

[🏠 How-To Home](#)**CLOUD NETWORKS**[Introduction](#)[FAQ](#)[All Articles](#)**HAVE FEEDBACK?**

We love customer feedback. Help us improve our products and service by [leaving your comments](#).

[🔗 Edit This Article](#)

Configure Remote Access VPN Service on a Vyatta Appliance

Last updated on: 2015-09-29 Authored by: Sameer Satyam

You can configure a Vyatta Appliance to act as a remote access VPN gateway so that clients can securely connect to their infrastructure in the Rackspace cloud.

Introduction

This article shows how to configure the Vyatta Appliance for Remote Access VPN using L2TP/IPsec with Pre-Shared Keys for authentication.

For a comprehensive guide to VPN configuration on the Vyatta, click [here](#).

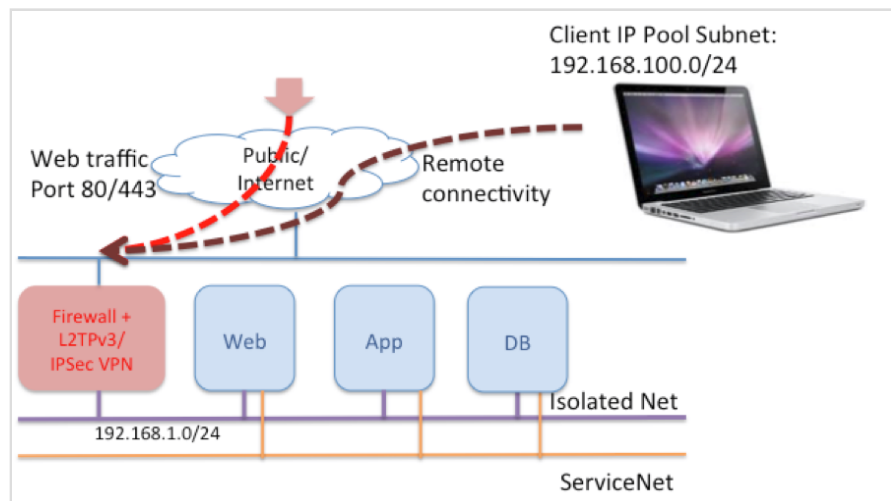
For guidance on configuring the relevant firewall rules to allow remote-access VPN on the Vyatta please refer to the following article:

[Configuring interface based firewall on the Vyatta network appliance](#)

The VPN access using L2TP/IPsec with pre-shared key works as follows:

1. The remote client first establishes an IPsec tunnel with the VPN server (Vyatta).
2. The L2TP client and server then establish an L2TP tunnel on top of the IPsec tunnel.
3. Finally, a PPP session is established on top of the L2TP tunnel, i.e., the PPP packets are encapsulated and sent/received inside the L2TP tunnel.

In the following illustration, traffic from remote access clients enters on the Public interface on the Vyatta appliance. 192.168.100.0/24, is the subnet assigned to the clients when the VPN session is established. The outside-address X.X.X.X address is the Vyatta's Public IP address.



Configure the L2TP/IPsec VPN on the Vyatta Appliance

Step 1. Set Up Vyatta as an L2TP/IPsec VPN Server

In the following example eth0 is the Public interface enabled for IPsec. The pre-shared secret is "SUPERSECRET".

1. Log onto the Vyatta Appliance using ssh:

```
ssh vyatta@X.X.X.X
```

Where X.X.X.X is the IP address of the vyatta's Public interface. You'll see a Welcome to Vyatta message and a prompt to enter your Vyatta password.

Once you're logged into the appliance, you can enter a "?" or press the Tab key for help.

2. Enter configuration mode:

```
vyatta@vyatta: configure
[edit]
vyatta@vyatta#
```

The # symbol indicates you're in configuration mode.

3. Define the interface used for IPsec; in this case eth0 is the public interface enabled for IPsec :

```
set vpn ipsec ipsec-interfaces interface eth0
```

4. Enable NAT traversal allowing IPsec packets to travel through NAT points in the network:

```
set vpn ipsec nat-traversal enable
```

5. Set the remote client IP subnet from which connection is initiated. To allow clients to connect from anywhere specify 0.0.0.0/0 as the allowed-network

```
set vpn ipsec nat-networks allowed-network 0.0.0.0/0
```

6. Commit the change:

```
vyatta@vyatta# commit
```

7. Save the change:

```
vyatta@vyatta# save
```

```
Saving configuration to /config/config.boot
```

8. Show the IPsec configuration:

```
vyatta@vyatta# show vpn ipsec
ipsec-interfaces {
  interface eth0
}
nat-networks {
  allowed-network 0.0.0.0/0 {
  }
}
nat-traversal enable
```

Step 2. Configure L2TP remote access address and the client pool

1. Bind the L2TP server to the external address:

```
set vpn l2tp remote-access outside-address X.X.X.X
```

Where X.X.X.X represents the Vyatta eth0 interface IP address.

2. Set up the pool of IP addresses that remote VPN clients will assume.

```
set vpn l2tp remote-access client-ip-pool start 192.168.100.1
```

Where 192.168.100.10 represents the start IP address for the client pool.

```
set vpn l2tp remote-access client-ip-pool stop 192.168.100.100
```

Where 192.168.100.100 represents the end IP address for the client pool.

Step 3. Configure the IPsec pre-shared secret and user authentication

1. Set the IPsec authentication mode to the pre-shared secret:

```
set vpn l2tp remote-access ipsec-settings authentication mode pre-shared-secret
```

2. Set the pre-shared secret:

```
set vpn l2tp remote-access ipsec-settings authentication pre-shared-secret SUPERSECRE
```



3. Set the L2TP remote access authentication mode to local:

```
set vpn l2tp remote-access authentication mode local
```

This indicates that user authentication occurs locally on the Vyatta Appliance.

4. Set the L2TP remote access username and password:

```
set vpn l2tp remote-access authentication local-users username test password test
```

test and **test** represent the client username and password.

5. Commit the change:

```
vyatta@vyatta# commit
```

6. Save the change:

```
vyatta@vyatta# save  
Saving configuration to /config/config.boot
```

7. View the L2TP configuration:

```
vyatta@vyatta# show vpn l2tp remote-access
authentication {
  local-users {
    username test {
      password test
    }
  }
  mode local
}
client-ip-pool {
  start 192.168.100.1
  stop 192.168.100.100
}
ipsec-settings {
  authentication {
    mode pre-shared-secret
    pre-shared-secret SUPERSECRET
  }
}
outside-address X.X.X.X
```

This completes the L2TP configuration on the Vyatta Appliance. If you later want to edit the L2TP remote access configuration, enter `remote-access` while in the `edit` mode on the Vyatta Appliance.

```
vyatta@vyatta# edit vpn l2tp remote-access
[edit vpn l2tp remote-access]
vyatta@vyatta#
```

The following section describes how to configure client VPN settings on the Mac and Windows clients.

Mac Client Configuration

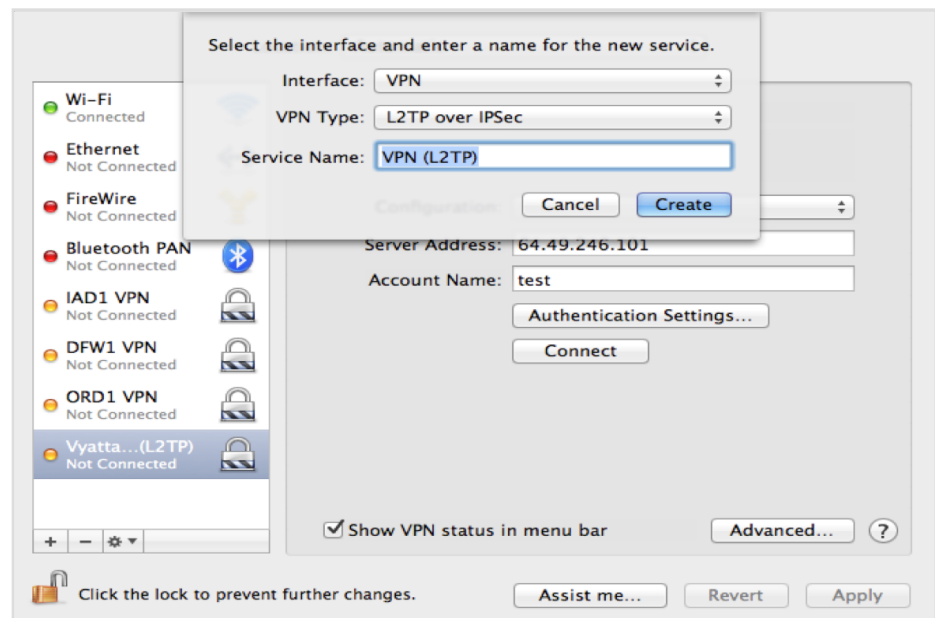
For Mac clients you'll need to configure the following options:

- Network Preferences
- Connection Details
- Authentication Settings

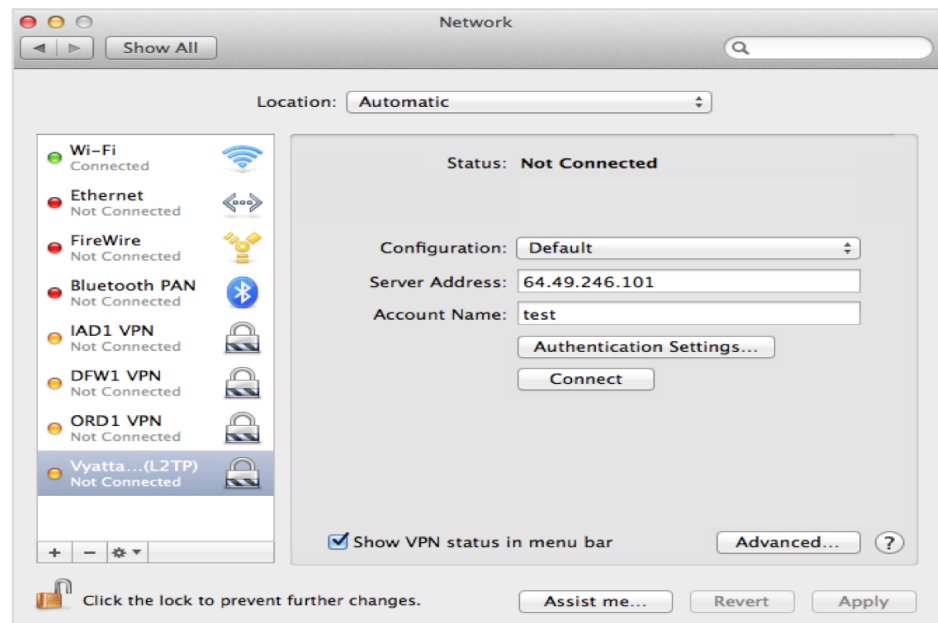
Mac Client Network Preferences

Select System Preferences from the Apple menu, then click Network.

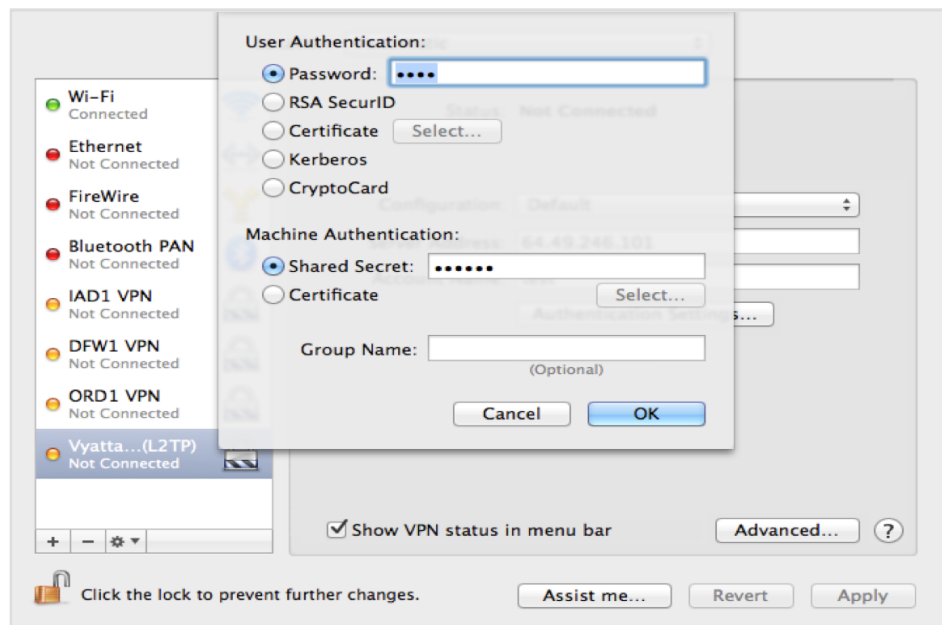
Select the Vyatta VPN (LT2P) network and update the following options:



Mac Client Connection Details

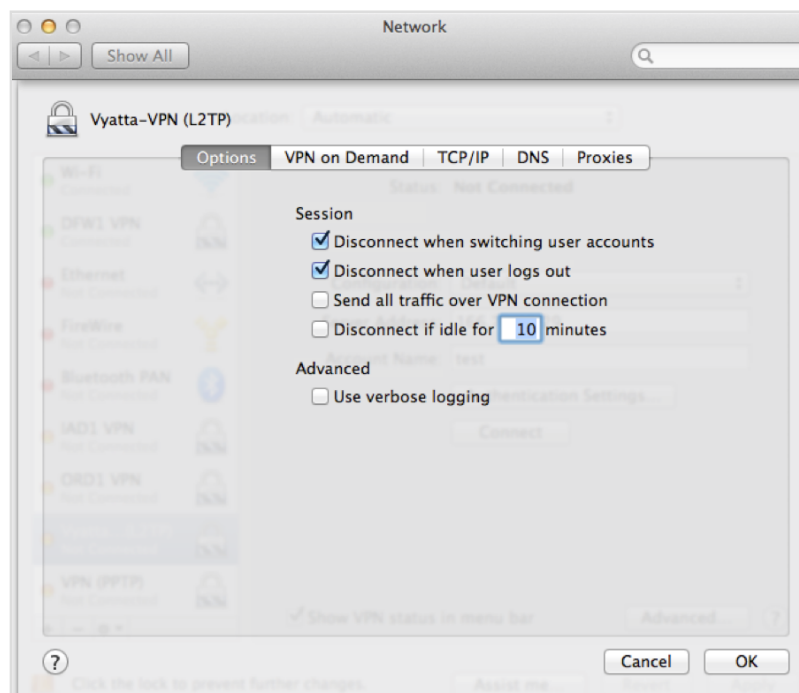


Mac Client Authentication Settings



Configure Split Tunnel on the Mac Native IPsec Client

If you want the VPN connection to be used only to access your cloud servers, and all other traffic (internet traffic) will not use the IPsec tunnel, ensure that **Send all traffic over VPN connection** is unchecked under Options.

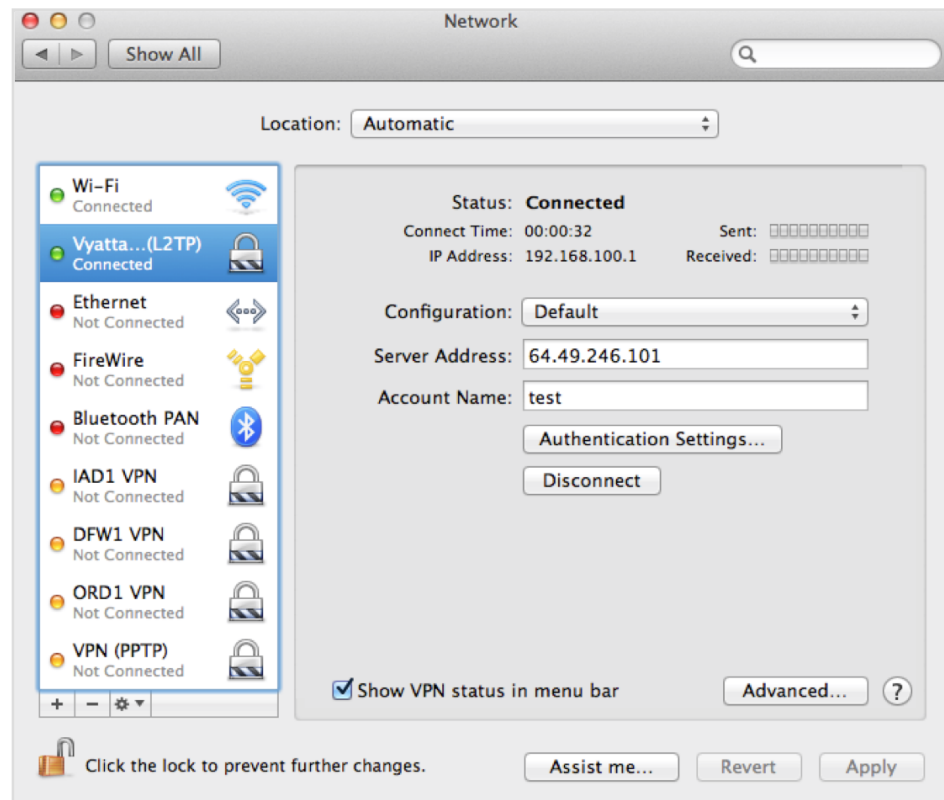


After enabling split tunnel on a MAC client, you may need to add a static route to force all traffic destined to the VPN network over the PPP interface. For example:

```
sudo /sbin/route add -net 192.168.x.0/24 -interface ppp0
```

Where 192.168.x.0/24 is the CIDR of your Cloud Network.

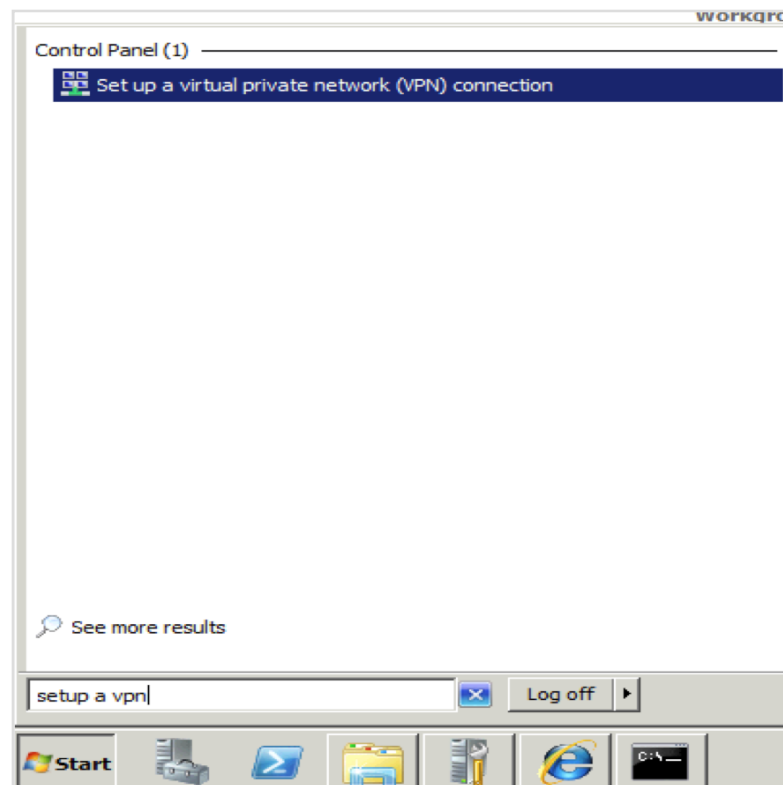
The following screenshot shows a successful connection:



Windows Client Configuration

To configure Windows clients, update the following network options.

Set up a virtual private network (VPN) connection



Type the Internet Address to Connect To

Create a VPN connection

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

☐ Use a smart card

☐ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☒ Don't connect now; just set it up so I can connect later

Next **Cancel**

Enter Login Credentials

Create a VPN connection

Type your user name and password

User name:

Password:

☒ Show characters

☒ Remember this password



Domain (optional):


Create **Cancel**

Connect to the VPN

Create a VPN connection

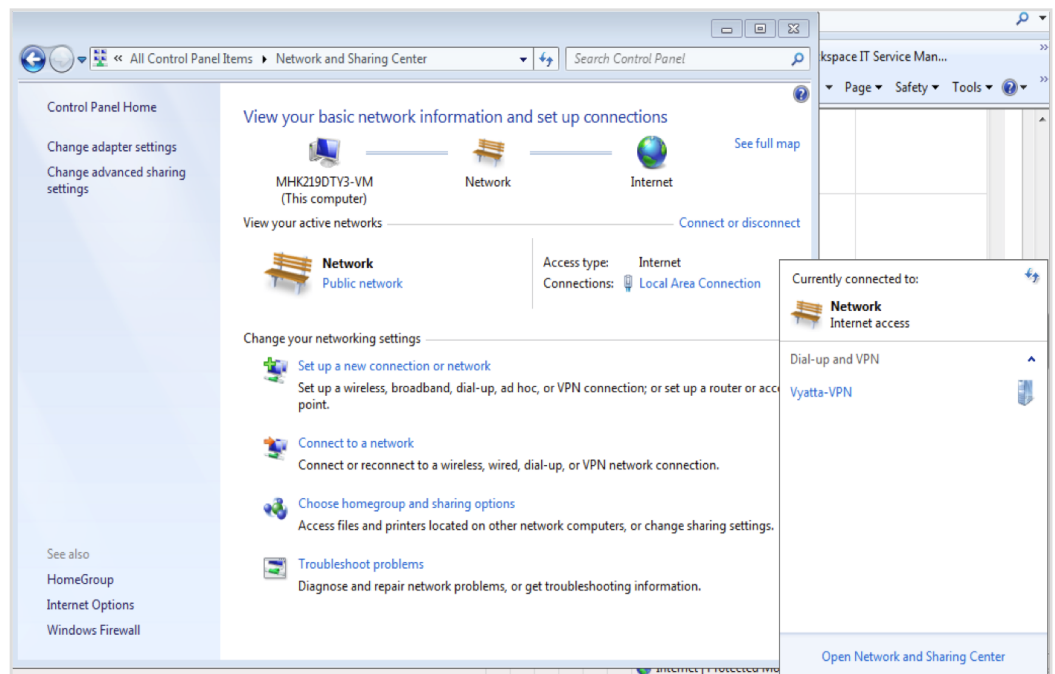
The connection is ready to use

 ————— 

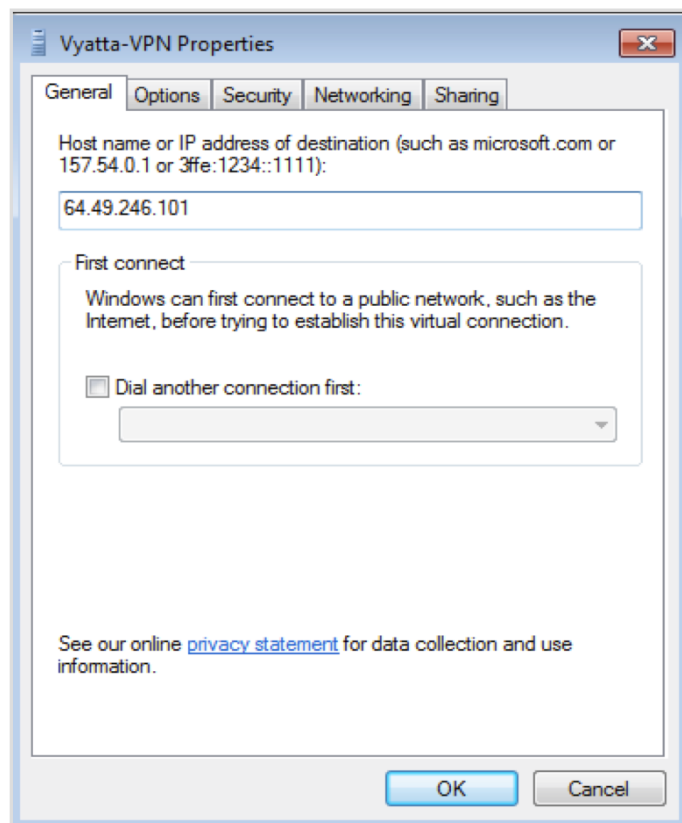
 **Connect now**

Close

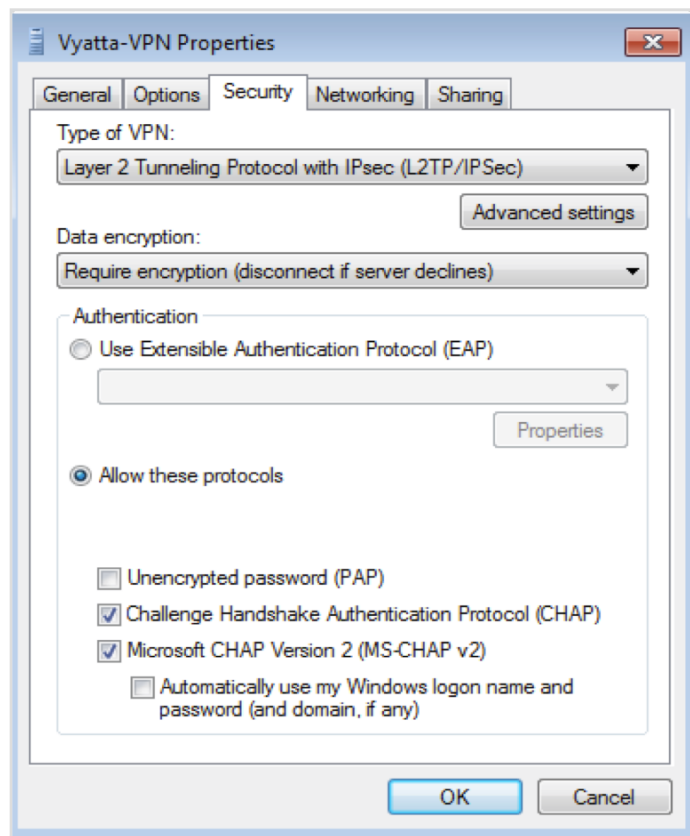
Configure Vyatta VPN Properties



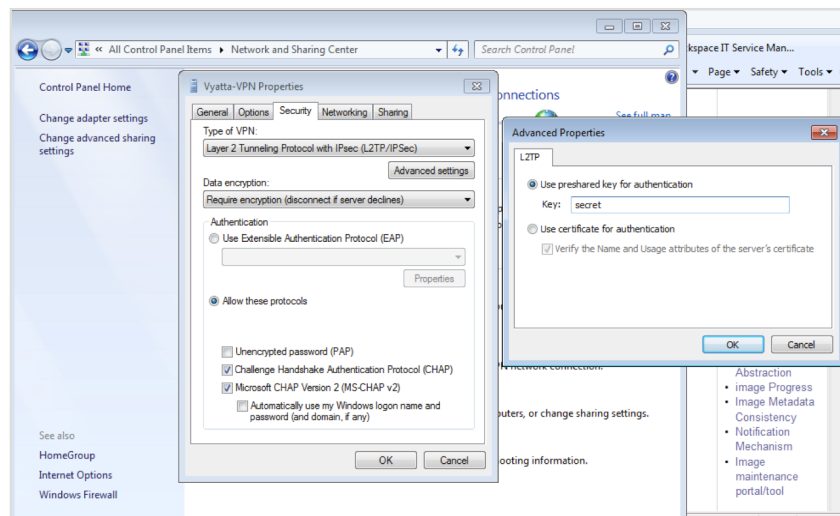
Configure VPN Properties General Configuration Tab



Configure VPN Security Settings Tab



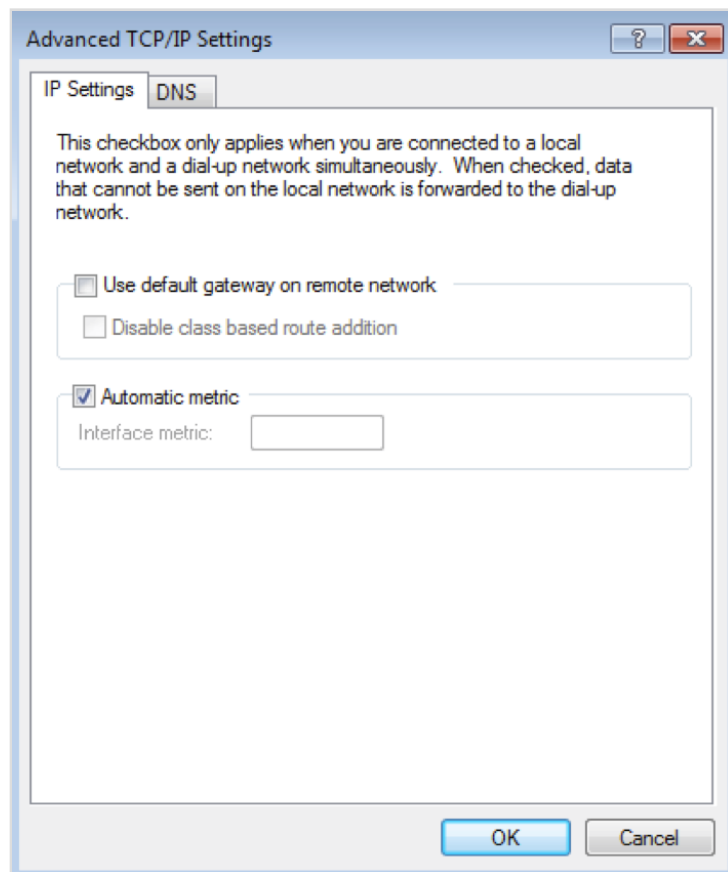
Configure Advanced Properties



Configure Split Tunnel on the Windows Native IPsec Client

On a Windows client, by default, after the VPN configuration is created, the client is configured for Full Tunneling (all traffic flows across the VPN.) If you want to configure the client for Split Tunneling (where internet traffic does not flow across the VPN), you can modify the client VPN configuration as follows:

1. Select, Start, Control Panel, Network Connections.
2. Right-click the icon for the VPN connection (Vyatta-L2TP), then click Properties.
3. Click Advanced. Uncheck the "Use default gateway on remove network" checkbox.
4. Click OK three times.



View Client Connection

Do the following to check the client's connection:

View the Network and Sharing Center to see client logged into Vyatta VPN.

Run ipconfig in a Command Prompt window to see the client's IP address.

Show the configuration on the Vyatta Appliance:

```
vyatta@vyatta:~$ show vpn remote-access
Active remote access VPN sessions:
User      Proto Iface  Tunnel IP      TX byte RX byte  Time
-----
test      L2TP  l2tp0   192.168.100.1  1.0K    6.1K    00h01m26s
```



Continue the conversation in the [Rackspace Community](#).

Start building on our Managed Cloud today.

[Sign Up Now](#)

©2017 Rackspace US, Inc.

Except where otherwise noted, content on this site is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License



[See license specifics and DISCLAIMER](#)

SUPPORT NETWORK

[Support Network Home](#)
[Rackspace How-To](#)
[White Papers](#)
[API Documentation](#)
[Developer Center](#)
[Rackspace Community](#)

ABOUT RACKSPACE

[About](#)
[Customer Stories](#)
[Events](#)
[Programs](#)
[News](#)
[Contact Information](#)
[Legal](#)
[Careers](#)

BLOGS

[The Rackspace Blog](#)
[Developer Blog](#)

SITE INFORMATION

[Privacy Statement](#)
[Website Terms](#)
[Trademarks](#)
[Sitemap](#)

© 2017 Rackspace US, Inc.