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.

FatPipe is a member of the DevConnect Service Provider program. 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 branch site were connected via FatPipe MPVPN® virtual appliances. The enterprise site consisted of Avaya Aura® environment, Avaya Session Broder Control for Enterprise (Avaya SBCE) and endpoints as shown in **Section 3** and the branch site consisted of similar configuration as the enterprise site. FatPipe MPVPN® virtual appliances were deployed on both enterprise and branch site.

2. General Test Approach and Test Results

The general test approach was to verify telephony functionality between the enterprise site and branch 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 branch site.
- Outgoing calls from the enterprise site to branch site.
- Incoming and outgoing PSTN calls to/from both enterprise site and branch site.
- Audio and video calls between enterprise and branch site.
- Fax calls between enterprise and branch site.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID presentation and caller ID restriction.

Additionally, QoS for SIP and RTP was also tested. QoS was applied based on port and IP address range. 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 serviced 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 branch 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 on the right is branch site composed of branch users. Both sites were connected via FatPipe MPVPN® WAN links.

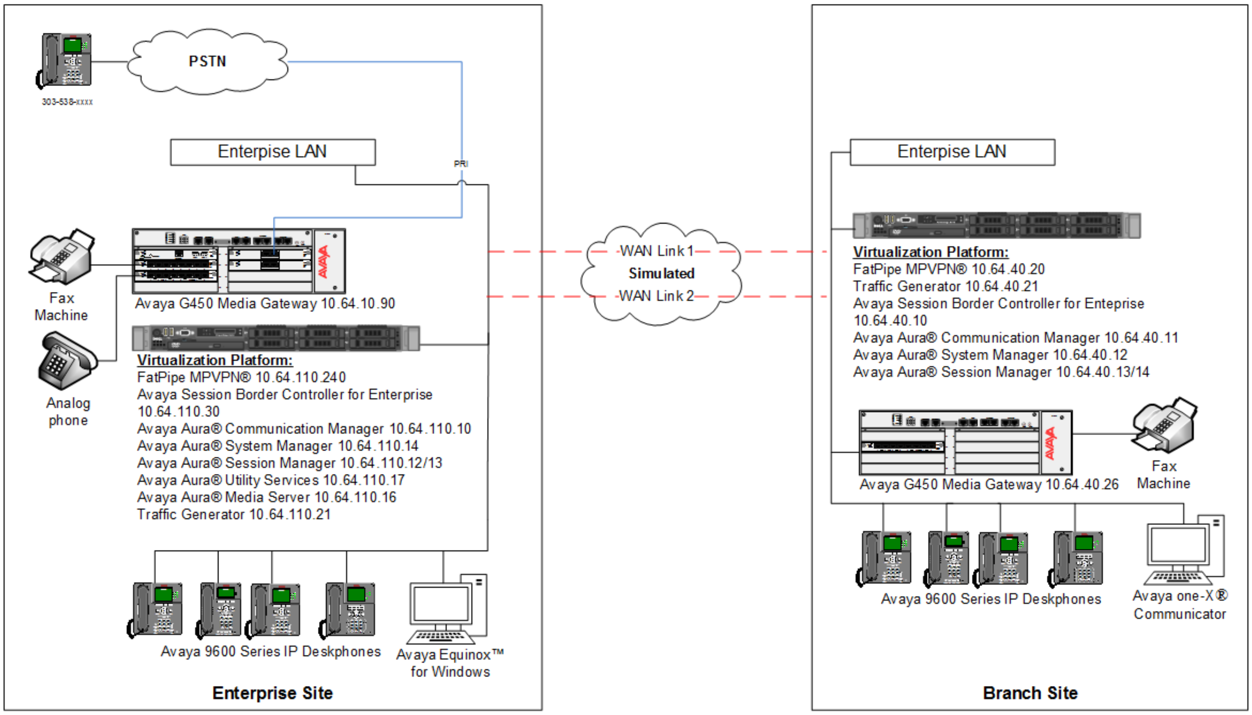

303-538-xxxx
PSTN
Enterpise LAN
PRI
Fax Machine
Avaya G450 Media Gateway 10.64.10.90
Analog phone
Virtualization Platform:
FatPipe MPVPN® 10.64.110.240
Avaya Session Border Controller for Enterprise 10.64.110.30
Avaya Aura® Communication Manager 10.64.110.10
Avaya Aura® System Manager 10.64.110.14
Avaya Aura® Session Manager 10.64.110.12/13
Avaya Aura® Utility Services 10.64.110.17
Avaya Aura® Media Server 10.64.110.16
Traffic Generator 10.64.110.21
Avaya 9600 Series IP Deskphones
Avaya Equinox™ for Windows
Enterprise Site
WAN Link 1
Simulated
WAN Link 2
Enterpise LAN
Virtualization Platform:
FatPipe MPVPN® 10.64.40.20
Traffic Generator 10.64.40.21
Avaya Session Border Controller for Enteprise 10.64.40.10
Avaya Aura® Communication Manager 10.64.40.11
Avaya Aura® System Manager 10.64.40.12
Avaya Aura® Session Manager 10.64.40.13/14
Avaya G450 Media Gateway 10.64.40.26
Fax Machine
Avaya 9600 Series IP Deskphones
Avaya one-X® Communicator
Branch Site

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

Figure 2 illustrates the logical diagram below. SIP and RTP traffic between the two sites was routed via FatPipe MPVPN® appliances.

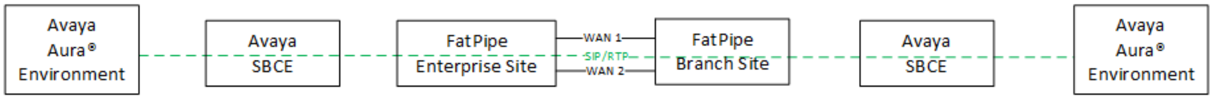


Figure 2: Logical diagram

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Session Border Controller for Enterprise	7.2.2.1
Avaya Aura® Session Manager	8.0.0.0.800035
Avaya Aura® System Manager	8.0.0.0.931077
Avaya Aura® Communication Manager	8.0.0.1.2 Service Pack 1 Patch 2
Avaya G450 Media Gateway	40.10.1
Avaya Aura® Media Server	8.0.0.150
Avaya 9600 Series IP Deskphones SIP 96x0 SIP 96x1 H.323 96x0 H.323 96x1	 2.6.17 7.1.2.0 3.2.8 6.7.0
Avaya one-X® Communicator	6.2 SP 12
Avaya Equinox™ for Windows	3.4.10
Analogue Handset	N/A
Analogue Fax	N/A
FatPipe MPVPN	10.1.2r25vx9

5. Configure Avaya Aura® Environment

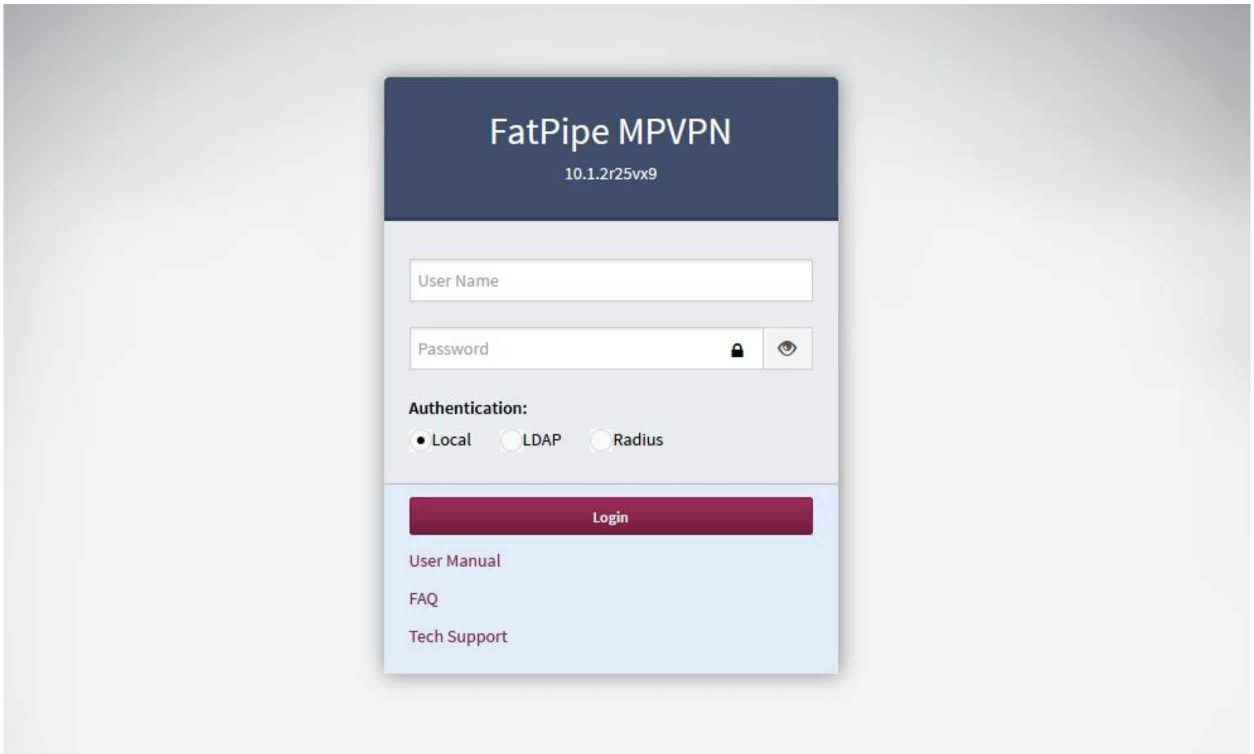
A standard set configuration of all Avaya Aura® core components was used. Avaya Aura® core components and endpoints on enterprise site were part of 10.64.110.1/24 network. Branch users/endpoints on branch site were on 10.64.40.1/24 network. Both 10.64.110.1 and 10.64.40.1 network were configured to not reach each other without the use of FatPipe MPVPN®. Enterprise site and branch site were reachable via 10.64.101.1/24 and 10.64.102.1/24 networks (simulated WAN links).

6. Configure FatPipe MPVPN®

Configuration for FatPipe MPVPN® is performed via a web browser.

6.1. Enterprise Site

Open a web browser and point the browser to the FatPipe MPVPN®'s IP Address. Log on using appropriate credentials.



FatPipe MPVPN

10.1.2r25vx9

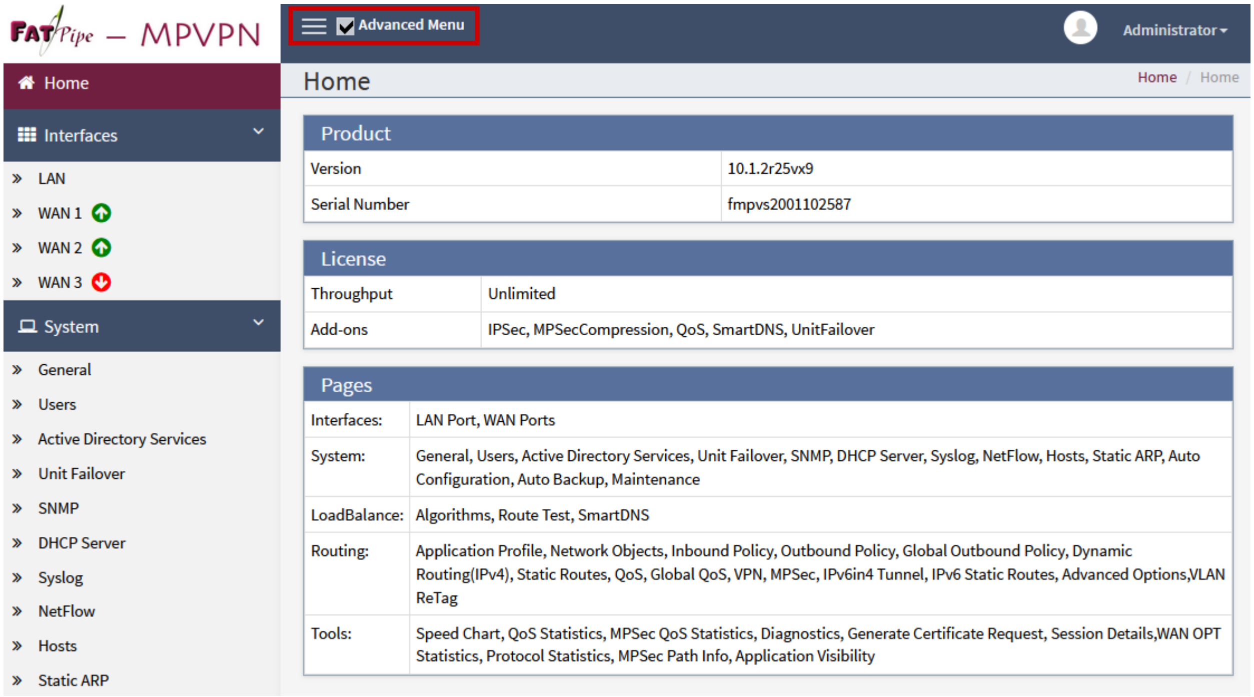
User Name

Password

Authentication:

● Local ○ LDAP ○ Radius

Once logged in, FatPipe MPVPN® Home is shown. Select the **Advanced Menu** check box to show all the available options in left pane.



Product

Version	10.1.2r25vx9
Serial Number	fmpvs2001102587

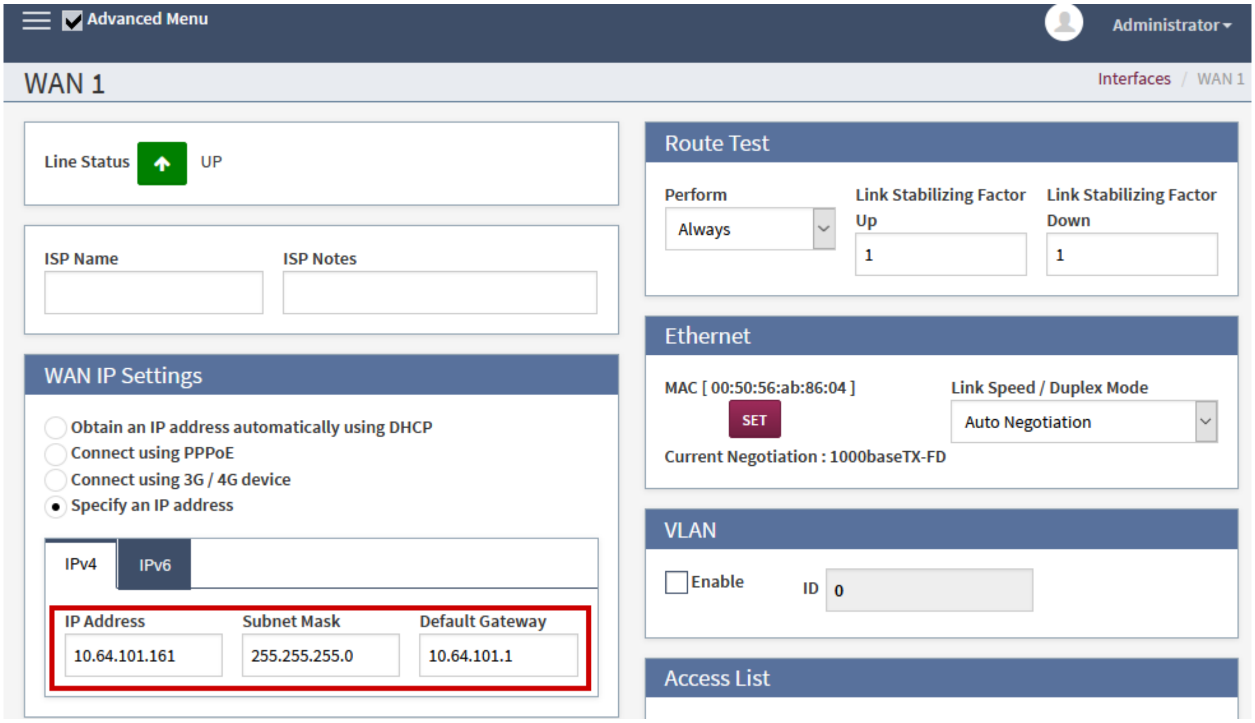
License

Throughput	Unlimited
Add-ons	IPSec, MPSecCompression, QoS, SmartDNS, UnitFailover

Pages

Interfaces:	LAN Port, WAN Ports
System:	General, Users, Active Directory Services, Unit Failover, SNMP, DHCP Server, Syslog, NetFlow, Hosts, Static ARP, Auto Configuration, Auto Backup, Maintenance
LoadBalance:	Algorithms, Route Test, SmartDNS
Routing:	Application Profile, Network Objects, Inbound Policy, Outbound Policy, Global Outbound Policy, Dynamic Routing(IPv4), Static Routes, QoS, Global QoS, VPN, MPSec, IPv6in4 Tunnel, IPv6 Static Routes, Advanced Options,VLAN ReTag
Tools:	Speed Chart, QoS Statistics, MPSec QoS Statistics, Diagnostics, Generate Certificate Request, Session Details,WAN OPT Statistics, Protocol Statistics, MPSec Path Info, Application Visibility

On the left pane under **Interfaces;** select the **WAN 1** and configure the **IPv4** information. During Compliance testing, 10.64.101.161 IP Address was used for WAN 1 connectivity. Click **Save** once done (not shown).



Line Status UP

ISP Name

ISP Notes

WAN IP Settings

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

IP Address	Subnet Mask	Default Gateway
10.64.101.161	255.255.255.0	10.64.101.1

Route Test

Perform	Link Stabilizing Factor Up	Link Stabilizing Factor Down
Always	1	1

Ethernet

MAC [00:50:56:ab:86:04]

Link Speed / Duplex Mode: Auto Negotiation

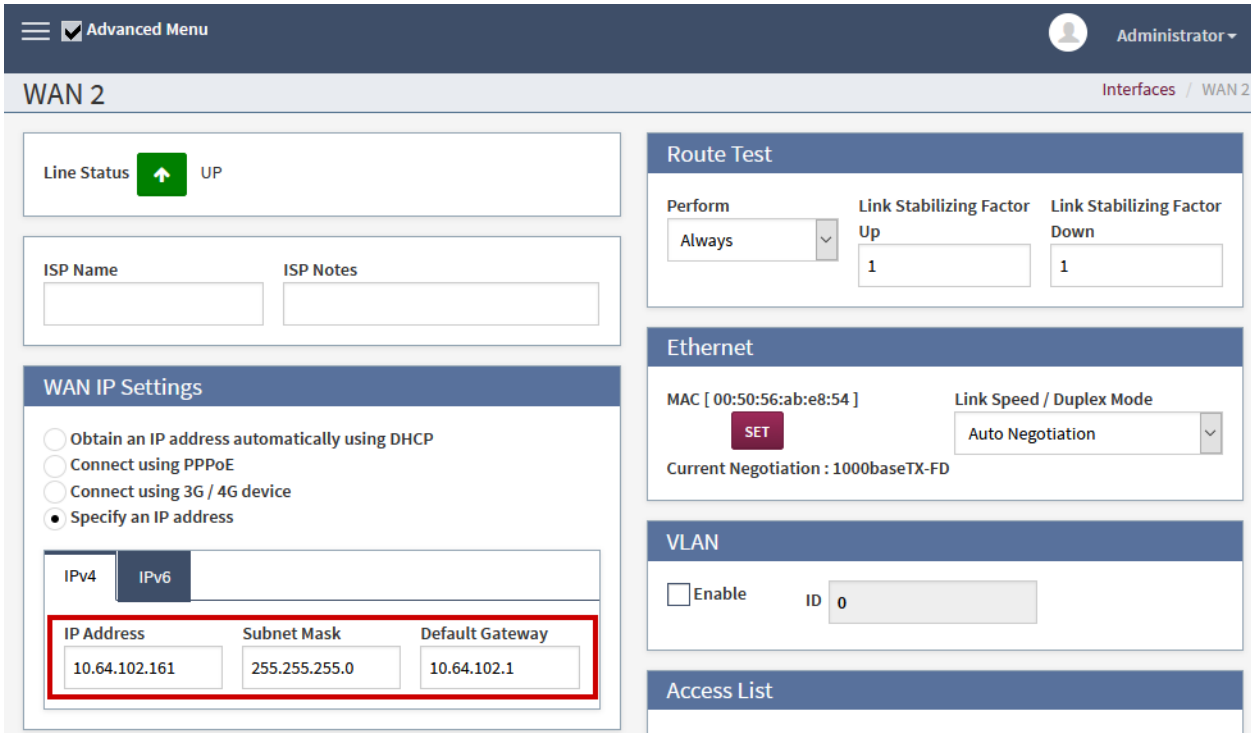
Current Negotiation : 1000baseTX-FD

VLAN

□ Enable ID 0

Access List

Continuing from above, select the **WAN 2** tab and configure the **IPv4** information. During Compliance testing, 10.64.102.161 IP Address was used for WAN 2 connectivity. Click **Save** once done (not shown).



WAN 2

Line Status UP

ISP Name

ISP Notes

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	Subnet Mask	Default Gateway
10.64.102.161	255.255.255.0	10.64.102.1

Route Test

Perform	Link Stabilizing Factor Up	Link Stabilizing Factor Down
Always	1	1

Ethernet

MAC [00:50:56:ab:e8:54] SET

Link Speed / Duplex Mode: Auto Negotiation

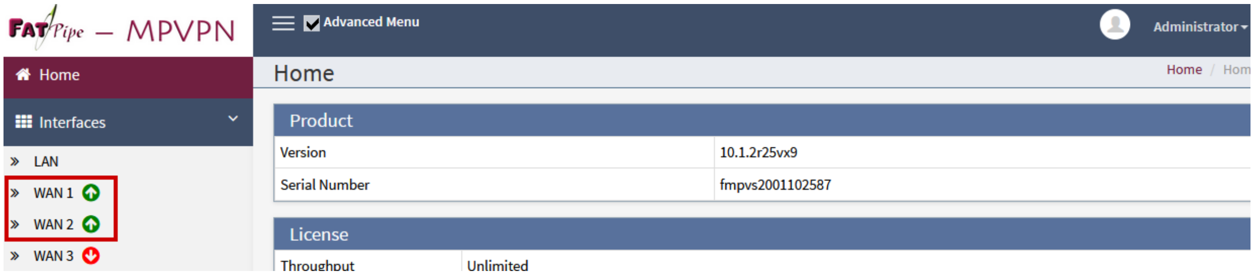
Current Negotiation : 1000baseTX-FD

VLAN

□ Enable ID 0

Access List

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



Home

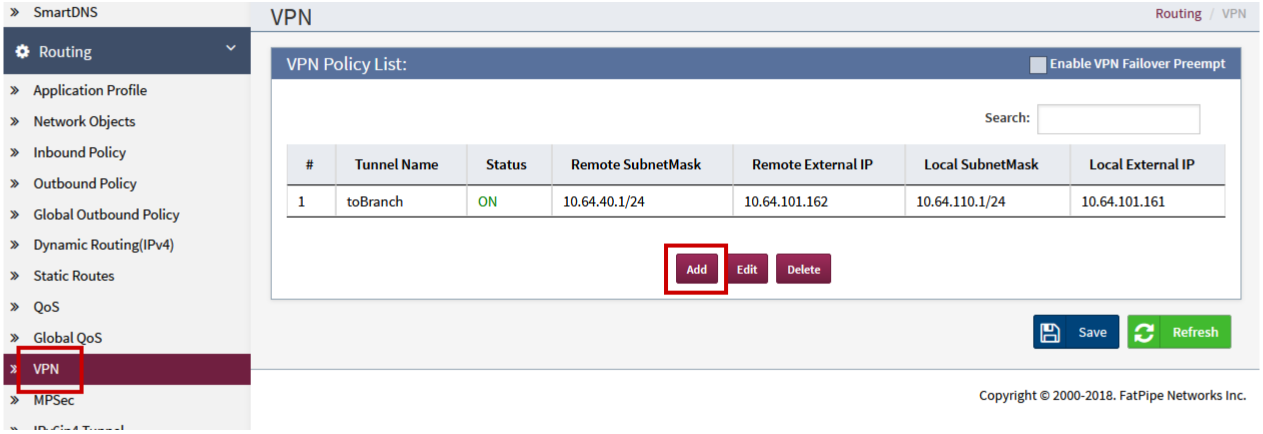
Product

Version	10.1.2r25vx9
Serial Number	fmpvs2001102587

License

Throughput	Unlimited

On the left pane, select **VPN** under the **Routing** sub section. Click **Add** to add a VPN connection.



VPN

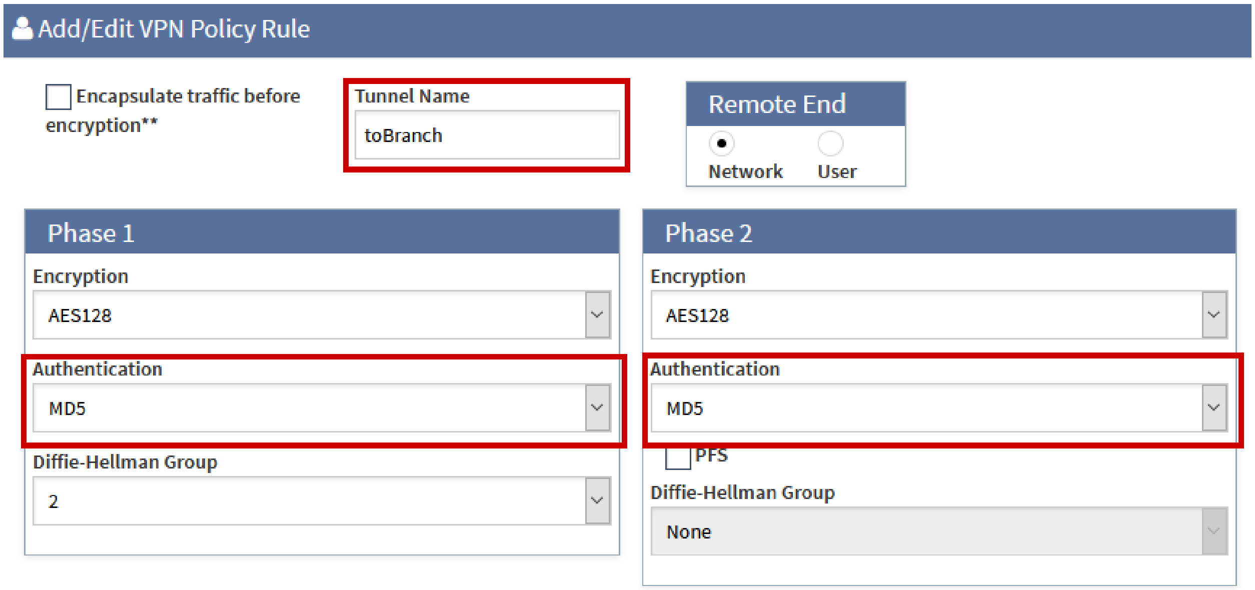
VPN Policy List: □ Enable VPN Failover Preempt

Search:

#	Tunnel Name	Status	Remote SubnetMask	Remote External IP	Local SubnetMask	Local External IP
1	toBranch	ON	10.64.40.1/24	10.64.101.162	10.64.110.1/24	10.64.101.161

Copyright © 2000-2018. FatPipe Networks Inc.

An **Add/Edit VPN Policy Rule** window will open; type in a **Tunnel Name** and set **Authentication** to **MD5** for both **Phase 1** and **Phase 2**.



Add/Edit VPN Policy Rule

□ Encapsulate traffic before encryption**

Tunnel Name: toBranch

Remote End: ● Network ○ User

Phase 1

Encryption: AES128

Authentication: MD5

Diffie-Hellman Group: 2

Phase 2

Encryption: AES128

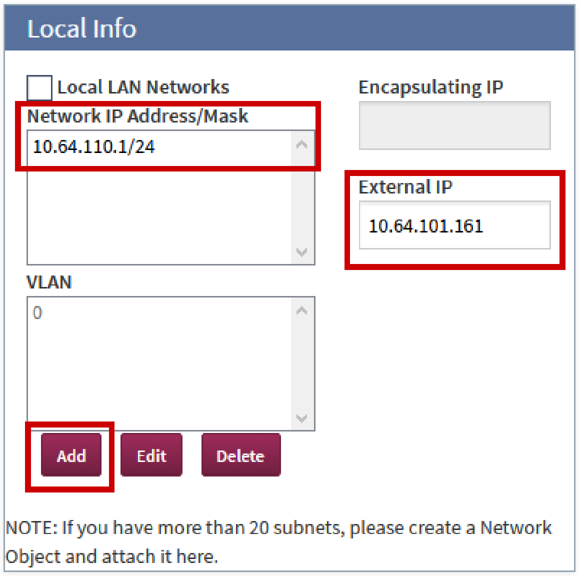
Authentication: MD5

□ PFS

Diffie-Hellman Group: None

Continuing from above:

- Under the **Local Info** section, select **Add**:
  - Type in the network information for local network on the enterprise site. E.g.,10.64.110.1/24 with VLAN tag of 0.
  - Type in the **External IP** that was used for **WAN 1**.
- Under the **Remote Info** section, select **Add**:
  - Type in the network information for branch site. E.g., 10.64.40.1/24
  - Type in the **External IP** that will be used by FatPipe MPVPN® on branch site for **WAN 1**.



Local Info

□ Local LAN Networks

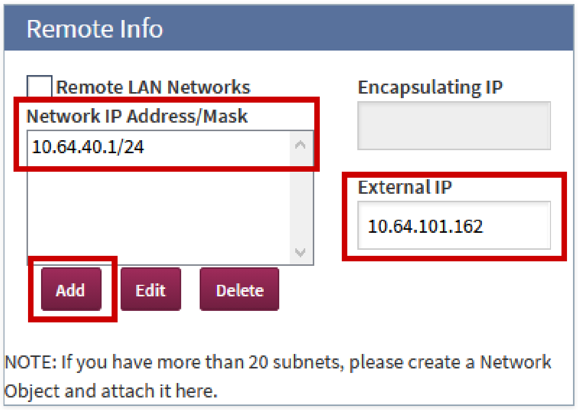
Network IP Address/Mask: 10.64.110.1/24

VLAN: 0

Encapsulating IP:

External IP: 10.64.101.161

NOTE: If you have more than 20 subnets, please create a Network Object and attach it here.



Remote Info

□ Remote LAN Networks

Network IP Address/Mask: 10.64.40.1/24

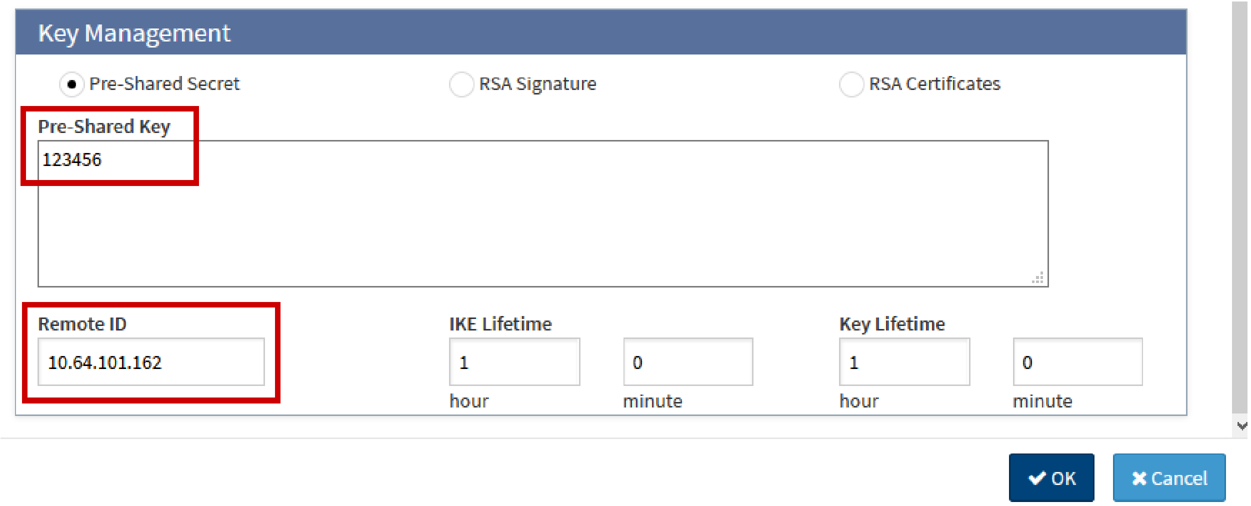
Encapsulating IP:

External IP: 10.64.101.162

NOTE: If you have more than 20 subnets, please create a Network Object and attach it here.

Continuing from above:

- 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 branch site.
- In the **Remote ID** field, type in the IP Address will be used by FatPipe MPVPN® on branch site for **WAN 1**. Select **OK** once done.



Key Management

● Pre-Shared Secret ○ RSA Signature ○ RSA Certificates

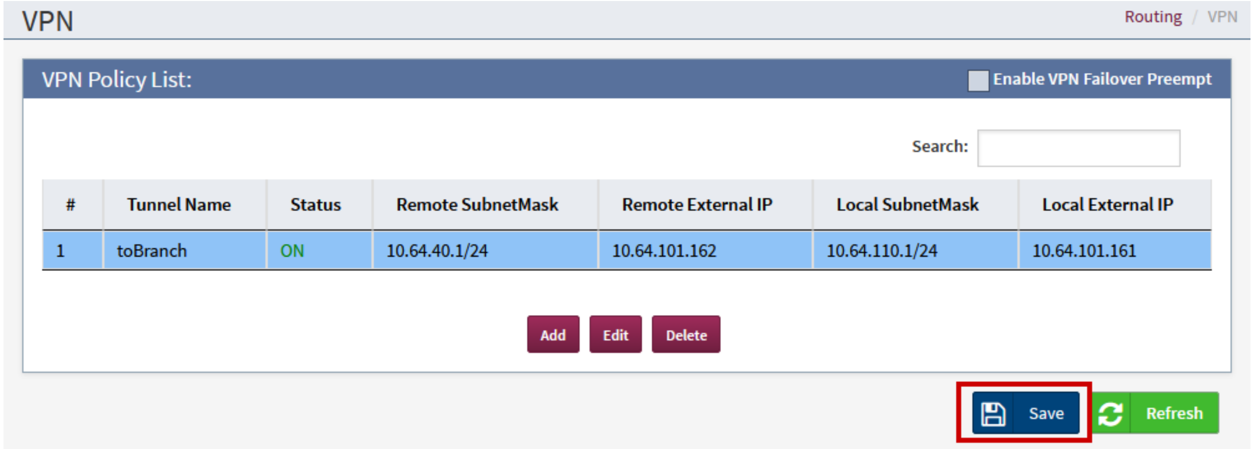
Pre-Shared Key: 123456

Remote ID: 10.64.101.162

IKE Lifetime: 1 hour 0 minute

Key Lifetime: 1 hour 0 minute

At the bottom of the page, select **Save**.



VPN Policy List:

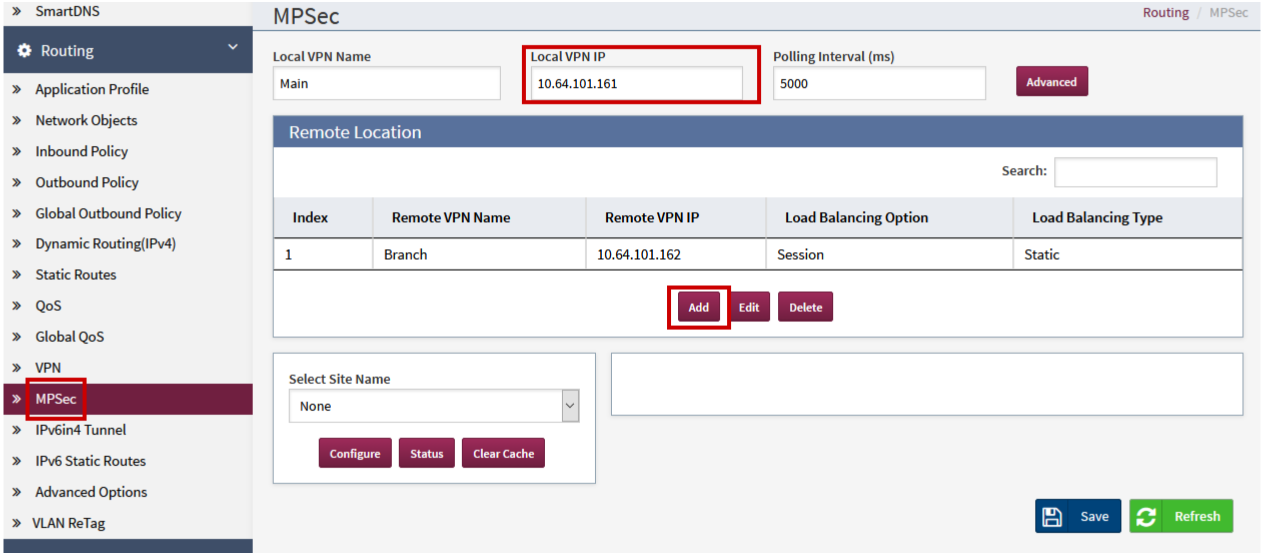
□ Enable VPN Failover Preempt

Search:

#	Tunnel Name	Status	Remote SubnetMask	Remote External IP	Local SubnetMask	Local External IP
1	toBranch	ON	10.64.40.1/24	10.64.101.162	10.64.110.1/24	10.64.101.161

Continuing from above, select the **MPSec**:

- Type in the **WAN 1** IP Address in **Local VPN IP** field.
- Select **Add** to add an MPSec connection to the branch site.



Local VPN Name: Main

Local VPN IP: 10.64.101.161

Polling Interval (ms): 5000

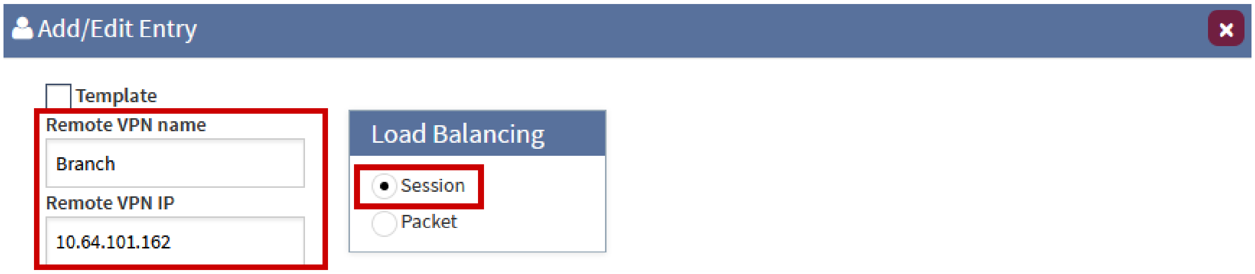
Remote Location

Search:

Index	Remote VPN Name	Remote VPN IP	Load Balancing Option	Load Balancing Type
1	Branch	10.64.101.162	Session	Static

Select Site Name: None

An **Add/Edit Entry** window will open; type in a name for **Remote VPN Name**. For the **Remote VPN IP**, type in the WAN 1 IP Address of FatPipe MPVPN® on the branch site. Once done, click **OK** (not shown)**.**



Add/Edit Entry

□ Template

Remote VPN name: Branch

Remote VPN IP: 10.64.101.162

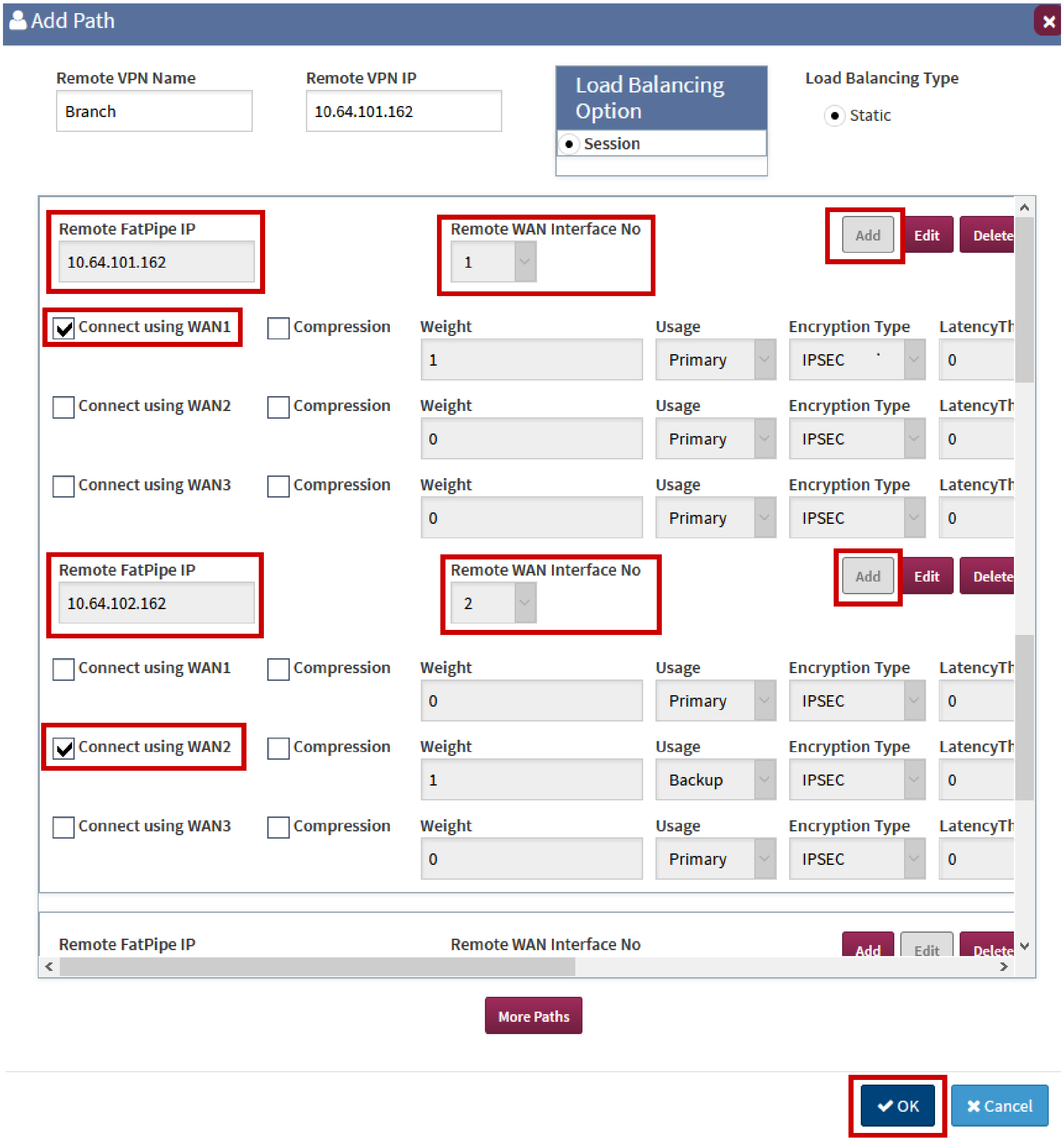
Load Balancing

● Session

○ Packet

An **Add Path** window will open:

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



Add Path

Remote VPN Name: Branch

Remote VPN IP: 10.64.101.162

Load Balancing Option: ● Session

Load Balancing Type: ● Static

Remote FatPipe IP: 10.64.101.162

Remote WAN Interface No: 1

☑ Connect using WAN1	□ Compression	Weight: 1	Usage: Primary	Encryption Type: IPSEC	LatencyTh: 0
□ Connect using WAN2	□ Compression	Weight: 0	Usage: Primary	Encryption Type: IPSEC	LatencyTh: 0
□ Connect using WAN3	□ Compression	Weight: 0	Usage: Primary	Encryption Type: IPSEC	LatencyTh: 0

Remote FatPipe IP: 10.64.102.162

Remote WAN Interface No: 2

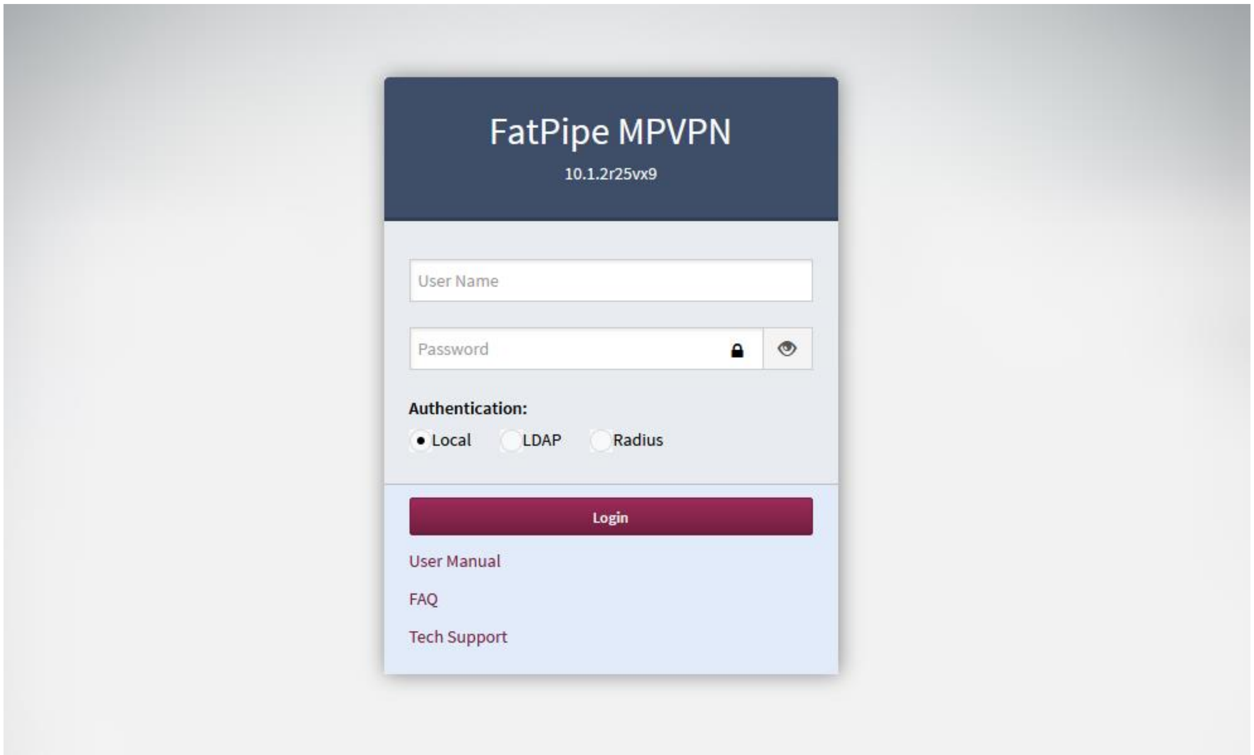
□ Connect using WAN1	□ Compression	Weight: 0	Usage: Primary	Encryption Type: IPSEC	LatencyTh: 0
☑ Connect using WAN2	□ Compression	Weight: 1	Usage: Backup	Encryption Type: IPSEC	LatencyTh: 0
□ Connect using WAN3	□ Compression	Weight: 0	Usage: Primary	Encryption Type: IPSEC	LatencyTh: 0

Remote FatPipe IP

Remote WAN Interface No

6.2. Branch Site

Open a web browser and point the browser to the FatPipe MPVPN®'s IP Address. Log on using appropriate credentials.



FatPipe MPVPN

10.1.2r25vx9

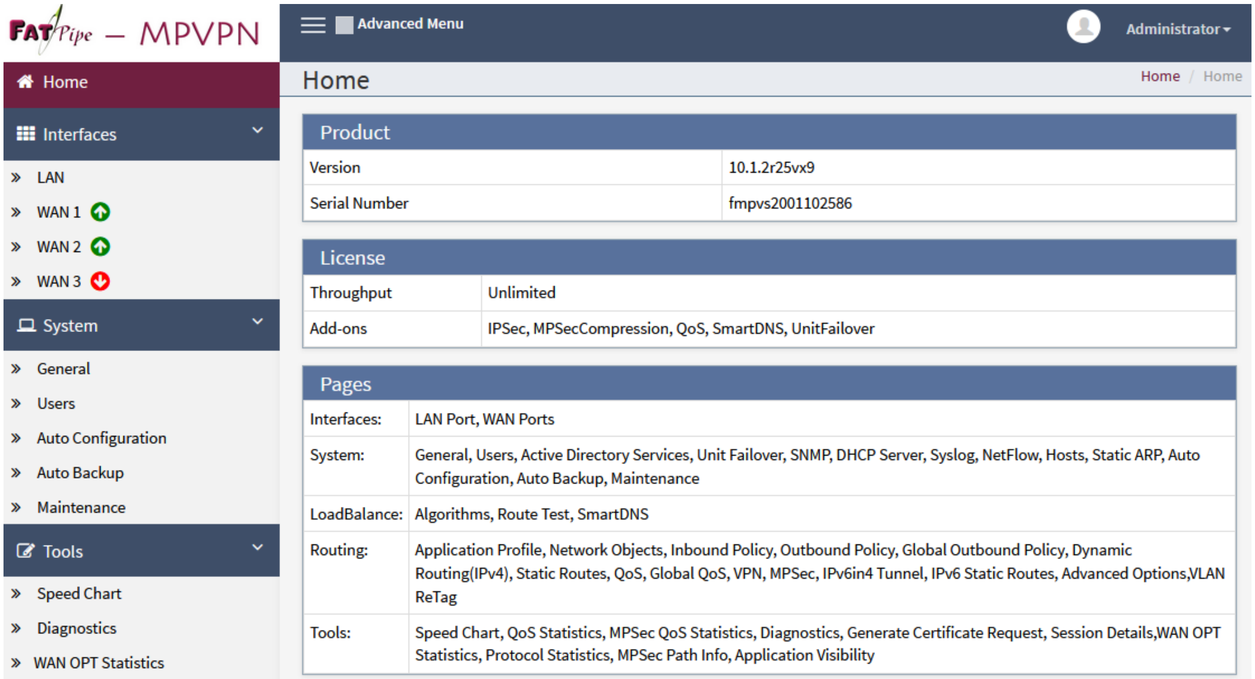
User Name

Password

Authentication:

● Local ○ LDAP ○ Radius

Once logged in, FatPipe MPVPN® Home is shown. Select the **Advanced Menu** check box to show all the available options in left pane.



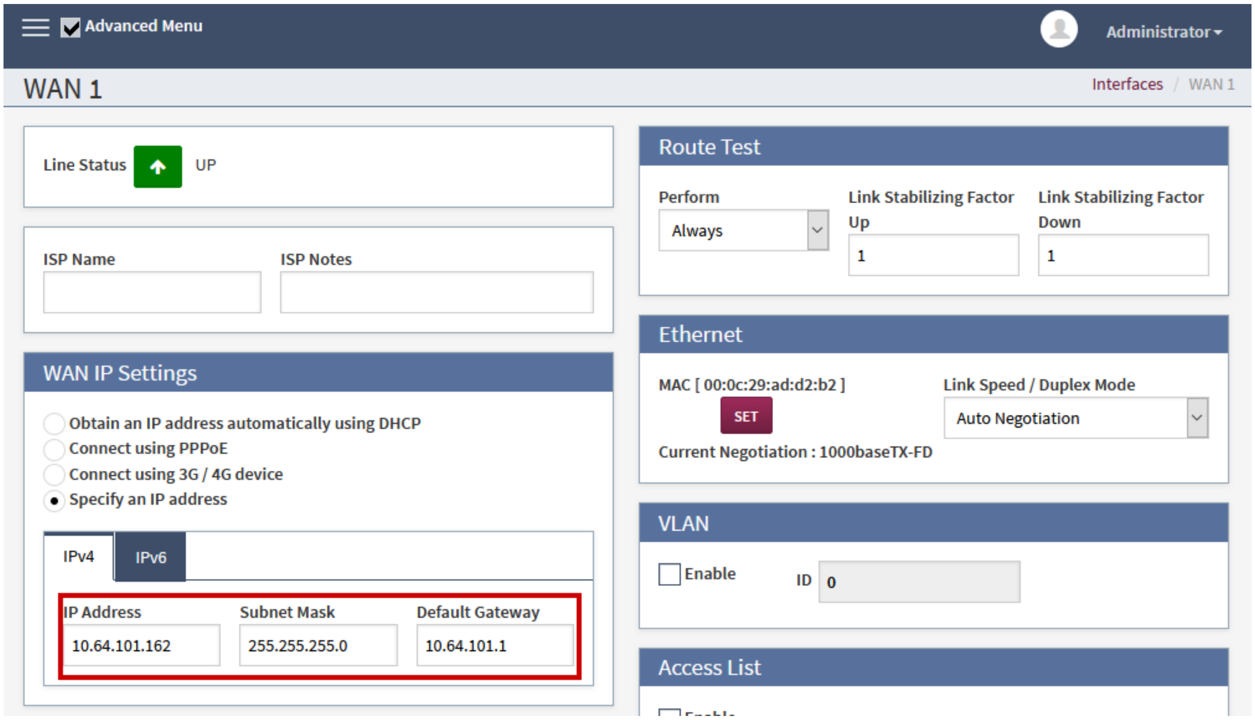
Home

Product	
Version	10.1.2r25vx9
Serial Number	fmpvs2001102586

License	
Throughput	Unlimited
Add-ons	IPSec, MPSecCompression, QoS, SmartDNS, UnitFailover

Pages	
Interfaces:	LAN Port, WAN Ports
System:	General, Users, Active Directory Services, Unit Failover, SNMP, DHCP Server, Syslog, NetFlow, Hosts, Static ARP, Auto Configuration, Auto Backup, Maintenance
LoadBalance:	Algorithms, Route Test, SmartDNS
Routing:	Application Profile, Network Objects, Inbound Policy, Outbound Policy, Global Outbound Policy, Dynamic Routing(IPv4), Static Routes, QoS, Global QoS, VPN, MPSec, IPv6in4 Tunnel, IPv6 Static Routes, Advanced Options,VLAN ReTag
Tools:	Speed Chart, QoS Statistics, MPSec QoS Statistics, Diagnostics, Generate Certificate Request, Session Details,WAN OPT Statistics, Protocol Statistics, MPSec Path Info, Application Visibility

On the left pane under **Interfaces;** select the **WAN 1** and configure the **IPv4** information. During Compliance testing, 10.64.101.162 IP Address was used for WAN 1 connectivity. Click **Save** once done (not shown).



WAN 1

Line Status UP

ISP Name

ISP Notes

WAN IP Settings

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

IP Address	Subnet Mask	Default Gateway
10.64.101.162	255.255.255.0	10.64.101.1

Route Test

Perform	Link Stabilizing Factor Up	Link Stabilizing Factor Down
Always	1	1

Ethernet

MAC [00:0c:29:ad:d2:b2]

Link Speed / Duplex Mode: Auto Negotiation

Current Negotiation : 1000baseTX-FD

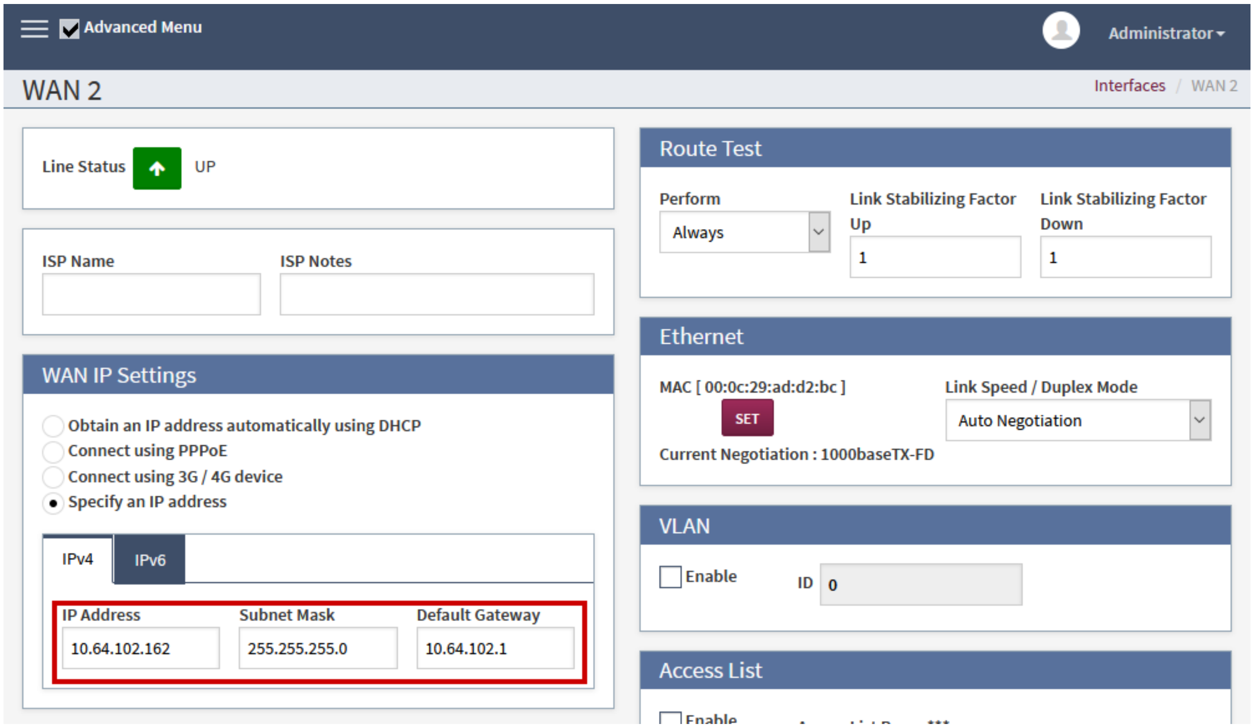
VLAN

☐ Enable ID 0

Access List

☐ Enable

Continuing from above, select the **WAN 2** tab and configure the **IPv4** information. During Compliance testing, 10.64.102.162 IP Address was used for WAN 2 connectivity. Click **Save** once done (not shown).



WAN 2

Line Status: UP

ISP Name:

ISP Notes:

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	Subnet Mask	Default Gateway
10.64.102.162	255.255.255.0	10.64.102.1

Route Test

Perform	Link Stabilizing Factor Up	Link Stabilizing Factor Down
Always	1	1

Ethernet

MAC [00:0c:29:ad:d2:bc] SET

Link Speed / Duplex Mode: Auto Negotiation

Current Negotiation : 1000baseTX-FD

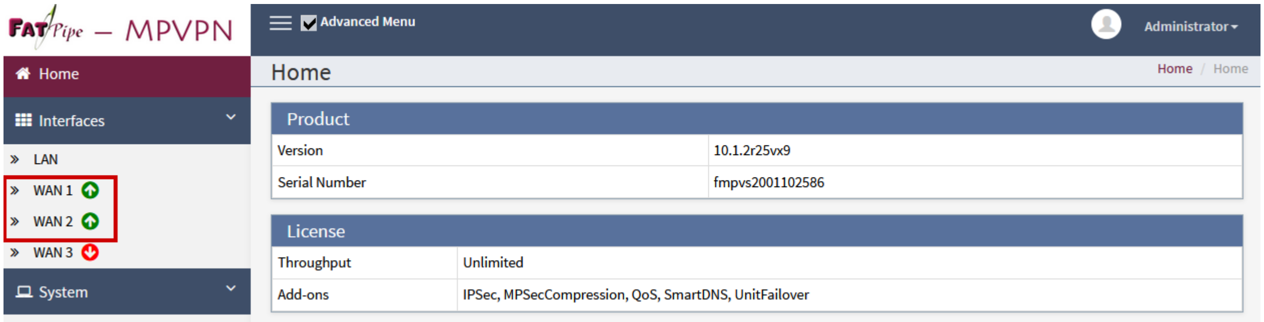
VLAN

□ Enable ID 0

Access List

□ Enable

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



Home

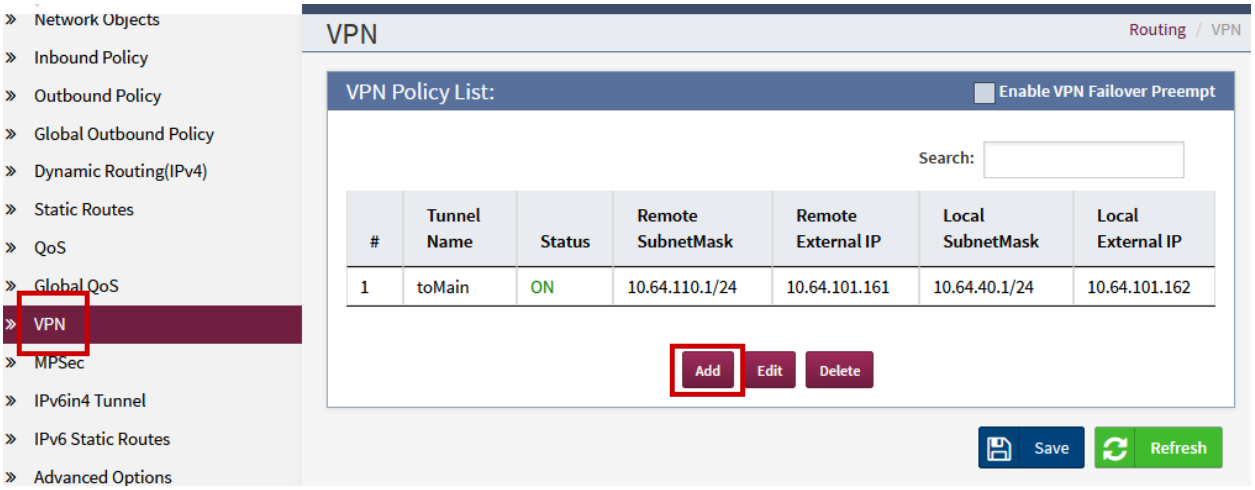
Product

Version	10.1.2r25vx9
Serial Number	fmpvs2001102586

License

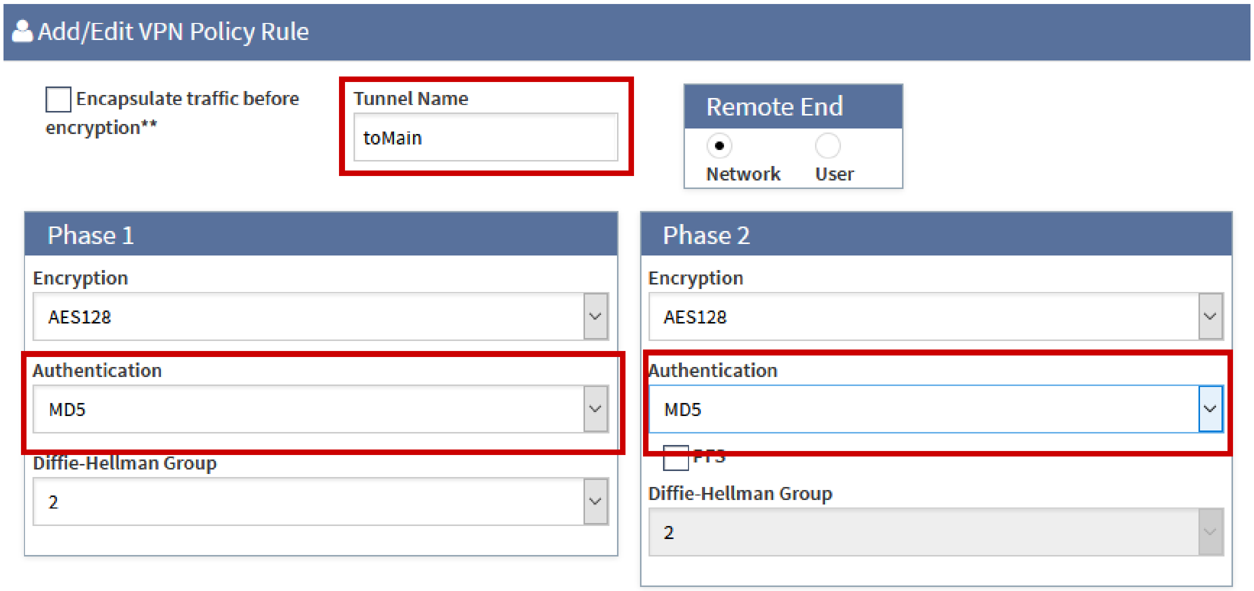
Throughput	Unlimited
Add-ons	IPSec, MPSecCompression, QoS, SmartDNS, UnitFailover

On the left pane, select **VPN** under the **Routing** sub section. Click **Add** to add a VPN connection.



#	Tunnel Name	Status	Remote SubnetMask	Remote External IP	Local SubnetMask	Local External IP
1	toMain	ON	10.64.110.1/24	10.64.101.161	10.64.40.1/24	10.64.101.162

An **Add/Edit VPN Policy Rule** window will open; type in a **Tunnel Name** and set **Authentication** to **MD5** for both **Phase 1** and **Phase 2**.



□ Encapsulate traffic before encryption**

Tunnel Name: toMain

Remote End: ● Network ○ User

Phase 1

Encryption: AES128

Authentication: MD5

Diffie-Hellman Group: 2

Phase 2

Encryption: AES128

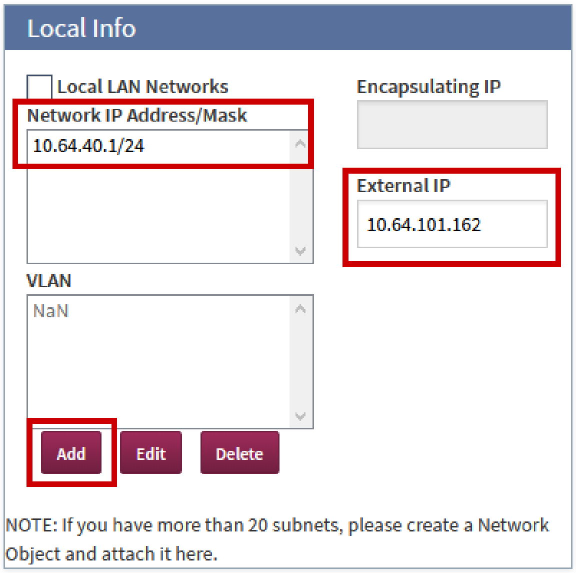
Authentication: MD5

□ PFS

Diffie-Hellman Group: 2

Continuing from above:

- Under the **Local Info** section, select **Add**:
  - Type in the network information for local network on the enterprise site. E.g.,10.64.40.1/24 with no VLAN.
  - Type in the **External IP** that was used for **WAN 1**.
- Under the **Remote Info** section, select **Add**:
  - Type in the network information for branch site. E.g., 10.64.40.1/24
  - Type in the **External IP** that was used by FatPipe MPVPN® on enterprise site for **WAN 1**.



Local Info

□ Local LAN Networks

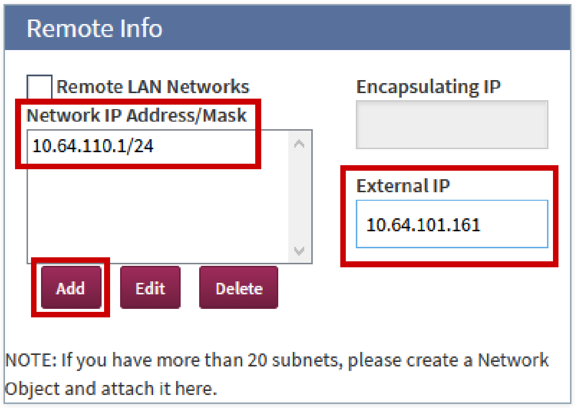
Network IP Address/Mask: 10.64.40.1/24

VLAN: NaN

Encapsulating IP:

External IP: 10.64.101.162

NOTE: If you have more than 20 subnets, please create a Network Object and attach it here.



Remote Info

□ Remote LAN Networks

Network IP Address/Mask: 10.64.110.1/24

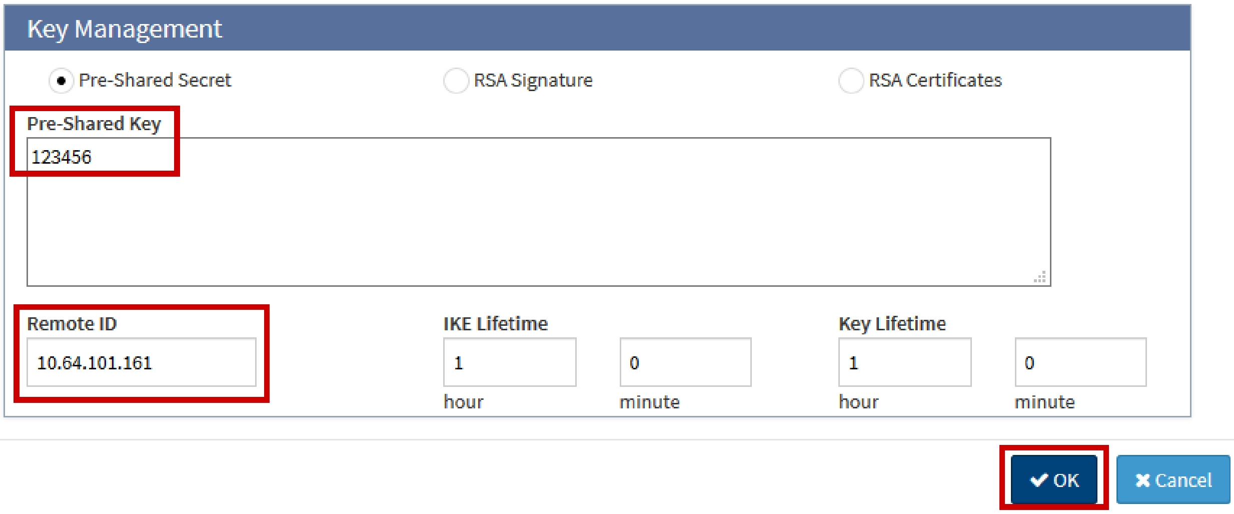
Encapsulating IP:

External IP: 10.64.101.161

NOTE: If you have more than 20 subnets, please create a Network Object and attach it here.

Continuing from above:

- Under the **Key Management** section, type in a **Pre-Share Key**. This key must be the same as that was configured on enterprise site.
- In the **Remote ID** field, type in the IP Address that was used by FatPipe MPVPN® on enterprise site for **WAN 1**. Select **OK** once done.



Key Management

● Pre-Shared Secret ○ RSA Signature ○ RSA Certificates

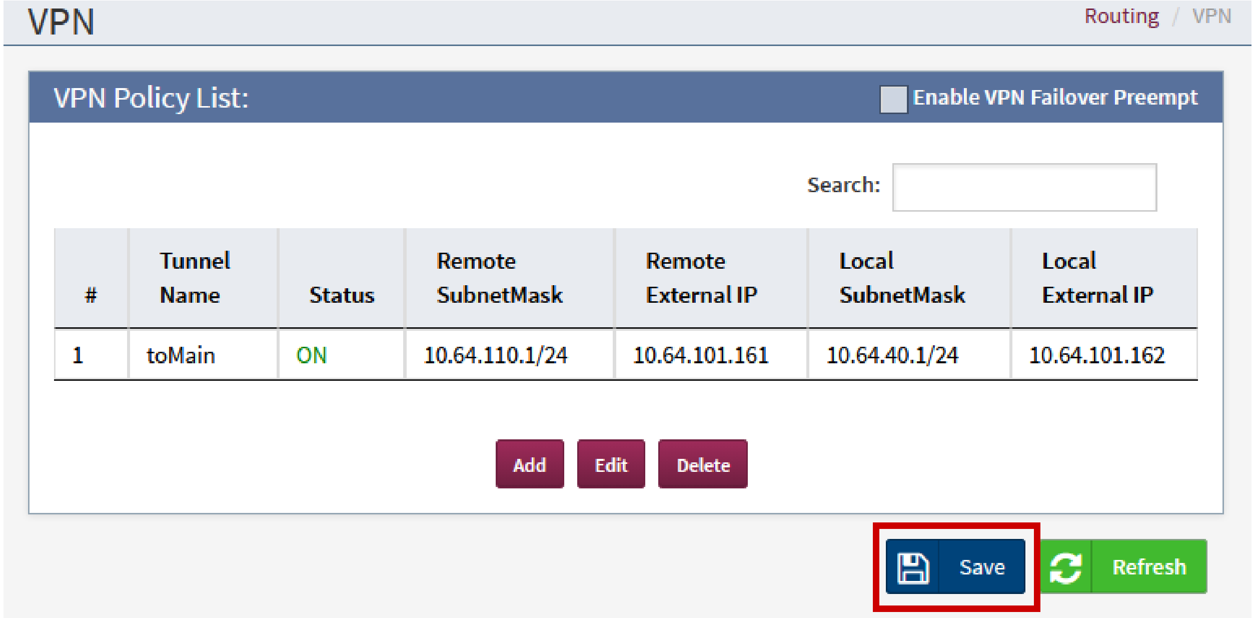
Pre-Shared Key: 123456

Remote ID: 10.64.101.161

IKE Lifetime: 1 hour 0 minute

Key Lifetime: 1 hour 0 minute

At the bottom of the page, select **Save**.



VPN

Routing / VPN

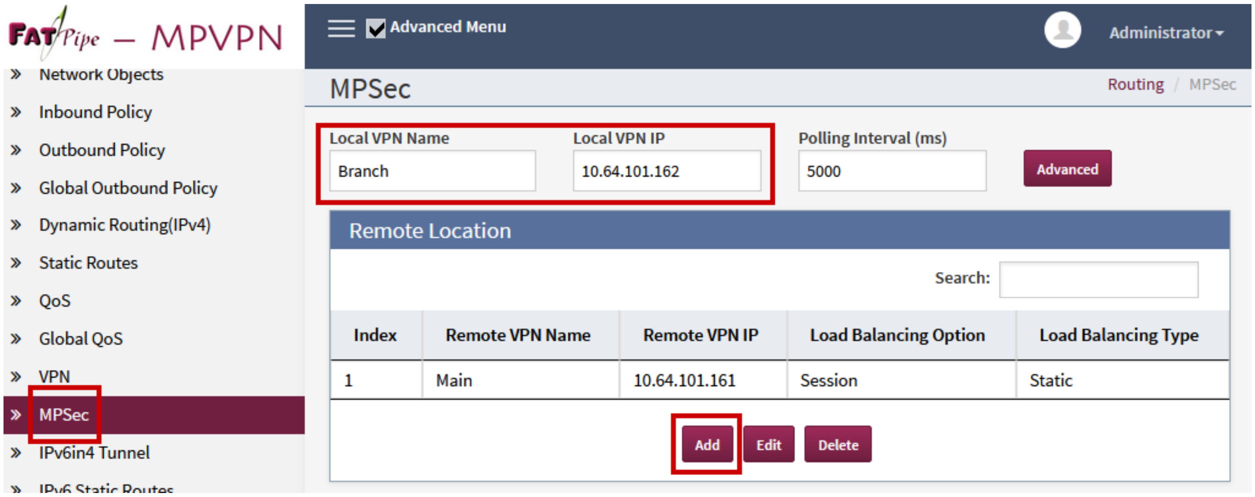
VPN Policy List: □ Enable VPN Failover Preempt

Search:

#	Tunnel Name	Status	Remote SubnetMask	Remote External IP	Local SubnetMask	Local External IP
1	toMain	ON	10.64.110.1/24	10.64.101.161	10.64.40.1/24	10.64.101.162

Continuing from above, on the left pane, select the **MPSec**:

- Type in the **WAN 1** IP Address in **Local VPN IP** field and a name.
- Select **Add** to add an MPSec connection to the enterprise site.



MPSec

Local VPN Name: Branch

Local VPN IP: 10.64.101.162

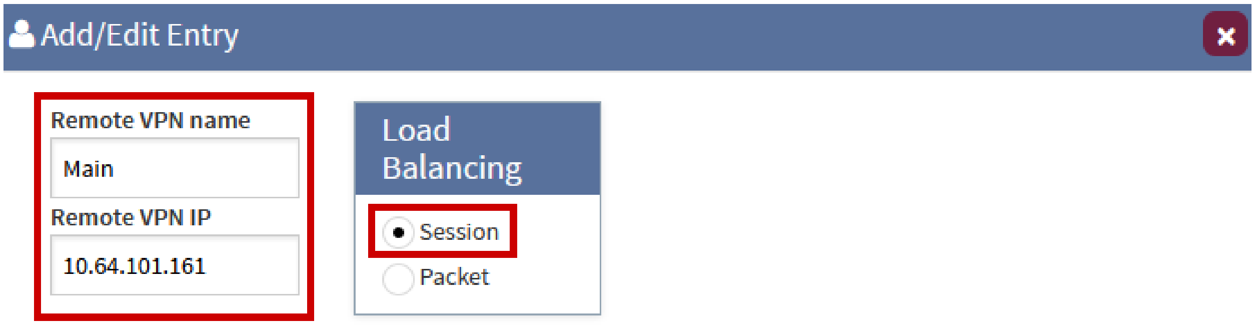
Polling Interval (ms): 5000

Remote Location

Search:

Index	Remote VPN Name	Remote VPN IP	Load Balancing Option	Load Balancing Type
1	Main	10.64.101.161	Session	Static

An **Add/Edit Entry** window will open; type in a name for **Remote VPN Name**. For the **Remote VPN IP**, type in the WAN 1 IP Address of FatPipe MPVPN® on the enterprise site. Once done, click **OK** (not shown)**.**



Add/Edit Entry

Remote VPN name: Main

Remote VPN IP: 10.64.101.161

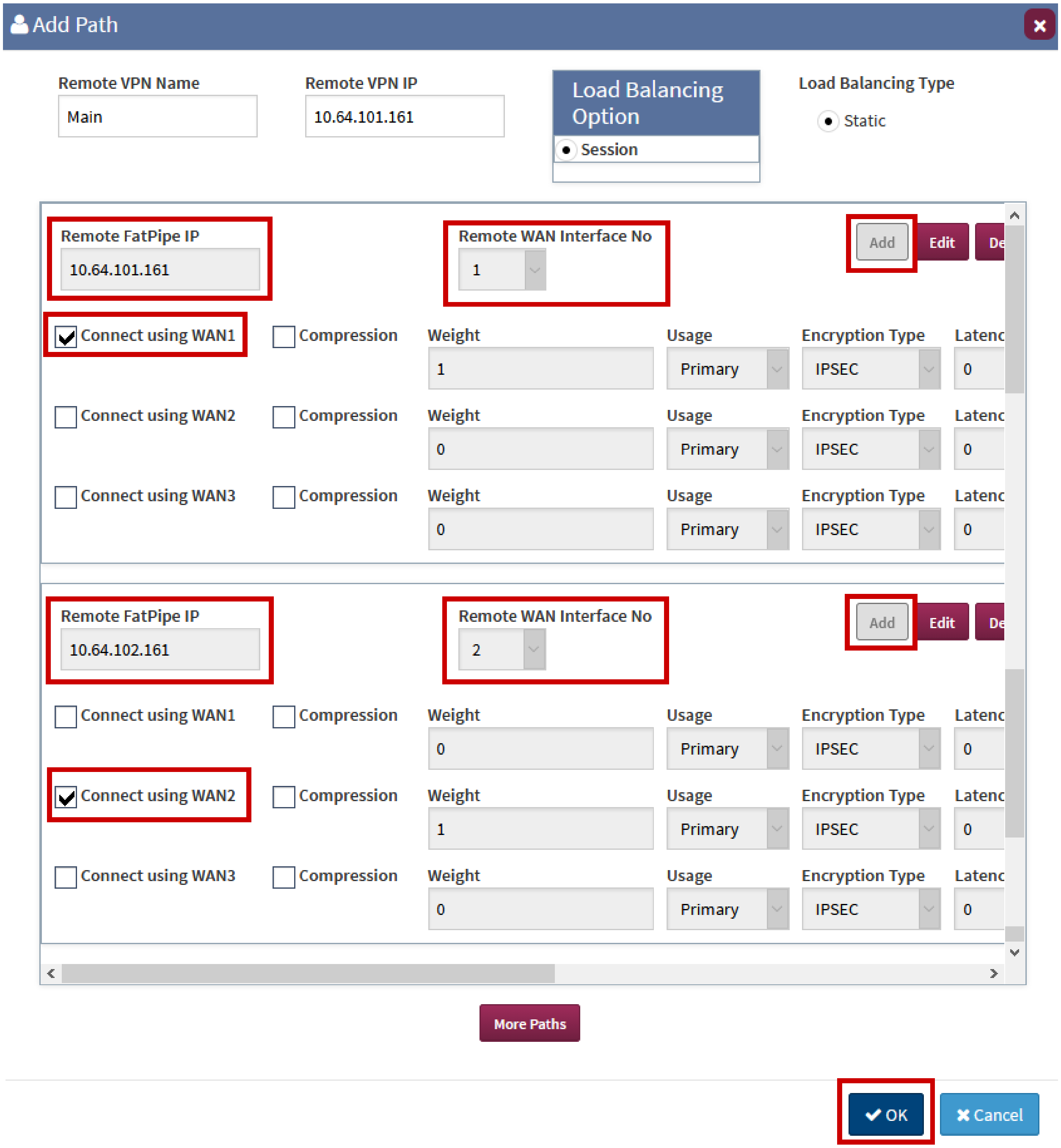
Load Balancing

● Session

○ Packet

An **Add Path** window will open:

- Select **Add** for Remote WAN Interface 1 and type in the WAN 1 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**.



Remote VPN Name: Main

Remote VPN IP: 10.64.101.161

Load Balancing Option: ● Session

Load Balancing Type: ● Static

Remote FatPipe IP: 10.64.101.161

Remote WAN Interface No: 1

		Weight	Usage	Encryption Type	Latenc
☑ Connect using WAN1	□ Compression	1	Primary	IPSEC	0
□ Connect using WAN2	□ Compression	0	Primary	IPSEC	0
□ Connect using WAN3	□ Compression	0	Primary	IPSEC	0

Remote FatPipe IP: 10.64.102.161

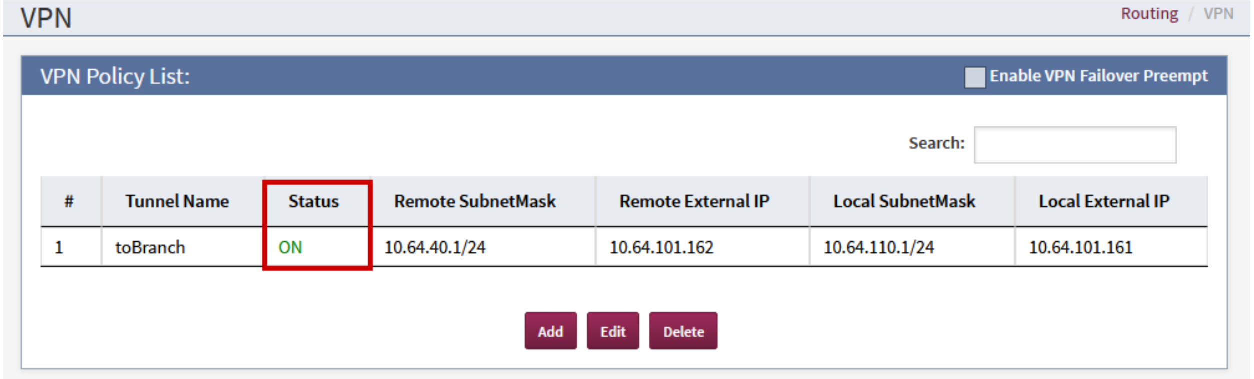
Remote WAN Interface No: 2

		Weight	Usage	Encryption Type	Latenc
□ Connect using WAN1	□ Compression	0	Primary	IPSEC	0
☑ Connect using WAN2	□ Compression	1	Primary	IPSEC	0
□ Connect using WAN3	□ Compression	0	Primary	IPSEC	0

7. Verification Steps

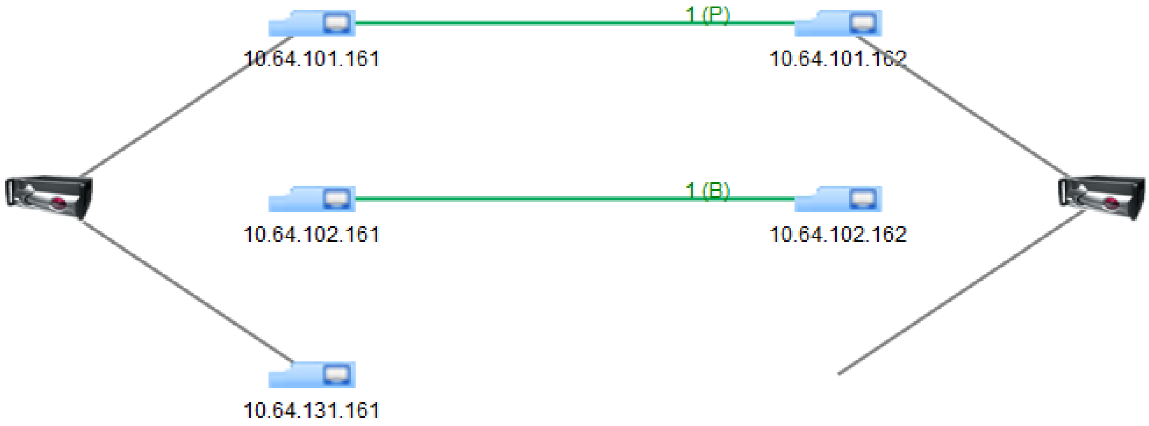
This section provides steps that may be performed to verify that the solution is configured correctly.

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

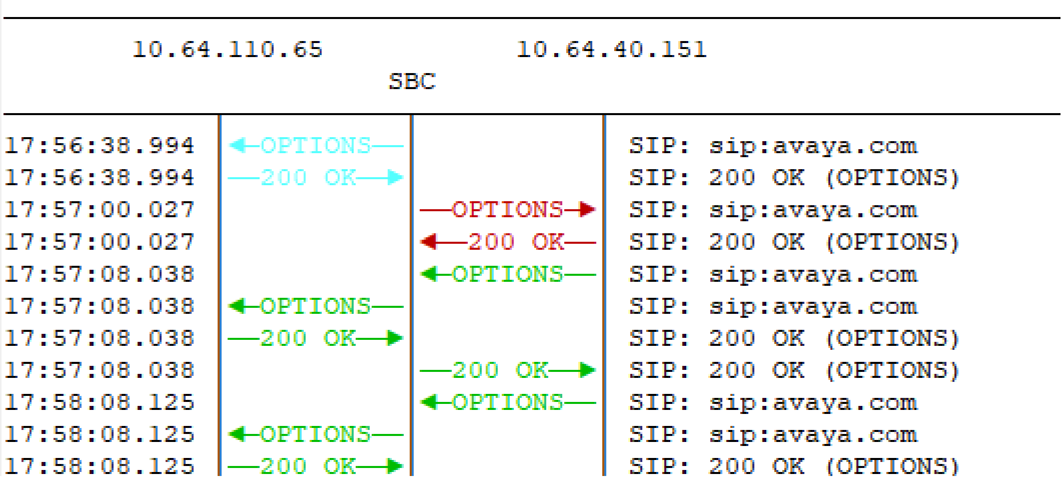


#	Tunnel Name	Status	Remote SubnetMask	Remote External IP	Local SubnetMask	Local External IP
1	toBranch	ON	10.64.40.1/24	10.64.101.162	10.64.110.1/24	10.64.101.161

2. Continuing from above, select the **MPSec** (not shown). At the bottom, select the configured MPSec connection from the **Select Site Name** drop down; click **Status**. If both MPSec connections to the branch site are successful, the connecting lines will turn green.



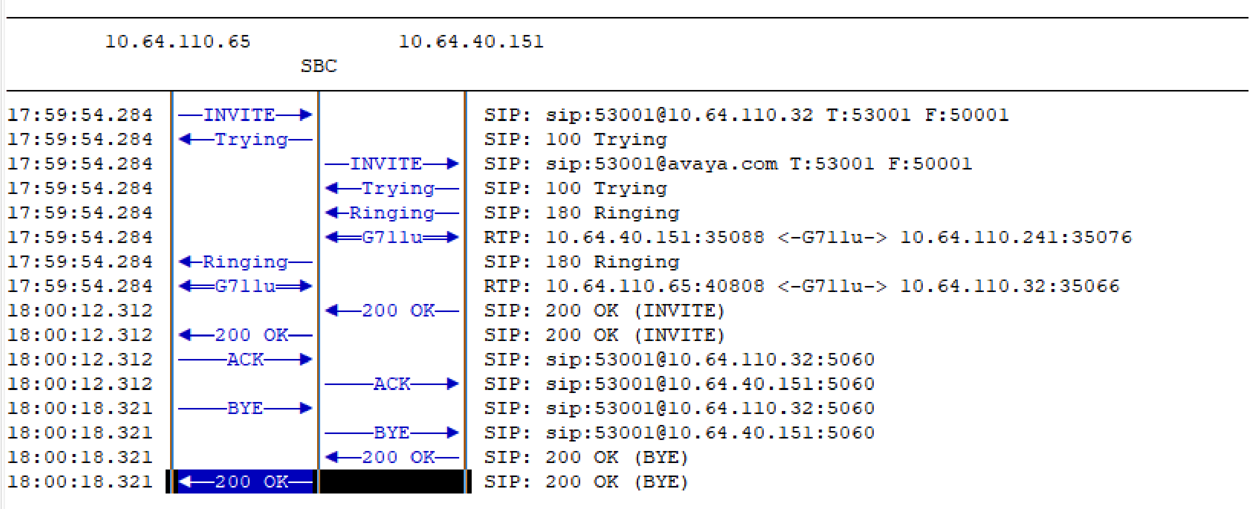
3. Connect to Avaya SBCE via SSH and run the **tracesbc** command. Verify SIP OPTIONS to and from the branch sites are successful. Note that 10.64.110.65 is the external IP Address of Avaya SBCE on enterprise site and 10.64.40.151 is the external IP Address of Avaya SBCE on branch site.



```
        10.64.110.65              10.64.40.151
                            SBC

17:56:38.994  ←OPTIONS─                   SIP: sip:avaya.com
17:56:38.994  ─200 OK→                    SIP: 200 OK (OPTIONS)
17:57:00.027              ─OPTIONS→       SIP: sip:avaya.com
17:57:00.027              ←200 OK─        SIP: 200 OK (OPTIONS)
17:57:08.038              ←OPTIONS─       SIP: sip:avaya.com
17:57:08.038  ←OPTIONS─                   SIP: sip:avaya.com
17:57:08.038  ─200 OK→                    SIP: 200 OK (OPTIONS)
17:57:08.038              ─200 OK→        SIP: 200 OK (OPTIONS)
17:58:08.125              ←OPTIONS─       SIP: sip:avaya.com
17:58:08.125  ←OPTIONS─                   SIP: sip:avaya.com
17:58:08.125  ─200 OK→                    SIP: 200 OK (OPTIONS)
```

4. Continuing from above, place a call from enterprise site to branch site. Verify SIP signaling and two way audio for the call.



```
        10.64.110.65        10.64.40.151
                       SBC

17:59:54.284  ─INVITE→              SIP: sip:53001@10.64.110.32 T:53001 F:50001
17:59:54.284  ←Trying─              SIP: 100 Trying
17:59:54.284             ─INVITE→   SIP: sip:53001@avaya.com T:53001 F:50001
17:59:54.284             ←Trying─   SIP: 100 Trying
17:59:54.284             ←Ringing─  SIP: 180 Ringing
17:59:54.284             ⇐G711u⇒    RTP: 10.64.40.151:35088 <-G711u-> 10.64.110.241:35076
17:59:54.284  ←Ringing─             SIP: 180 Ringing
17:59:54.284  ⇐G711u⇒               RTP: 10.64.110.65:40808 <-G711u-> 10.64.110.32:35066
18:00:12.312             ←200 OK─   SIP: 200 OK (INVITE)
18:00:12.312  ←200 OK─              SIP: 200 OK (INVITE)
18:00:12.312  ──ACK─→               SIP: sip:53001@10.64.110.32:5060
18:00:12.312             ──ACK─→    SIP: sip:53001@10.64.40.151:5060
18:00:18.321  ──BYE─→               SIP: sip:53001@10.64.110.32:5060
18:00:18.321             ──BYE─→    SIP: sip:53001@10.64.40.151:5060
18:00:18.321             ←200 OK─   SIP: 200 OK (BYE)
18:00:18.321  ←200 OK─              SIP: 200 OK (BYE)
```

8. Conclusion

These Application Notes describe the configuration necessary to configure FatPipe MPVPN® in Avaya Aura® enterprise and branch 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] *Administering Avaya Aura® Communication Manager,* Release 8.0.1, December 2018

[2] *Administering Avaya Aura® System Manager for Release 8.0.1,* December 2018

[3] *Administering Avaya Aura® Session Manager,* Release 8.0.1, Issue 3, December 2018

[4] *Administering Avaya Aura Session Border Controller for Enterprise,* Release 7.2.2, Issue 11, November 2018

Documentation related to MPVPN can directly be obtained from FatPipe.

©2019 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.