Tech Tip
Contivity Secure IP Services Gateway

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

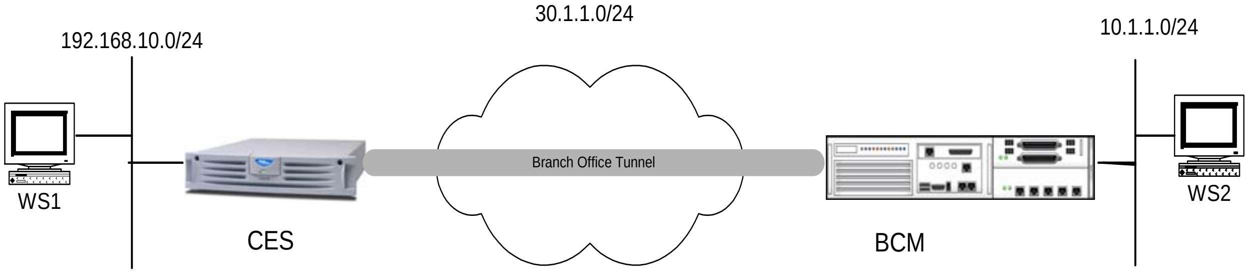
Contents

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.

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
```

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:

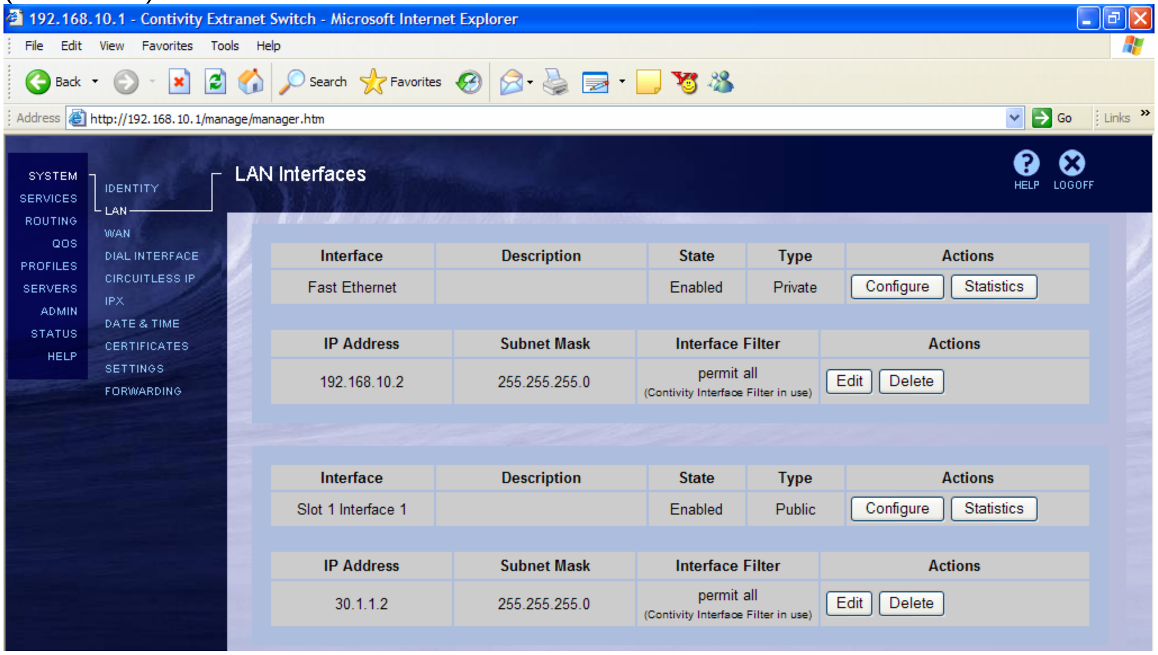
```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection 2:

        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:



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

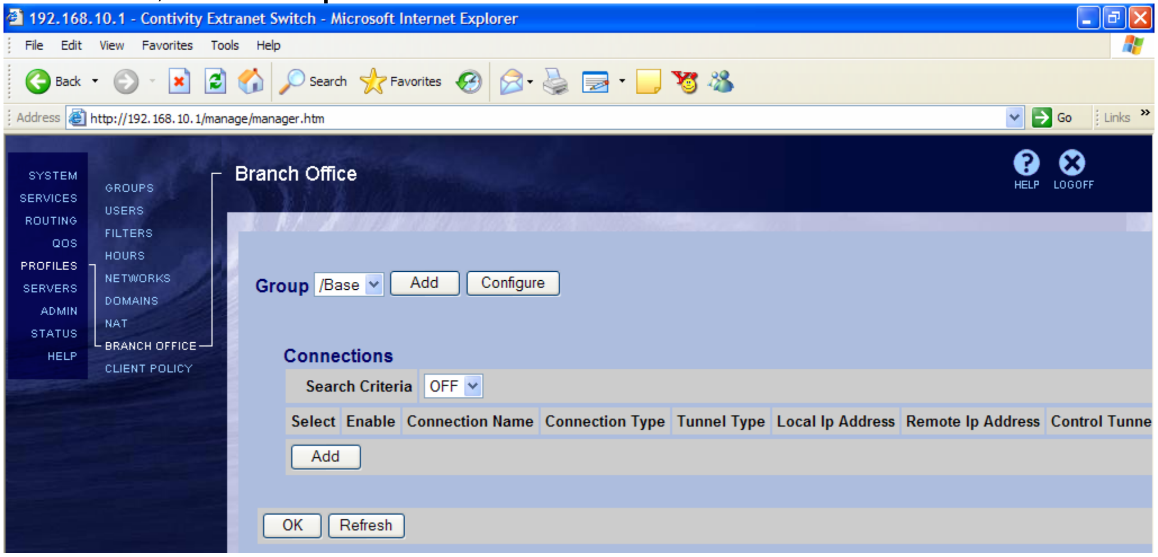
IP Address	Subnet Mask	Interface Filter	Actions
30.1.1.2	255.255.255.0	permit all (Contivity Interface Filter in use)	Edit Delete

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.

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**:



Branch Office

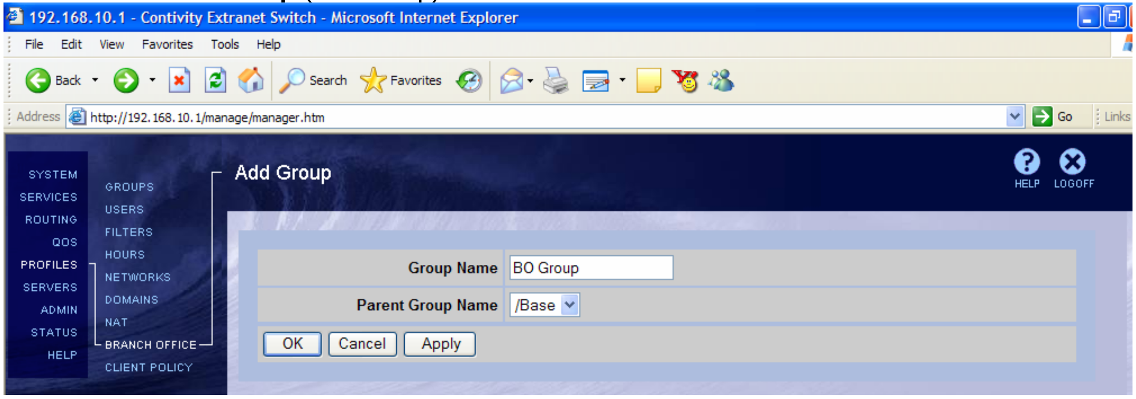
Group /Base

Connections

Search Criteria OFF

Select	Enable	Connection Name	Connection Type	Tunnel Type	Local Ip Address	Remote Ip Address	Control Tunne

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



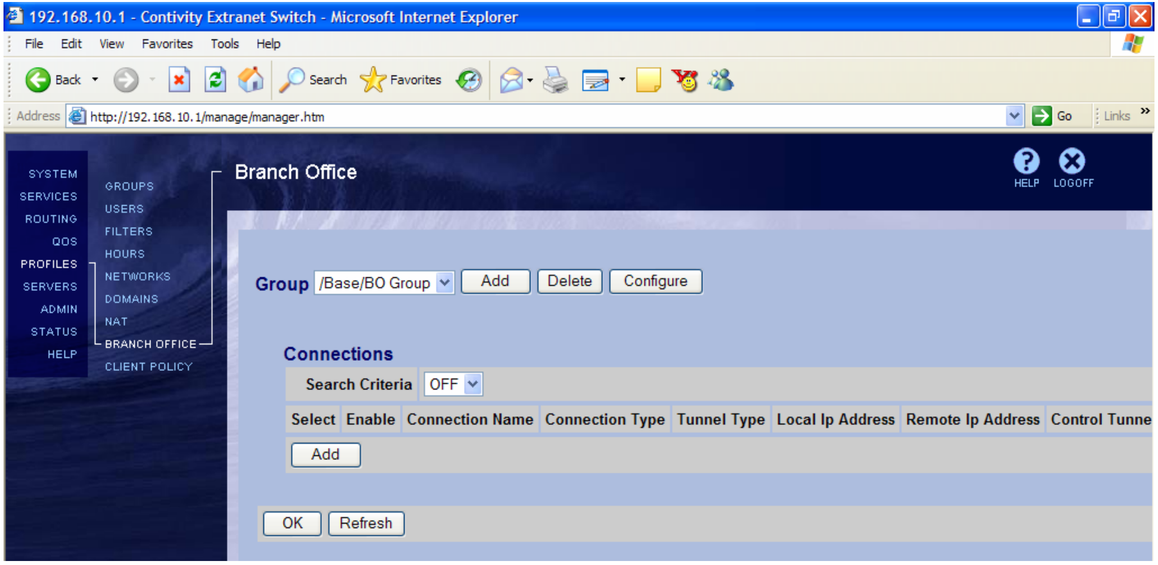
Add Group

Group Name: BO Group

Parent Group Name: /Base

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**:



Branch Office

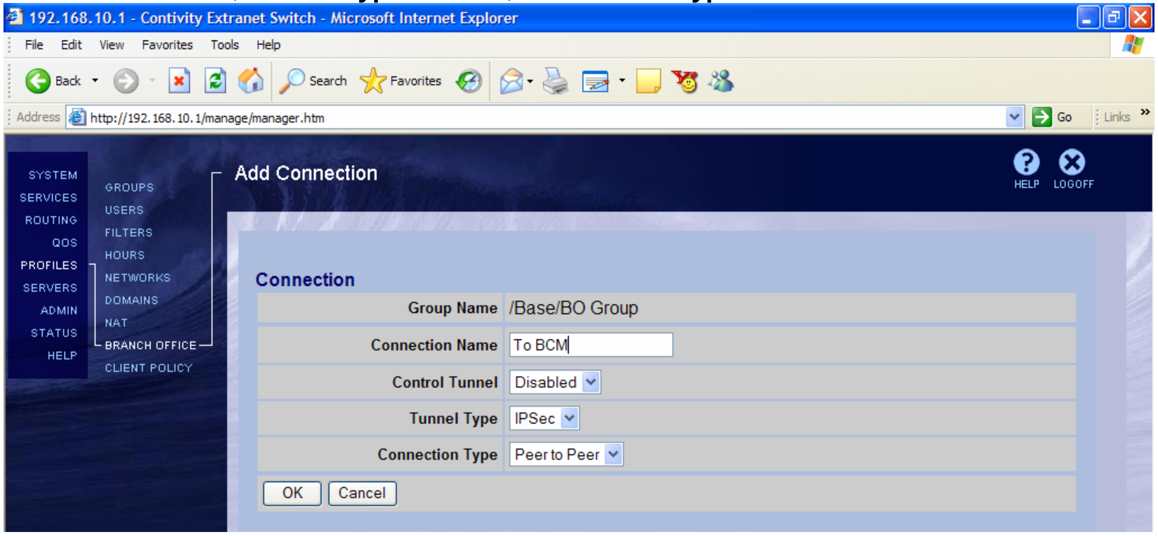
Group /Base/BO Group

Connections

Search Criteria OFF

Select	Enable	Connection Name	Connection Type	Tunnel Type	Local Ip Address	Remote Ip Address	Control Tunne

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**:

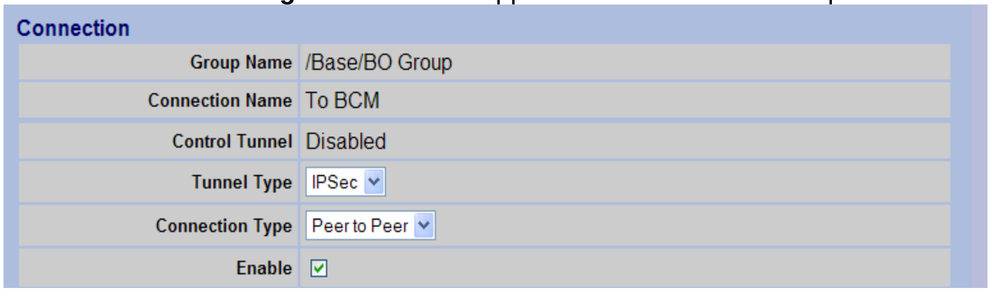


Add Connection

Connection

Group Name	/Base/BO Group
Connection Name	To BCM
Control Tunnel	Disabled
Tunnel Type	IPSec
Connection Type	Peer to Peer

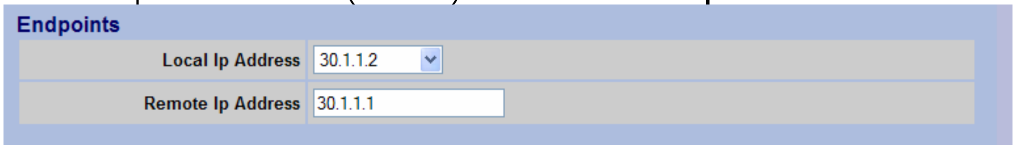
The **Connection Configuration** screen appears. Select the **Enable** option:



Connection

Group Name	/Base/BO Group
Connection Name	To BCM
Control Tunnel	Disabled
Tunnel Type	IPSec
Connection Type	Peer to Peer
Enable	☑

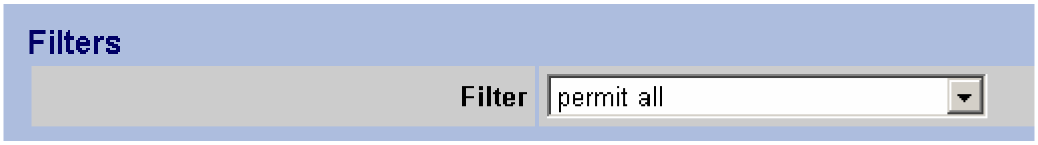
Select CES public IP address (30.1.1.2) as the **Local Endpoint IP Address**;
Enter BCM public IP address (30.1.1.1) as the **Remote Endpoint IP Address**:



Endpoints

Local Ip Address	30.1.1.2
Remote Ip Address	30.1.1.1

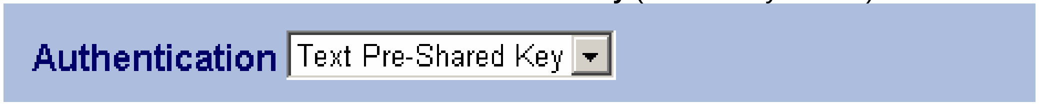
Leave the **Filter** at **Permit All**:



Filters

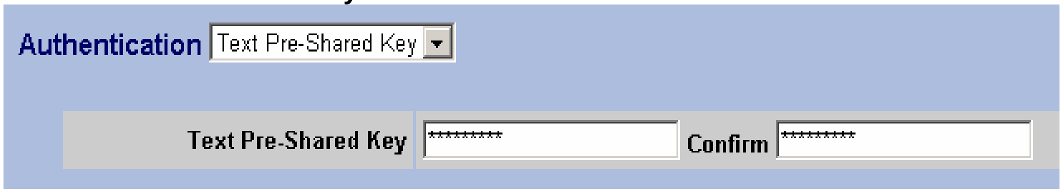
Filter	permit all

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



Authentication Text Pre-Shared Key

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

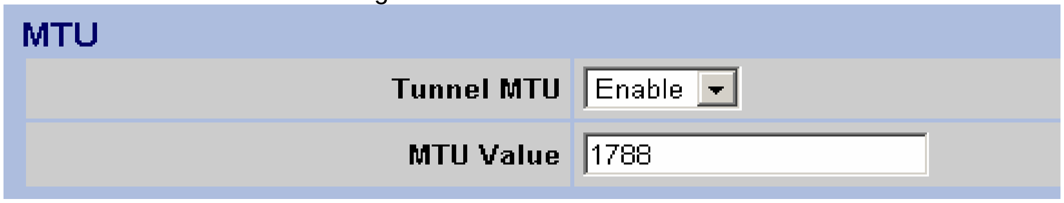


Authentication Text Pre-Shared Key

Text Pre-Shared Key ********** Confirm **********

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

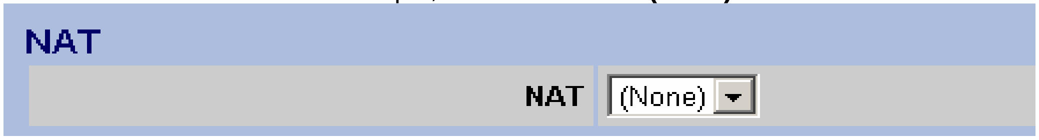
Leave **MTU** at the default setting:


MTU

Tunnel MTU: Enable

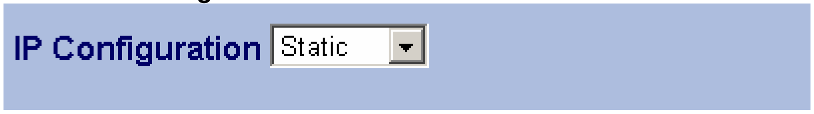
MTU Value: 1788

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

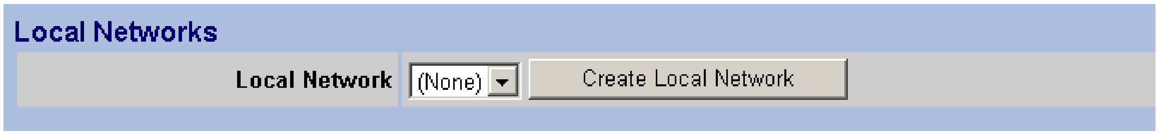

NAT

NAT: (None)

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

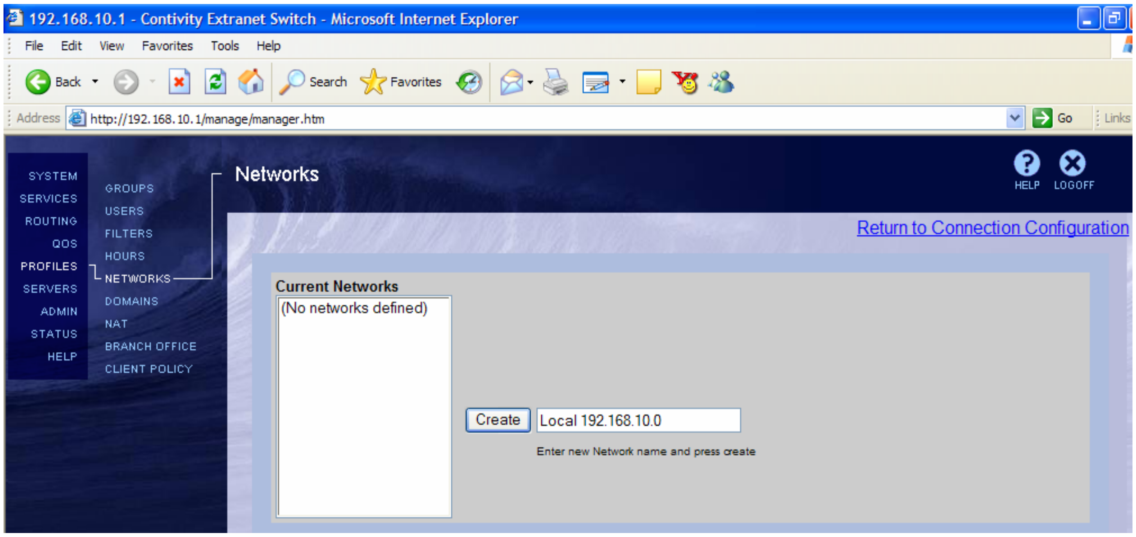

IP Configuration: Static

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


Local Networks

Local Network: (None)

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
Search
Favorites
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
Return to Connection Configuration
Create

Networks

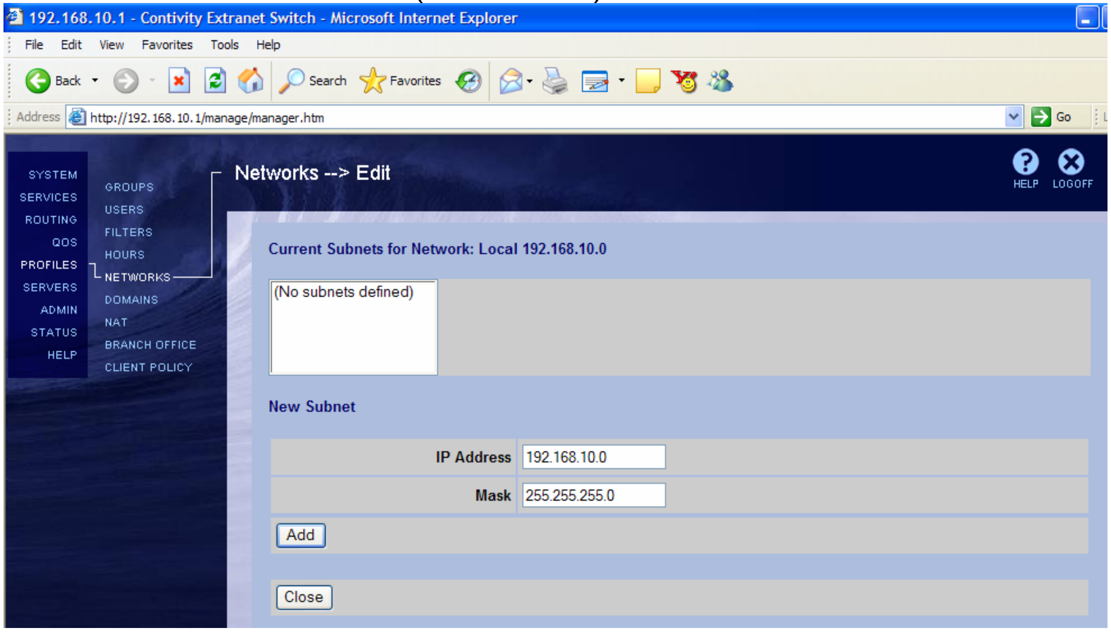
Current Networks
(No networks defined)

Local 192.168.10.0

Enter new Network name and press create

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**:



Networks --> Edit

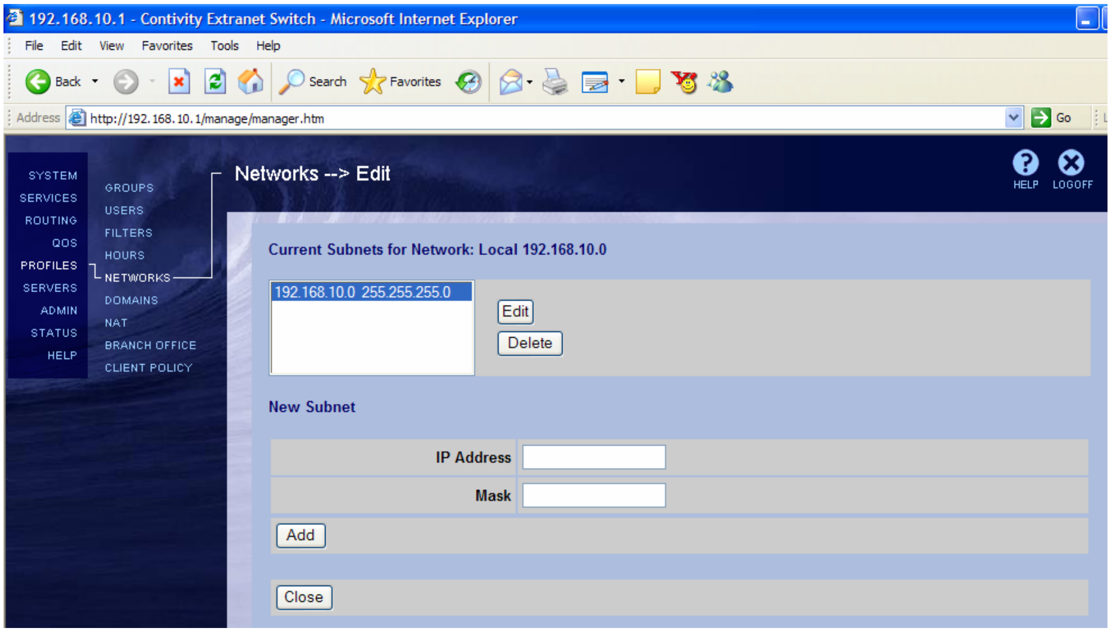
Current Subnets for Network: Local 192.168.10.0

(No subnets defined)

New Subnet

IP Address	192.168.10.0
Mask	255.255.255.0

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



Networks --> Edit

Current Subnets for Network: Local 192.168.10.0

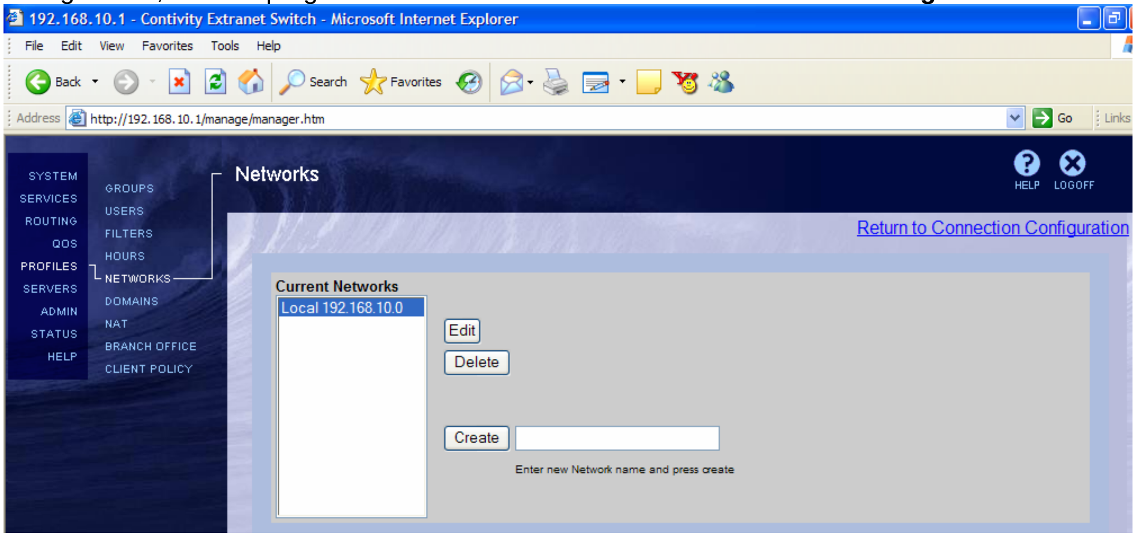
192.168.10.0 255.255.255.0

New Subnet

IP Address	
Mask	

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**:

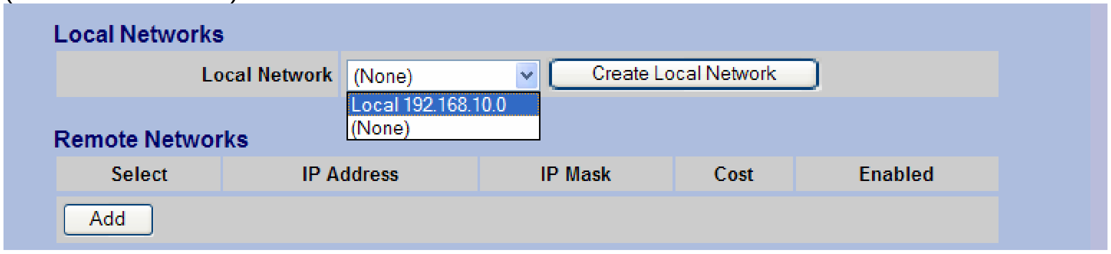


Current Networks

Local 192.168.10.0

Enter new Network name and press create

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

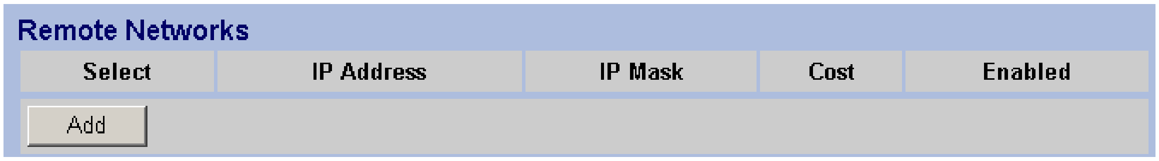


Local Network (None)

Local 192.168.10.0
(None)

Select	IP Address	IP Mask	Cost	Enabled

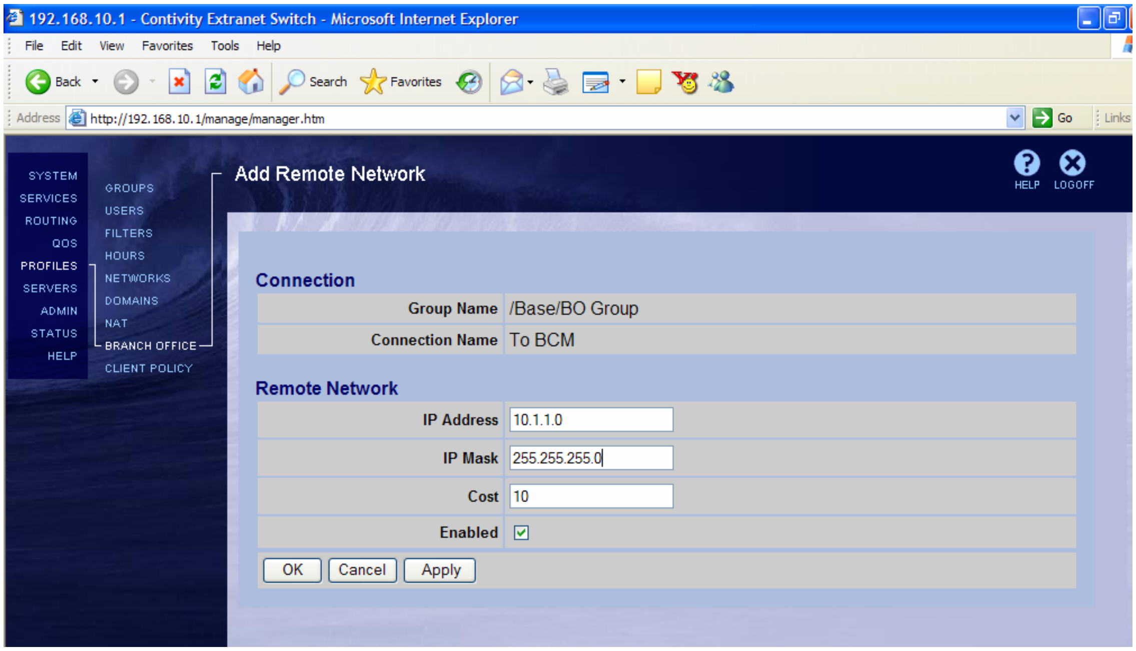
Define the remote accessible networks. Under the **Remote Networks** click **Add**:



Select	IP Address	IP Mask	Cost	Enabled

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 Search Favorites
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

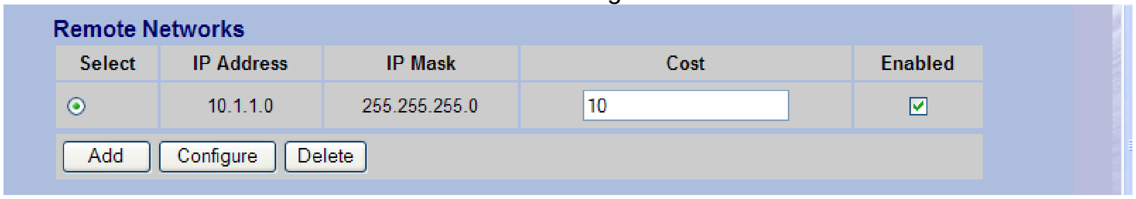
Group Name	/Base/BO Group
Connection Name	To BCM

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:



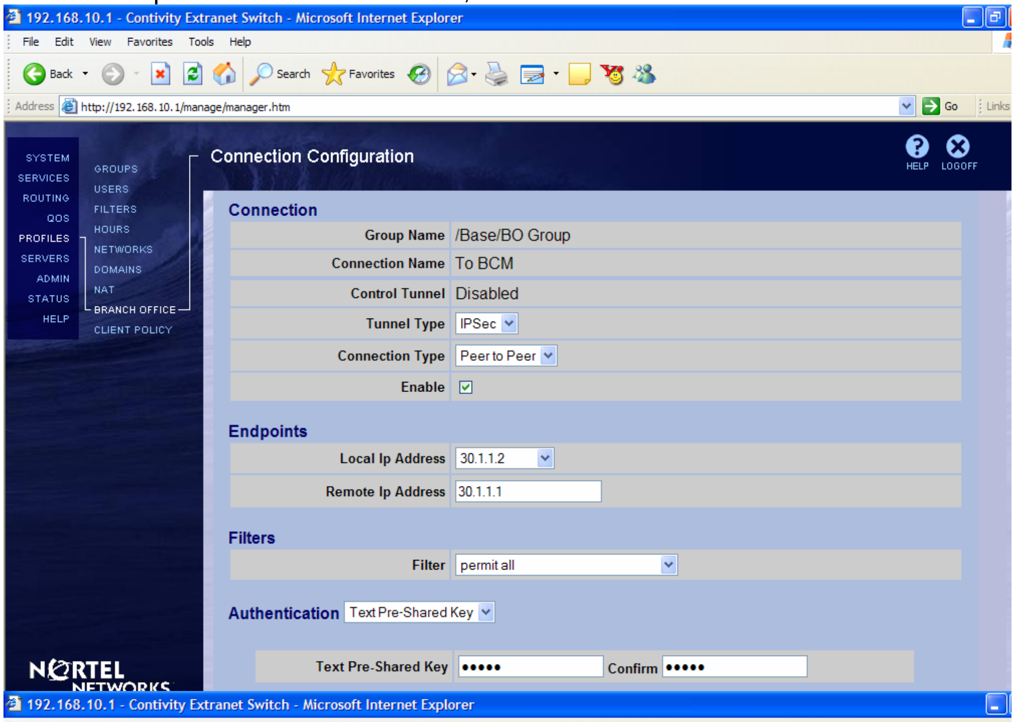
Remote Networks

Select	IP Address	IP Mask	Cost	Enabled
●	10.1.1.0	255.255.255.0	10	☑

Add Configure Delete

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**:



Connection Configuration

Connection

Group Name	/Base/BO Group
Connection Name	To BCM
Control Tunnel	Disabled
Tunnel Type	IPSec
Connection Type	Peer to Peer
Enable	☑

Endpoints

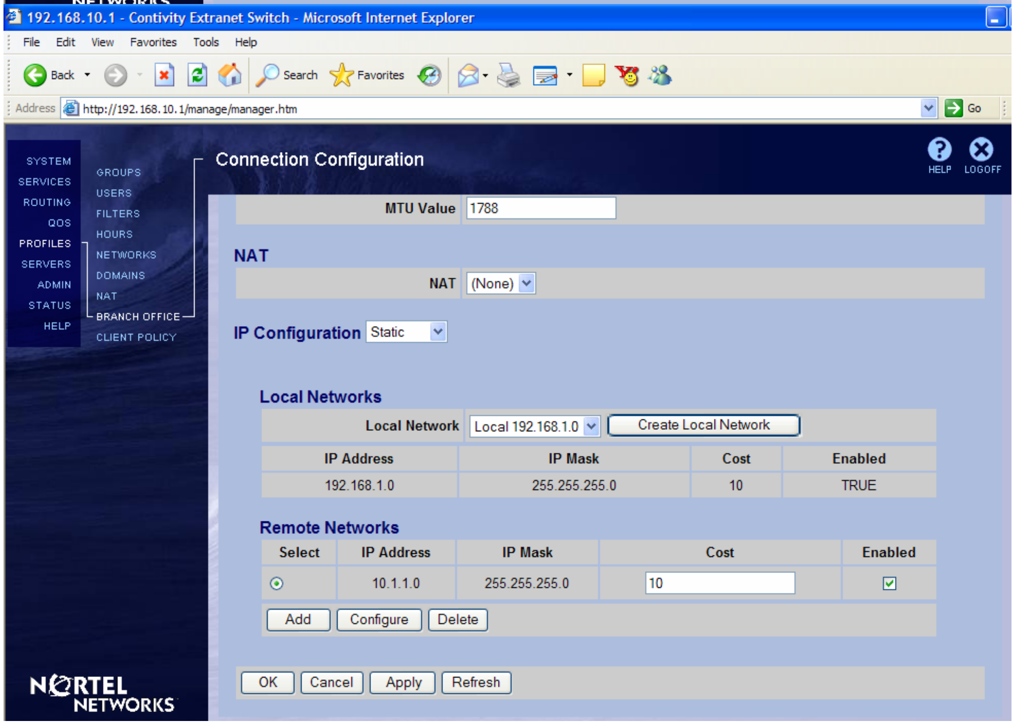
Local Ip Address	30.1.1.2
Remote Ip Address	30.1.1.1

Filters

Filter	permit all

Authentication Text Pre-Shared Key

Text Pre-Shared Key ••••• Confirm •••••



Connection Configuration

MTU Value 1788

NAT

NAT (None)

IP Configuration Static

Local Networks

Local Network Local 192.168.1.0

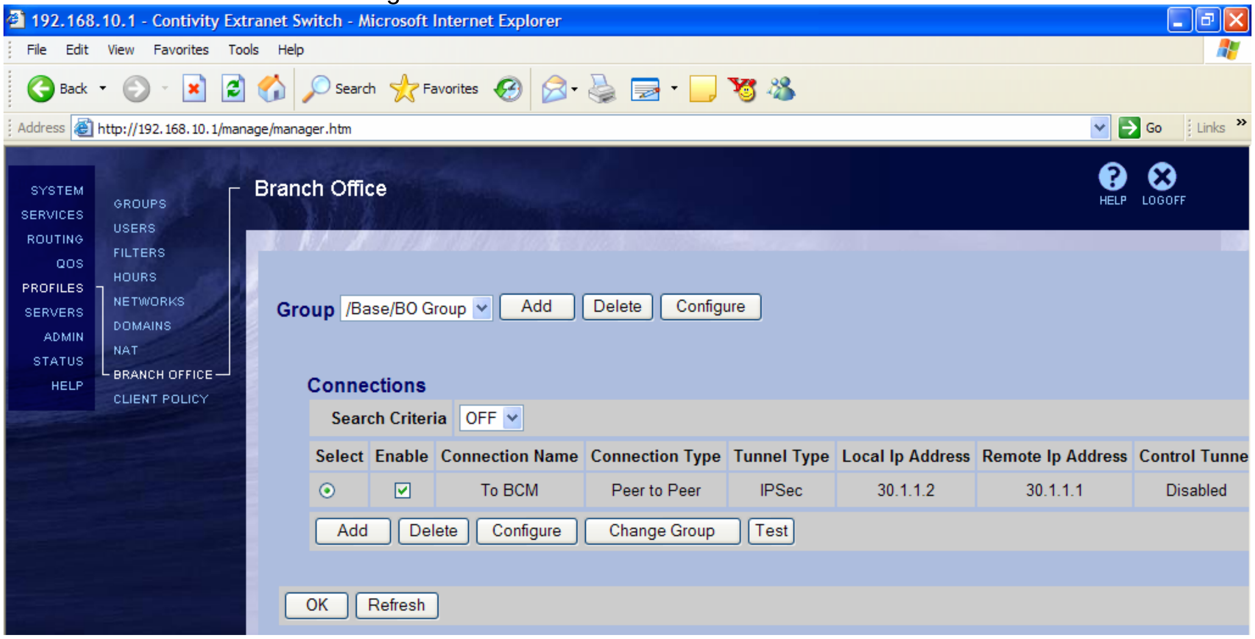
IP Address	IP Mask	Cost	Enabled
192.168.1.0	255.255.255.0	10	TRUE

Remote Networks

Select	IP Address	IP Mask	Cost	Enabled
●	10.1.1.0	255.255.255.0	10	☑

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

Branch office connection is configured:



Branch Office

Group /Base/BO Group

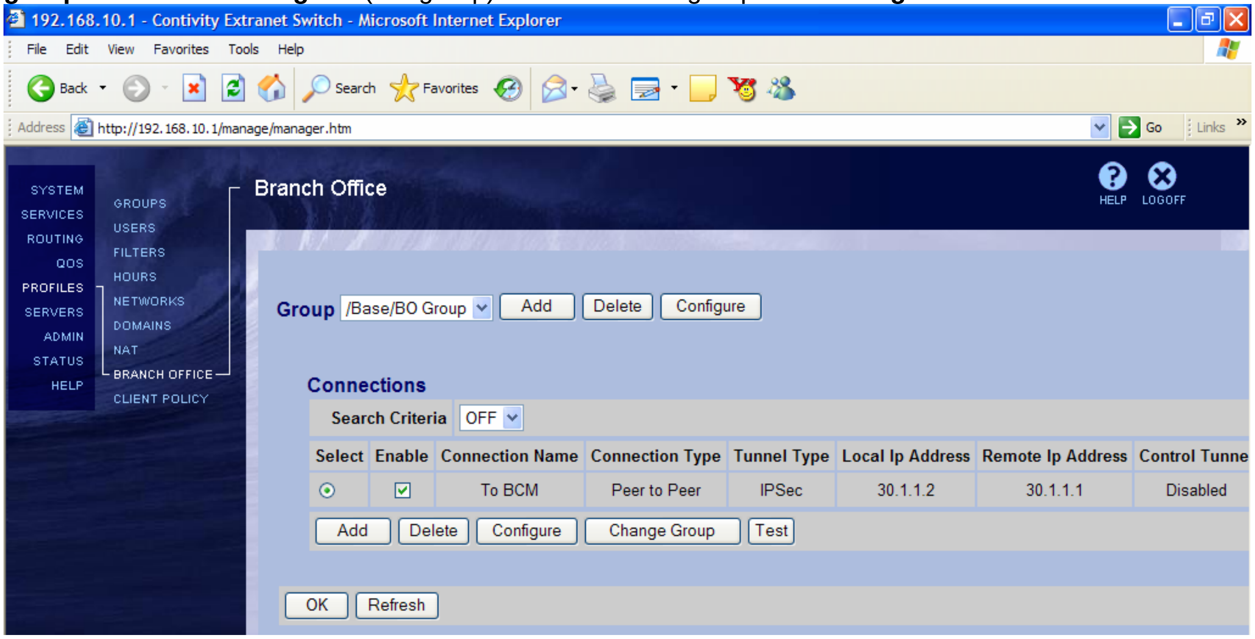
Connections

Search Criteria OFF

Select	Enable	Connection Name	Connection Type	Tunnel Type	Local Ip Address	Remote Ip Address	Control Tunne
●	☑	To BCM	Peer to Peer	IPSec	30.1.1.2	30.1.1.1	Disabled

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**:



Branch Office

Group /Base/BO Group

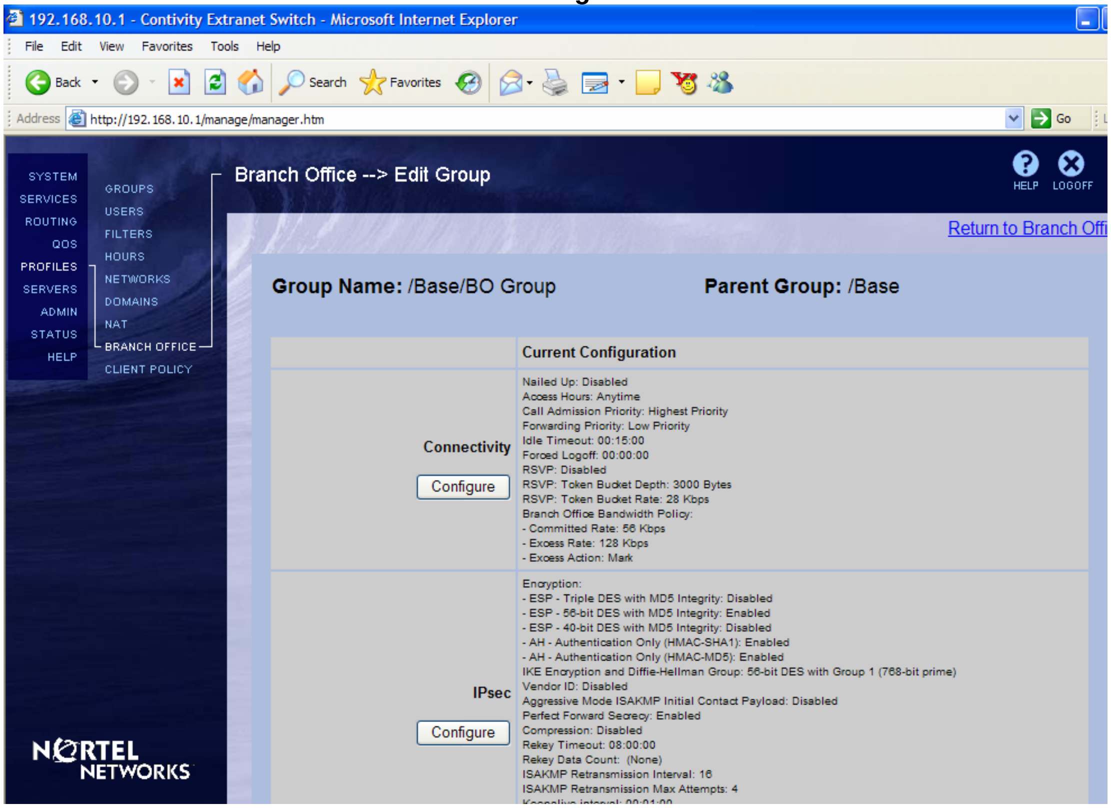
Connections

Search Criteria OFF

Select	Enable	Connection Name	Connection Type	Tunnel Type	Local Ip Address	Remote Ip Address	Control Tunne
●	☑	To BCM	Peer to Peer	IPSec	30.1.1.2	30.1.1.1	Disabled

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

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



Branch Office --> Edit Group

Group Name: /Base/BO Group **Parent Group:** /Base

Current Configuration

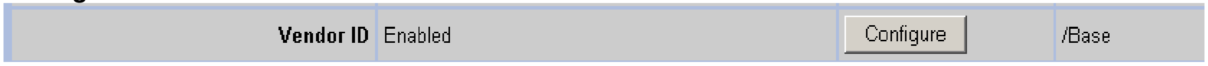
Connectivity

Nailed Up: Disabled
Access Hours: Anytime
Call Admission Priority: Highest Priority
Forwarding Priority: Low Priority
Idle Timeout: 00:15:00
Forced Logoff: 00:00:00
RSVP: Disabled
RSVP: Token Bucket Depth: 3000 Bytes
RSVP: Token Bucket Rate: 28 Kbps
Branch Office Bandwidth Policy:
- Committed Rate: 56 Kbps
- Excess Rate: 128 Kbps
- Excess Action: Mark

IPsec

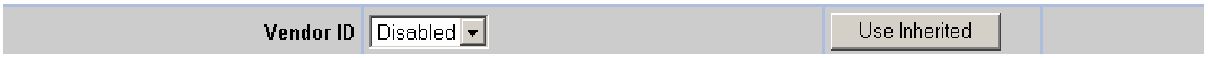
Encryption:
- ESP - Triple DES with MD5 Integrity: Disabled
- ESP - 56-bit DES with MD5 Integrity: Enabled
- ESP - 40-bit DES with MD5 Integrity: Disabled
- AH - Authentication Only (HMAC-SHA1): Enabled
- AH - Authentication Only (HMAC-MD5): Enabled
IKE Encryption and Diffie-Hellman Group: 56-bit DES 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: (None)
ISAKMP Retransmission Interval: 16
ISAKMP Retransmission Max Attempts: 4
Keepalive interval: 00:01:00

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



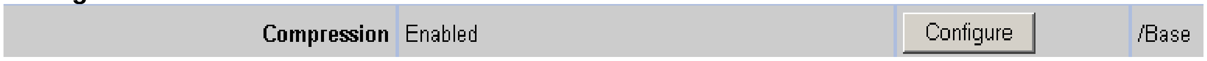
Vendor ID Enabled /Base

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



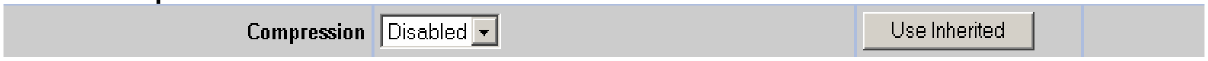
Vendor ID Disabled

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



Compression Enabled /Base

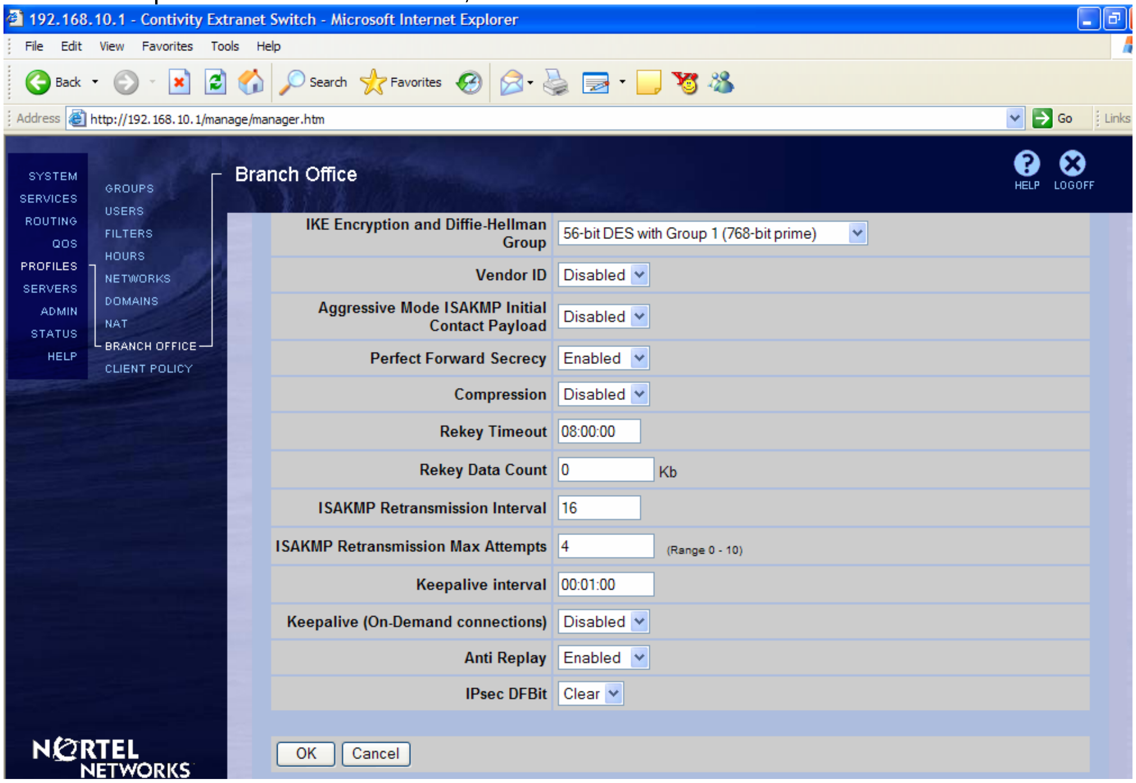
Next to **Compression** select **Disabled**:



Compression Disabled

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**:



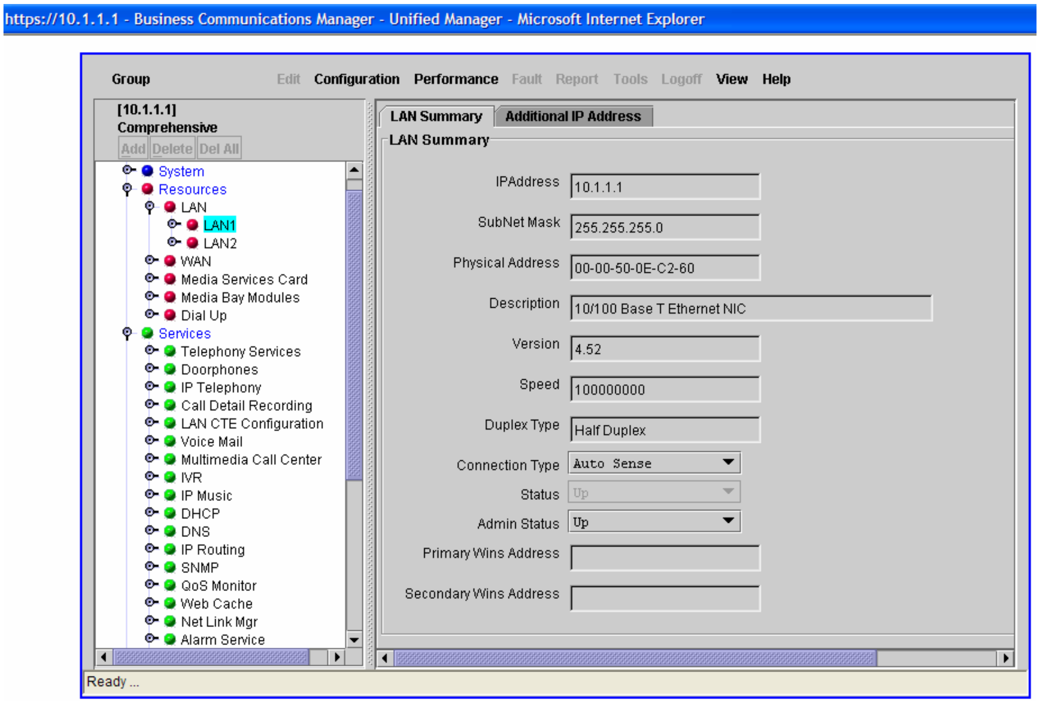
IKE Encryption and Diffie-Hellman Group	56-bit DES with Group 1 (768-bit prime)
Vendor ID	Disabled
Aggressive Mode ISAKMP Initial Contact Payload	Disabled
Perfect Forward Secrecy	Enabled
Compression	Disabled
Rekey Timeout	08:00:00
Rekey Data Count	0 Kb
ISAKMP Retransmission Interval	16
ISAKMP Retransmission Max Attempts	4 (Range 0 - 10)
Keepalive interval	00:01:00
Keepalive (On-Demand connections)	Disabled
Anti Replay	Enabled
IPsec DFBit	Clear

The Contivity gateway is now configured.

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:

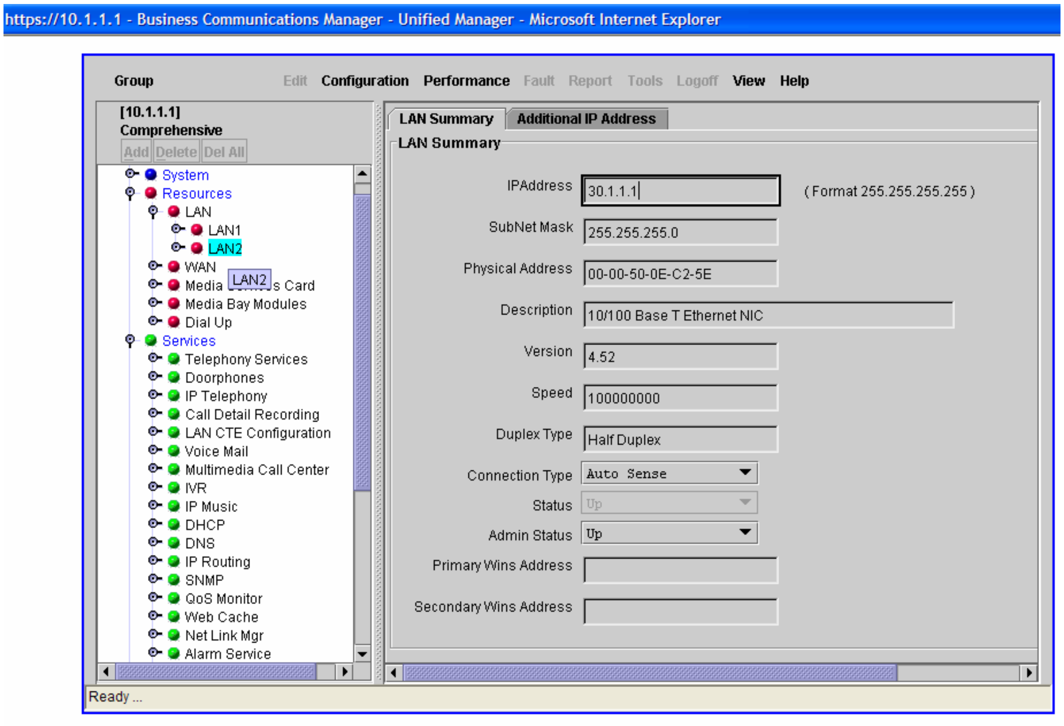


LAN Summary

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
Status: Up
Admin Status: Up
Primary Wins Address:
Secondary Wins Address:

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:



LAN Summary

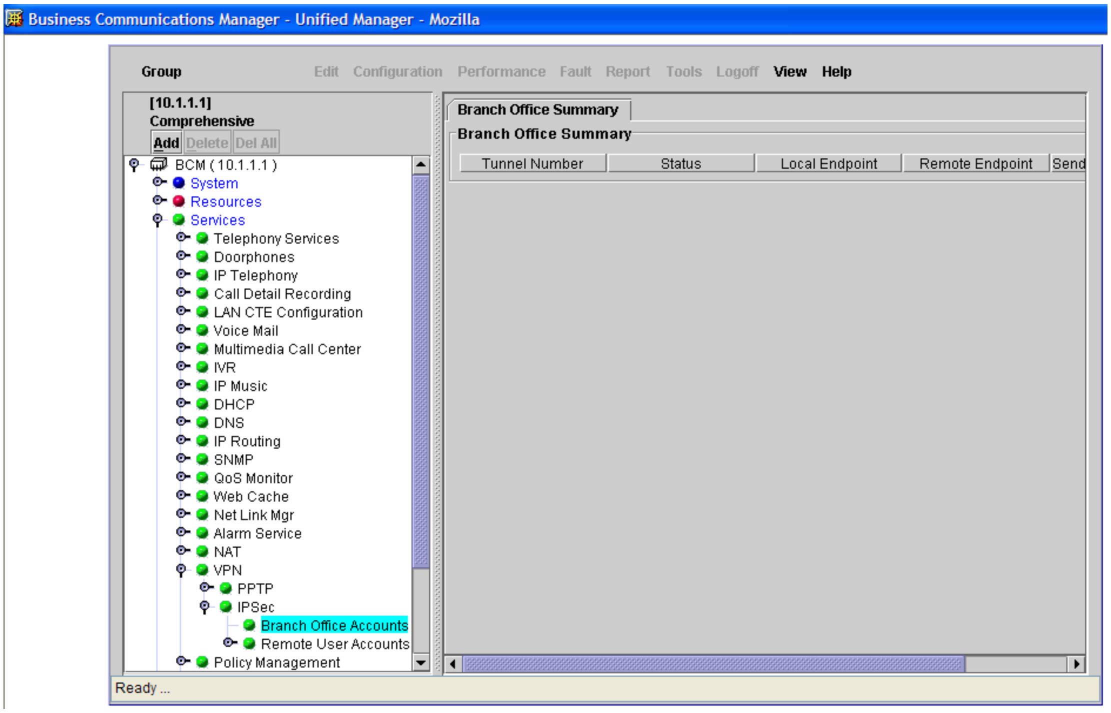
IPAddress: 30.1.1.1 (Format 255.255.255.255)
SubNet Mask: 255.255.255.0
Physical Address: 00-00-50-0E-C2-5E
Description: 10/100 Base T Ethernet NIC
Version: 4.52
Speed: 100000000
Duplex Type: Half Duplex
Connection Type: Auto Sense
Status: Up
Admin Status: Up
Primary Wins Address:
Secondary Wins Address:

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 **<u>'Add'</u>** button under the heading **Comprehensive.**

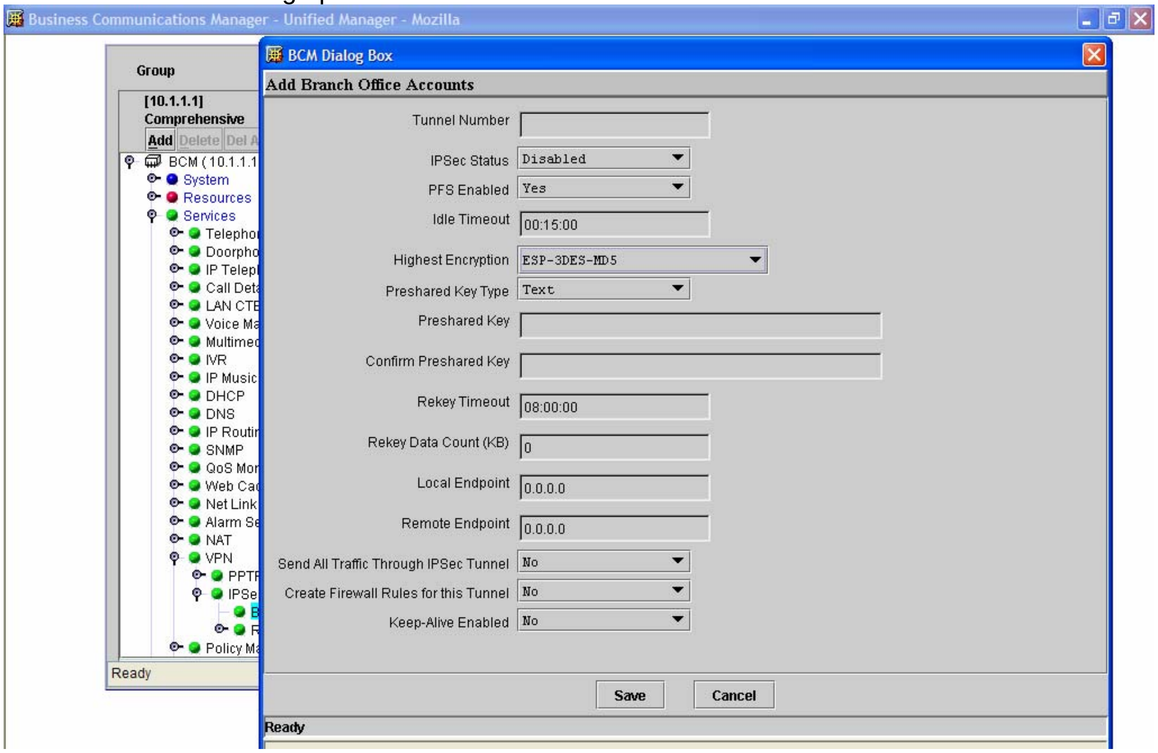


Branch Office Summary

Tunnel Number	Status	Local Endpoint	Remote Endpoint	Send

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

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

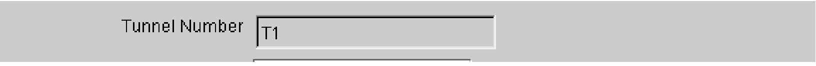


Add Branch Office Accounts

Tunnel Number:
IPSec Status: Disabled
PFS Enabled: Yes
Idle Timeout: 00:15:00
Highest Encryption: ESP-3DES-MD5
Preshared Key Type: Text
Preshared Key:
Confirm Preshared Key:
Rekey Timeout: 08:00:00
Rekey Data Count (KB): 0
Local Endpoint: 0.0.0.0
Remote Endpoint: 0.0.0.0
Send All Traffic Through IPSec Tunnel: No
Create Firewall Rules for this Tunnel: No
Keep-Alive Enabled: No

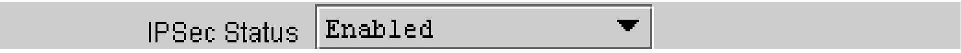
Fill out the “Add Branch Office Accounts” window as follows:

Enter the **Tunnel Number**, T1:



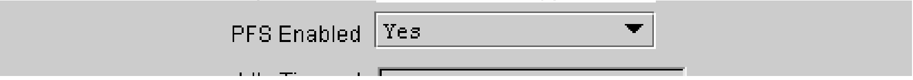
Tunnel Number: T1

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



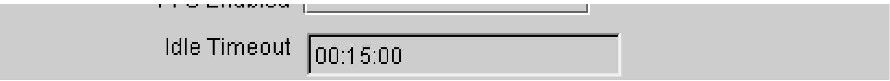
IPSec Status: Enabled

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



PFS Enabled: Yes

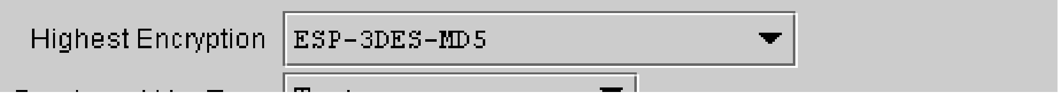
Leave the **Idle Timeout** as the default value:



Idle Timeout: 00:15:00

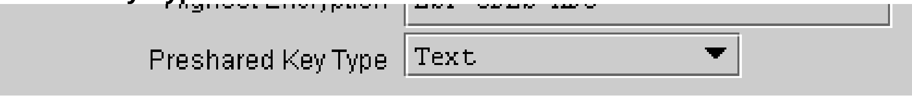
Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

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:



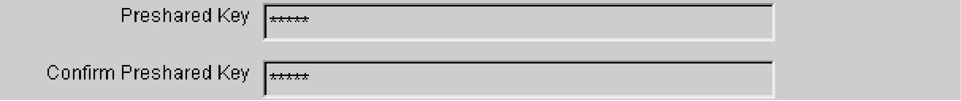
Highest Encryption ESP-3DES-MD5

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



Preshared Key Type Text

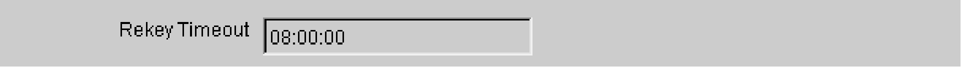
Set the **Pre-shared Key** to **12345** and confirm it to match the key entered in Contivity configuration:



Preshared Key *****

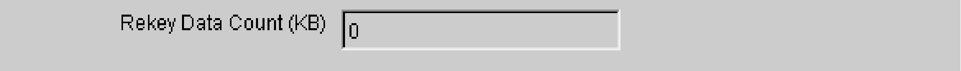
Confirm Preshared Key *****

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



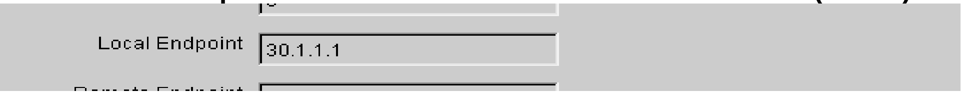
Rekey Timeout 08:00:00

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



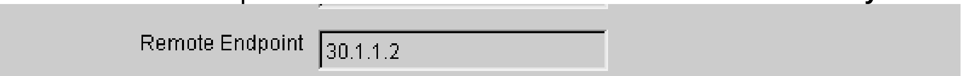
Rekey Data Count (KB) 0

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



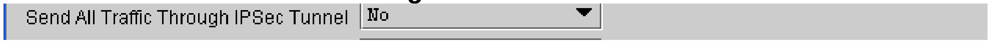
Local Endpoint 30.1.1.1

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



Remote Endpoint 30.1.1.2

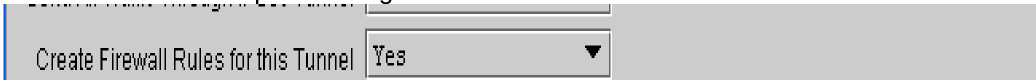
Leave the **Send All Traffic Through IPSec Tunnel** to default of **No**:



Send All Traffic Through IPSec Tunnel No

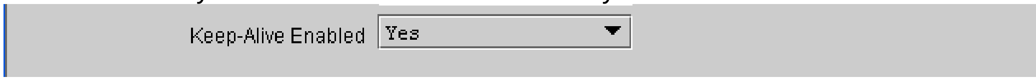
Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

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



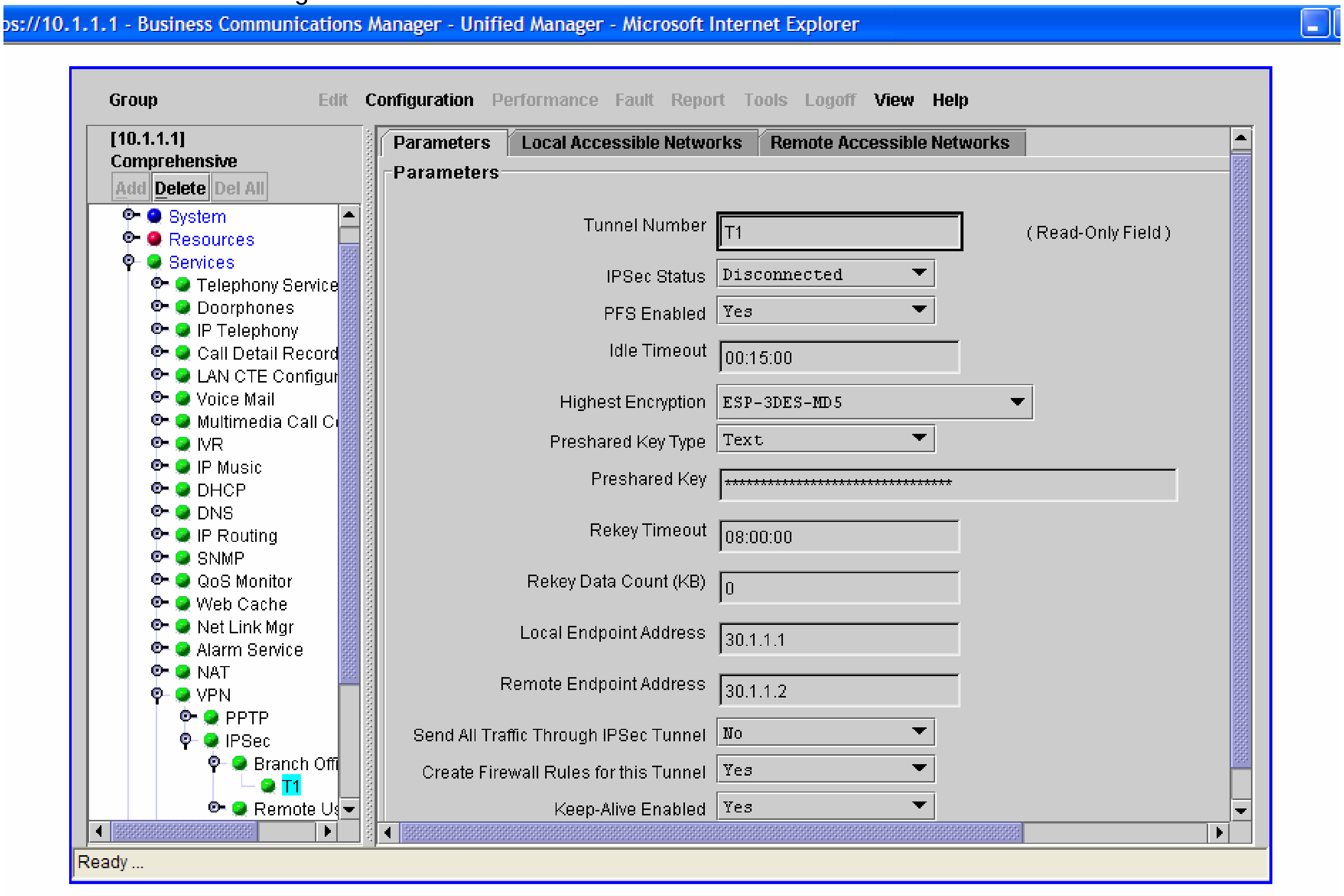
Create Firewall Rules for this Tunnel: Yes

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

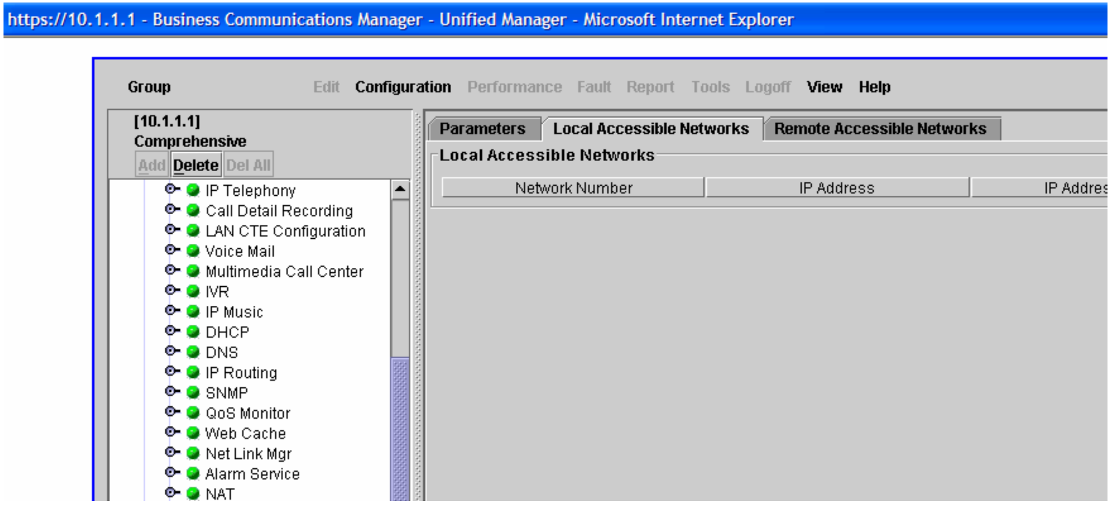
Below are all the settings:



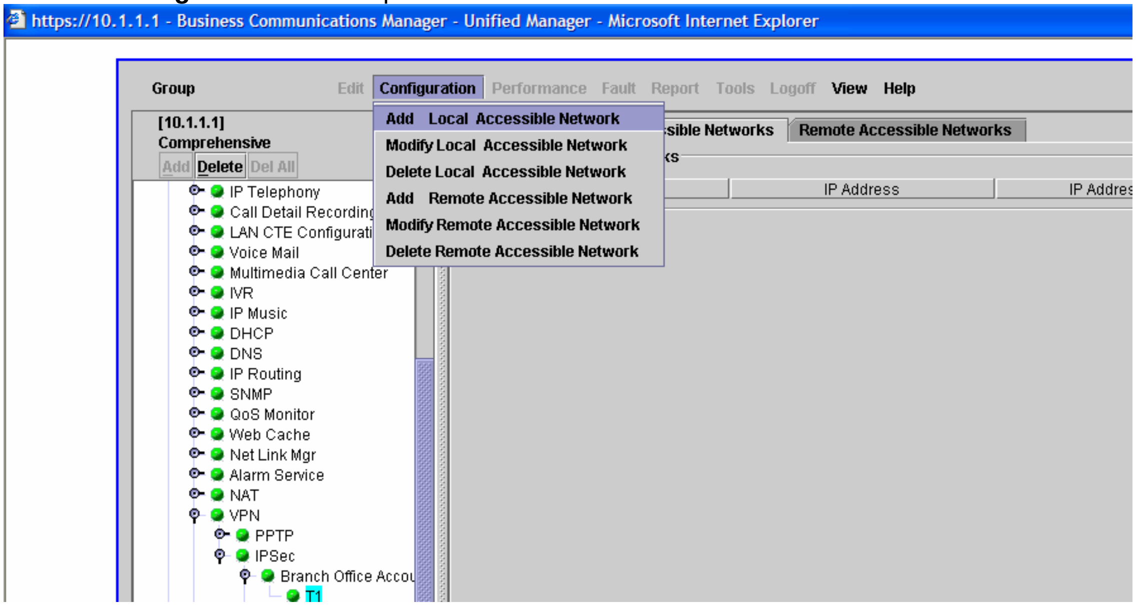
Tunnel Number	T1 (Read-Only Field)
IPSec Status	Disconnected
PFS Enabled	Yes
Idle Timeout	00:15:00
Highest Encryption	ESP-3DES-MD5
Preshared Key Type	Text
Preshared Key	************************************
Rekey Timeout	08:00:00
Rekey Data Count (KB)	0
Local Endpoint Address	30.1.1.1
Remote Endpoint Address	30.1.1.2
Send All Traffic Through IPSec Tunnel	No
Create Firewall Rules for this Tunnel	Yes
Keep-Alive Enabled	Yes

Configuring local and remote accessible networks

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

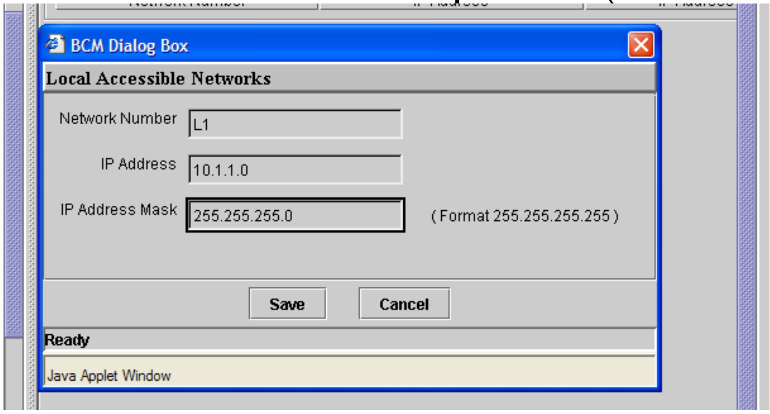


Click on **Configuration** in the top menu bar and select **Add Local Accessible Network**:



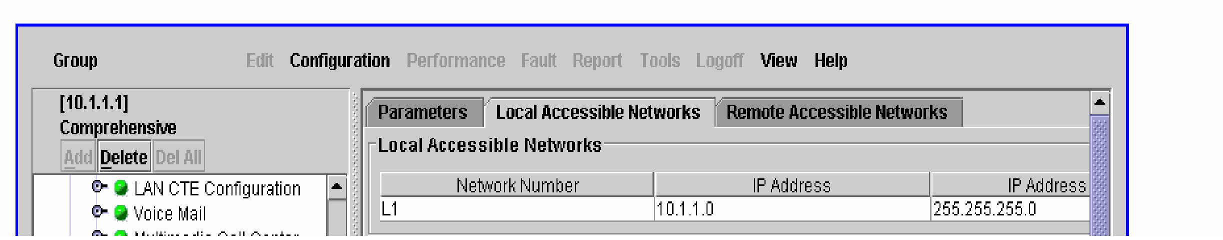
Contivity – BCM IPSec Peer-to-Peer Tunnel Using Pre-Shared Key Authentication

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



BCM Dialog Box
Local Accessible Networks
Network Number: L1
IP Address: 10.1.1.0
IP Address Mask: 255.255.255.0 (Format 255.255.255.255)

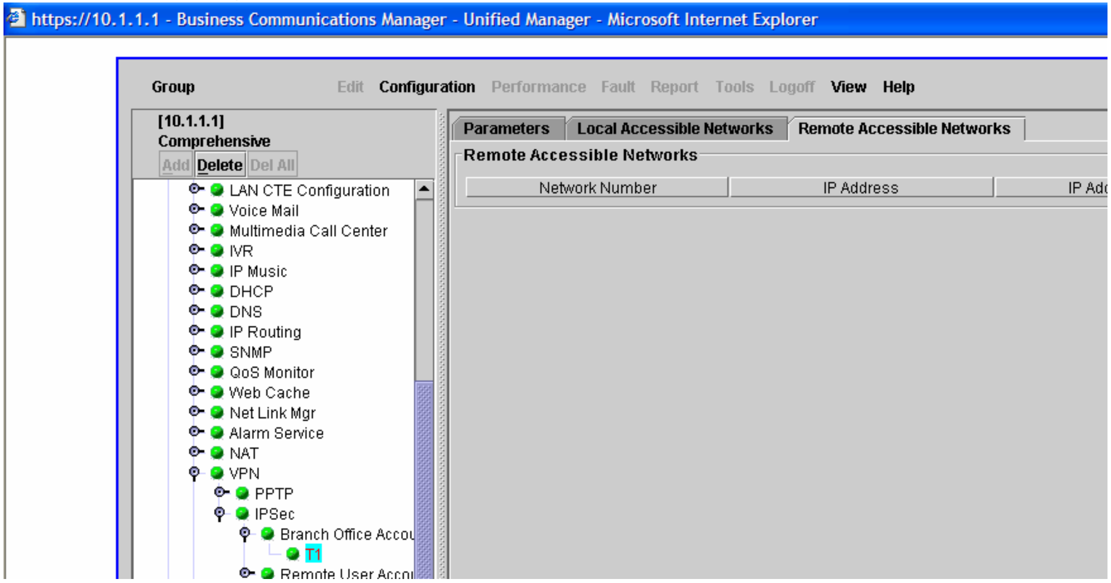
A local network is defined:



Local Accessible Networks

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:

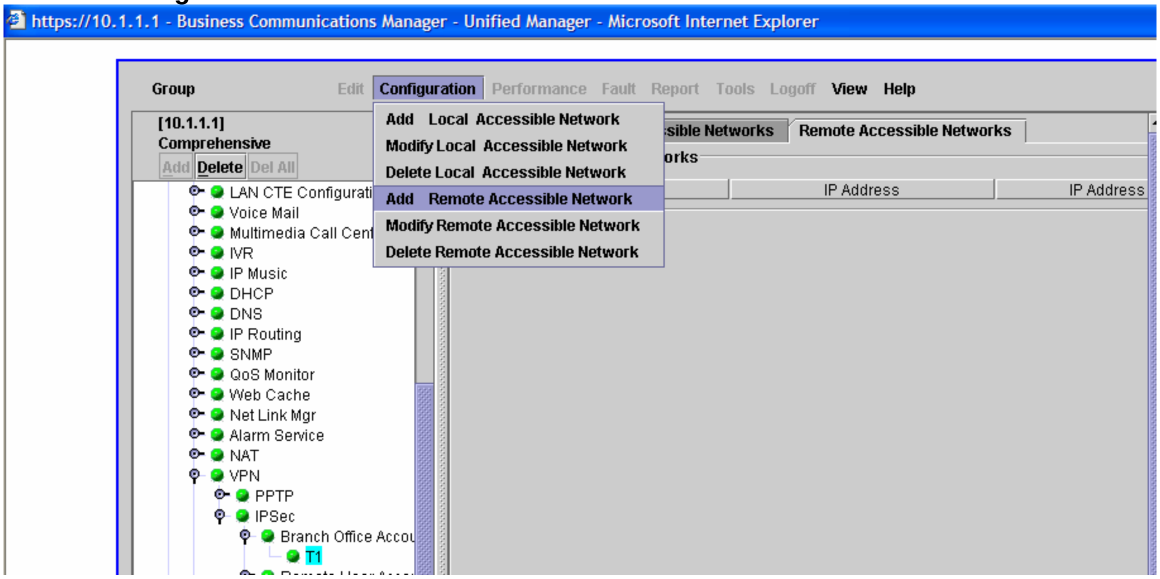


https://10.1.1.1 - Business Communications Manager - Unified Manager - Microsoft Internet Explorer

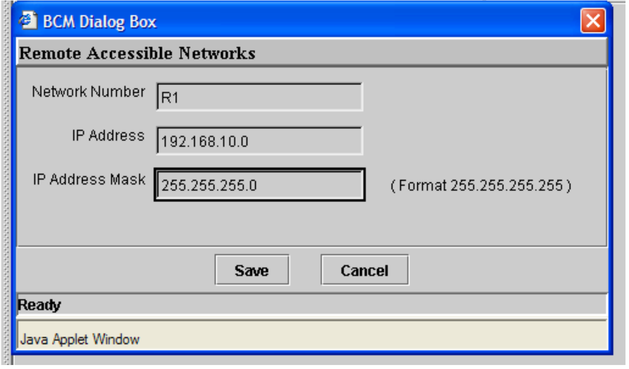
Remote Accessible Networks

Network Number	IP Address	IP Add

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


https://10.1.1.1 - Business Communications Manager - Unified Manager - Microsoft Internet Explorer
Group
Edit
Configuration
Performance
Fault
Report
Tools
Logoff
View
Help
[10.1.1.1]
Comprehensive
Add
Delete
Del All
Add Local Accessible Network
Modify Local Accessible Network
Delete Local Accessible Network
Add Remote Accessible Network
Modify Remote Accessible Network
Delete Remote Accessible Network
sible Networks
Remote Accessible Networks
orks
IP Address
IP Address
LAN CTE Configurati
Voice Mail
Multimedia Call Cent
IVR
IP Music
DHCP
DNS
IP Routing
SNMP
QoS Monitor
Web Cache
Net Link Mgr
Alarm Service
NAT
VPN
PPTP
IPSec
Branch Office Accou
T1

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

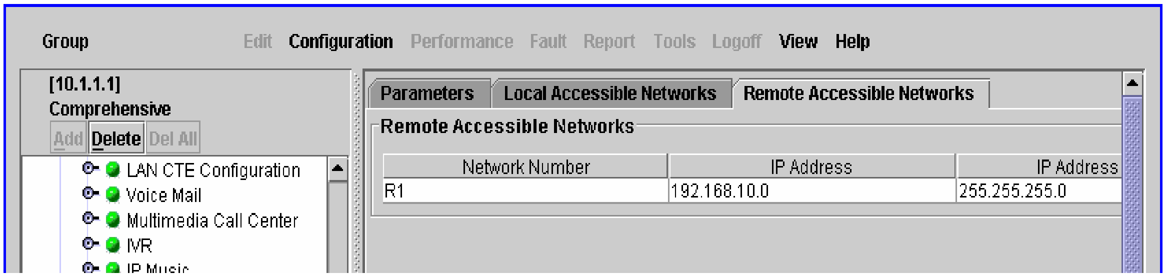


Network Number: R1

IP Address: 192.168.10.0

IP Address Mask: 255.255.255.0 (Format 255.255.255.255)

A remote network is created:



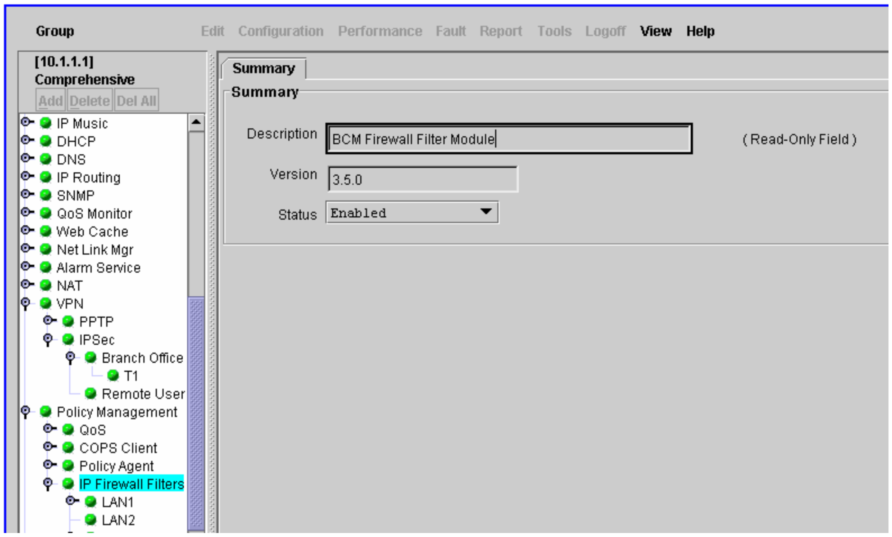
Remote Accessible Networks

Network Number	IP Address	IP Address
R1	192.168.10.0	255.255.255.0

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 section Configuring Branch Office tunnel parameters

On the navigation Tree, expand **Policy Management** key and click on **IP Firewall Filters**:



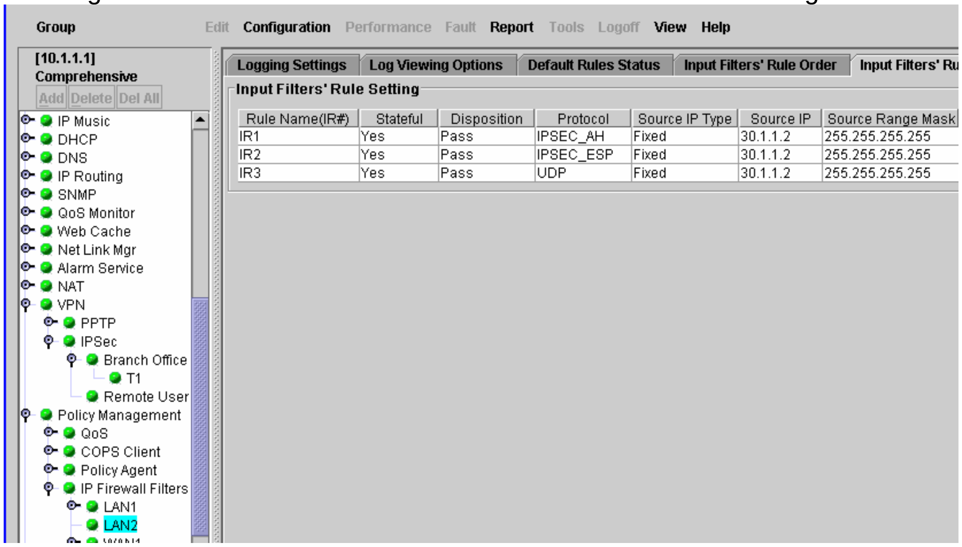
Summary

Description: BCM Firewall Filter Module (Read-Only Field)

Version: 3.5.0

Status: Enabled

Expand **Policy Management** key, then expand **IP Firewall Filters** Key and click on **LAN2**. The following three rules illustrated on a screen shot below must be configured:



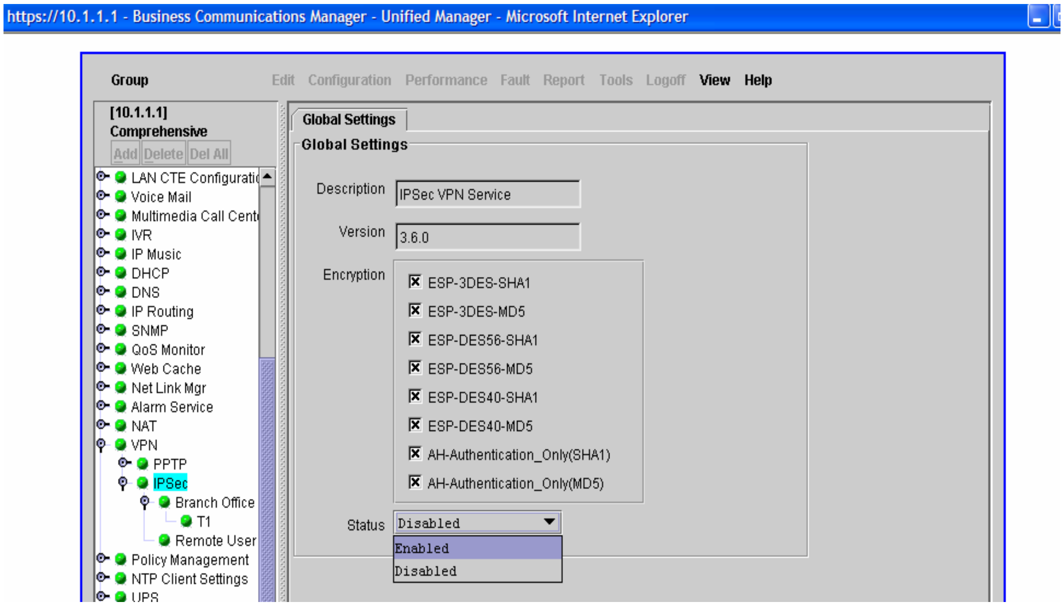
Input Filters' Rule Setting

Rule Name(IR#)	Stateful	Disposition	Protocol	Source IP Type	Source IP	Source Range Mask
IR1	Yes	Pass	IPSEC_AH	Fixed	30.1.1.2	255.255.255.255
IR2	Yes	Pass	IPSEC_ESP	Fixed	30.1.1.2	255.255.255.255
IR3	Yes	Pass	UDP	Fixed	30.1.1.2	255.255.255.255

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**:



Global Settings

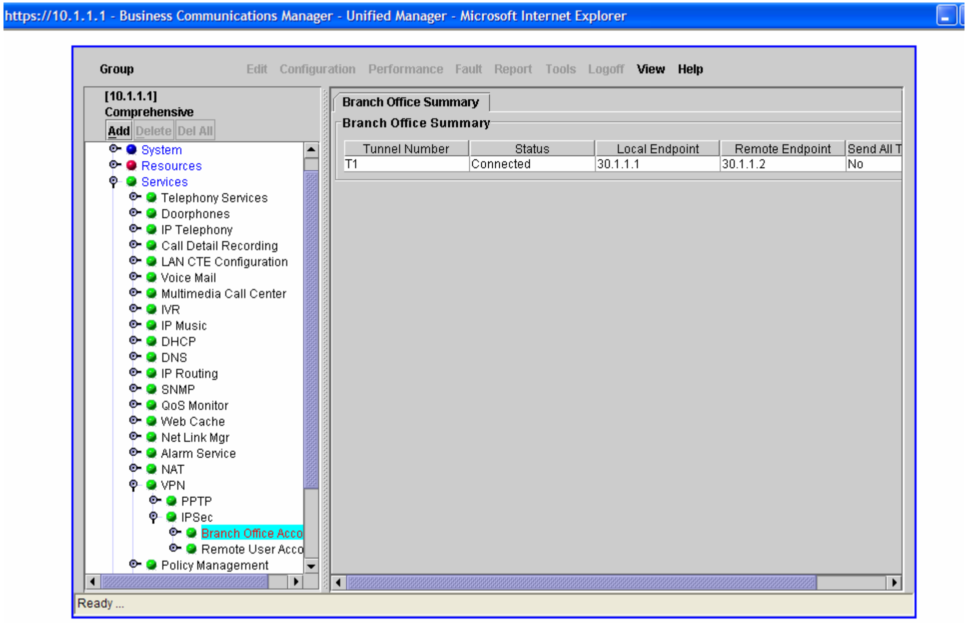
Description: IPSec VPN Service

Version: 3.6.0

Encryption:
- ☒ ESP-3DES-SHA1
- ☒ ESP-3DES-MD5
- ☒ ESP-DES56-SHA1
- ☒ ESP-DES56-MD5
- ☒ ESP-DES40-SHA1
- ☒ ESP-DES40-MD5
- ☒ AH-Authentication_Only(SHA1)
- ☒ AH-Authentication_Only(MD5)

Status: Disabled
- Enabled
- Disabled

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



Branch Office Summary

Branch Office Summary

Tunnel Number	Status	Local Endpoint	Remote Endpoint	Send All T
T1	Connected	30.1.1.1	30.1.1.2	No

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
```

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).

We welcome you 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

Author: Hitesh Patel