Avaya Solution & Interoperability Test Lab

Application Notes for configuring FatPipe MPVPN® in Avaya Aura® Environments - Issue 1.0

Abstract

These Application Notes describe the steps used to configure FatPipe MPVPN® in Avaya Aura® Environments. FatPipe MPVPN® provides WAN link Disaster Recovery and Business Continuity Planning for Virtual Private Network (VPN) connectivity.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps used to configure FatPipe MPVPN® in Avaya Aura® Infrastructure. FatPipe MPVPN® provides WAN link Disaster Recovery and Business Continuity Planning for VPN connectivity.

During the DevConnect Compliance test, an enterprise site and a remote site were connected via FatPipe MPVPN® virtual appliances. The enterprise site consisted of Avaya Aura® core products and endpoints as shown in **Figure 1** and the remote site consisted of remote endpoints and an Avaya G450 gateway. FatPipe MPVPN® virtual appliances were deployed on both enterprise and remote site.

2. General Test Approach and Test Results

The general test approach was to verify telephony functionality between the enterprise site and remote site connected via FatPipe MPVPN.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from remote site.
- Outgoing calls from the enterprise site to remote site.
- Incoming and Outgoing PSTN calls to/from both enterprise site and remote site.
- Audio and Video calls between enterprise and remote site.
- Fax calls between enterprise and remote site.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Direct IP-to-IP media enterprise and remote sites using SIP and H.323 endpoints.

Additionally, QoS for SIP and RTP was also tested. QoS was applied based of port and IP address. Data traffic generator was used while placing audio/video calls to ensure that they are successful.

Failover tests included testing for WAN link redundancy. Upon failure of the first WAN link, second WAN link services the traffic.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for FatPipe MPVPN® with the following observations:

- During WAN link failover test, a small call load test run was started from the remote site. When the primary WAN link is failed, a small number of “calls in progress” calls failed, which was expected. Calls that were connected continued to work.

2.3. Support

For technical support on FatPipe can be obtained via following means:

- **Phone:** +1-801-281-3434, option 3
- **Email:** support@fatpipeinc.com
- **Web:** http://www.fatpipeinc.com/support

3. Reference Configuration

Figure 1 illustrates the test configuration. On the left is enterprise site composed of Avaya Aura® core components and remote site composed of remote users. Both sites were connected via FatPipe MPVPN® WAN links.

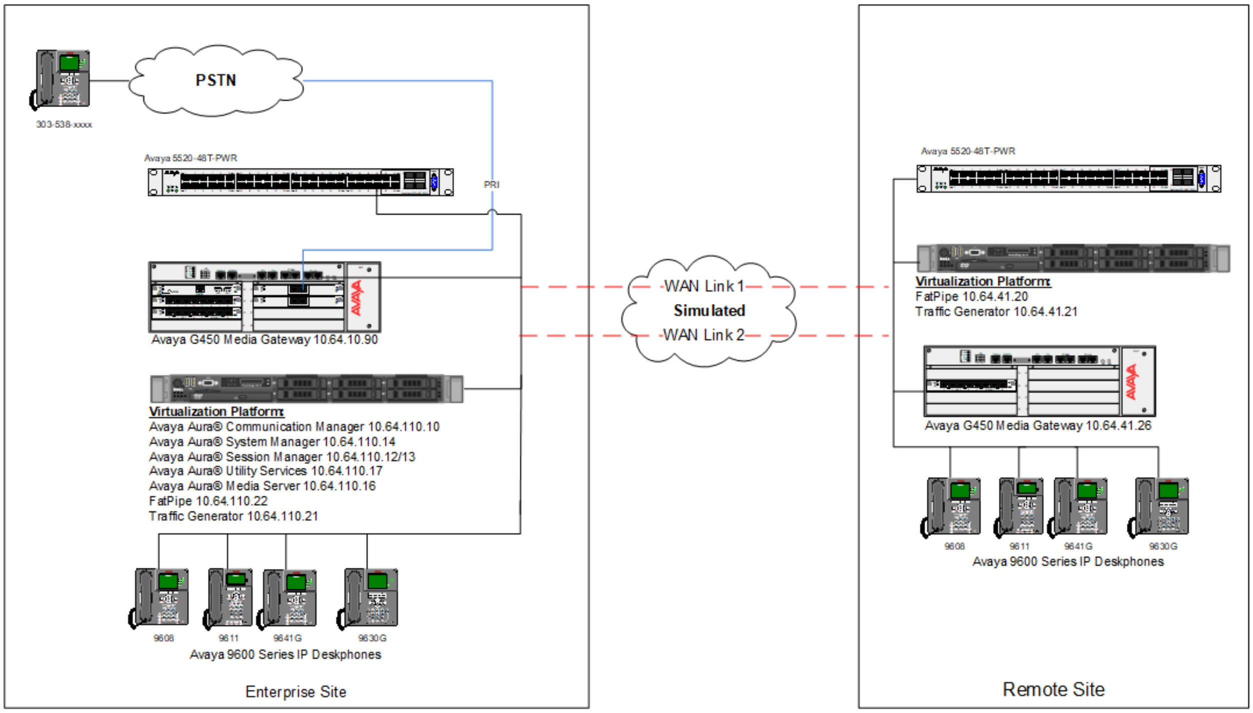

PSTN
303-538-xxxx
Avaya 5520-48T-PWR
PRI
Avaya G450 Media Gateway 10.64.10.90
Virtualization Platform:
Avaya Aura® Communication Manager 10.64.110.10
Avaya Aura® System Manager 10.64.110.14
Avaya Aura® Session Manager 10.64.110.12/13
Avaya Aura® Utility Services 10.64.110.17
Avaya Aura® Media Server 10.64.110.16
FatPipe 10.64.110.22
Traffic Generator 10.64.110.21
9608
9611
9641G
9630G
Avaya 9600 Series IP Deskphones
Enterprise Site
WAN Link 1
Simulated
WAN Link 2
Avaya 5520-48T-PWR
Virtualization Platform:
FatPipe 10.64.41.20
Traffic Generator 10.64.41.21
Avaya G450 Media Gateway 10.64.41.26
9608
9611
9641G
9630G
Avaya 9600 Series IP Deskphones
Remote Site

Figure 1: Test Setup of FatPipe in Avaya Aura® infrastructure

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Session Manager	7.1.1.0.711008
Avaya Aura® System Manager	7.1.1.0 711006931
Avaya Aura® Communication Manager	7.1.1.0.0.532.23985
Avaya G450 Media Gateway	38.20.1
Avaya Aura® Utility Services	7.1.0.0.0.18
Avaya Aura® Media Server	7.8.0.333
Avaya 9600 Series IP Deskphones SIP 96x0 SIP 9608 H.323 96x0 H.323 9608	 2.6.17 7.1.0.1 3.2.8 6.6.5
Avaya one-X® Communicator	6.2 SP 12
Avaya Equinox™ for Windows	3.2.1.11
FatPipe MPVPN®	7.1.2r180vx13

5. Configure Avaya Aura® Environment

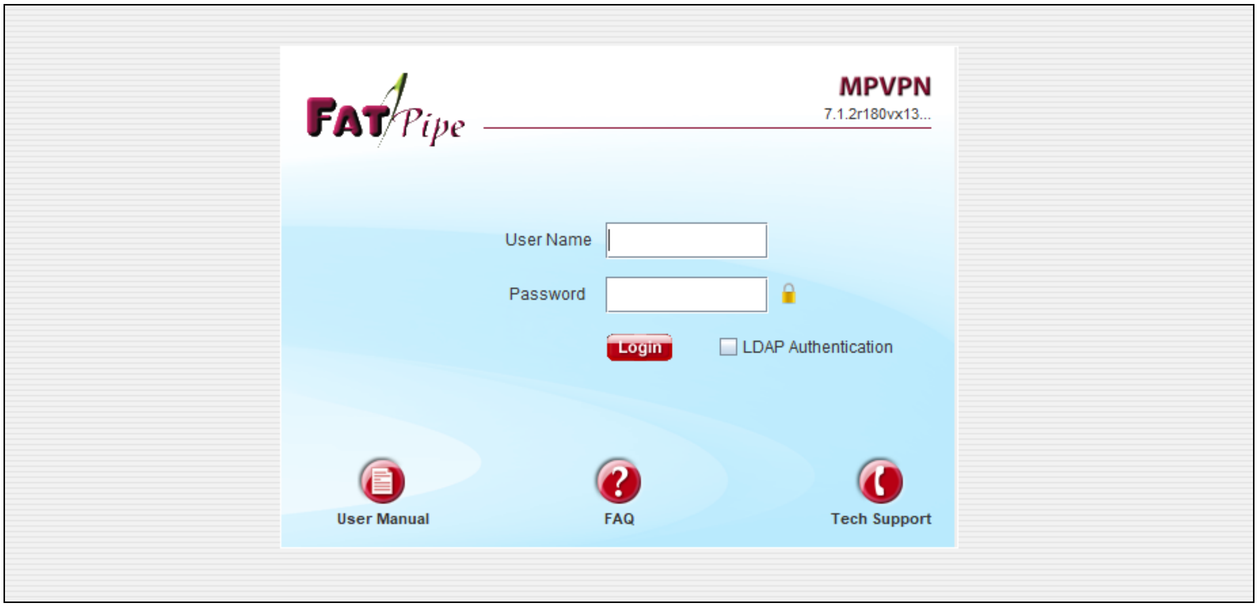
A standard set configuration of all Avaya Aura® core components was used. Avaya Aura® core components and endpoints on enterprise site were part of 10.64.110.0/24 network. Remote users/endpoints on remote site were of 10.64.40.0/24 network. Both of the 10.64.110.0 and 10.64.40.0 network were configured to not reach each other without the use of FatPipe MPVPN®. Enterprise site and remote site were reachable via 10.64.101.0 and 10.64.102.0 networks (simulated WAN links).

6. Configure FatPipe MPVPN®

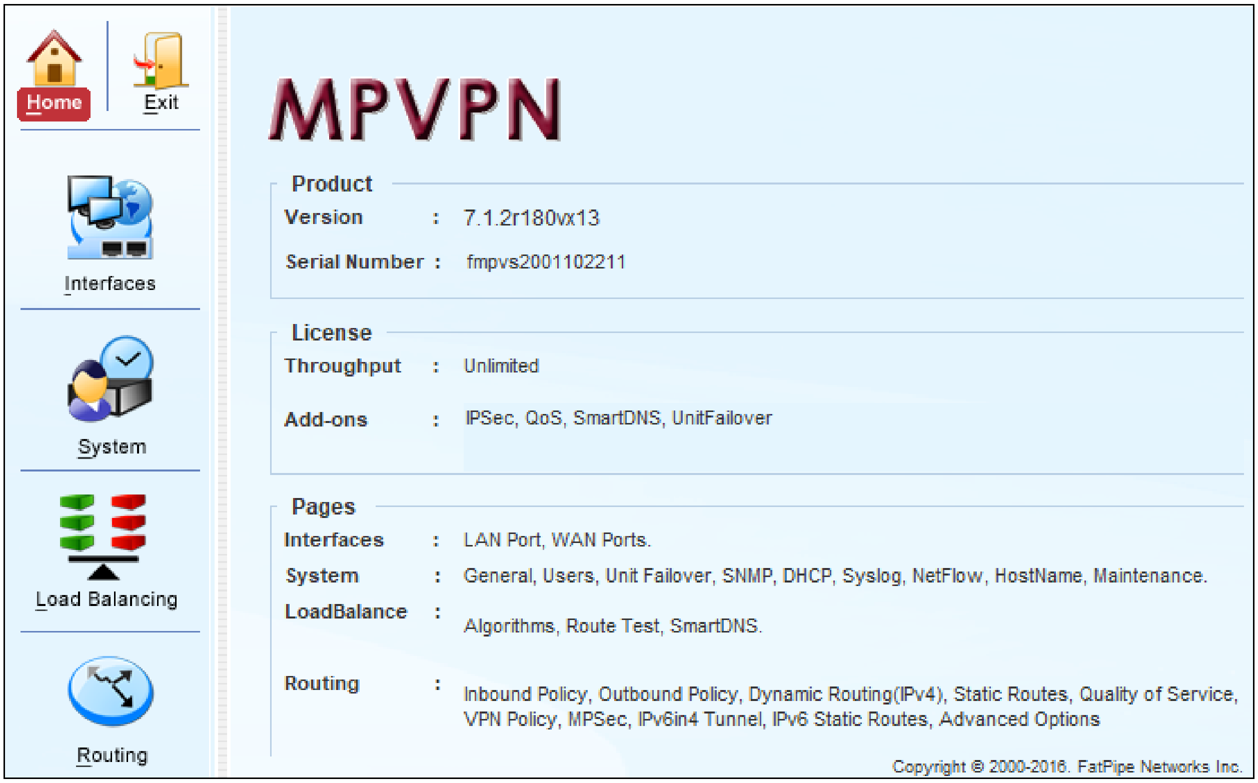
Configuration for FatPipe MPVPN® is performed via Internet Explorer browser.

6.1. Enterprise Site

Open Internet Explorer and point the browser to the FatPipe MPVPN®'s IP Address. Log in using appropriate credentials.



Once logged in, FatPipe MPVPN® configuration window (Java based) will open.



Product

Version : 7.1.2r180vx13

Serial Number : fmpvs2001102211

License

Throughput : Unlimited

Add-ons : IPSec, QoS, SmartDNS, UnitFailover

Pages

Interfaces : LAN Port, WAN Ports.

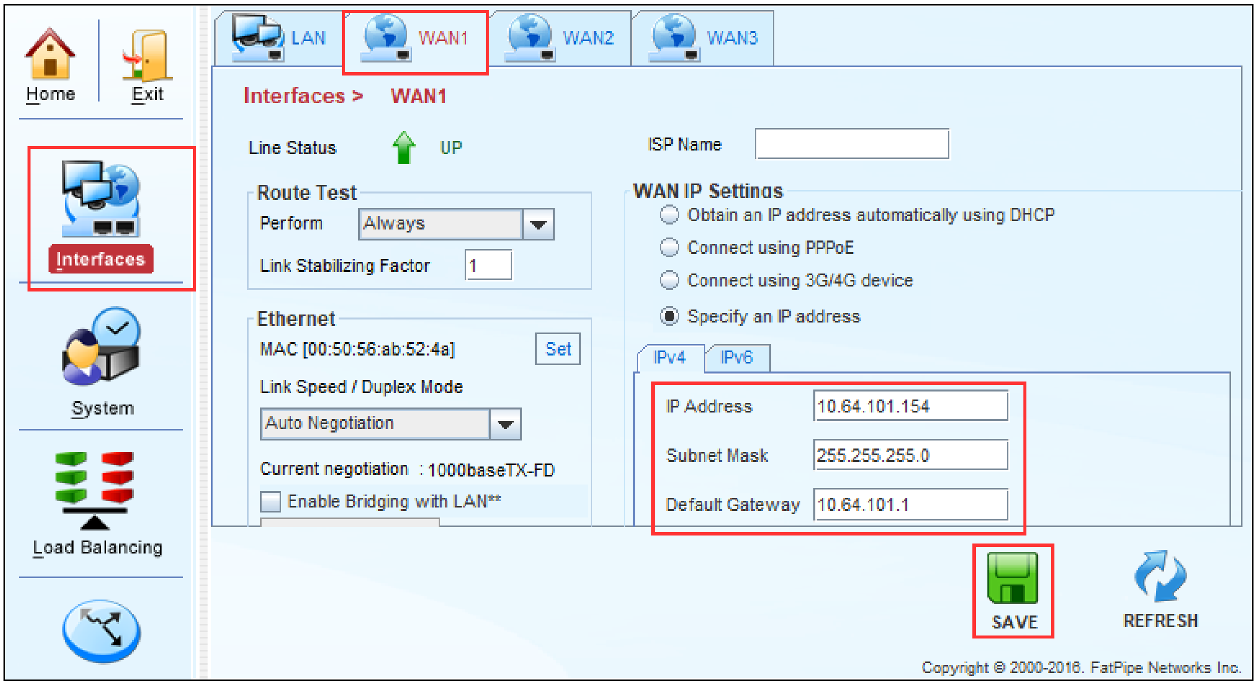
System : General, Users, Unit Failover, SNMP, DHCP, Syslog, NetFlow, HostName, Maintenance.

LoadBalance : Algorithms, Route Test, SmartDNS.

Routing : Inbound Policy, Outbound Policy, Dynamic Routing(IPv4), Static Routes, Quality of Service, VPN Policy, MPSec, IPv6in4 Tunnel, IPv6 Static Routes, Advanced Options

Copyright © 2000-2016. FatPipe Networks Inc.

On the left pane select **Interfaces;** select the **WAN1** tab and configure the **IPv4** information. During Compliance testing, 10.64.101.154 IP Address was used for WAN1 connectivity. Click **SAVE** once done.



Interfaces > WAN1

Line Status UP

ISP Name

Route Test

Perform Always

Link Stabilizing Factor 1

Ethernet

MAC [00:50:56:ab:52:4a]

Link Speed / Duplex Mode

Auto Negotiation

Current negotiation : 1000baseTX-FD

□ Enable Bridging with LAN**

WAN IP Settings

○ Obtain an IP address automatically using DHCP

○ Connect using PPPoE

○ Connect using 3G/4G device

● Specify an IP address

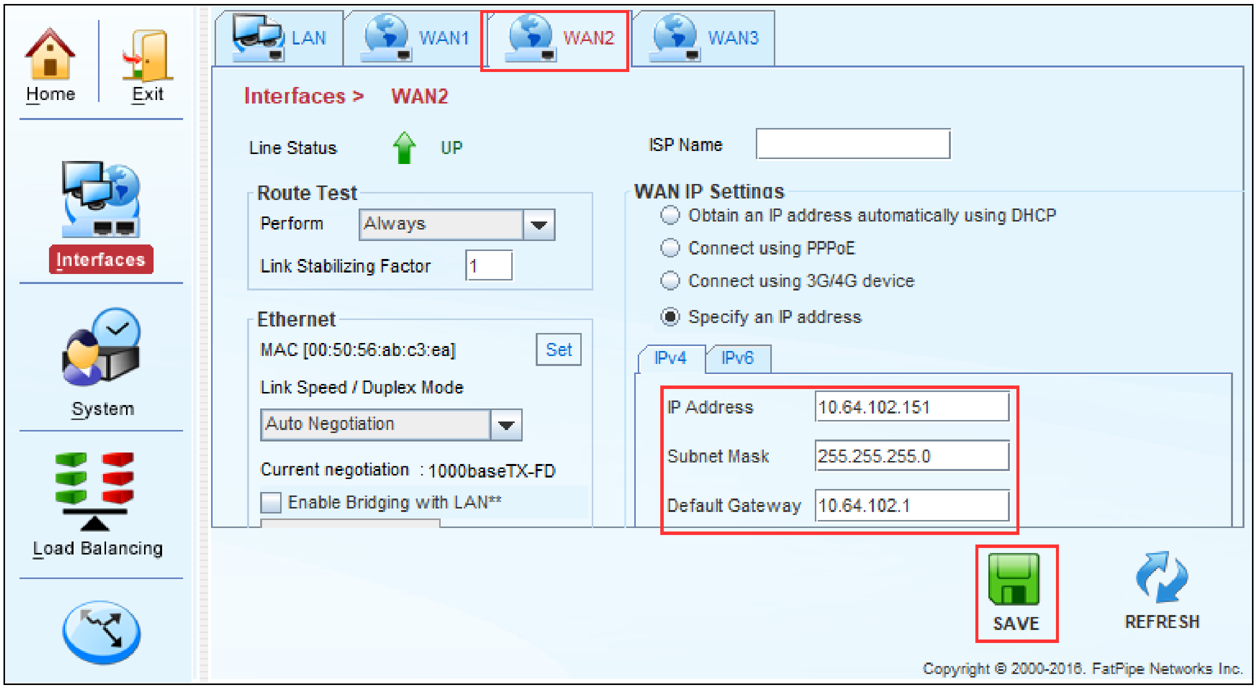
IP Address 10.64.101.154

Subnet Mask 255.255.255.0

Default Gateway 10.64.101.1

Copyright © 2000-2016. FatPipe Networks Inc.

Continuing from above, select the **WAN2** tab and configure the **IPv4** information. During Compliance testing, 10.64.102.151 IP Address was used for WAN2 connectivity. Click **SAVE** once done.



Interfaces > WAN2

Line Status UP

ISP Name

Route Test

Perform: Always

Link Stabilizing Factor: 1

Ethernet

MAC [00:50:56:ab:c3:ea] Set

Link Speed / Duplex Mode: Auto Negotiation

Current negotiation : 1000baseTX-FD

□ Enable Bridging with LAN**

WAN IP Settings

○ Obtain an IP address automatically using DHCP

○ Connect using PPPoE

○ Connect using 3G/4G device

● Specify an IP address

IPv4 | IPv6

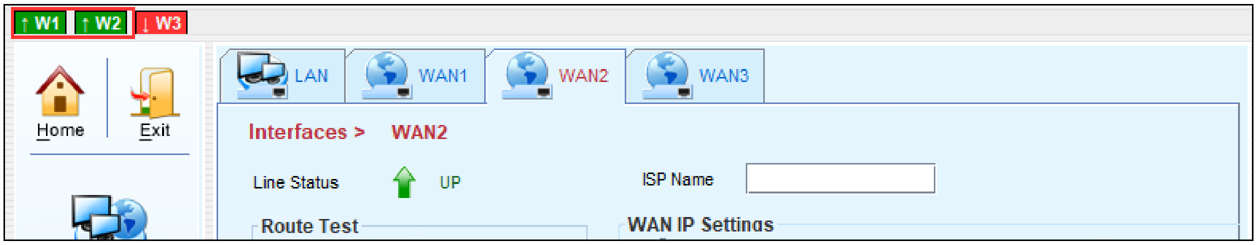
IP Address: 10.64.102.151

Subnet Mask: 255.255.255.0

Default Gateway: 10.64.102.1

Copyright © 2000-2016. FatPipe Networks Inc.

If the connectivity to both WAN connections is successful, **W1** and **W2** icons on the top left corner of the window will turn green.



Interfaces > WAN2

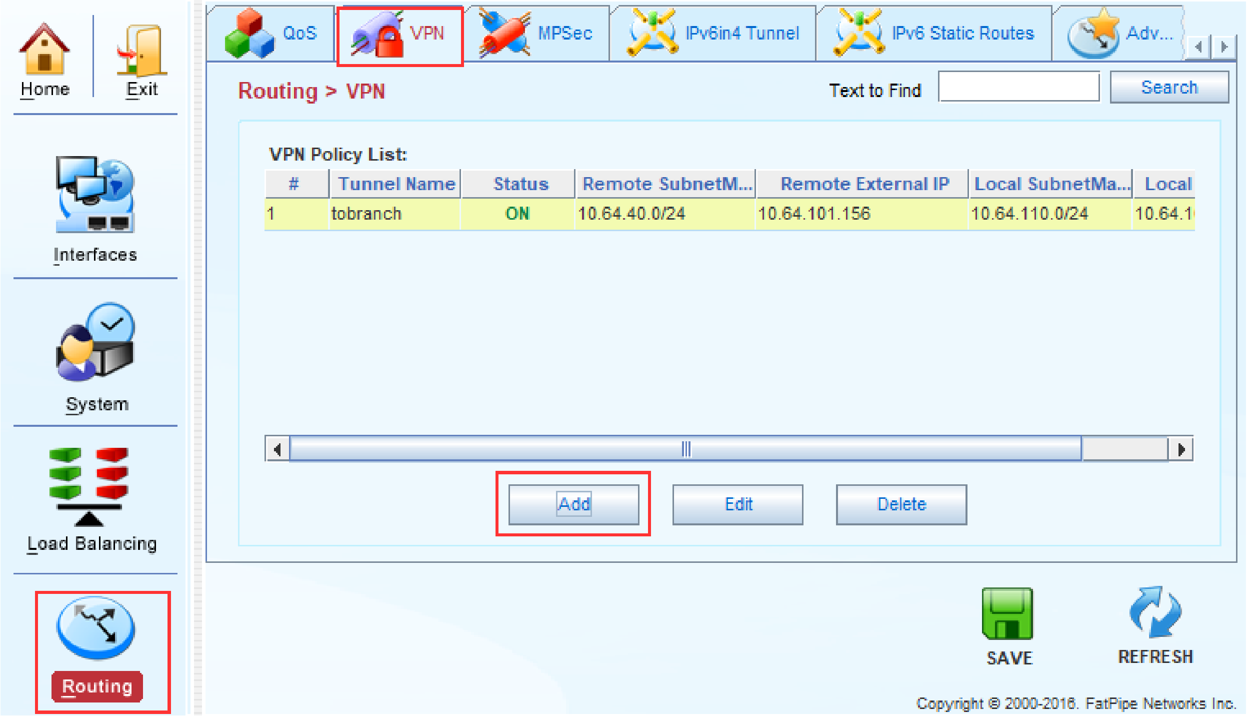
Line Status UP

ISP Name

Route Test

WAN IP Settings

On the left pane, select **Routing;** select the **VPN** tab. Click **Add** to add a VPN connection.

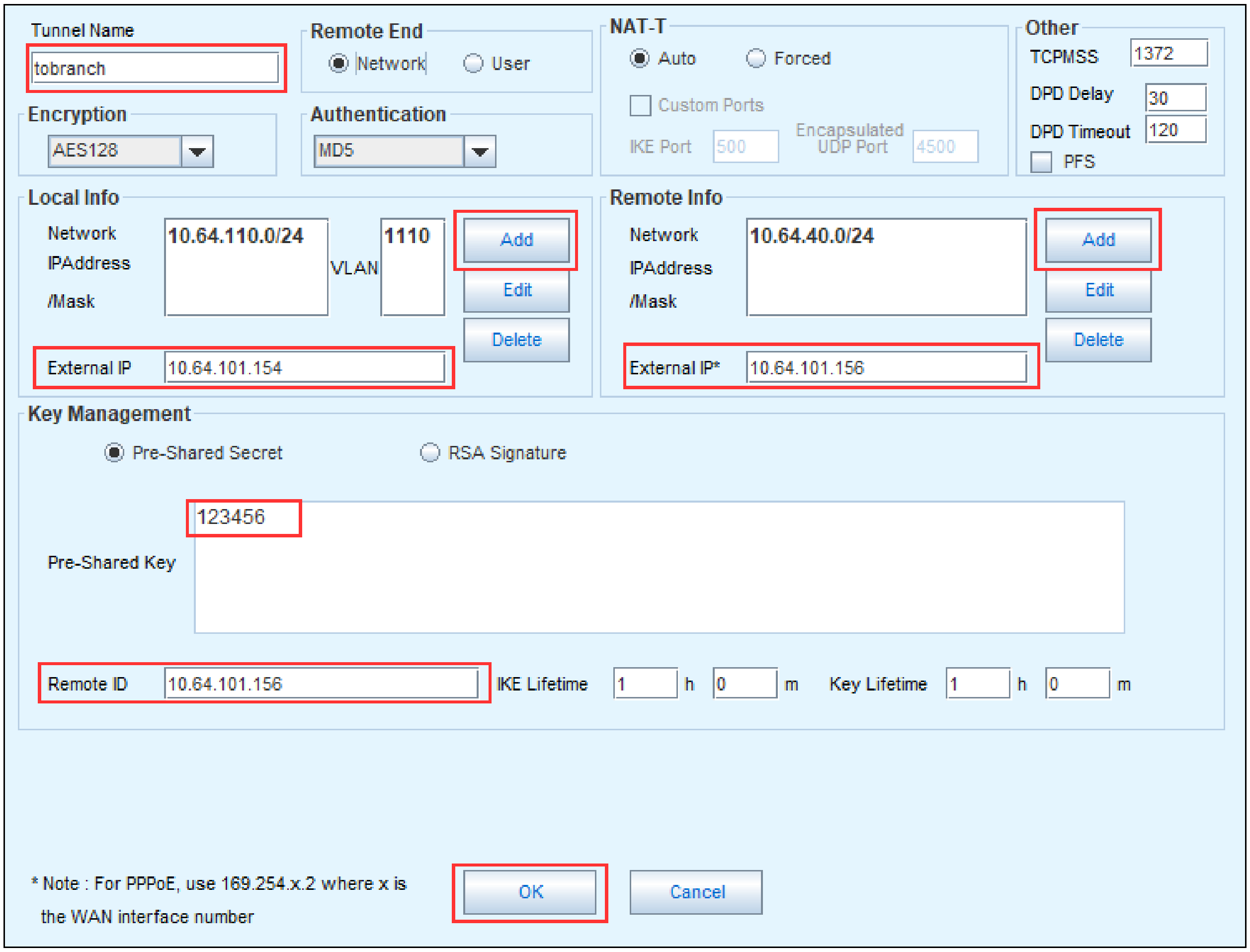


VPN Policy List:

#	Tunnel Name	Status	Remote SubnetM...	Remote External IP	Local SubnetMa...	Local
1	tobranch	ON	10.64.40.0/24	10.64.101.156	10.64.110.0/24	10.64.1

An **Add VPN Policy Rule** window will open, configure as follows:

- Type in a **Tunnel Name.**
- Under the **Local Info** section, select **Add:**
    - Type in the network information for local network on the Enterprise site. E.g.,10.64.110.0/24 with VLAN tag of 1110.
    - Type in the **External IP** that was used for **WAN1**
- Under the **Remote Info** section, select **Add:**
    - Type in the network information for remote site. E.g., 10.64.40.0/24
    - Type in the **External IP** that will be used for **WAN1** when configuring FatPipe MPVPN® on remote site.
- Under the **Key Management** section, type in a **Pre-Share Key**. Note down the key, it will be used again when configuring FatPipe MPVPN® on remote site.
    - In the **Remote ID** field, type in the IP Address will be used for **WAN1** when configuring FatPipe MPVPN® on remote site.
- Select **OK** once done.



Tunnel Name: tobranch

Remote End: ● Network ○ User

NAT-T: ● Auto ○ Forced

□ Custom Ports

IKE Port: 500 Encapsulated UDP Port: 4500

Other

TCPMSS: 1372

DPD Delay: 30

DPD Timeout: 120

□ PFS

Encryption: AES128

Authentication: MD5

Local Info

Network IPAddress /Mask: 10.64.110.0/24 VLAN: 1110

External IP: 10.64.101.154

Remote Info

Network IPAddress /Mask: 10.64.40.0/24

External IP*: 10.64.101.156

Key Management

● Pre-Shared Secret ○ RSA Signature

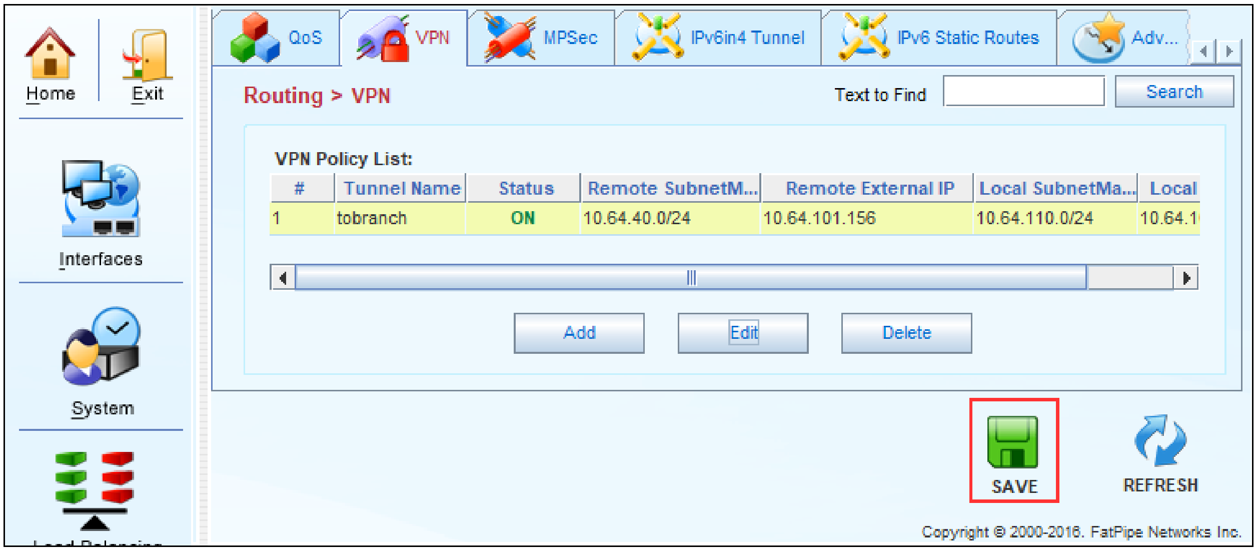
Pre-Shared Key: 123456

Remote ID: 10.64.101.156

IKE Lifetime: 1 h 0 m Key Lifetime: 1 h 0 m

* Note : For PPPoE, use 169.254.x.2 where x is the WAN interface number

At the bottom of the windows, select **SAVE.**



Routing > VPN

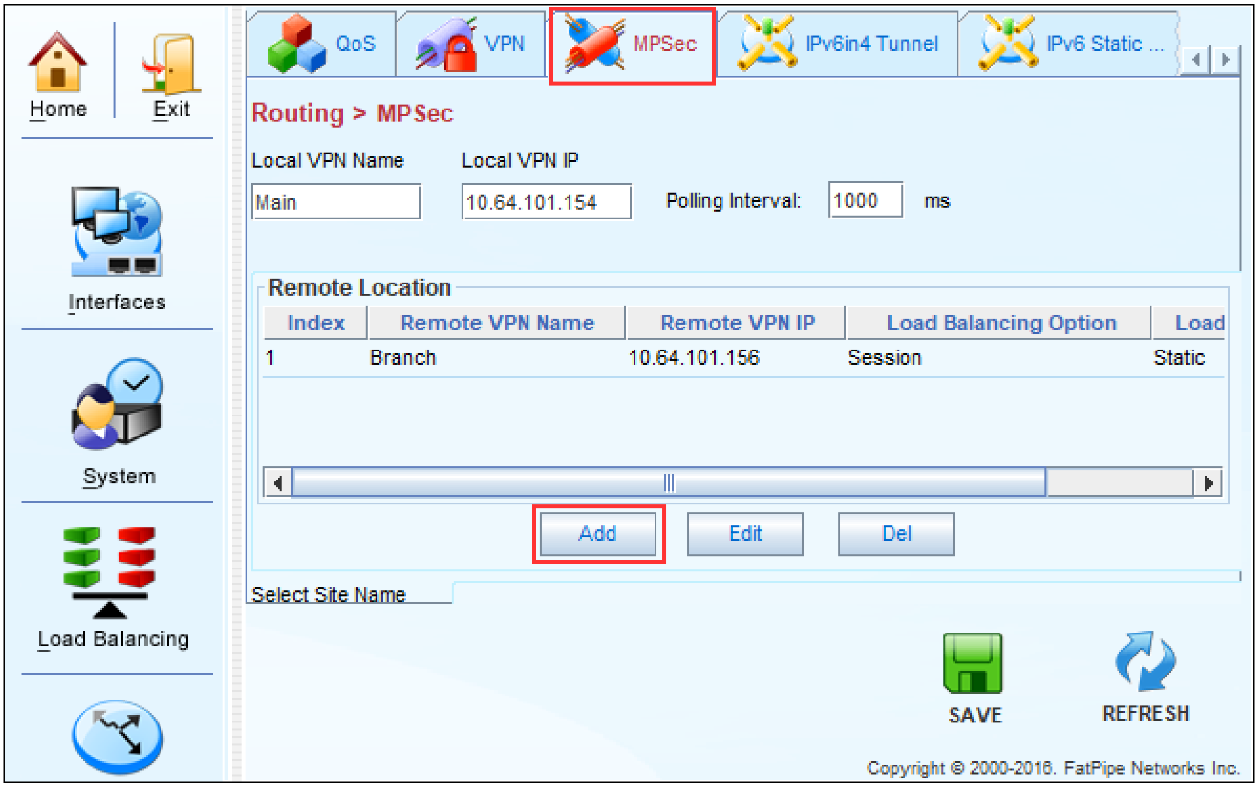
Text to Find:

VPN Policy List:

#	Tunnel Name	Status	Remote SubnetM...	Remote External IP	Local SubnetMa...	Local
1	tobranch	ON	10.64.40.0/24	10.64.101.156	10.64.110.0/24	10.64.1

Copyright © 2000-2016. FatPipe Networks Inc.

Continuing from above, select the **MPSec** tab; select **Add** to add an MPSec connection to the remote site.



Routing > MPSec

Local VPN Name: Main

Local VPN IP: 10.64.101.154

Polling Interval: 1000 ms

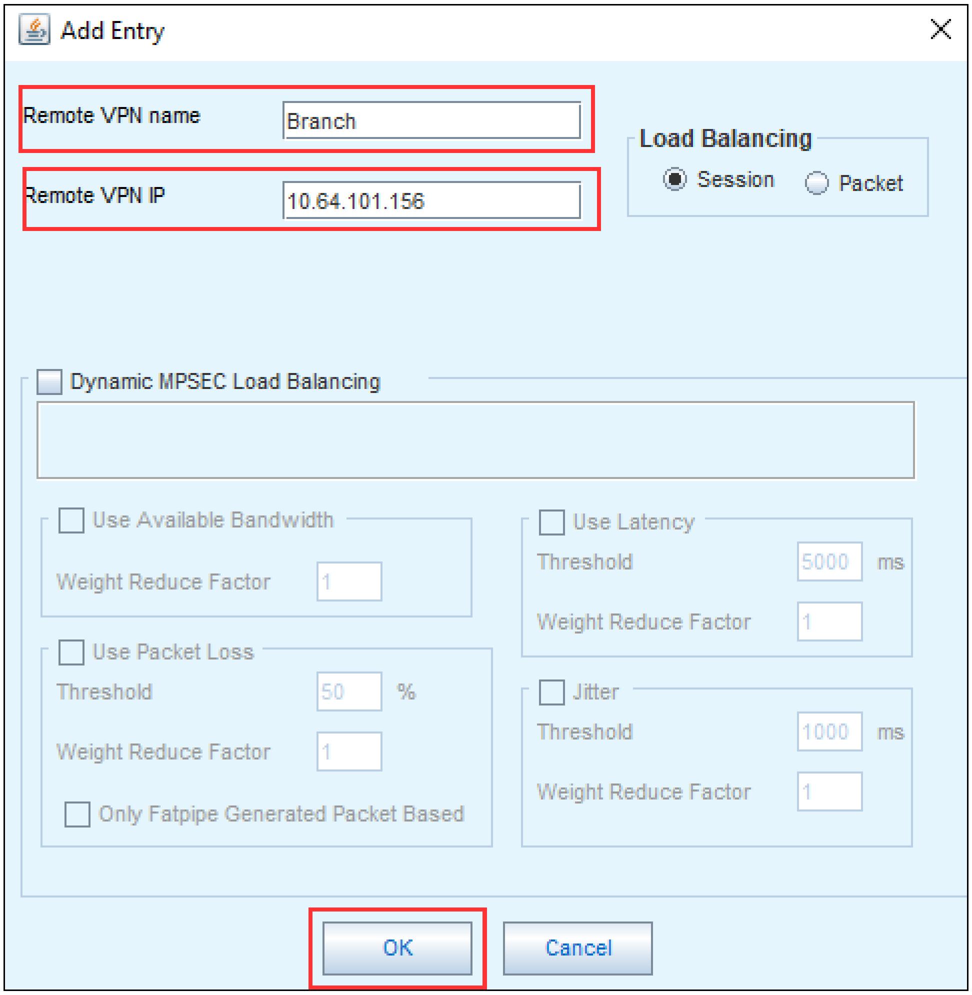
Remote Location

Index	Remote VPN Name	Remote VPN IP	Load Balancing Option	Load
1	Branch	10.64.101.156	Session	Static

Select Site Name

Copyright © 2000-2016. FatPipe Networks Inc.

An **Add Entry** window will open; type in a name for **Remote VPN Name**. For the **Remote VPN IP**, type in the WAN1 IP Address of FatPipe MPVPN® on the remote site. Once done, click **OK.**



Remote VPN name: Branch

Remote VPN IP: 10.64.101.156

Load Balancing: ● Session ○ Packet

□ Dynamic MPSEC Load Balancing

□ Use Available Bandwidth
Weight Reduce Factor: 1

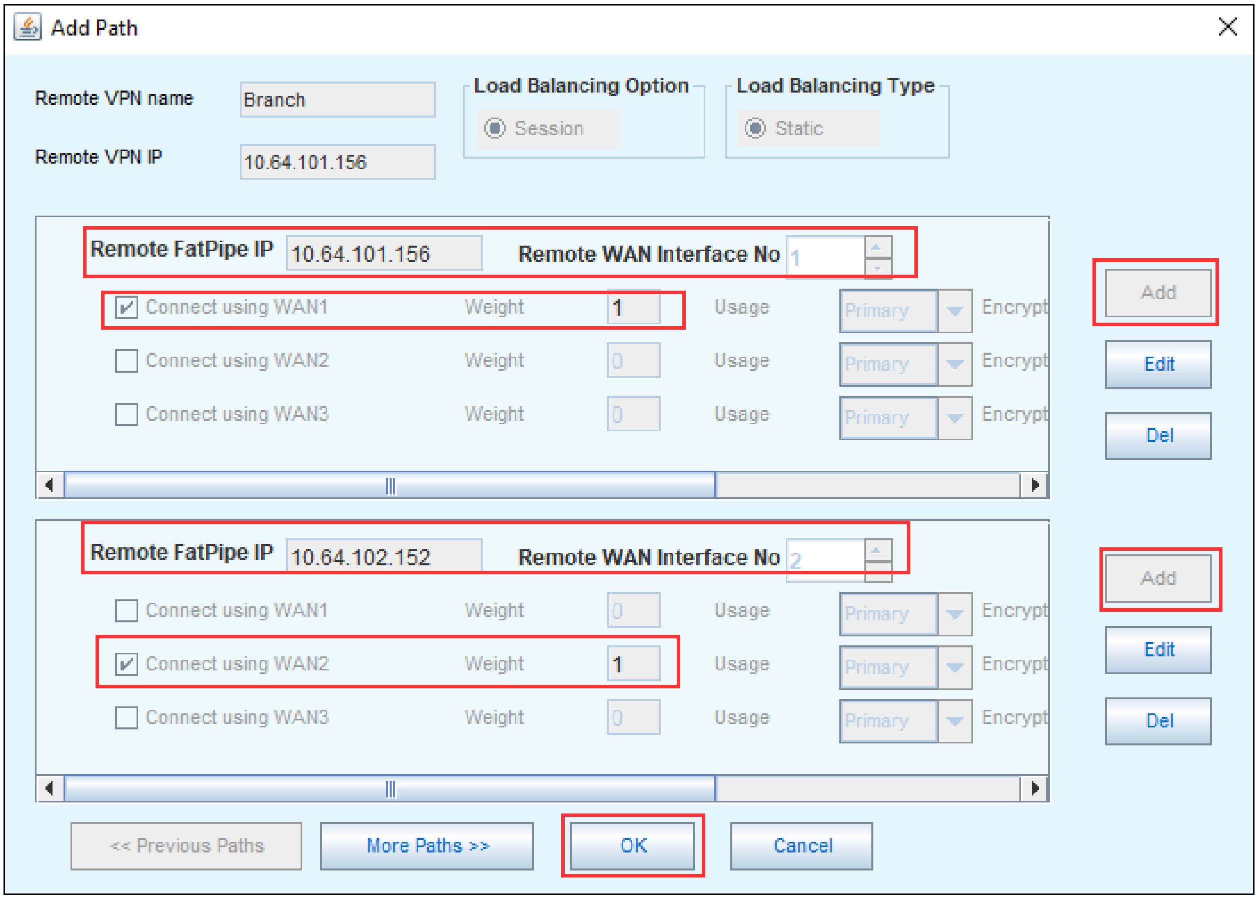
□ Use Latency
Threshold: 5000 ms
Weight Reduce Factor: 1

□ Use Packet Loss
Threshold: 50 %
Weight Reduce Factor: 1
□ Only Fatpipe Generated Packet Based

□ Jitter
Threshold: 1000 ms
Weight Reduce Factor: 1

An **Add Path** window will open:

- Select **Add** for Remote WAN Interface 1 and type in the WAN1 IP Address of FatPipe MPVPN® on remote site; check box for **Connect using WAN1.**
- Select **Add** for Remote WAN Interface 2 and type in the WAN2 IP Address of FatPipe MPVPN® on remote site; check box for **Connect using WAN2.**
- Once done, click **OK.**



Add Path

Remote VPN name: Branch

Remote VPN IP: 10.64.101.156

Load Balancing Option: ● Session

Load Balancing Type: ● Static

Remote FatPipe IP: 10.64.101.156 Remote WAN Interface No: 1

☑ Connect using WAN1 Weight: 1 Usage: Primary Encrypt

□ Connect using WAN2 Weight: 0 Usage: Primary Encrypt

□ Connect using WAN3 Weight: 0 Usage: Primary Encrypt

Remote FatPipe IP: 10.64.102.152 Remote WAN Interface No: 2

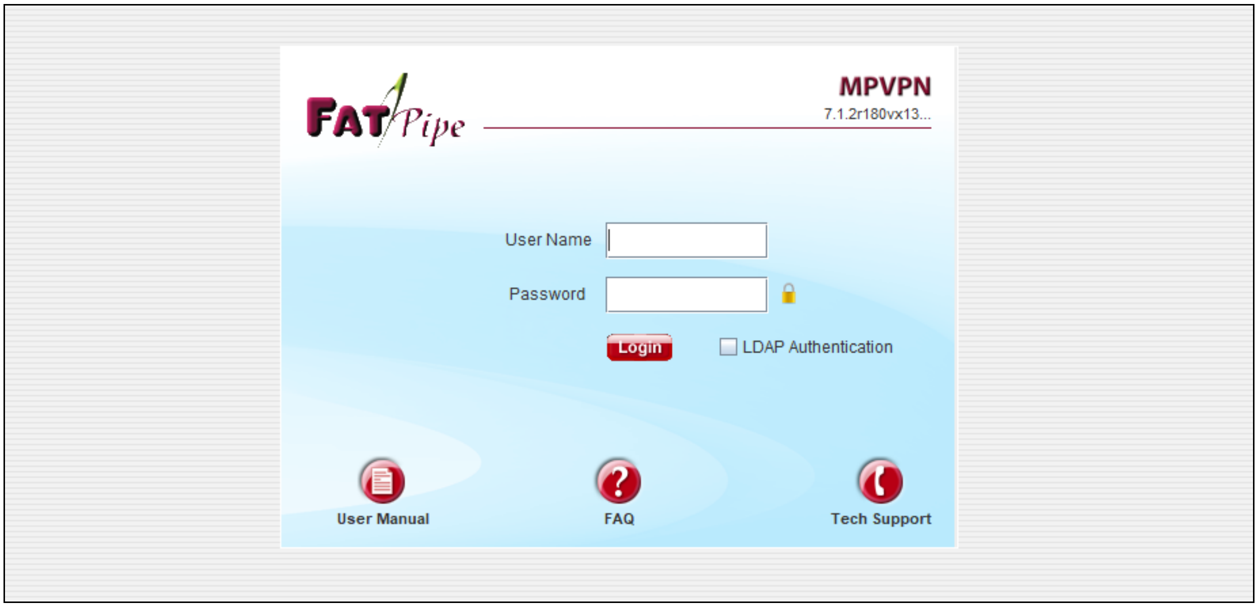
□ Connect using WAN1 Weight: 0 Usage: Primary Encrypt

☑ Connect using WAN2 Weight: 1 Usage: Primary Encrypt

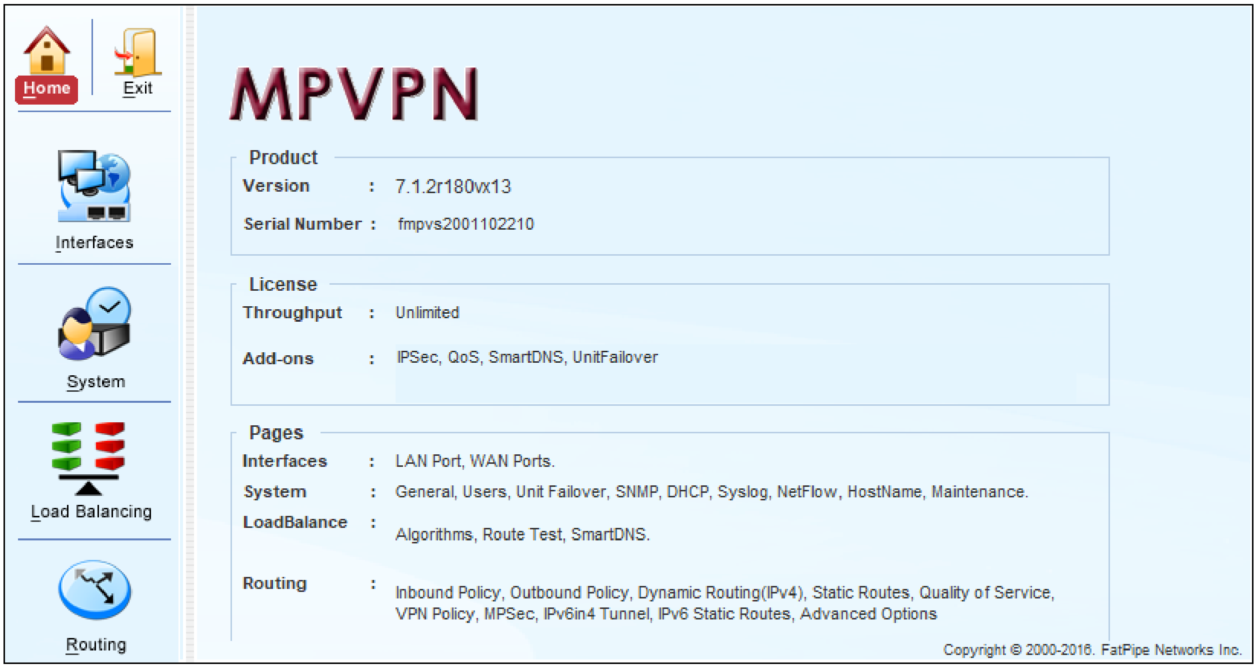
□ Connect using WAN3 Weight: 0 Usage: Primary Encrypt

6.2. Remote Site

Open Internet Explorer and point the browser to the FatPipe MPVPN's IP Address of remote site. Log in using appropriate credentials.



Once logged in, FatPipe MPVPN® configuration window (Java based) will open.



Product

Version : 7.1.2r180vx13

Serial Number : fmpvs2001102210

License

Throughput : Unlimited

Add-ons : IPSec, QoS, SmartDNS, UnitFailover

Pages

Interfaces : LAN Port, WAN Ports.

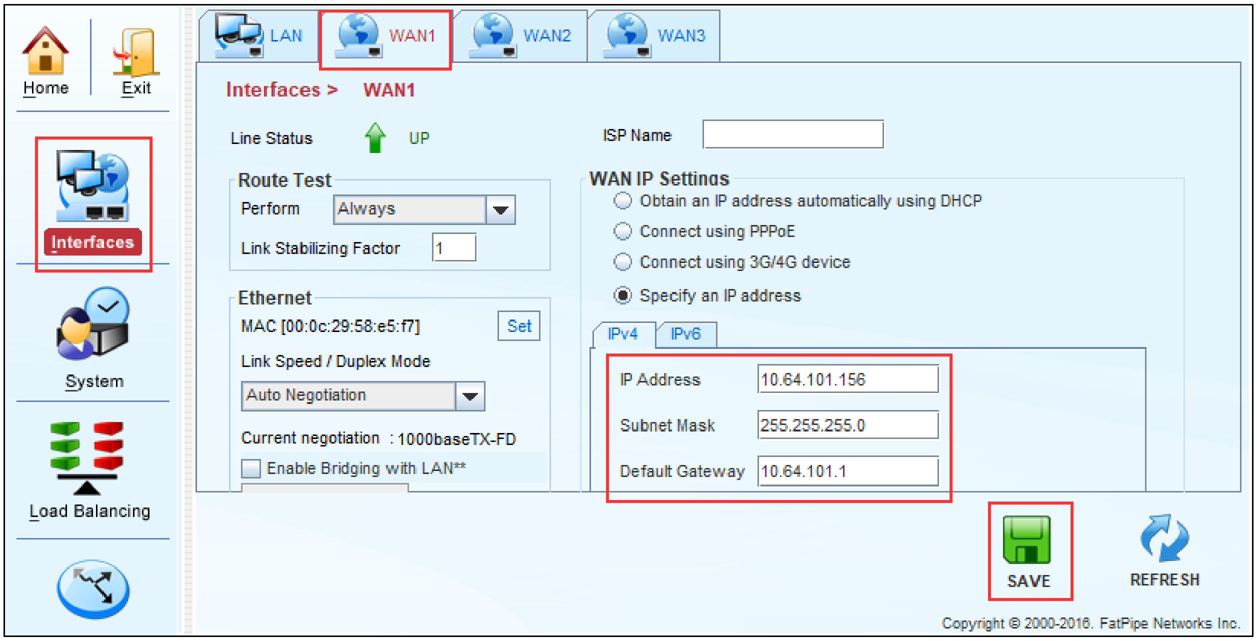
System : General, Users, Unit Failover, SNMP, DHCP, Syslog, NetFlow, HostName, Maintenance.

LoadBalance : Algorithms, Route Test, SmartDNS.

Routing : Inbound Policy, Outbound Policy, Dynamic Routing(IPv4), Static Routes, Quality of Service, VPN Policy, MPSec, IPv6in4 Tunnel, IPv6 Static Routes, Advanced Options

Copyright © 2000-2016. FatPipe Networks Inc.

On the left pane select **Interfaces;** select the **WAN1** tab and configure the **IPv4** information. During Compliance testing, 10.64.101.156 IP Address was used for WAN1 connectivity. Click **SAVE** once done.



Interfaces > WAN1

Line Status UP

ISP Name

Route Test
Perform: Always
Link Stabilizing Factor: 1

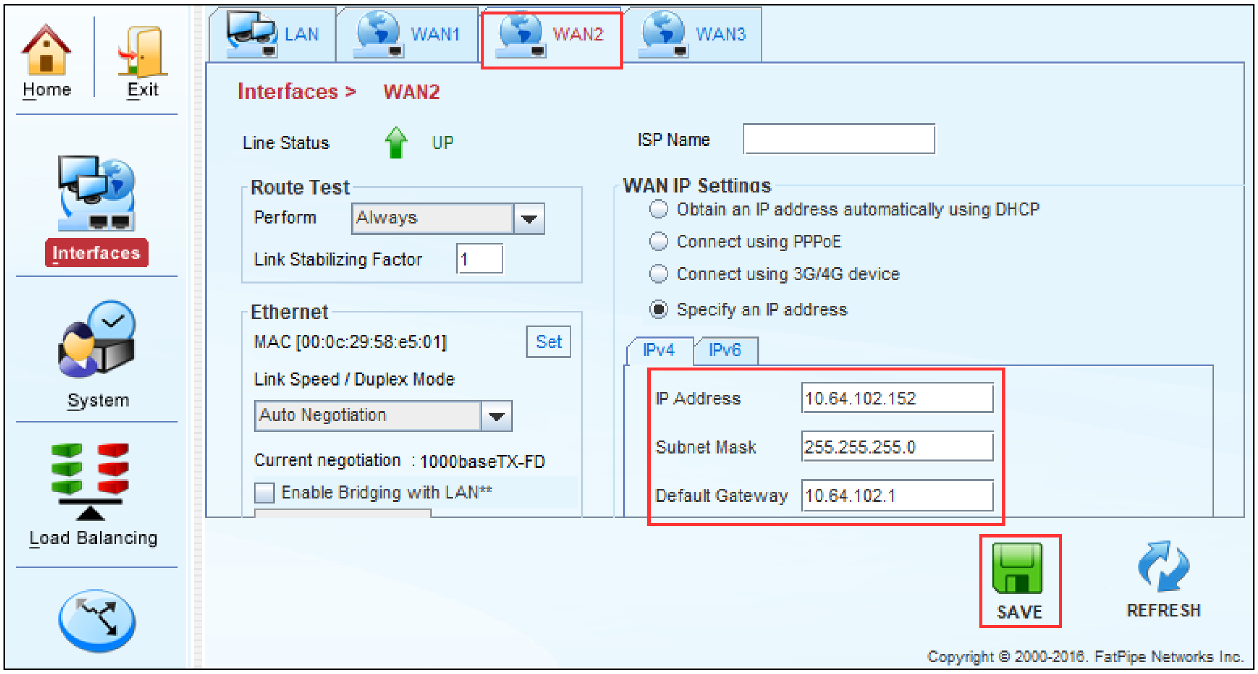
Ethernet
MAC [00:0c:29:58:e5:f7] Set
Link Speed / Duplex Mode: Auto Negotiation
Current negotiation : 1000baseTX-FD
☐ Enable Bridging with LAN**

WAN IP Settings
○ Obtain an IP address automatically using DHCP
○ Connect using PPPoE
○ Connect using 3G/4G device
● Specify an IP address

IP Address: 10.64.101.156
Subnet Mask: 255.255.255.0
Default Gateway: 10.64.101.1

Copyright © 2000-2016. FatPipe Networks Inc.

Continuing from above, select the **WAN2** tab and configure the **IPv4** information. During Compliance testing, 10.64.102.152 IP Address was used for WAN2 connectivity. Click **SAVE** once done.



Interfaces > WAN2

Line Status UP

ISP Name

Route Test
Perform: Always
Link Stabilizing Factor: 1

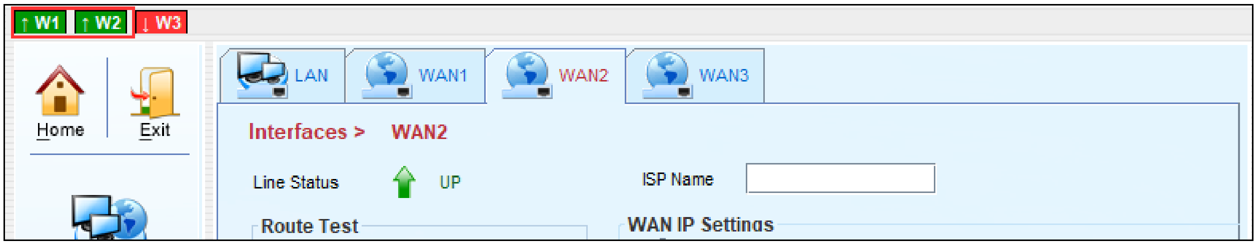
Ethernet
MAC [00:0c:29:58:e5:01] Set
Link Speed / Duplex Mode: Auto Negotiation
Current negotiation : 1000baseTX-FD
☐ Enable Bridging with LAN**

WAN IP Settings
○ Obtain an IP address automatically using DHCP
○ Connect using PPPoE
○ Connect using 3G/4G device
● Specify an IP address

IP Address: 10.64.102.152
Subnet Mask: 255.255.255.0
Default Gateway: 10.64.102.1

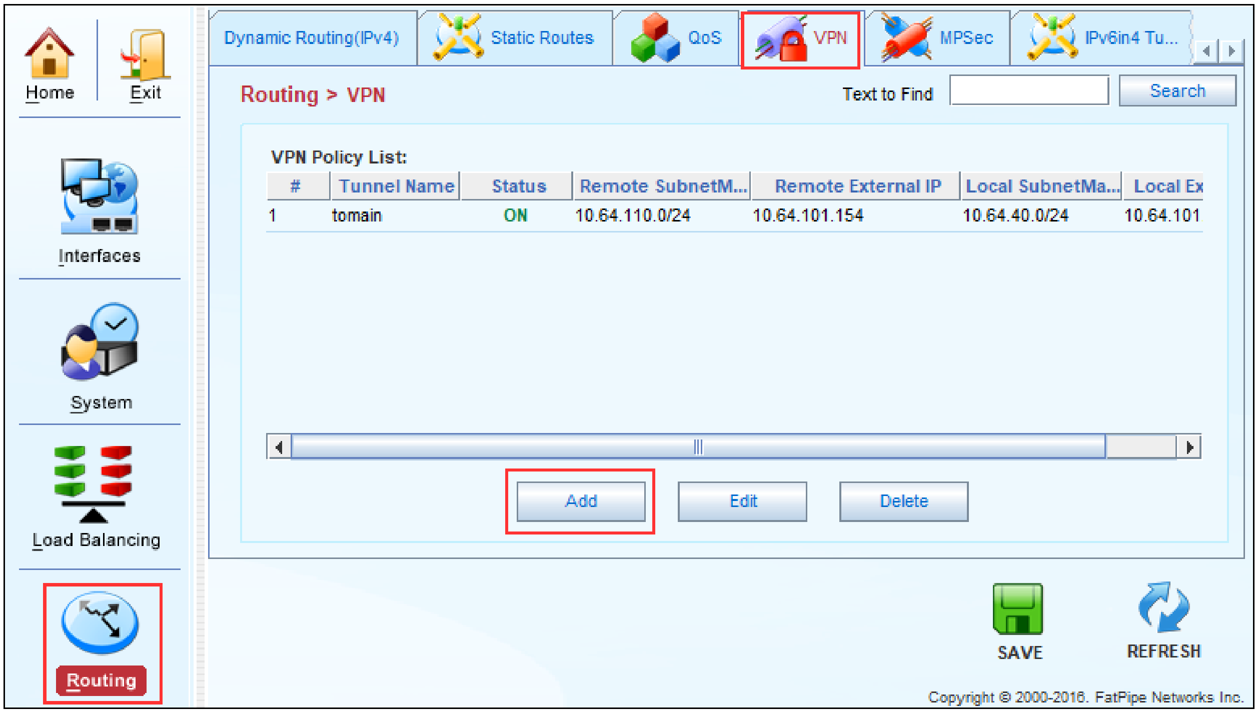
Copyright © 2000-2016. FatPipe Networks Inc.

If the connectivity to both WAN connections is successful, **W1** and **W2** icons on the top left corner of the window will turn green.



Line Status UP

On the left pane, select **Routing;** select the **VPN** tab. Click **Add** to add a VPN connection.

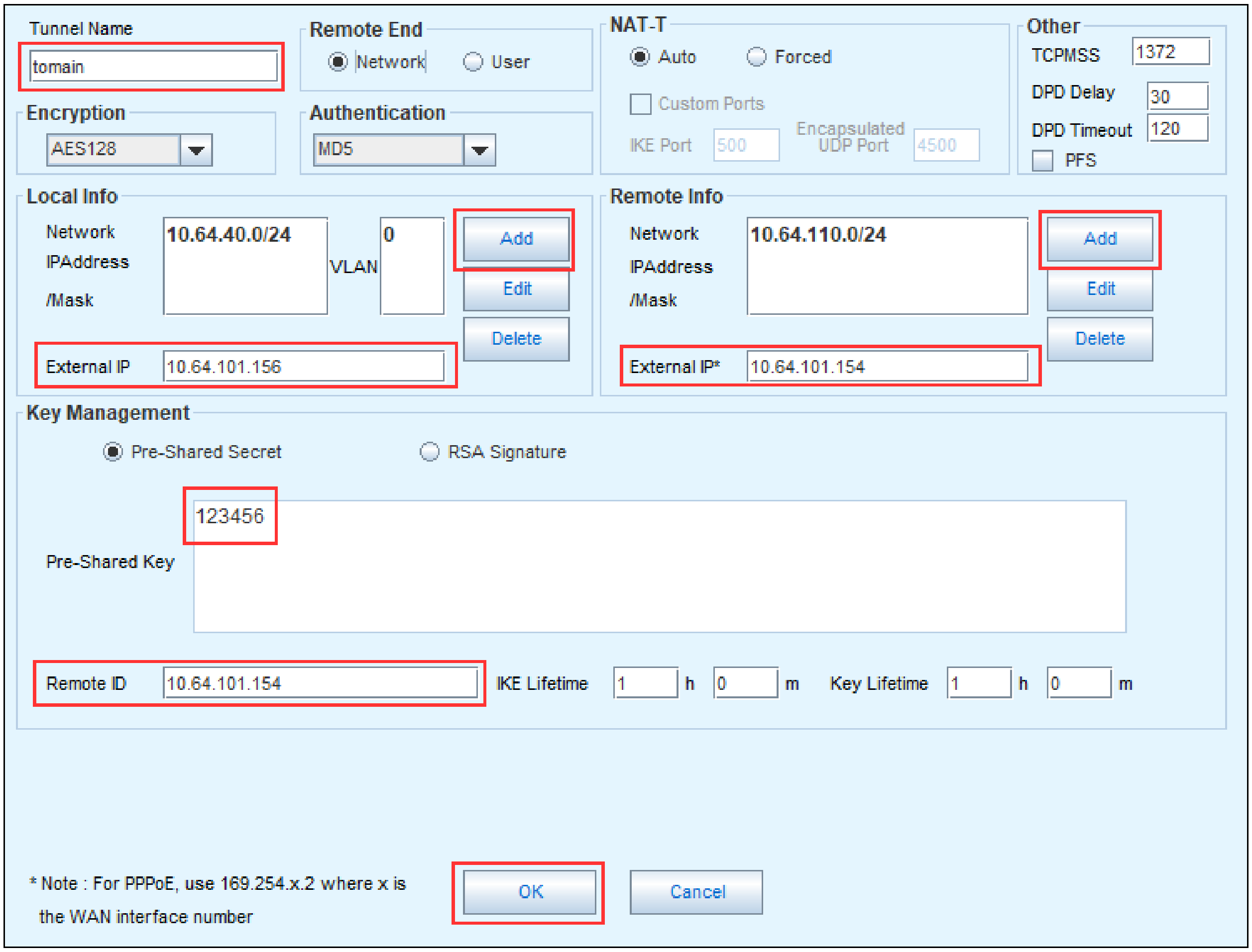


VPN Policy List:

#	Tunnel Name	Status	Remote SubnetM...	Remote External IP	Local SubnetMa...	Local Ex
1	tomain	ON	10.64.110.0/24	10.64.101.154	10.64.40.0/24	10.64.101

An **Add VPN Policy Rule** window will open, configure as follows:

- Type in a **Tunnel Name.**
- Under the **Local Info** section, select **Add:**
  - Type in the network information for local network on the remote site. E.g.,10.64.140.0/24.
  - Type in the **External IP** that was used for **WAN1.**
- Under the **Remote Info** section, select **Add:**
  - Type in the network information for remote site. E.g., 10.64.110.0/24.
  - Type in the **External IP** that was used for **WAN1** when configuring FatPipe MPVPN® on enterprise site. E.g., 10.64.101.154.
- Under the **Key Management** section, type in the **Pre-Share Key** that was configured on enterprise site.
  - In the **Remote ID** field, type in the IP Address was used for **WAN1** when configuring FatPipe MPVPN® on remote site. E.g., 10.64.101.154.
- Select **OK** once done.



Tunnel Name: tomain

Remote End: ● Network ○ User

NAT-T: ● Auto ○ Forced

□ Custom Ports

IKE Port: 500 Encapsulated UDP Port: 4500

Other

TCPMSS: 1372

DPD Delay: 30

DPD Timeout: 120

□ PFS

Encryption: AES128

Authentication: MD5

Local Info

Network IPAddress /Mask: 10.64.40.0/24 VLAN: 0

External IP: 10.64.101.156

Remote Info

Network IPAddress /Mask: 10.64.110.0/24

External IP*: 10.64.101.154

Key Management

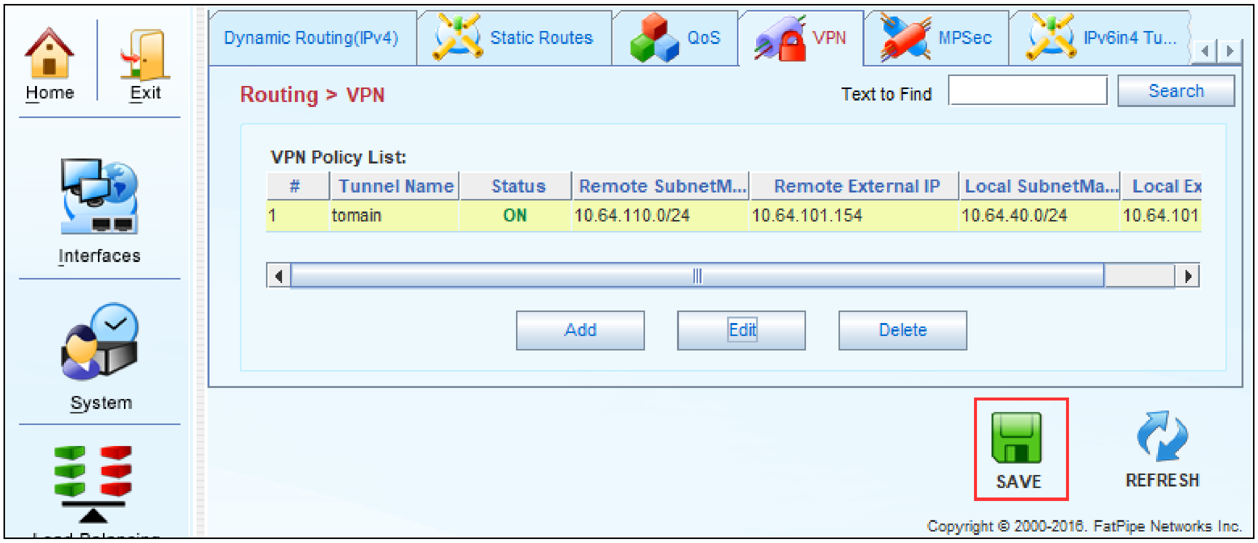
● Pre-Shared Secret ○ RSA Signature

Pre-Shared Key: 123456

Remote ID: 10.64.101.154 IKE Lifetime: 1 h 0 m Key Lifetime: 1 h 0 m

* Note : For PPPoE, use 169.254.x.2 where x is the WAN interface number

At the bottom of the windows, select **SAVE.**



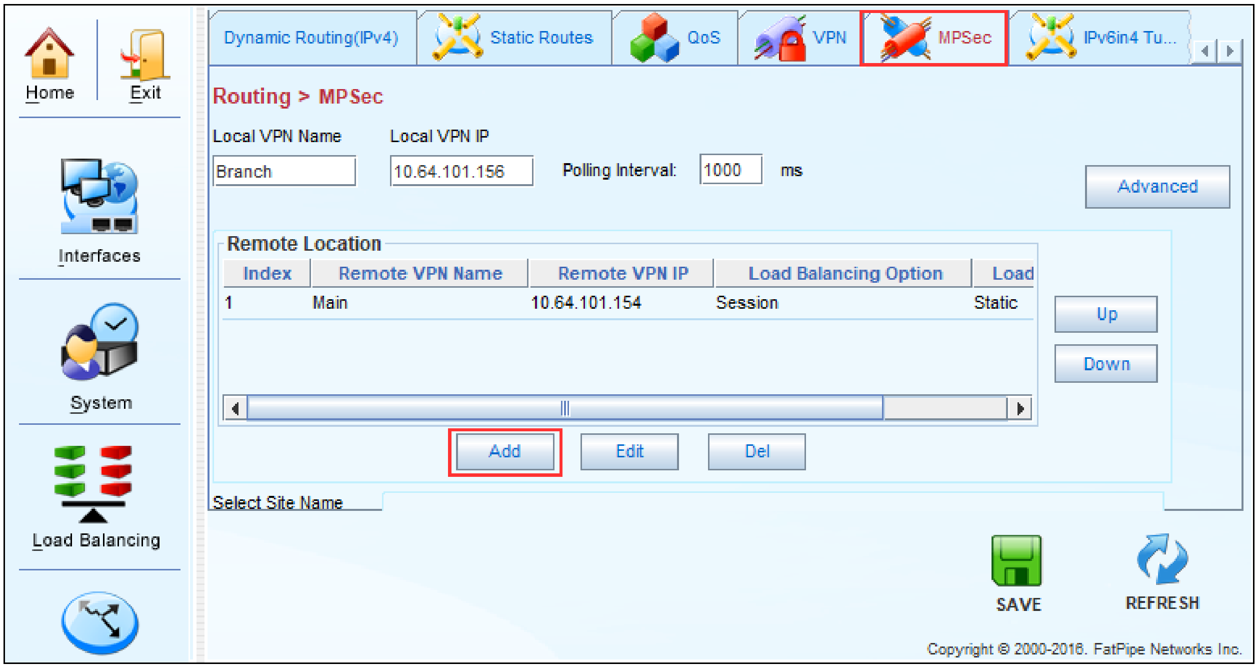
Routing > VPN

VPN Policy List:

#	Tunnel Name	Status	Remote SubnetM...	Remote External IP	Local SubnetMa...	Local Ex
1	tomain	ON	10.64.110.0/24	10.64.101.154	10.64.40.0/24	10.64.101

Copyright © 2000-2016. FatPipe Networks Inc.

Continuing from above, select the **MPSec** tab; select **Add** to add an MPSec connection to the remote site.



Routing > MPSec

Local VPN Name: Branch

Local VPN IP: 10.64.101.156

Polling Interval: 1000 ms

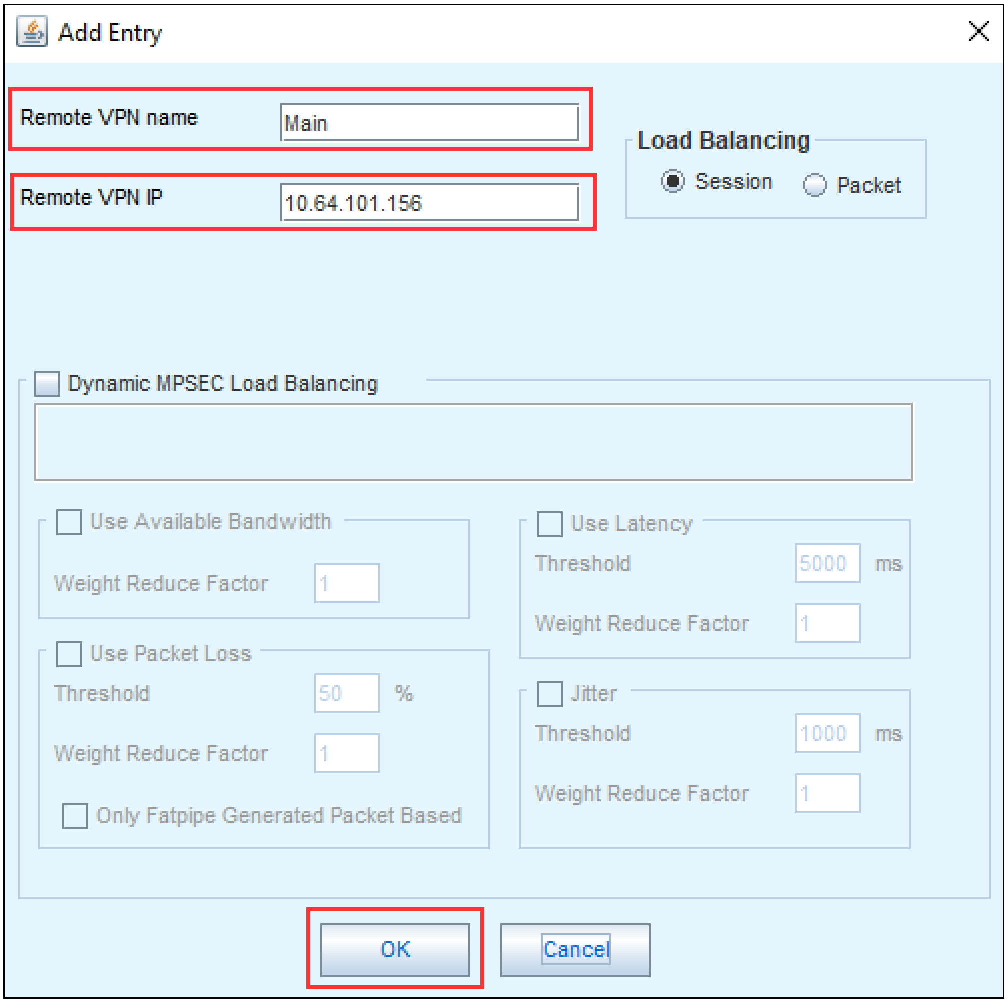
Remote Location

Index	Remote VPN Name	Remote VPN IP	Load Balancing Option	Load
1	Main	10.64.101.154	Session	Static

Select Site Name

Copyright © 2000-2016. FatPipe Networks Inc.

An **Add Entry** window will open; type in a name for **Remote VPN Name**. For the **Remote VPN IP**, type in the WAN1 IP Address of FatPipe MPVPN® on the remote site. Once done, click **OK.**



Remote VPN name: Main

Remote VPN IP: 10.64.101.156

Load Balancing: ● Session ○ Packet

□ Dynamic MPSEC Load Balancing

□ Use Available Bandwidth — Weight Reduce Factor: 1

□ Use Latency — Threshold: 5000 ms — Weight Reduce Factor: 1

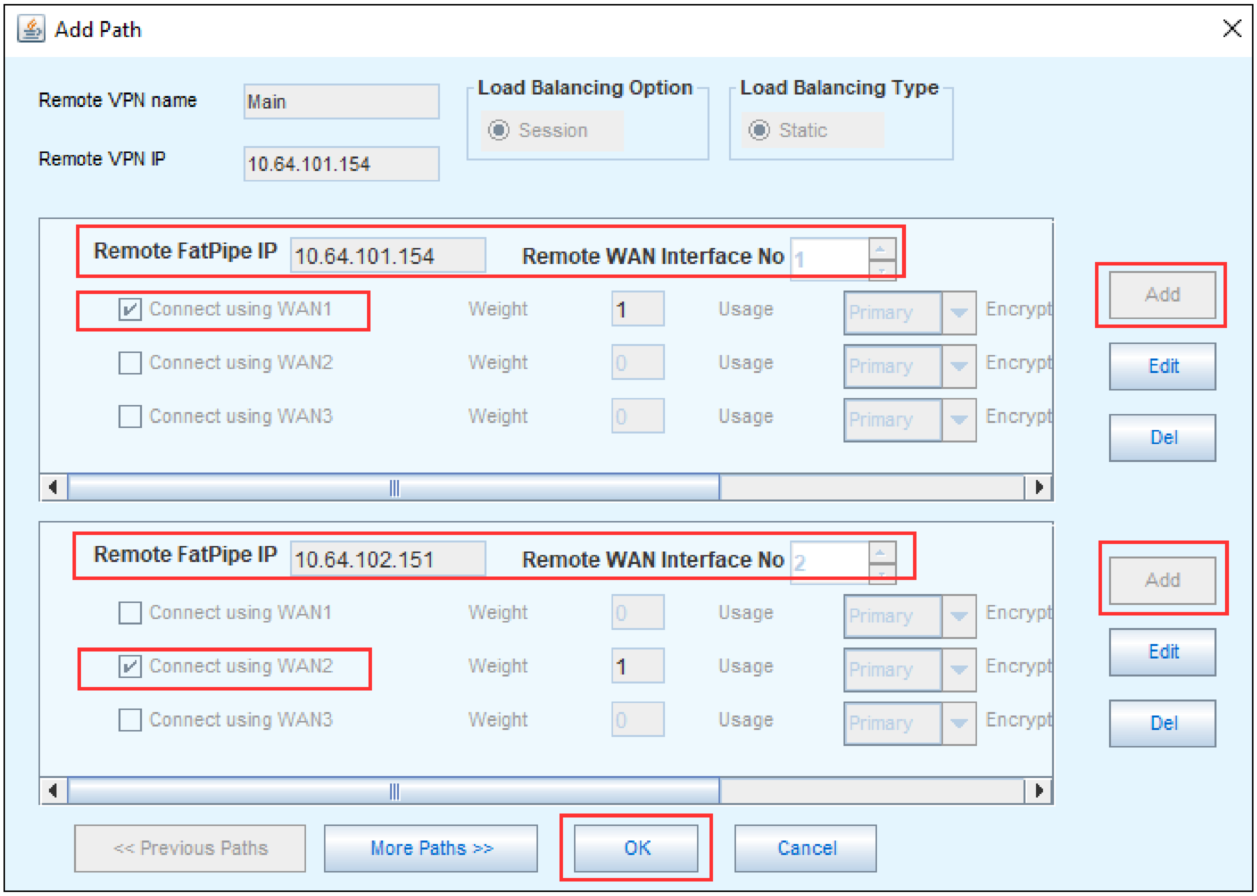
□ Use Packet Loss — Threshold: 50 % — Weight Reduce Factor: 1

□ Only Fatpipe Generated Packet Based

□ Jitter — Threshold: 1000 ms — Weight Reduce Factor: 1

An **Add Path** window will open:

- Select **Add** for Remote WAN Interface 1 and type in the WAN1 IP Address of FatPipe MPVPN® on enterprise site; check box for **Connect using WAN1.**
- Select **Add** for Remote WAN Interface 2 and type in the WAN2 IP Address of FatPipe MPVPN® on enterprise site; check box for **Connect using WAN2.**
- Once done, click **OK.**



Add Path

Remote VPN name: Main
Remote VPN IP: 10.64.101.154
Load Balancing Option: ● Session
Load Balancing Type: ● Static

Remote FatPipe IP: 10.64.101.154 Remote WAN Interface No: 1

☑ Connect using WAN1	Weight	1	Usage	Primary	Encrypt
□ Connect using WAN2	Weight	0	Usage	Primary	Encrypt
□ Connect using WAN3	Weight	0	Usage	Primary	Encrypt

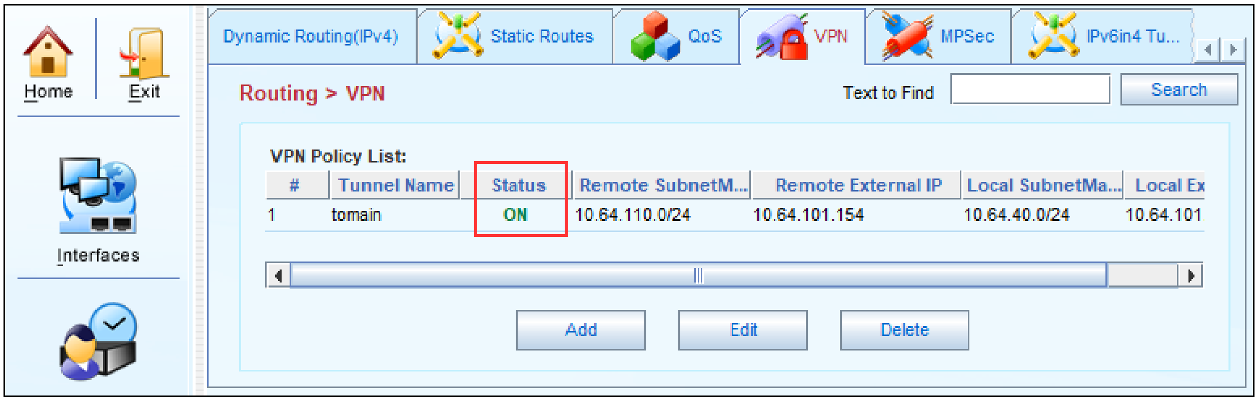
Remote FatPipe IP: 10.64.102.151 Remote WAN Interface No: 2

□ Connect using WAN1	Weight	0	Usage	Primary	Encrypt
☑ Connect using WAN2	Weight	1	Usage	Primary	Encrypt
□ Connect using WAN3	Weight	0	Usage	Primary	Encrypt

7. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

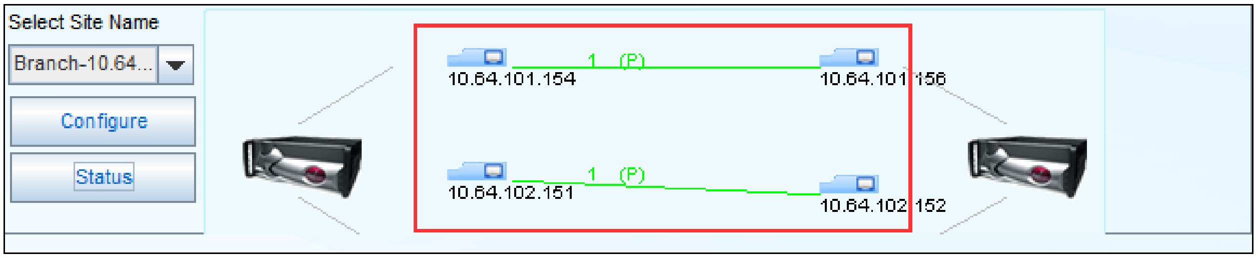
1. Via the FatPipe MPVPN® window for the enterprise site, navigate to **Routing → VPN**. If the VPN connection between both sites is successful, the status will be shown as **ON.**



VPN Policy List:

#	Tunnel Name	Status	Remote SubnetM...	Remote External IP	Local SubnetMa...	Local Ex
1	tomain	ON	10.64.110.0/24	10.64.101.154	10.64.40.0/24	10.64.101

2. Continuing from above, select the **MPSec** tab. At the bottom, select the configured MPSec connection from the **Select Site Name** drop down; click **Status.** If both MPSec connections to the remote site are successful, the connecting lines will turn green.



3. Register an endpoint from the remote site and place a call. This ensures successful connectivity between the sites.

8. Conclusion

These Application Notes describe the configuration necessary to configure FatPipe MPVPN® in Avaya Aura® ® enterprise and remote sites. FatPipe MPVPN® was successfully tested with an observation listed in **Section 2.2**.

9. Additional References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at http://support.avaya.com.

[1] *Migrating and Installing Avaya Appliance Virtualization Platform*, Release 7.1, May 2017.

[2] *Upgrading and Migrating Avaya Aura® applications to Release 7.1.1 from System Manager*, Aug 2017.

[3] *Deploying Avaya Aura® applications from System Manager*, Release 7.1.1, Aug 2017

[4] *Deploying Avaya Aura® Communication Manager*, Release 7.1.1, Aug 2017

[5] *Administering Avaya Aura® Communication Manager*, Release 7.1.1, Aug 2017.

[6] *Upgrading Avaya Aura® Communication Manager*, Release 7.1.1, Aug 2017

[7] *Deploying Avaya Aura® System Manager Release 7.1.1*, Aug 2017

[8] *Upgrading Avaya Aura® System Manager to Release 7.1.1*, Aug 2017.

[9] *Administering Avaya Aura® System Manager for Release 7.1.1*, Aug 2017

[10] *Deploying Avaya Aura® Session Manager*, Release 7.1 May 2017

[11] *Upgrading Avaya Aura® Session Manager* Release 7.1.1, Aug 2017

[12] *Administering Avaya Aura® Session Manager* Release 7.1.1, Aug 2017,

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.