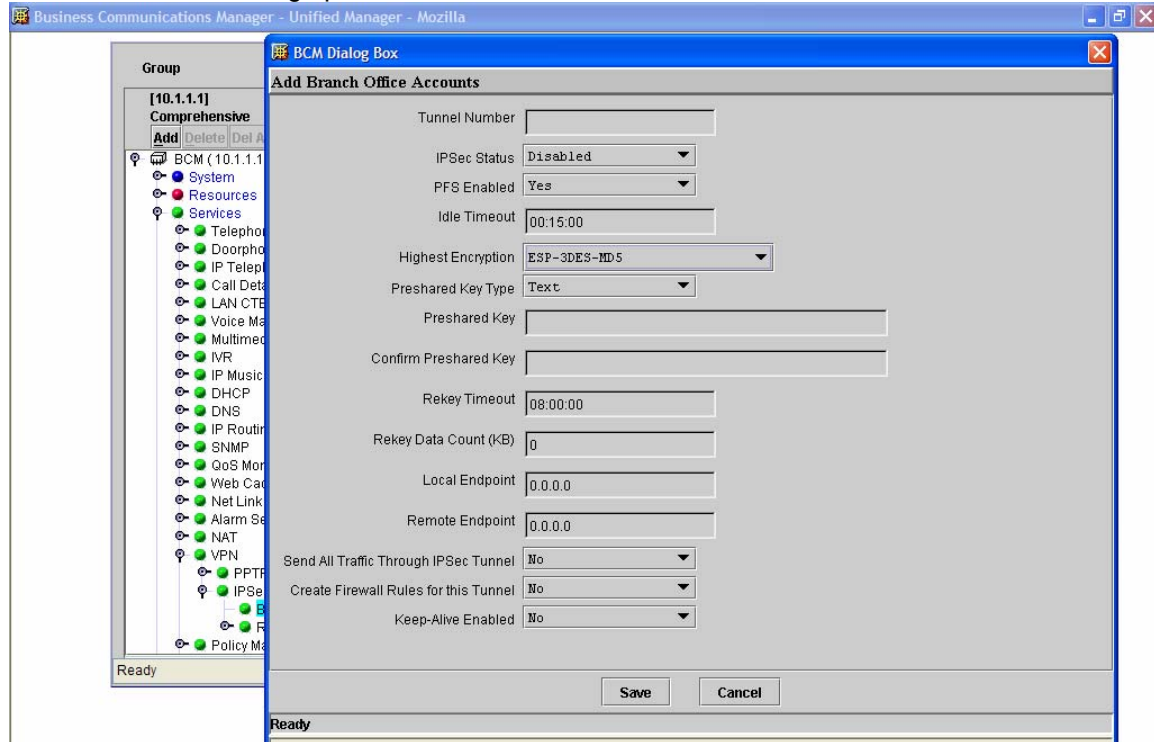


# Tech Tip

## Contivity Secure IP Services Gateway

### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

Click **Add**. This will bring up the **Add Branch Office Accounts** window:



Fill out the “Add Branch Office Accounts” window as follows:

Enter the **Tunnel Number**, T1:

Tunnel Number

Set the **IPSec Status** to **Enabled**:

IPSec Status

Leave **PFS Enabled** (Perfect Forward Secrecy) as **Yes**:

PFS Enabled

Leave the **Idle Timeout** as the default value:

Idle Timeout

## Tech Tip

### Contivity Secure IP Services Gateway



#### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

---

Set the **Highest Encryption** as desired and make sure it matches the Contivity setting. We will set it to **ESP-3DES-MD5** as decided. This setting is enabled by default on the Contivity:

Highest Encryption	ESP-3DES-MD5
--------------------	--------------

Set the **Key Type** to **Text**.

Preshared Key Type	Text
--------------------	------

Set the **Pre-shared Key** to **12345** and confirm it to match the key entered in Contivity configuration:

Preshared Key	*****
Confirm Preshared Key	*****

Leave the **Rekey Timeout** as the default value:

Rekey Timeout	08:00:00
---------------	----------

Leave the **Rekey Data Count(KB)** at **0**. We are not using this for this setup:

Rekey Data Count (KB)	0
-----------------------	---

Set the **Local Endpoint** to **30.1.1.1- LAN 2 IP Address of the BCM (Public)**:

Local Endpoint	30.1.1.1
----------------	----------

Set the **Remote Endpoint** to **30.1.1.2 - Public IP address of the Contivity**:

Remote Endpoint	30.1.1.2
-----------------	----------

Leave the **Send All Traffic Through IPSec Tunnel** to default of **No**:

Send All Traffic Through IPSec Tunnel	No
---------------------------------------	----

# Tech Tip

## Contivity Secure IP Services Gateway

### Contivity – BCM IPsec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

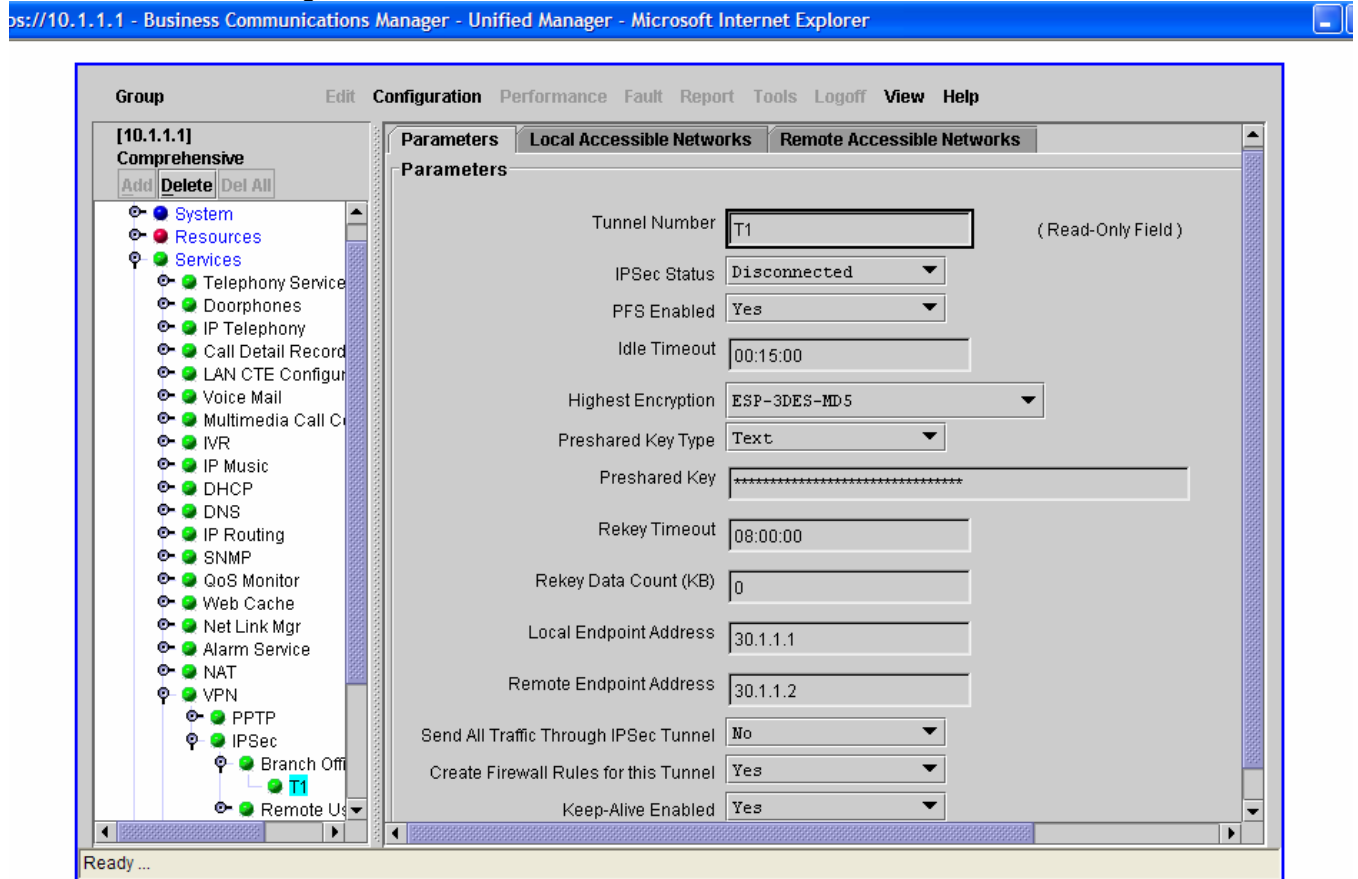
Set **Create Firewall Rules for This Tunnel** to **Yes**. This will create appropriate Firewall rules \ to allow tunnel traffic to pass through the Firewall:

Create Firewall Rules for this Tunnel	Yes
---------------------------------------	-----

Set **Keep-Alive Enabled** to **Yes**. Leave this setting at the default value of **No** for IPsec tunnel connections to systems other than BCM or Contivity:

Keep-Alive Enabled	Yes
--------------------	-----

Below are all the settings:



# Tech Tip

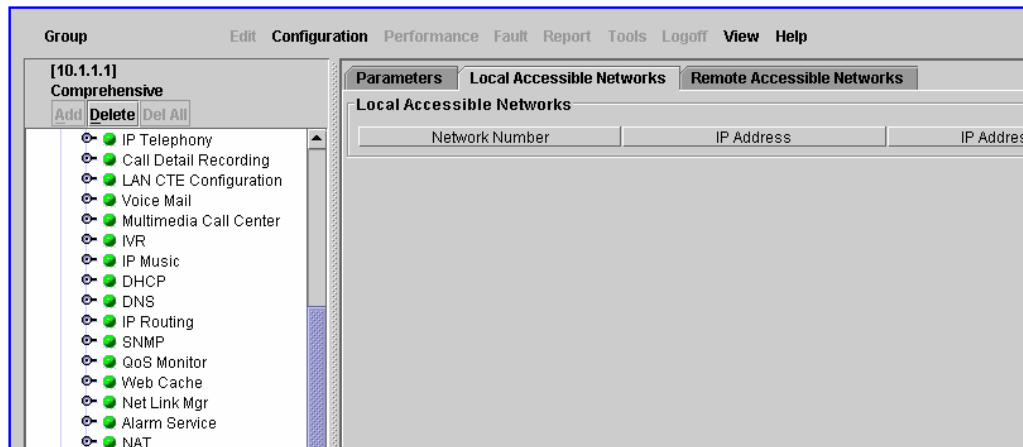
## Contivity Secure IP Services Gateway

### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

#### Configuring local and remote accessible networks

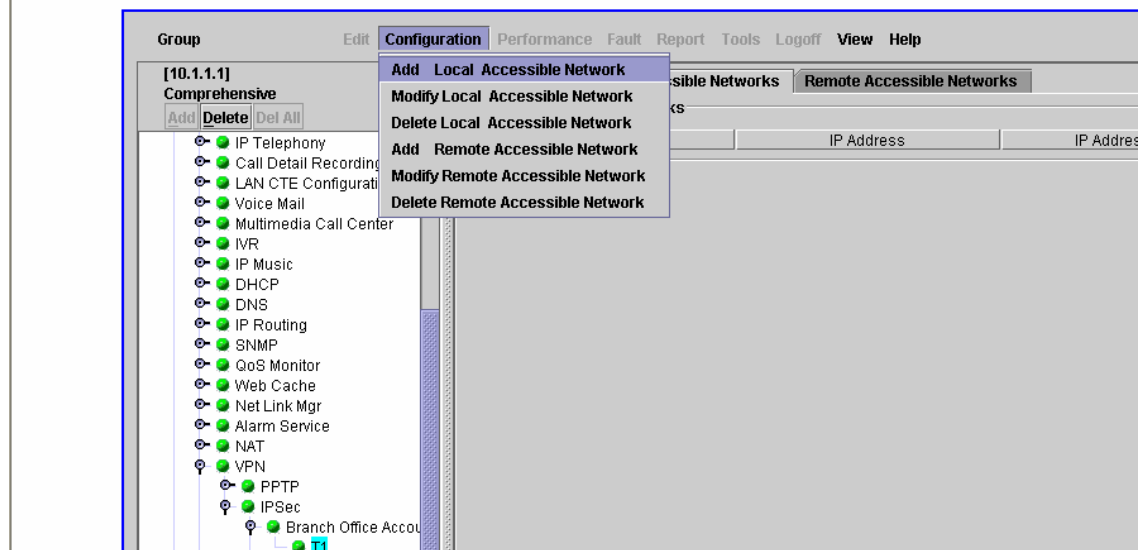
On the BOT screen, Click on **Local Accessible Networks** tab:

<https://10.1.1.1> - Business Communications Manager - Unified Manager - Microsoft Internet Explorer



Click on **Configuration** in the top menu bar and select **Add Local Accessible Network**:

<https://10.1.1.1> - Business Communications Manager - Unified Manager - Microsoft Internet Explorer



# Tech Tip

## Contivity Secure IP Services Gateway

### Contivity – BCM IPsec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

Enter the **Local Accessible Network** parameters (L1 - 10.1.1.0/24) and click **Save**:

The screenshot shows a 'BCM Dialog Box' with a title bar. Inside, there's a section titled 'Local Accessible Networks'. It contains three input fields: 'Network Number' with the value 'L1', 'IP Address' with the value '10.1.1.0', and 'IP Address Mask' with the value '255.255.255.0'. To the right of the mask field is a note '(Format 255.255.255.255)'. At the bottom of the dialog are 'Save' and 'Cancel' buttons. Below the dialog, there's a status bar that says 'Ready' and 'Java Applet Window'.

A local network is defined:

The screenshot shows the Contivity configuration interface. On the left is a tree view with a 'Group' button and a list of services including 'LAN CTE Configuration', 'Voice Mail', 'Multimedia Call Center', 'IVR', 'IP Music', 'DHCP', 'DNS', 'IP Routing', 'SNMP', 'QoS Monitor', 'Web Cache', 'Net Link Mgr', 'Alarm Service', 'NAT', 'VPN', 'PPTP', 'IPSec', 'Branch Office Account', and 'Remote User Account'. The 'IPSec' service is selected. On the right, there's a 'Parameters' tab with sub-tabs for 'Local Accessible Networks' and 'Remote Accessible Networks'. The 'Local Accessible Networks' sub-tab is active, showing a table with one entry:

Network Number	IP Address	IP Address
L1	10.1.1.0	255.255.255.0

On the BOT screen, Click on **Remote Accessible Networks** tab:

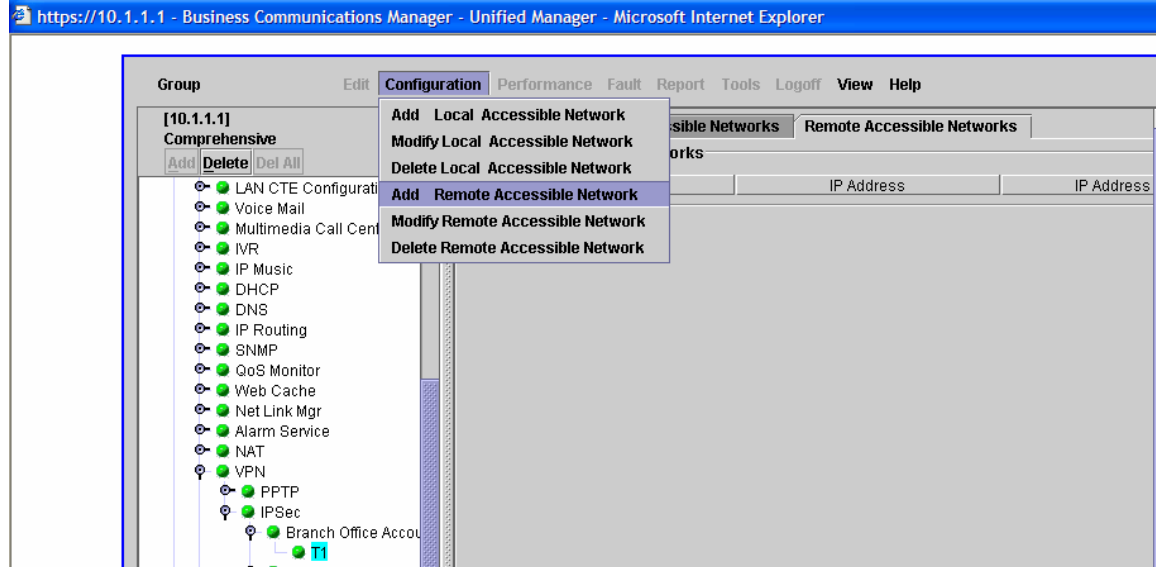
The screenshot shows the same Contivity configuration interface as before, but now the 'Remote Accessible Networks' sub-tab is active. The table for 'Remote Accessible Networks' is empty, showing only the column headers: 'Network Number', 'IP Address', and 'IP Address'.

# Tech Tip

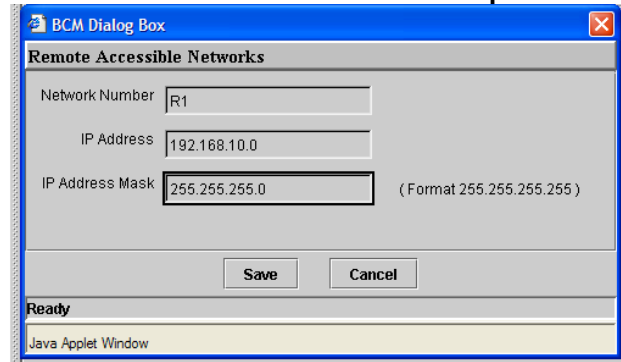
## Contivity Secure IP Services Gateway

### Contivity – BCM IPsec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

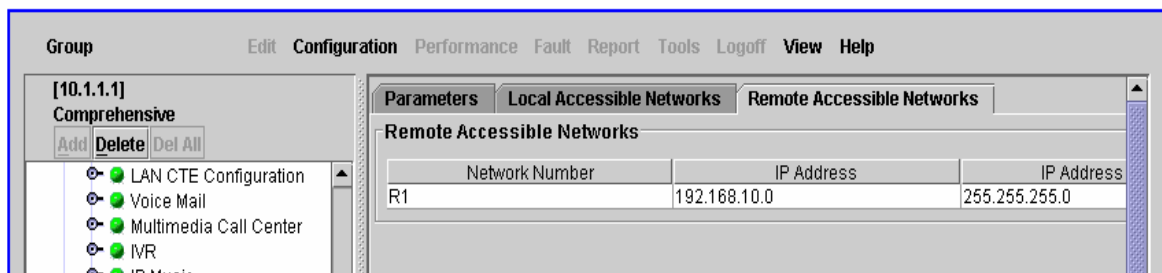
Click on **Configuration** on the menu bar and select **Add Remote Accessible Network**:



Enter the **Remote Accessible Network** parameters (R1 - 192.168.10.0/24) and click **Save**:



A remote network is created:



## Tech Tip

### Contivity Secure IP Services Gateway



## Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

---

### Verifying firewall rules

On the BCM, for a branch office tunnel to work, the **Firewall has to enabled** and the rules have to be configured to allow traffic through. The rules get created automatically when “**Create**

**Firewall Rules for this Tunnel**” is set to **Yes** in sec in sec in sec in s7 4368a1P02 90.00015 608.6999etce7tpanTEM



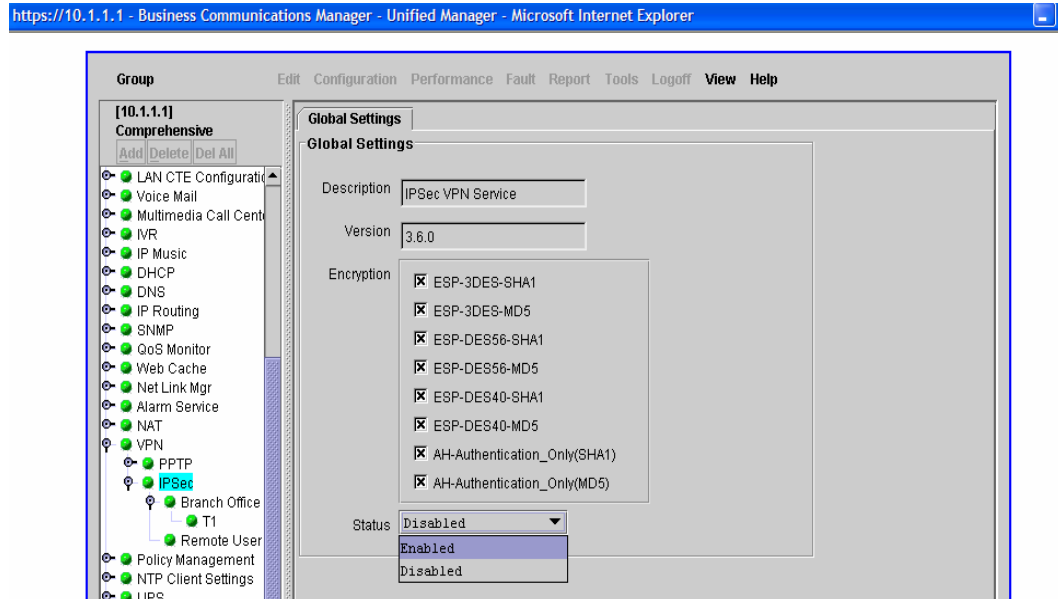
# Tech Tip

## Contivity Secure IP Services Gateway

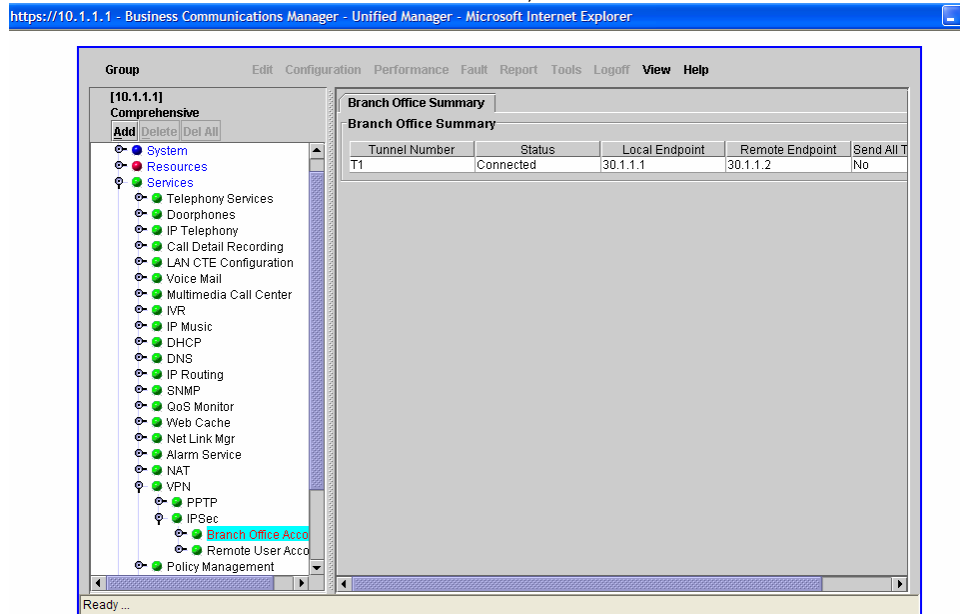
### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

#### Enabling IPSec

From the navigation tree, expand the **VPN** key and click on **IPSec** and select **Enabled** next to **Status**:



Once the branch office tunnel is established, the BOT status is shown as **Connected**:



# Tech Tip

## Contivity Secure IP Services Gateway



### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

---

#### Event Log

Below is CES event log of the successful tunnel establishment:

```
09/20/2004 16:34:13 0 Branch Office [01] IPSEC branch office connection initiated to rem[10.1.1.0-255.255.255.0]@[30.1.1.1] loc[192.168.10.0-255.255.255.0]
09/20/2004 16:34:13 0 Security [11] Session: IPSEC[30.1.1.1] attempting login
09/20/2004 16:34:13 0 Security [01] Session: IPSEC[30.1.1.1] has no active sessions
09/20/2004 16:34:13 0 Security [01] Session: IPSEC[30.1.1.1] T0 BCM has no active accounts
09/20/2004 16:34:13 0 Security [01] Session: IPSEC[30.1.1.1]:11 SHARED-SECRET authenticate attempt...
09/20/2004 16:34:13 0 Security [01] Session: IPSEC[30.1.1.1]:11 attempting authentication using LOCAL
09/20/2004 16:34:13 0 Security [11] Session: IPSEC[30.1.1.1]:11 authenticated using LOCAL
09/20/2004 16:34:13 0 Security [11] Session: IPSEC[30.1.1.1]:11 bound to group /Base/BO Group/T0 BCM
09/20/2004 16:34:13 0 Security [01] Session: IPSEC[30.1.1.1]:11 Building group filter permit all
09/20/2004 16:34:13 0 Security [01] Session: IPSEC[30.1.1.1]:11 Applying group filter permit all
09/20/2004 16:34:13 0 Security [11] Session: IPSEC[30.1.1.1]:11 authorized
09/20/2004 16:34:13 0 Security [11] Session: network IPSEC[10.1.1.0-255.255.255.0] attempting login
09/20/2004 16:34:13 0 Security [11] Session: network IPSEC[10.1.1.0-255.255.255.0] logged in from gateway [30.1.1.1]
09/20/2004 16:34:13 0 ISAKMP [02] ISAKMP SA established with 30.1.1.1
09/20/2004 16:34:13 0 Security [12] Session: IPSEC[30.1.1.1]:11 physical addresses: remote 30.1.1.1 local 30.1.1.2
09/20/2004 16:34:13 0 Security [12] Session: IPSEC[-]:12 physical addresses: remote 30.1.1.1 local 30.1.1.2
09/20/2004 16:34:13 0 Outbound ESP from 30.1.1.2 to 30.1.1.1 SPI 0x00163b9d [03] ESP encap session SPI 0x9d3b1600 bound to s/w on cpu 0
09/20/2004 16:34:13 0 Inbound ESP from 30.1.1.1 to 30.1.1.2 SPI 0x00094683 [03] ESP decap session SPI 0x83460900 bound to s/w on cpu 0
09/20/2004 16:34:13 0 Branch Office [00] 4f899f0
BranchOfficeCtxtCls::RegisterTunnel: rem[10.1.1.0-255.255.255.0]@[30.1.1.1] loc[192.168.10.0-255.255.255.0] overwriting tunnel context [ffffffff] with [4f7b8b8]
09/20/2004 16:34:13 0 ISAKMP [03] Established IPsec SAs with 30.1.1.1:
09/20/2004 16:34:13 0 ISAKMP [03] ESP 3DES-CBC-HMAC-MD5 outbound SPI 0x163b9d
09/20/2004 16:34:13 0 ISAKMP [03] ESP 3DES-CBC-HMAC-MD5 inbound SPI 0x94683
```

# Tech Tip

## Contivity Secure IP Services Gateway



### Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

---

---

Copyright © 2005 Nortel Networks Limited - All Rights Reserved. Nortel, Nortel Networks, the Nortel logo, Globemark, and Contivity are trademarks of Nortel Networks Limited.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Limited.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Nortel Networks Technical Support on the web at: <http://www.nortel.com/support>

If after following this guide you are still having problems, please ensure you have carried out the steps exactly as in this document. If problems still persist, please contact Nortel Networks Technical Support (contact information is available online at: [http://www.nortel.com/cgi-bin/comments/comments.cgi?key=techsupport\\_cu](http://www.nortel.com/cgi-bin/comments/comments.cgi?key=techsupport_cu)).

We welcome your comments and suggestions on the quality and usefulness of this document. If you would like to leave a feedback please send your comments to: [CRCONT@nortel.com](mailto:CRCONT@nortel.com)

Author: Hitesh Patel