FATPipe®

MPVPN®

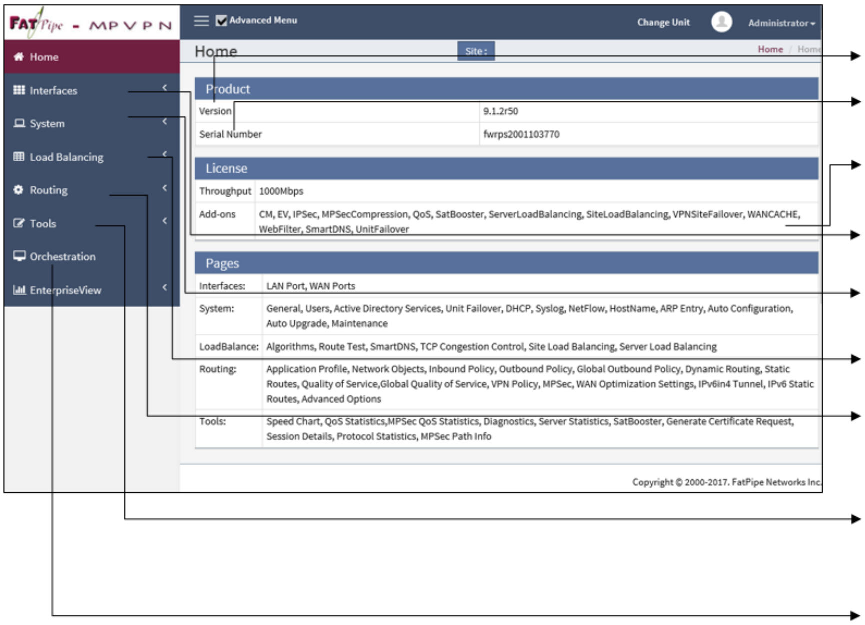
Quick Installation Guide

Version 9.1.2

Address: 4455 South 700 East
Salt Lake City, Utah 84107
Phone Number: 801-683-5656 Ext: 1800
Technical Support: 1(800)724-8521 Ext: 3
Email: support@fatpipeinc.com

HOME PAGE

Provides Information and Features in FatPipe



Product

Version	9.1.2r50
Serial Number	fwrps2001103770

License

Throughput	1000Mbps
Add-ons	CM, EV, IPSec, MPSecCompression, QoS, SatBooster, ServerLoadBalancing, SiteLoadBalancing, VPNSiteFailover, WANCACHE, WebFilter, SmartDNS, UnitFailover

Pages

Interfaces:	LAN Port, WAN Ports
System:	General, Users, Active Directory Services, Unit Failover, DHCP, Syslog, NetFlow, HostName, ARP Entry, Auto Configuration, Auto Upgrade, Maintenance
LoadBalance:	Algorithms, Route Test, SmartDNS, TCP Congestion Control, Site Load Balancing, Server Load Balancing
Routing:	Application Profile, Network Objects, Inbound Policy, Outbound Policy, Global Outbound Policy, Dynamic Routing, Static Routes, Quality of Service,Global Quality of Service, VPN Policy, MPSec, WAN Optimization Settings, IPv6in4 Tunnel, IPv6 Static Routes, Advanced Options
Tools:	Speed Chart, QoS Statistics,MPSec QoS Statistics, Diagnostics, Server Statistics, SatBooster, Generate Certificate Request, Session Details, Protocol Statistics, MPSec Path Info

Copyright © 2000-2017. FatPipe Networks Inc.

Tells the version FatPipe is running on.

Unique Serial Number given to each FatPipe Unit.

Add-on features on FatPipe.

LAN and WAN IP addresses can be configured under Interface tab.

Systems tab has all the features like general user settings, save a configuration file backup, and establish unit failover.

Balancing option, Route Test configuration and SmartDNS.

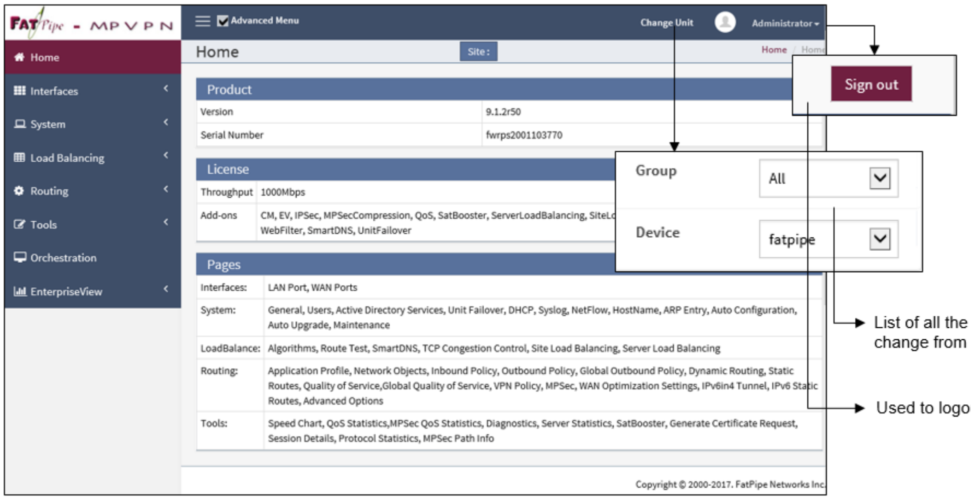
Setup and schedule Inbound and Outbound Policies, Static Routes, Quality of Service (QoS) Rules

Used to monitor the performance of your network. You can check the status of routers and Internet connections using Diagnostic Tools and view the speed of connections using the Speed Chart.

Configure and manage all you FatPipe devices from one central location.

HOME PAGE

Provides Information and Features in FatPipe



Product

Version	9.1.2r50
Serial Number	fwrps2001103770

License

Throughput	1000Mbps
Add-ons	CM, EV, IPSec, MPSecCompression, QoS, SatBooster, ServerLoadBalancing, SiteL WebFilter, SmartDNS, UnitFailover

Pages

Interfaces:	LAN Port, WAN Ports
System:	General, Users, Active Directory Services, Unit Failover, DHCP, Syslog, NetFlow, HostName, ARP Entry, Auto Configuration, Auto Upgrade, Maintenance
LoadBalance:	Algorithms, Route Test, SmartDNS, TCP Congestion Control, Site Load Balancing, Server Load Balancing
Routing:	Application Profile, Network Objects, Inbound Policy, Outbound Policy, Global Outbound Policy, Dynamic Routing, Static Routes, Quality of Service,Global Quality of Service, VPN Policy, MPSec, WAN Optimization Settings, IPv6in4 Tunnel, IPv6 Static Routes, Advanced Options
Tools:	Speed Chart, QoS Statistics,MPSec QoS Statistics, Diagnostics, Server Statistics, SatBooster, Generate Certificate Request, Session Details, Protocol Statistics, MPSec Path Info

Copyright © 2000-2017. FatPipe Networks Inc.

Group: All

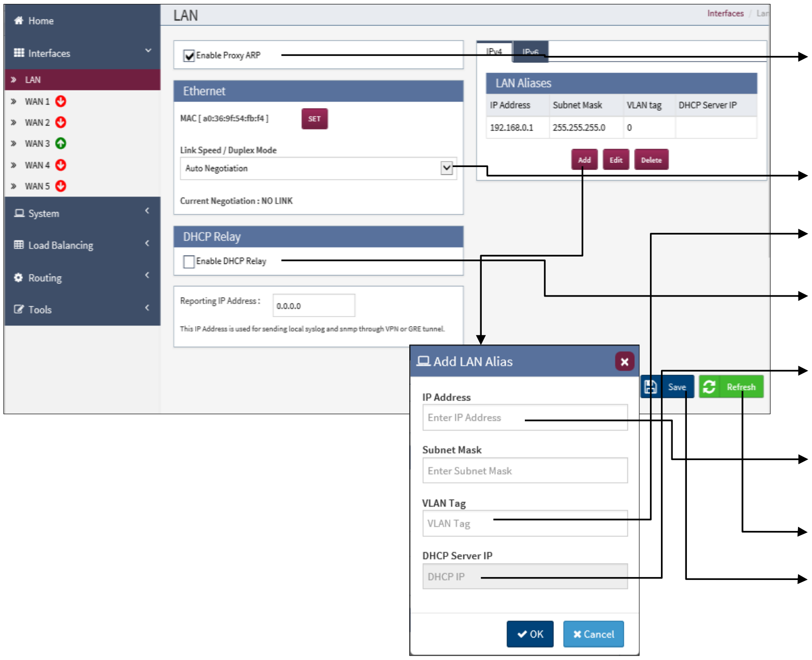
Device: fatpipe

List of all the FatPipes in the group to change from one unit to the other.

Used to logout from the FatPipe Unit.

LOCAL AREA NETWORK INTERFACE

Used to configure or change the IPv4 LAN interface parameters



☑ Enable Proxy ARP

MAC [a0:36:9f:54:fb:f4]

Link Speed / Duplex Mode: Auto Negotiation

Current Negotiation : NO LINK

□ Enable DHCP Relay

Reporting IP Address : 0.0.0.0

This IP Address is used for sending local syslog and snmp through VPN or GRE tunnel.

LAN Aliases

IP Address	Subnet Mask	VLAN tag	DHCP Server IP
192.168.0.1	255.255.255.0	0	

Add LAN Alias

IP Address: Enter IP Address

Subnet Mask: Enter Subnet Mask

VLAN Tag: VLAN Tag

DHCP Server IP: DHCP IP

Enable to have the LAN interface respond to ARP request for WAN-side IPs (makes the MPVPN transparent).(more Info…)

Select to configure Ethernet link speed and the duplex mode. (more Info…)

VLAN ID Configuration (more Info…)

Enable to relay DHCP packets between LAN & WAN.(more Info…)

Used to configure the DHCP Server IP address for DHCP

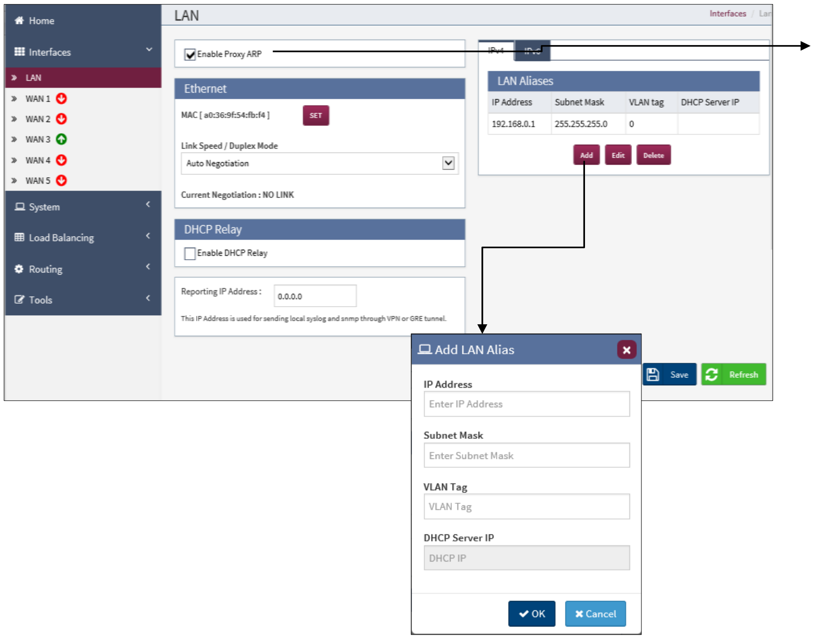
Used to configure IP address and Subnet Mask.

Used to refresh the page for changes.

Used to commit changes.

LOCAL AREA NETWORK INTERFACE

Used to configure or change the IPv4 LAN interface parameters



☑ Enable Proxy ARP

MAC [a0:36:9f:54:fb:f4]

Link Speed / Duplex Mode: Auto Negotiation

Current Negotiation : NO LINK

□ Enable DHCP Relay

Reporting IP Address : 0.0.0.0

This IP Address is used for sending local syslog and snmp through VPN or GRE tunnel.

LAN Aliases

IP Address	Subnet Mask	VLAN tag	DHCP Server IP
192.168.0.1	255.255.255.0	0	

Add LAN Alias

IP Address: Enter IP Address

Subnet Mask: Enter Subnet Mask

VLAN Tag: VLAN Tag

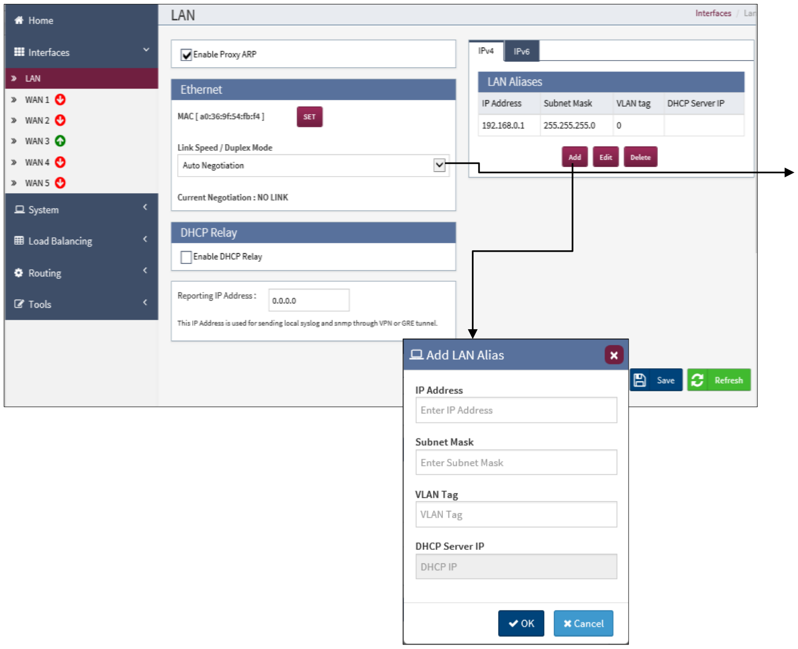
DHCP Server IP: DHCP IP

Enable to have the LAN interface respond to ARP request for WAN-side IPs (makes the MPVPN transparent).

The address resolution protocol (**ARP**) is a protocol used by IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. It is in enable state by default. If this option is disabled, you will not be able to communicate with devices directly connected to the WAN that are in the same subnet as where you are coming from. Proxy ARP is disabled only when devices on the LAN side have IPs from any of the WAN subnets.

LOCAL AREA NETWORK INTERFACE

Used to configure or change the IPv4 LAN interface parameters



LAN

☑ Enable Proxy ARP

Ethernet

MAC [a0:36:9f:54:fb:f4]

Link Speed / Duplex Mode: Auto Negotiation

Current Negotiation : NO LINK

DHCP Relay

□ Enable DHCP Relay

Reporting IP Address : 0.0.0.0

This IP Address is used for sending local syslog and snmp through VPN or GRE tunnel.

LAN Aliases

IP Address	Subnet Mask	VLAN tag	DHCP Server IP
192.168.0.1	255.255.255.0	0	

Add LAN Alias

IP Address: Enter IP Address

Subnet Mask: Enter Subnet Mask

VLAN Tag: VLAN Tag

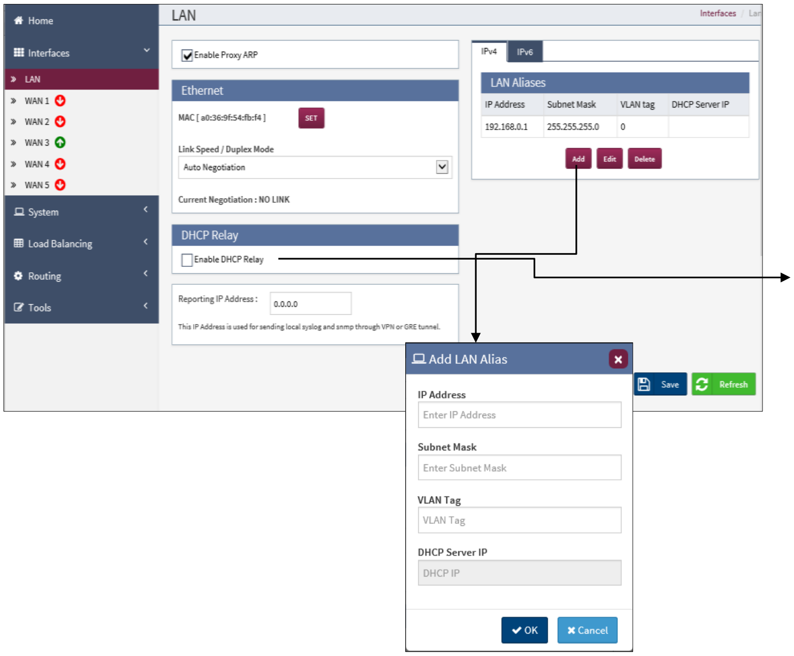
DHCP Server IP: DHCP IP

Select to configure Ethernet link speed and the duplex mode.

Link Speed is the connection speed between the router and FatPipe and Duplex Mode refers to the transmission of data in two way direction. The default value is set to "Auto-negotiation."

LOCAL AREA NETWORK INTERFACE

Used to configure or change the IPv4 LAN interface parameters



LAN

☑ Enable Proxy ARP

Ethernet

MAC [a0:36:9f:54:fb:f4]

Link Speed / Duplex Mode: Auto Negotiation

Current Negotiation : NO LINK

DHCP Relay

□ Enable DHCP Relay

Reporting IP Address : 0.0.0.0

This IP Address is used for sending local syslog and snmp through VPN or GRE tunnel.

LAN Aliases

IP Address	Subnet Mask	VLAN tag	DHCP Server IP
192.168.0.1	255.255.255.0	0	

Add LAN Alias

IP Address: Enter IP Address

Subnet Mask: Enter Subnet Mask

VLAN Tag: VLAN Tag

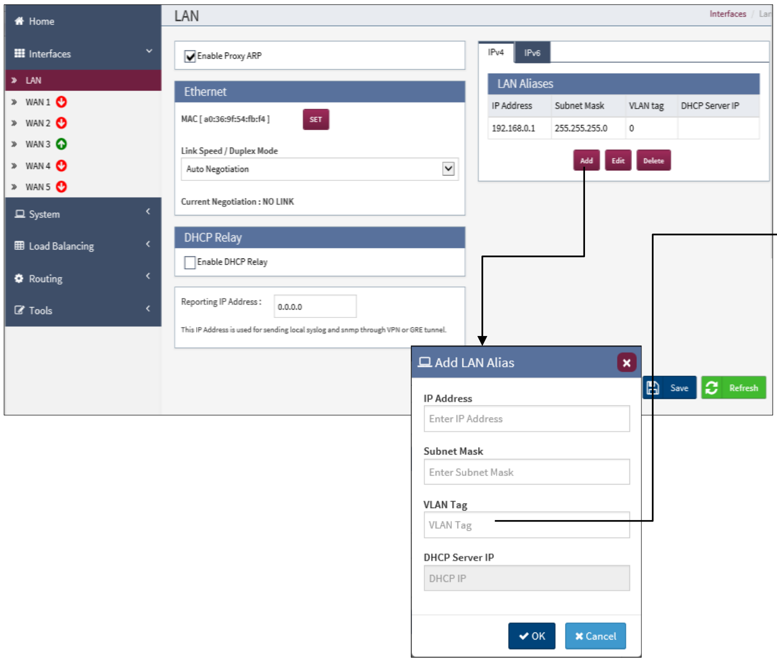
DHCP Server IP: DHCP IP

Enable to relay DHCP packets between LAN & WAN.

Dynamic Host Configuration Protocol is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers. This option allows you to relay DHCP requests from a LAN segment to a DHCP server on the WAN side.

LOCAL AREA NETWORK INTERFACE

Used to configure or change the IPv4 LAN interface parameters



LAN

☑ Enable Proxy ARP

Ethernet

MAC [a0:36:9f:54:fb:f4]

Link Speed / Duplex Mode: Auto Negotiation

Current Negotiation : NO LINK

DHCP Relay

□ Enable DHCP Relay

Reporting IP Address : 0.0.0.0

This IP Address is used for sending local syslog and snmp through VPN or GRE tunnel.

IPv4 | IPv6

LAN Aliases

IP Address	Subnet Mask	VLAN tag	DHCP Server IP
192.168.0.1	255.255.255.0	0	

Add LAN Alias

IP Address: Enter IP Address

Subnet Mask: Enter Subnet Mask

VLAN Tag: VLAN Tag

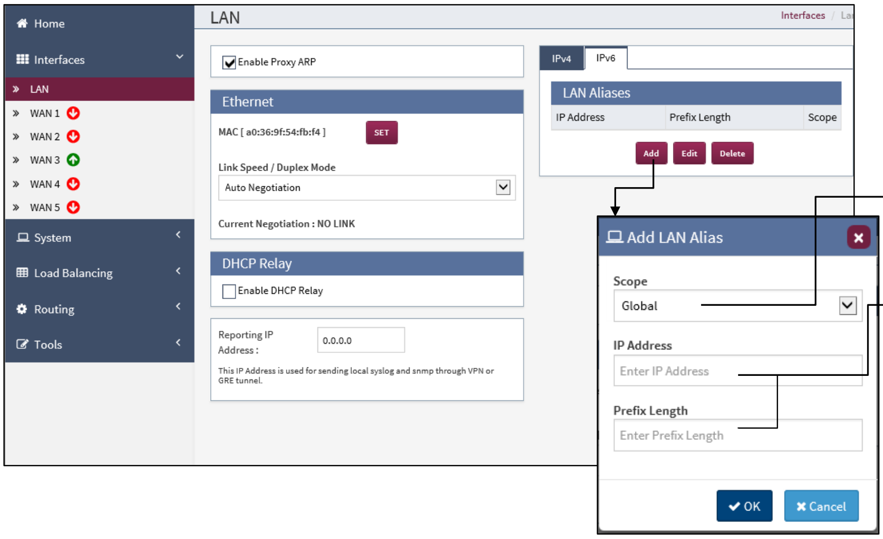
DHCP Server IP: DHCP IP

Used to enter the VLAN ID

VLANs separate network traffic by grouping hosts that communicate most frequently with each other. To enable participation with VLAN', click on the Active checkbox and enter a Valid VLAN ID Range 0 to 4096.

LOCAL AREA NETWORK INTERFACE

Used to configure or change IPv6 LAN interface parameters



LAN

☑ Enable Proxy ARP

Ethernet

MAC [a0:36:9f:54:fb:f4]

Link Speed / Duplex Mode: Auto Negotiation

Current Negotiation : NO LINK

DHCP Relay

□ Enable DHCP Relay

Reporting IP Address : 0.0.0.0

This IP Address is used for sending local syslog and snmp through VPN or GRE tunnel.

IPv4 | IPv6

LAN Aliases

IP Address	Prefix Length	Scope

Add LAN Alias

Scope: Global

IP Address: Enter IP Address

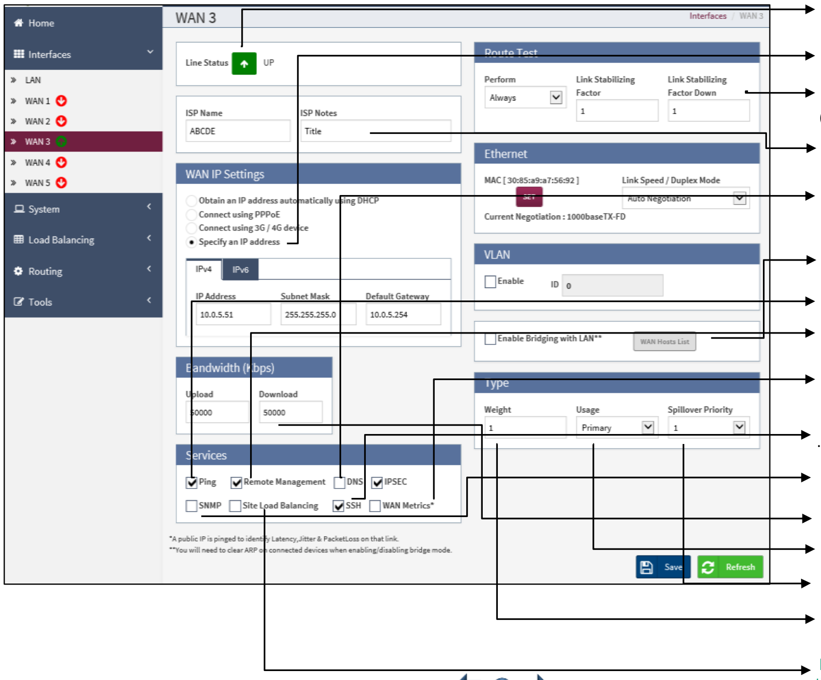
Prefix Length: Enter Prefix Length

Specify the scope.

Specify the IP and prefix length.

WIDE AREA NETWORK INTERFACE

Used to configure or change IP information for WAN interface by using DHCP



WAN 3

Line Status UP

ISP Name: ABCDE
ISP Notes: Title

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
10.0.5.51	255.255.255.0	10.0.5.254

Bandwidth (Kbps)

Upload	Download
50000	50000

Services
☑ Ping ☑ Remote Management □ DNS ☑ IPSEC
□ SNMP □ Site Load Balancing ☑ SSH □ WAN Metrics*

*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

Route Test

Perform	Link Stabilizing Factor	Link Stabilizing Factor Down
Always	1	1

Ethernet
MAC [30:85:a9:a7:56:92]
Link Speed / Duplex Mode: Auto Negotiation
Current Negotiation : 1000baseTX-FD

VLAN
□ Enable ID 0

□ Enable Bridging with LAN**

Type

Weight	Usage	Spillover Priority
1	Primary	1

Interface usability status will read UP or DOWN, indicating the status of the WAN link.

IP Addressing configuration methodologies

Select option to perform the route test.

(more Info…)

Link name identification

External ability to accept SmartDNS queries

Enable bridging for this interface with the LAN (more Info…)

External ability to ping to this interface. (more Info…)

External ability to access to GUI.

Enable to calculate WAN Metrics for this interface like Jitter, Latency and Packet Loss

External ability to allow Secure Shell.

External ability to SNMP access to this WAN Interface.

The maximum upload and download bandwidth of this link. (more Info…)

Select the role of the link.

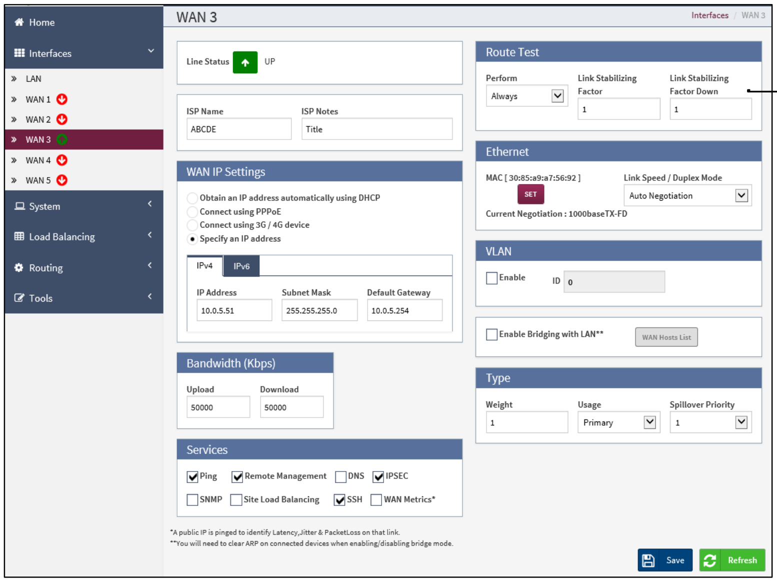
Spillover Load balancing assigns different priorities to WAN lines. (more Info…)

Used with Weighted Load balancing algorithm. (more Info…)

External ability to use Site Load Balancing on this link

WIDE AREA NETWORK INTERFACE

Used to configure or change IP information for WAN interface by using DHCP



WAN 3

Line Status UP

ISP Name: ABCDE
ISP Notes: Title

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 10.0.5.51 Subnet Mask 255.255.255.0 Default Gateway 10.0.5.254

Bandwidth (Kbps)
Upload 50000 Download 50000

Services
☑ Ping ☑ Remote Management □ DNS ☑ IPSEC
□ SNMP □ Site Load Balancing ☑ SSH □ WAN Metrics*

*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

Route Test
Perform Always Link Stabilizing Factor 1 Link Stabilizing Factor Down 1

Ethernet
MAC [30:85:a9:a7:56:92]
Link Speed / Duplex Mode: Auto Negotiation
Current Negotiation : 1000baseTX-FD

VLAN
□ Enable ID 0

□ Enable Bridging with LAN**

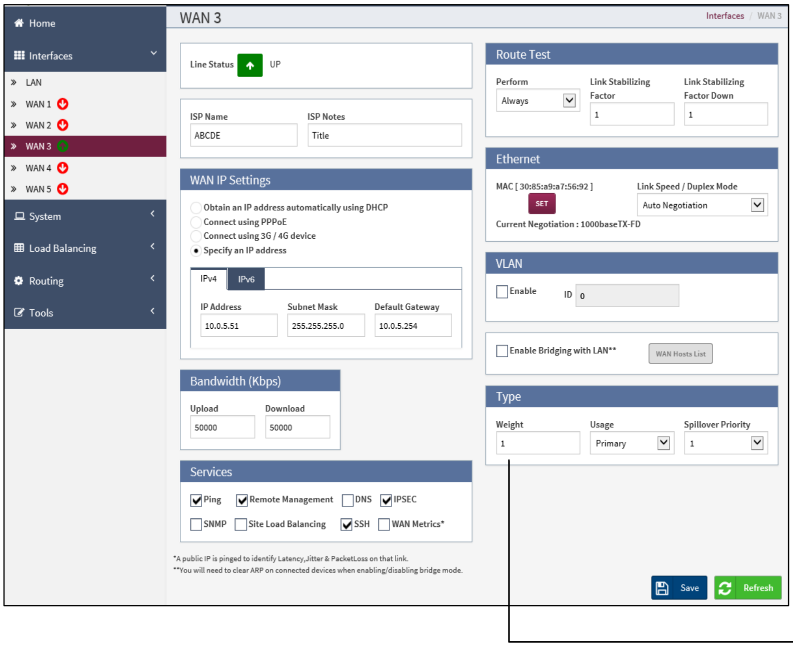
Type
Weight 1 Usage Primary Spillover Priority 1

Select option to perform the route test.

When Usage for an interface is set to "Backup," you can select when to perform the route test for that interface. It is set to “Always” by default. FatPipe will always check the line for Internet connectivity, even if the line is not actively being used for outbound sessions.
Link Stabilizing Factor is the number of consecutive Route Test failures or successes that must occur before Line Status is changed.

WIDE AREA NETWORK INTERFACE

Used to configure or change IP information for WAN interface by using DHCP



WAN 3

Line Status UP

ISP Name: ABCDE
ISP Notes: Title

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: 10.0.5.51
Subnet Mask: 255.255.255.0
Default Gateway: 10.0.5.254

Bandwidth (Kbps)

Upload: 50000
Download: 50000

Services

☑ Ping ☑ Remote Management □ DNS ☑ IPSEC
□ SNMP □ Site Load Balancing ☑ SSH □ WAN Metrics*

*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

Route Test

Perform: Always
Link Stabilizing Factor: 1
Link Stabilizing Factor Down: 1

Ethernet

MAC [30:85:a9:a7:56:92]
Link Speed / Duplex Mode: Auto Negotiation
Current Negotiation : 1000baseTX-FD

VLAN

□ Enable ID 0

□ Enable Bridging with LAN**

Type

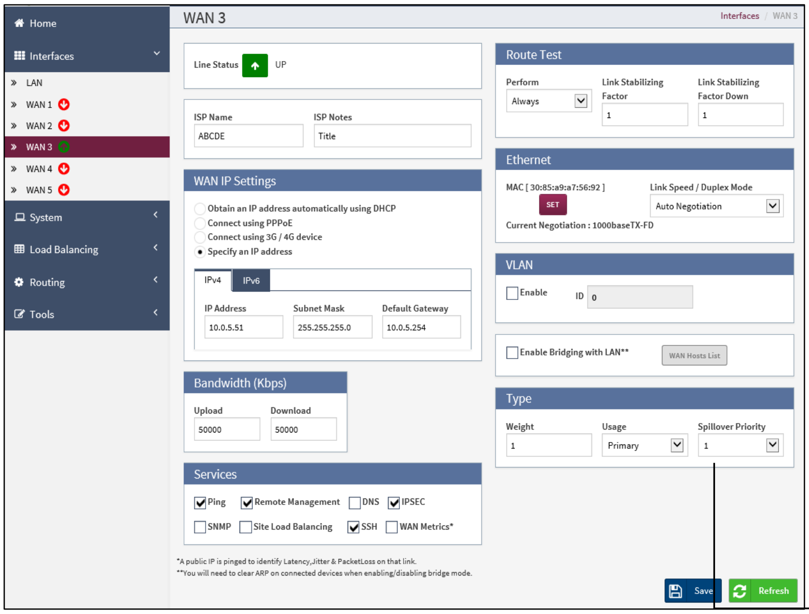
Weight: 1
Usage: Primary
Spillover Priority: 1

This setting is for use with the Weighted Load balancing algorithm. Values configured here will be assigned as the Weight for that WAN interface.

Used with Weighted Load balancing algorithm.

WIDE AREA NETWORK INTERFACE

Used to configure or change IP information for WAN interface by using DHCP



WAN 3

Line Status UP

ISP Name: ABCDE
ISP Notes: Title

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: 10.0.5.51
Subnet Mask: 255.255.255.0
Default Gateway: 10.0.5.254

Bandwidth (Kbps)

Upload: 50000
Download: 50000

Services

☑ Ping ☑ Remote Management □ DNS ☑ IPSEC
□ SNMP □ Site Load Balancing ☑ SSH □ WAN Metrics*

*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

Route Test

Perform: Always
Link Stabilizing Factor: 1
Link Stabilizing Factor Down: 1

Ethernet

MAC [30:85:a9:a7:56:92]
Link Speed / Duplex Mode: Auto Negotiation
Current Negotiation : 1000baseTX-FD

VLAN

□ Enable ID 0

□ Enable Bridging with LAN**

Type

Weight: 1
Usage: Primary
Spillover Priority: 1

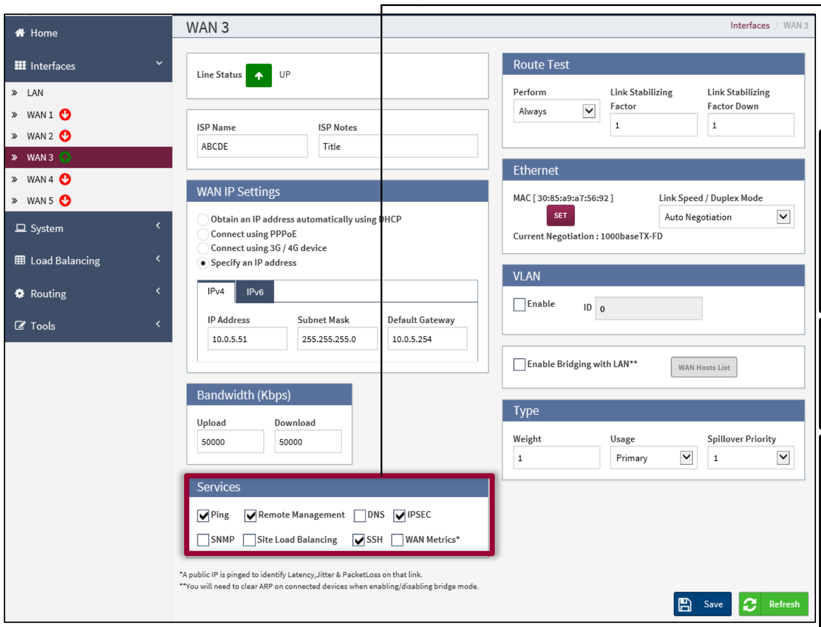
’1’ has the highest priority and decreases as the numeric value increases, depending on the number of WAN interfaces. Traffic is sent over the lower priority lines only after at least 90% throughput of higher priority lines is reached. You have the option of marking a line as ‘backup’. Traffic will be sent out of a ‘backup’ link only if all the other “primary” links are down.

This approach provides a solution for users that are charged for line usage that is proportionate to the traffic they generate. This feature can be used as backup when the network carries a high load by assigning low priority to such a link to minimize the cost.

Spillover Load balancing assigns different priorities to WAN lines.

WIDE AREA NETWORK INTERFACE

Used to configure or change IP information for WAN interface by using DHCP



WAN 3

Line Status: UP

ISP Name: ABCDE
ISP Notes: Title

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: 10.0.5.51
Subnet Mask: 255.255.255.0
Default Gateway: 10.0.5.254

Bandwidth (Kbps)
Upload: 50000
Download: 50000

Services
☑ Ping ☑ Remote Management ☐ DNS ☑ IPSEC
☐ SNMP ☐ Site Load Balancing ☑ SSH ☐ WAN Metrics*

Route Test
Perform: Always
Link Stabilizing Factor: 1
Link Stabilizing Factor Down: 1

Ethernet
MAC [30:85:a9:a7:56:92] SET
Link Speed / Duplex Mode: Auto Negotiation
Current Negotiation : 1000baseTX-FD

VLAN
☐ Enable ID 0

☐ Enable Bridging with LAN** WAN Hosts List

Type
Weight: 1
Usage: Primary
Spillover Priority: 1

*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

Services

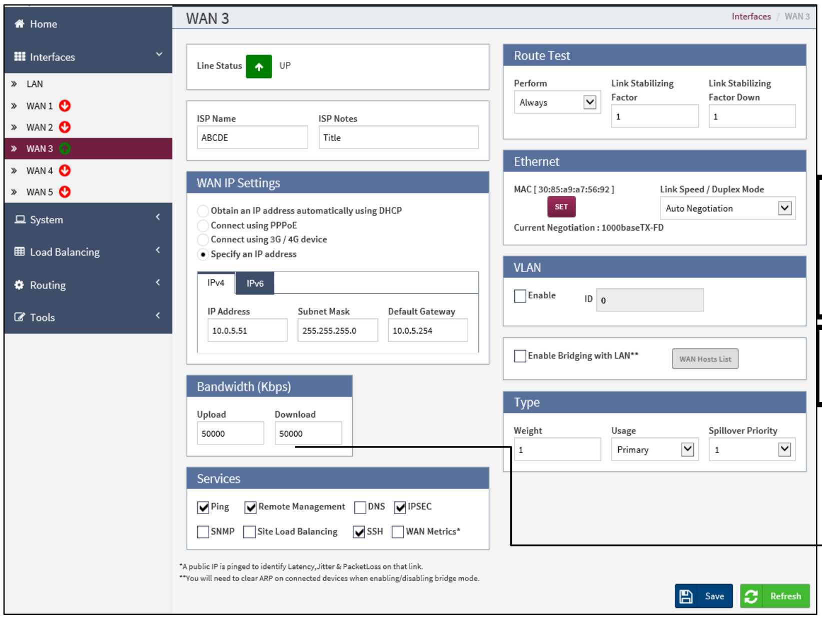
FatPipe is a secure system with most services disabled except those needed to be provided ad-hoc (I.E. Remote Management, SSH, DNS, SNMP and Site Load Balancing. One can enable or disable these features as needed for these services.

Ping requests for the WAN interface IP can be blocked. These options do not affect traffic routed through MPVPN.

Watch Parameters, when enabled, FatPipe monitors the link conditions like latency, jitter and packet loss and allows redirecting traffic to alternate links if a pre-defined threshold is crossed even if the link is UP. This is achieved by configuring the thresholds using Outbound Policy Routing Rules.

WIDE AREA NETWORK INTERFACE

Used to configure or change IP information for WAN interface by using DHCP



WAN 3

Line Status: UP

ISP Name: ABCDE
ISP Notes: Title

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: 10.0.5.51
Subnet Mask: 255.255.255.0
Default Gateway: 10.0.5.254

Bandwidth (Kbps)
Upload: 50000
Download: 50000

Services
☑ Ping ☑ Remote Management ☐ DNS ☑ IPSEC
☐ SNMP ☐ Site Load Balancing ☑ SSH ☐ WAN Metrics*

Route Test
Perform: Always
Link Stabilizing Factor: 1
Link Stabilizing Factor Down: 1

Ethernet
MAC [30:85:a9:a7:56:92] SET
Link Speed / Duplex Mode: Auto Negotiation
Current Negotiation : 1000baseTX-FD

VLAN
☐ Enable ID 0

☐ Enable Bridging with LAN** WAN Hosts List

Type
Weight: 1
Usage: Primary
Spillover Priority: 1

*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

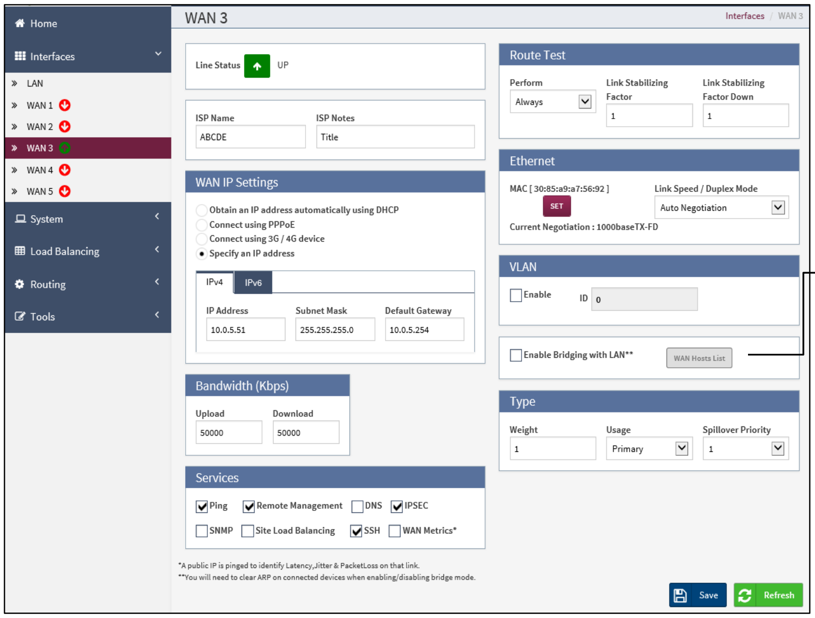
This setting is for use with Quality of Service (QoS). You should specify the maximum bandwidth available outbound in upload or inbound in download for your WAN line in Kbps (Kilobits per second).

For example, if you have 1.5Mbps of bandwidth inbound, you would enter 1536.

The maximum upload and download bandwidth of this line.

WIDE AREA NETWORK INTERFACE

Used to configure or change IP information for WAN interface by using DHCP



WAN 3

Line Status UP

ISP Name: ABCDE
ISP Notes: Title

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
10.0.5.51	255.255.255.0	10.0.5.254

Bandwidth (Kbps)

Upload	Download
50000	50000

Services

☑ Ping ☑ Remote Management □ DNS ☑ IPSEC
□ SNMP □ Site Load Balancing ☑ SSH □ WAN Metrics*

*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

Route Test

Perform	Link Stabilizing Factor	Link Stabilizing Factor Down
Always	1	1

Ethernet

MAC [30:85:a9:a7:56:92] SET
Link Speed / Duplex Mode: Auto Negotiation
Current Negotiation : 1000baseTX-FD

VLAN

□ Enable ID 0

□ Enable Bridging with LAN** WAN Hosts List

Type

Weight	Usage	Spillover Priority
1	Primary	1

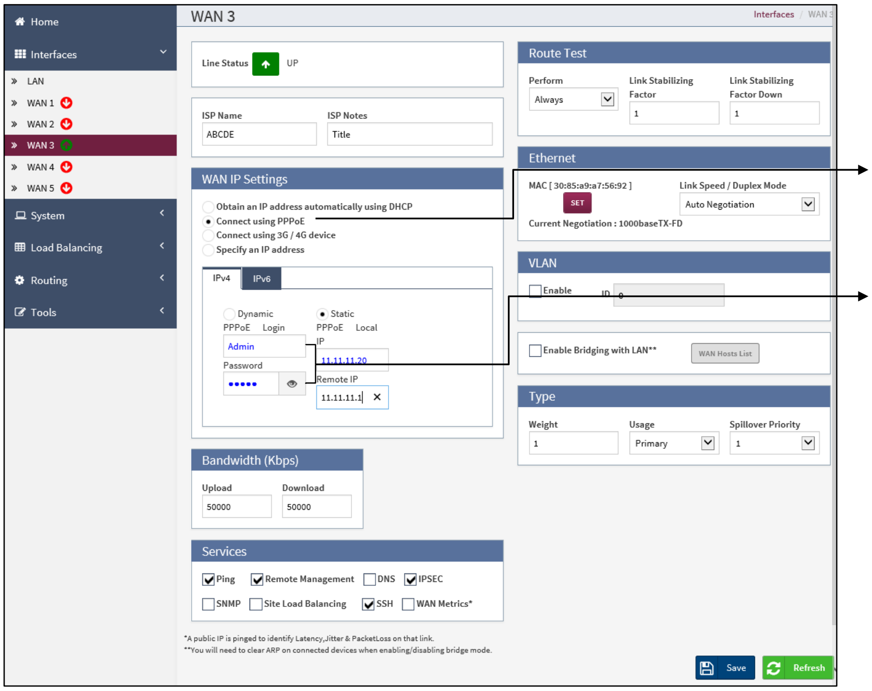
Save Refresh

Enable bridging for this interface with the LAN

In situations where we cannot split a network to create a separate small subnet, this option enables you to bridge the LAN with the WAN interface of that network.

WIDE AREA NETWORK INTERFACE

Used to configure or change IP information for WAN interface by Dynamic PPPoE



WAN 3

Line Status UP

ISP Name: ABCDE
ISP Notes: Title

WAN IP Settings

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

IPv4 | IPv6

○ Dynamic PPPoE Login
Admin
Password
●●●●●

● Static PPPoE Local IP
11.11.11.20
Remote IP
11.11.11.1

Bandwidth (Kbps)

Upload	Download
50000	50000

Services

☑ Ping ☑ Remote Management □ DNS ☑ IPSEC
□ SNMP □ Site Load Balancing ☑ SSH □ WAN Metrics*

*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

Route Test

Perform	Link Stabilizing Factor	Link Stabilizing Factor Down
Always	1	1

Ethernet

MAC [30:85:a9:a7:56:92] SET
Link Speed / Duplex Mode: Auto Negotiation
Current Negotiation : 1000baseTX-FD

VLAN

□ Enable ID 0

□ Enable Bridging with LAN** WAN Hosts List

Type

Weight	Usage	Spillover Priority
1	Primary	1

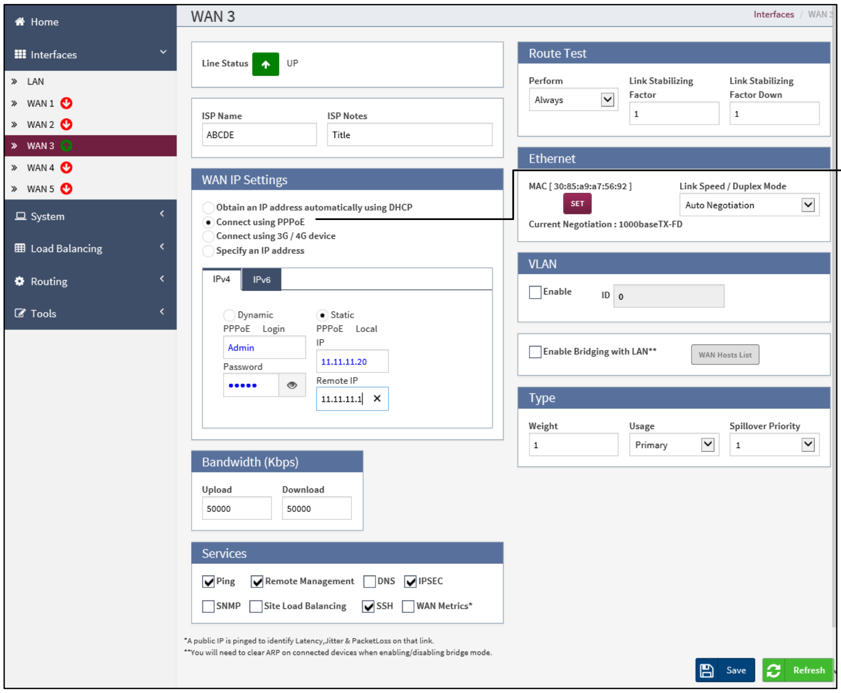
Save Refresh

Option to connect to your ISP using Dynamic PPPoE (more Info…)

Used to configure username and password for PPPoE connection

WIDE AREA NETWORK INTERFACE

Used to configure or change IP information for WAN interface by Dynamic PPPoE



WAN 3

Line Status: UP

ISP Name: ABCDE
ISP Notes: Title

WAN IP Settings

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

IPv4 | IPv6

○ Dynamic PPPoE
● Static PPPoE

Login: Admin
Password: ●●●●●
Local IP: 11.11.11.20
Remote IP: 11.11.11.1

Bandwidth (Kbps)

Upload: 50000
Download: 50000

Services

☑ Ping ☑ Remote Management ☐ DNS ☑ IPSEC
☐ SNMP ☐ Site Load Balancing ☑ SSH ☐ WAN Metrics*

*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

Route Test

Perform: Always
Link Stabilizing Factor: 1
Link Stabilizing Factor Down: 1

Ethernet

MAC [30:85:a9:a7:56:92] SET
Link Speed / Duplex Mode: Auto Negotiation
Current Negotiation : 1000baseTX-FD

VLAN

☐ Enable ID 0

☐ Enable Bridging with LAN** WAN Hosts List

Type

Weight: 1
Usage: Primary
Spillover Priority: 1

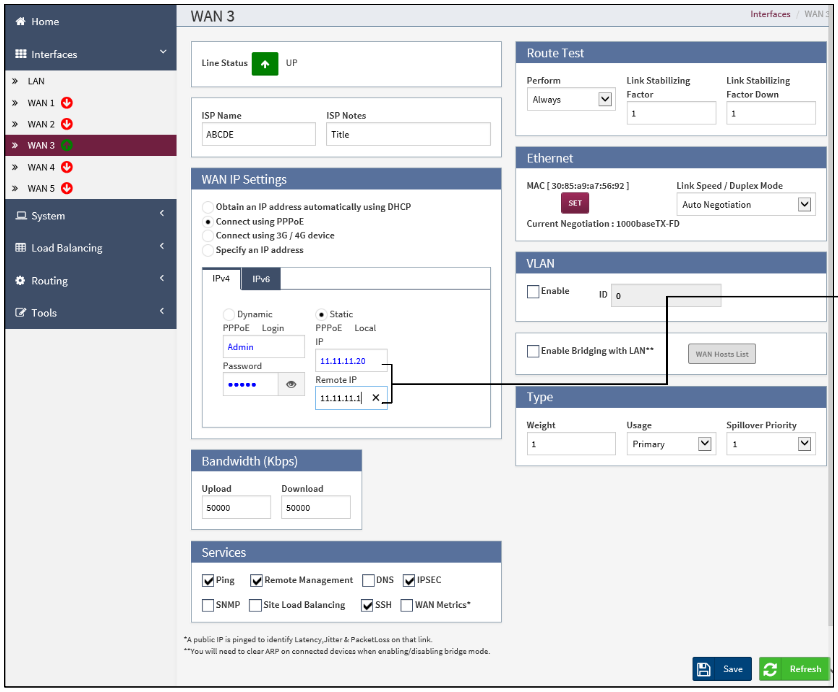
Save Refresh

Option to connect to your ISP using Dynamic PPPoE

PPPoE is a specification for connecting multiple computer users on an Ethernet local area network to a remote site through common customer premises equipment.

WIDE AREA NETWORK INTERFACE

Used to configure or change IP information for WAN interface by Static PPPoE



WAN 3

Line Status: UP

ISP Name: ABCDE
ISP Notes: Title

WAN IP Settings

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

IPv4 | IPv6

○ Dynamic PPPoE
● Static PPPoE

Login: Admin
Password: ●●●●●
Local IP: 11.11.11.20
Remote IP: 11.11.11.1

Bandwidth (Kbps)

Upload: 50000
Download: 50000

Services

☑ Ping ☑ Remote Management ☐ DNS ☑ IPSEC
☐ SNMP ☐ Site Load Balancing ☑ SSH ☐ WAN Metrics*

*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

Route Test

Perform: Always
Link Stabilizing Factor: 1
Link Stabilizing Factor Down: 1

Ethernet

MAC [30:85:a9:a7:56:92] SET
Link Speed / Duplex Mode: Auto Negotiation
Current Negotiation : 1000baseTX-FD

VLAN

☐ Enable ID 0

☐ Enable Bridging with LAN** WAN Hosts List

Type

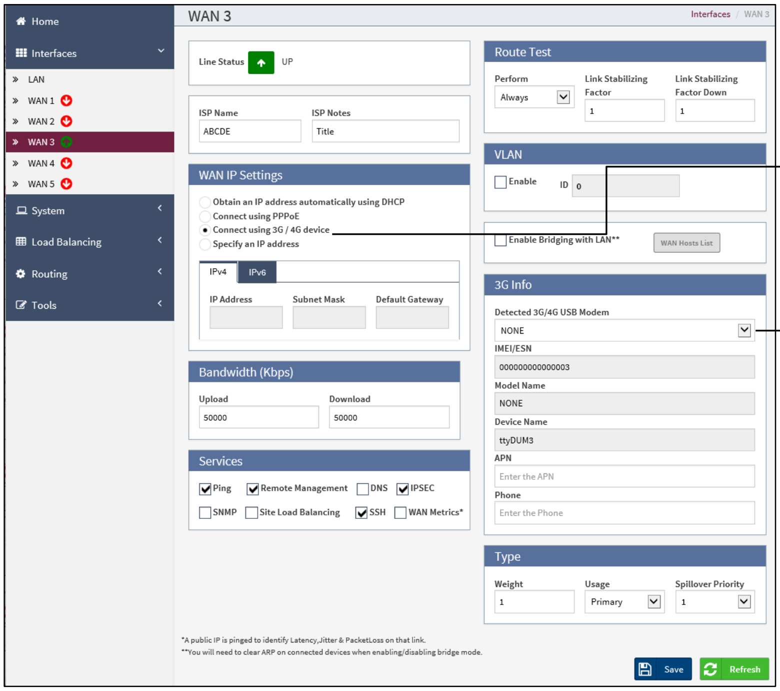
Weight: 1
Usage: Primary
Spillover Priority: 1

Save Refresh

Used to configure IPs provided for PPPoE connection

WIDE AREA NETWORK INTERFACE

Used to configure or change IP information for the WAN interface by 3G/4G Dongle



WAN 3

Line Status UP

ISP Name: ABCDE
ISP Notes: Title

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:

Bandwidth (Kbps)

Upload: 50000
Download: 50000

Services

☑ Ping ☑ Remote Management □ DNS ☑ IPSEC
□ SNMP □ Site Load Balancing ☑ SSH □ WAN Metrics*

Route Test

Perform: Always
Link Stabilizing Factor: 1
Link Stabilizing Factor Down: 1

VLAN

□ Enable ID 0

□ Enable Bridging with LAN**

3G Info

Detected 3G/4G USB Modem: NONE
IMEI/ESN: 000000000000003
Model Name: NONE
Device Name: ttyDUM3
APN: Enter the APN
Phone: Enter the Phone

Type

Weight: 1
Usage: Primary
Spillover Priority: 1

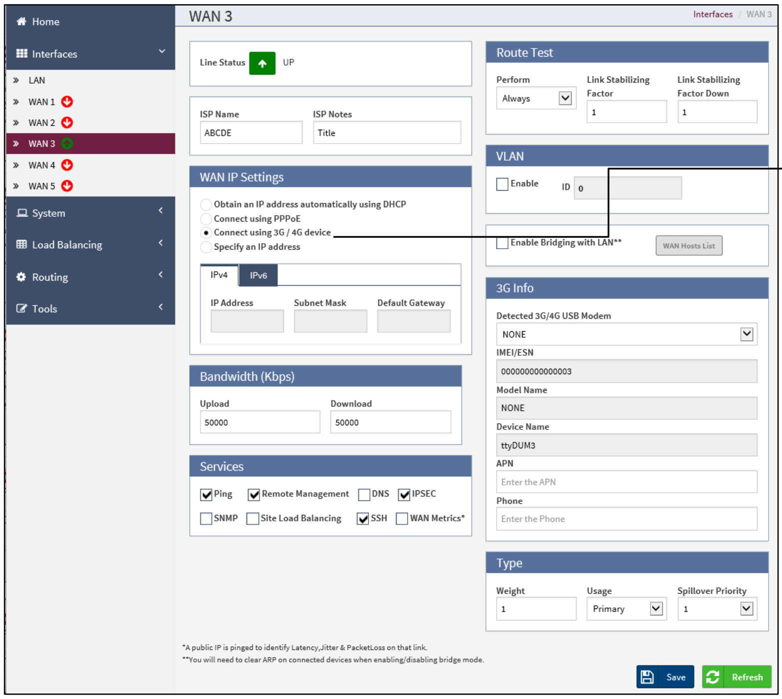
*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

Enable to connect using a 3G/4G cellular modem (more Info…)

Used to select a device model from the Detected 3G/4G modem from the drop-down list (more Info…)

WIDE AREA NETWORK INTERFACE

Used to configure or change IP information for the WAN interface by 3G/4G Dongle



WAN 3

Line Status UP

ISP Name: ABCDE
ISP Notes: Title

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:

Bandwidth (Kbps)

Upload: 50000
Download: 50000

Services

☑ Ping ☑ Remote Management □ DNS ☑ IPSEC
□ SNMP □ Site Load Balancing ☑ SSH □ WAN Metrics*

Route Test

Perform: Always
Link Stabilizing Factor: 1
Link Stabilizing Factor Down: 1

VLAN

□ Enable ID 0

□ Enable Bridging with LAN**

3G Info

Detected 3G/4G USB Modem: NONE
IMEI/ESN: 000000000000003
Model Name: NONE
Device Name: ttyDUM3
APN: Enter the APN
Phone: Enter the Phone

Type

Weight: 1
Usage: Primary
Spillover Priority: 1

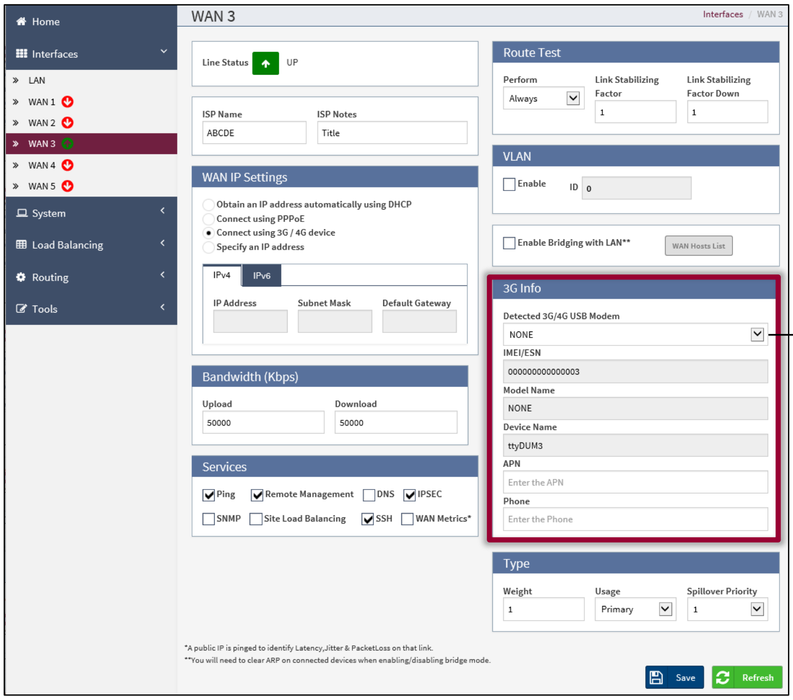
*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

Enable to connect using a 3G/4G cellular modem

To connect a 3G/4G line, plug a 3G/4G cellular modem to any of the USB interfaces on the MPVPN device. The USB Modem will be automatically detected. Select “Connect using 3G/4G device”.

WIDE AREA NETWORK INTERFACE

Used to configure or change IP information for the WAN interface by 3G/4G Dongle



WAN 3

Line Status UP

ISP Name: ABCDE
ISP Notes: Title

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

Bandwidth (Kbps)

Upload: 50000
Download: 50000

Services

☑ Ping ☑ Remote Management □ DNS ☑ IPSEC
□ SNMP □ Site Load Balancing ☑ SSH □ WAN Metrics*

Route Test

Perform: Always
Link Stabilizing Factor: 1
Link Stabilizing Factor Down: 1

VLAN

□ Enable ID 0

□ Enable Bridging with LAN**

3G Info

Detected 3G/4G USB Modem: NONE
IMEI/ESN: 000000000000003
Model Name: NONE
Device Name: ttyDUM3
APN: Enter the APN
Phone: Enter the Phone

Type

Weight: 1
Usage: Primary
Spillover Priority: 1

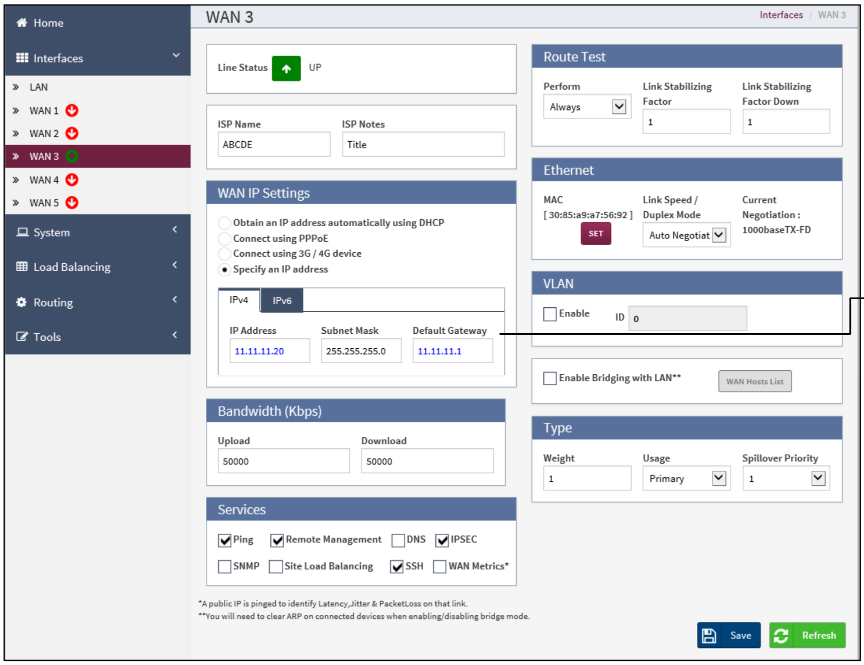
*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

Used to select a device model from the Detected 3G/4G modem from the drop-down list

IMEI/ESN and Model Name of the USB Modem will be displayed. This information cannot be modified. The APN and Phone Number will also be displayed. This information can be modified based on carrier recommendation. Click SAVE to make the changes permanent.

WIDE AREA NETWORK INTERFACE

Used to configure or change IP information for WAN Interface



WAN 3

Line Status UP

ISP Name: ABCDE
ISP Notes: Title

WAN IP Settings

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

IP Address: 11.11.11.20
Subnet Mask: 255.255.255.0
Default Gateway: 11.11.11.1

Bandwidth (Kbps)

Upload: 50000
Download: 50000

Services

☑ Ping ☑ Remote Management □ DNS ☑ IPSEC
□ SNMP □ Site Load Balancing ☑ SSH □ WAN Metrics*

Route Test

Perform: Always
Link Stabilizing Factor: 1
Link Stabilizing Factor Down: 1

Ethernet

MAC [30:85:a9:a7:56:92]
Link Speed / Duplex Mode: Auto Negotiat
Current Negotiation : 1000baseTX-FD

VLAN

□ Enable ID 0

□ Enable Bridging with LAN**

Type

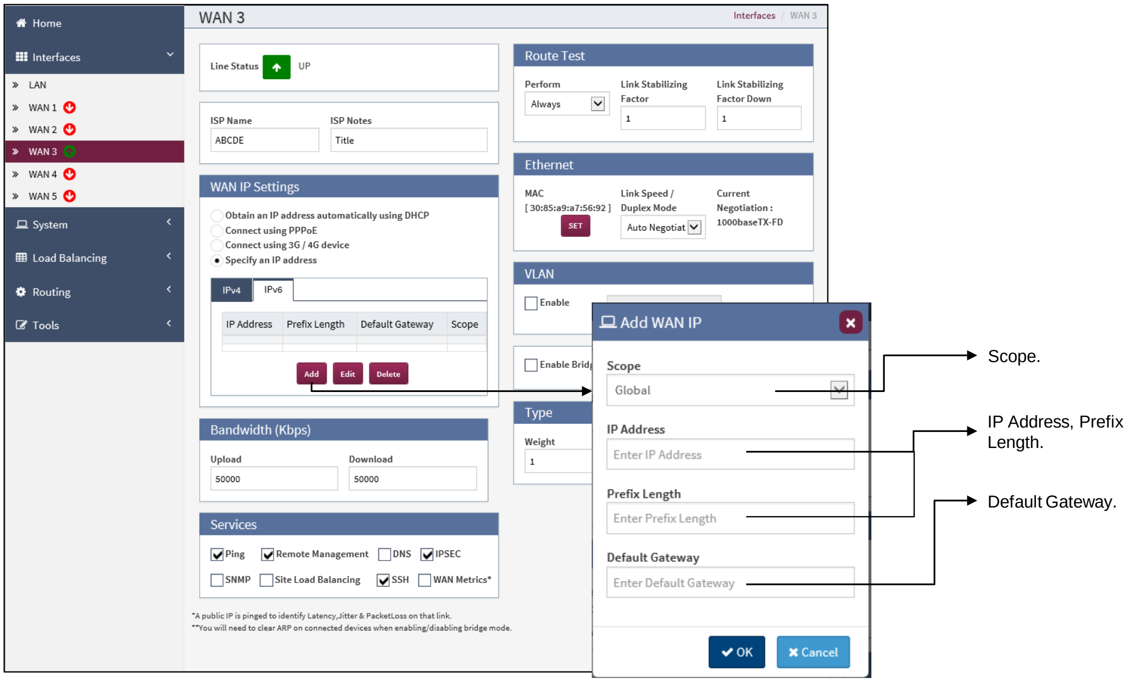
Weight: 1
Usage: Primary
Spillover Priority: 1

*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

IP Address, Subnet Mask, Default Gateway for the WAN Interface.
The Default Gateway is the IP address of the WAN router you use

WIDE AREA NETWORK INTERFACE

Used to configure or change IPv6 information for WAN Interface



WAN 3

Interfaces / WAN 3

Line Status: UP

ISP Name: ABCDE

ISP Notes: Title

WAN IP Settings

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

IP Address	Prefix Length	Default Gateway	Scope

Bandwidth (Kbps)

Upload: 50000

Download: 50000

Services

☑ Ping ☑ Remote Management □ DNS ☑ IPSEC
□ SNMP □ Site Load Balancing ☑ SSH □ WAN Metrics*

*A public IP is pinged to identify Latency,Jitter & PacketLoss on that link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.

Route Test

Perform: Always

Link Stabilizing Factor: 1

Link Stabilizing Factor Down: 1

Ethernet

MAC [30:85:a9:a7:56:92]

Link Speed / Duplex Mode: Auto Negotiat

Current Negotiation : 1000baseTX-FD

VLAN

□ Enable

□ Enable Bridg

Type

Weight: 1

Add WAN IP

Scope: Global

IP Address: Enter IP Address

Prefix Length: Enter Prefix Length

Default Gateway: Enter Default Gateway

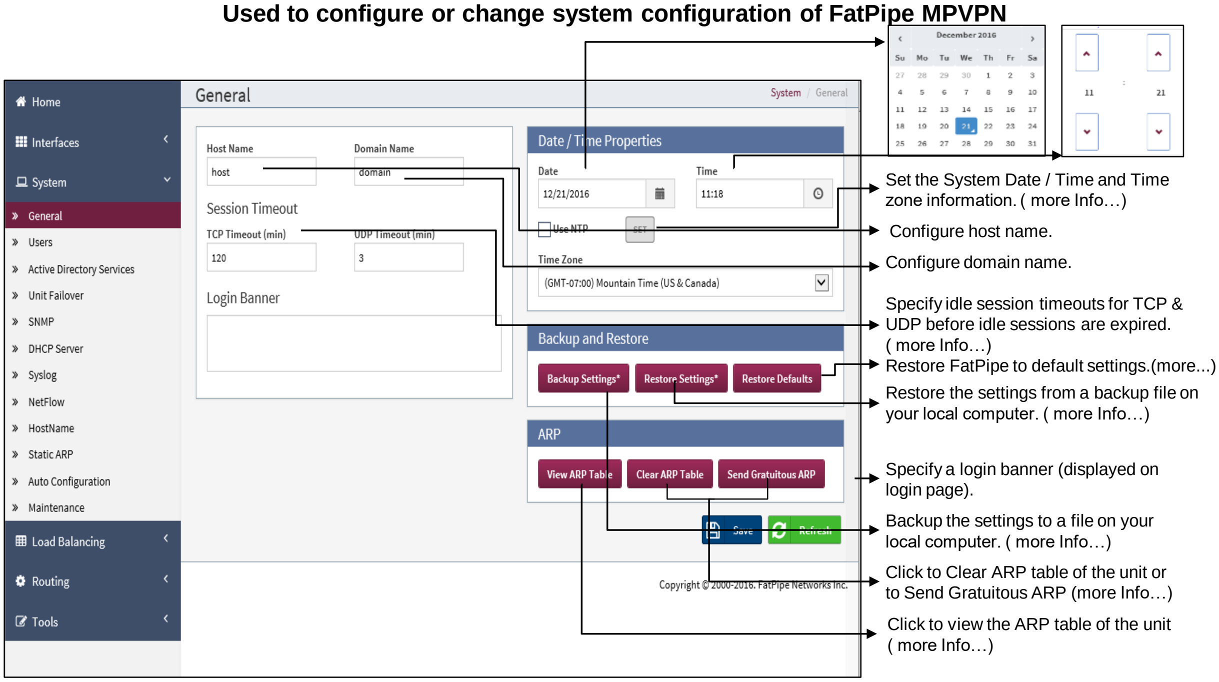
Scope.

IP Address, Prefix Length.

Default Gateway.

SYSTEM CONFIGURATION

Used to configure or change system configuration of FatPipe MPVPN



General

System / General

Host Name: host

Domain Name: domain

Session Timeout

TCP Timeout (min): 120

UDP Timeout (min): 3

Login Banner

Date / Time Properties

Date: 12/21/2016

Time: 11:18

□ Use NTP

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

Backup and Restore

ARP

Copyright © 2000-2016. FatPipe Networks Inc.

December 2016

Su	Mo	Tu	We	Th	Fr	Sa
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

11 : 21

Set the System Date / Time and Time zone information. (more Info…)

Configure host name.

Configure domain name.

Specify idle session timeouts for TCP & UDP before idle sessions are expired. (more Info…)

Restore FatPipe to default settings.(more...)

Restore the settings from a backup file on your local computer. (more Info…)

Specify a login banner (displayed on login page).

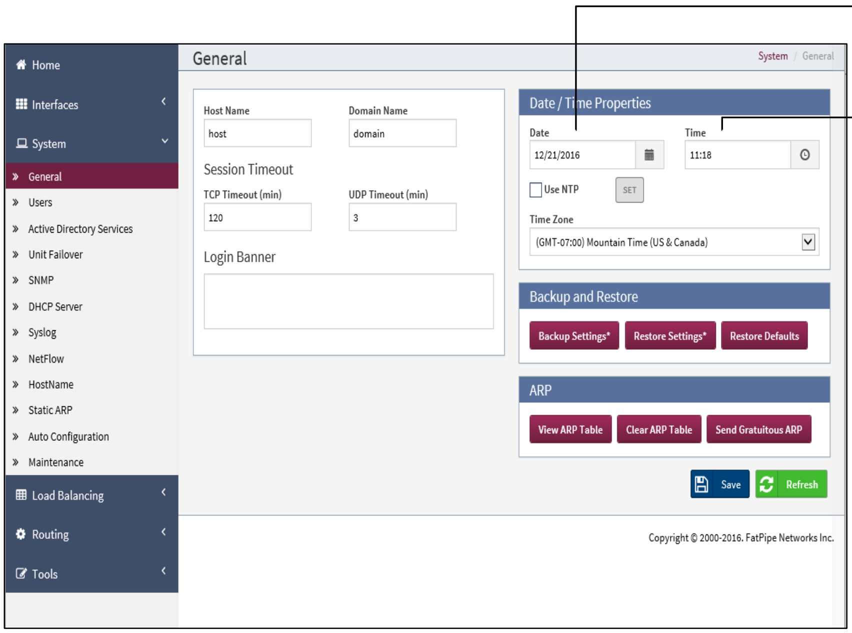
Backup the settings to a file on your local computer. (more Info…)

Click to Clear ARP table of the unit or to Send Gratuitous ARP (more Info…)

Click to view the ARP table of the unit (more Info…)

SYSTEM CONFIGURATION

Used to configure or change system configuration of FatPipe MPVPN



Home
Interfaces
System
» General
» Users
» Active Directory Services
» Unit Failover
» SNMP
» DHCP Server
» Syslog
» NetFlow
» HostName
» Static ARP
» Auto Configuration
» Maintenance
Load Balancing
Routing
Tools

General — System / General

Host Name: host
Domain Name: domain

Session Timeout
TCP Timeout (min): 120
UDP Timeout (min): 3

Login Banner

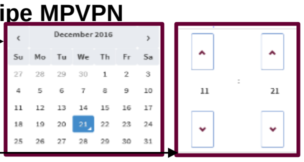
Date / Time Properties
Date: 12/21/2016
Time: 11:18
□ Use NTP SET
Time Zone: (GMT-07:00) Mountain Time (US & Canada)

Backup and Restore
Backup Settings* | Restore Settings* | Restore Defaults

ARP
View ARP Table | Clear ARP Table | Send Gratuitous ARP

Save | Refresh

Copyright © 2000-2016. FatPipe Networks Inc.

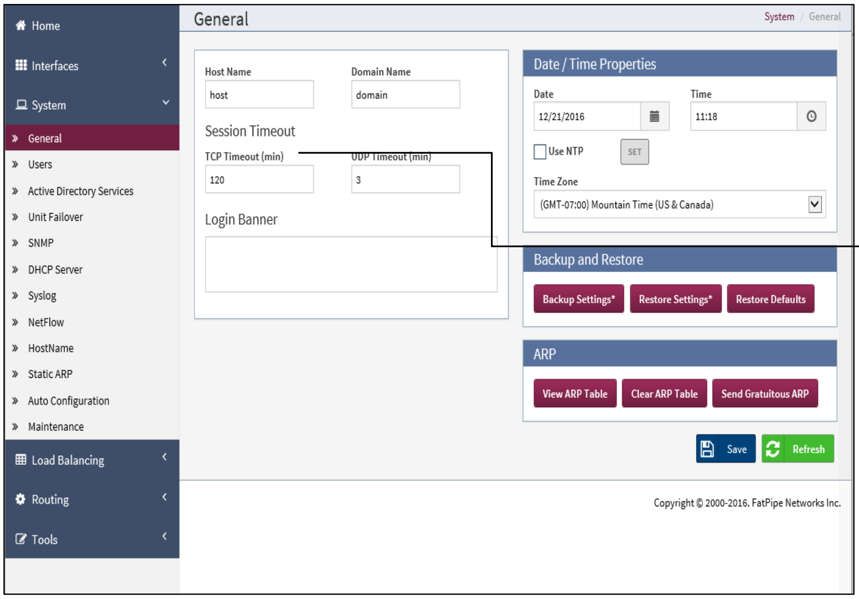


Set the System Date / Time and Time zone information.

You can set date and time using the NTP. Check the Use NTP checkbox and click the Set button to synchronize with external time servers.

SYSTEM CONFIGURATION

Used to configure or change system configuration of FatPipe MPVPN



Home
Interfaces
System
» General
» Users
» Active Directory Services
» Unit Failover
» SNMP
» DHCP Server
» Syslog
» NetFlow
» HostName
» Static ARP
» Auto Configuration
» Maintenance
Load Balancing
Routing
Tools

General — System / General

Host Name: host
Domain Name: domain

Session Timeout
TCP Timeout (min): 120
UDP Timeout (min): 3

Login Banner

Date / Time Properties
Date: 12/21/2016
Time: 11:18
□ Use NTP SET
Time Zone: (GMT-07:00) Mountain Time (US & Canada)

Backup and Restore
Backup Settings* | Restore Settings* | Restore Defaults

ARP
View ARP Table | Clear ARP Table | Send Gratuitous ARP

Save | Refresh

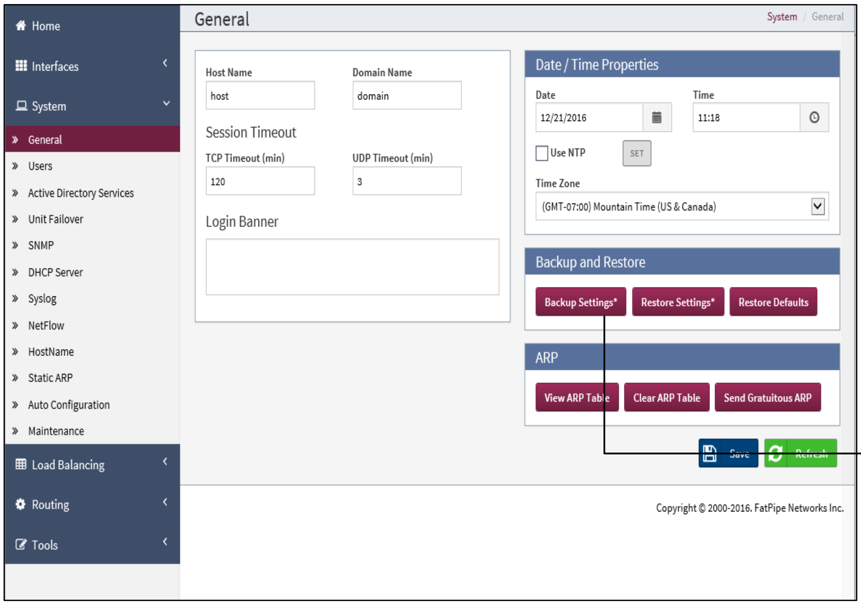
Copyright © 2000-2016. FatPipe Networks Inc.

Specify idle session timeouts for TCP & UDP before idle sessions are expired.

The defaults are 120 minutes (for TCP and 3 minutes for UDP. It is not recommended that you change these settings, except under rare circumstances.

SYSTEM CONFIGURATION

Used to configure or change system configuration of FatPipe MPVPN



General

Host Name: host

Domain Name: domain

Session Timeout

TCP Timeout (min): 120

UDP Timeout (min): 3

Login Banner

Date: 12/21/2016

Time: 11:18

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

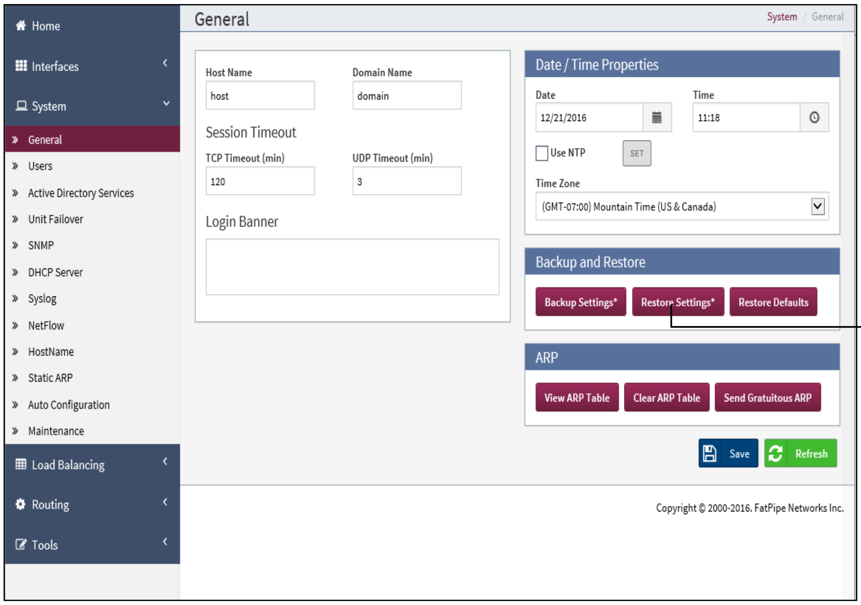
Copyright © 2000-2016. FatPipe Networks Inc.

If you click on the Backup Settings button you will be prompted to save a backup configuration file in a new popup window. All the modifications done on GUI will be saved as a point in time copy to the workstation youre making the backup from.

Backup the settings to a file on your local computer.

SYSTEM CONFIGURATION

Used to configure or change system configuration of FatPipe MPVPN



General

Host Name: host

Domain Name: domain

Session Timeout

TCP Timeout (min): 120

UDP Timeout (min): 3

Login Banner

Date: 12/21/2016

Time: 11:18

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

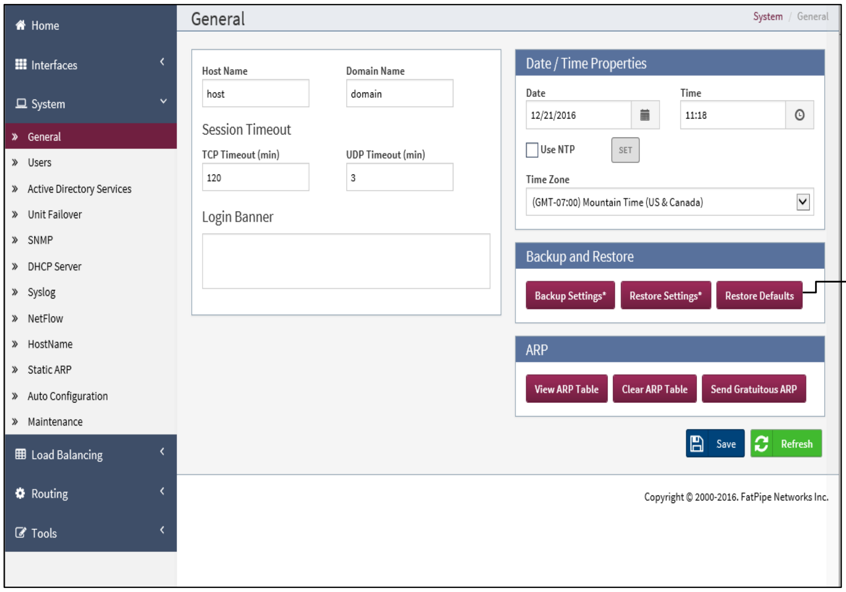
Copyright © 2000-2016. FatPipe Networks Inc.

If you click on the Restore Settings button, in a new popup window you will be prompted to import a previously saved backup configuration file.

Restore the settings from a backup file on your local computer.

SYSTEM CONFIGURATION

Used to configure or change system configuration of FatPipe MPVPN



General

Host Name: host

Domain Name: domain

Session Timeout

TCP Timeout (min): 120

UDP Timeout (min): 3

Login Banner

Date / Time Properties

Date: 12/21/2016

Time: 11:18

□ Use NTP SET

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

Backup and Restore

ARP

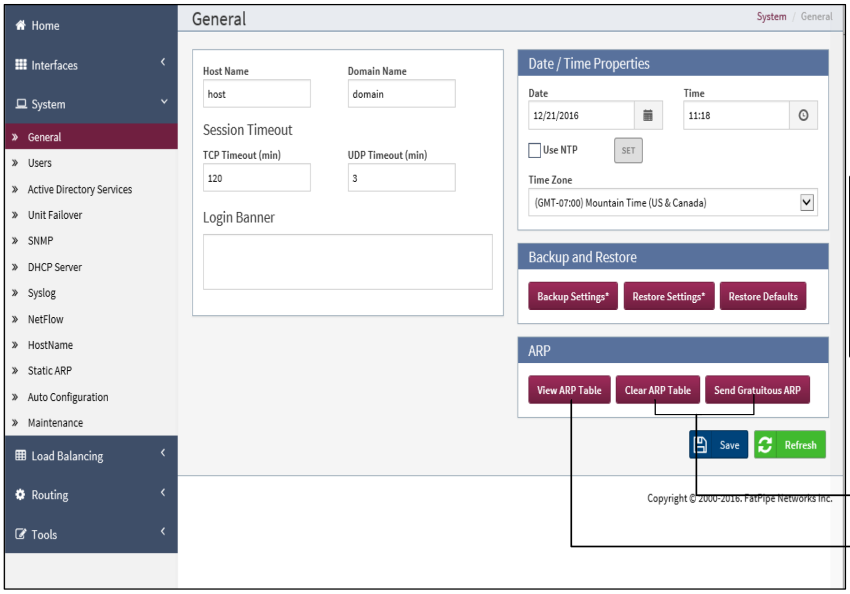
Copyright © 2000-2016. FatPipe Networks Inc.

Restore FatPipe to default settings.

If you click on the Restore Defaults button, you will be prompted to restore the system back to factory defaults. This will erase all the changes that are made and takes to the default values.

SYSTEM CONFIGURATION

Used to configure or change system configuration of FatPipe MPVPN


General

Host Name: host

Domain Name: domain

Session Timeout

TCP Timeout (min): 120

UDP Timeout (min): 3

Login Banner

Date / Time Properties

Date: 12/21/2016

Time: 11:18

□ Use NTP SET

Time Zone: (GMT-07:00) Mountain Time (US & Canada)

Backup and Restore

ARP

Copyright © 2000-2016. FatPipe Networks Inc.

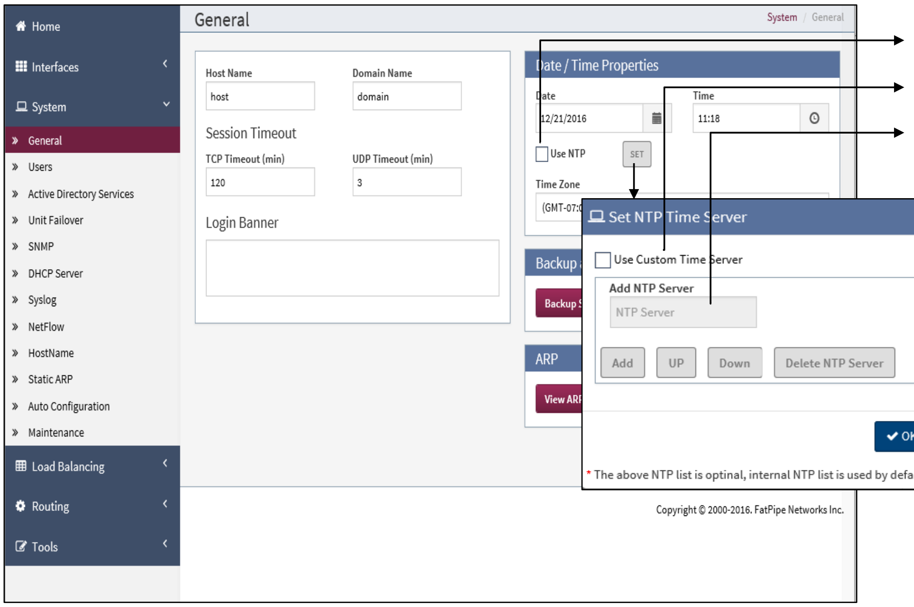
ARP is used for mapping an IPv4 address to a physical address like a MAC address.
IP Address, Hardware type and address, Flags, Mask and Interface table are displayed in the arp table view.

Click to Clear ARP table of the unit or to Send Gratuitous ARP

Click to view the ARP table of the unit

SYSTEM CONFIGURATION

Used to configure or change system configuration of FatPipe MPVPN



General

Host Name: host

Domain Name: domain

Session Timeout

TCP Timeout (min): 120

UDP Timeout (min): 3

Login Banner

Date / Time Properties

Date: 12/21/2016

Time: 11:18

□ Use NTP

Time Zone: (GMT-07:0

Set NTP Time Server

□ Use Custom Time Server

Add NTP Server: NTP Server

* The above NTP list is optinal, internal NTP list is used by default.

Copyright © 2000-2016. FatPipe Networks Inc.

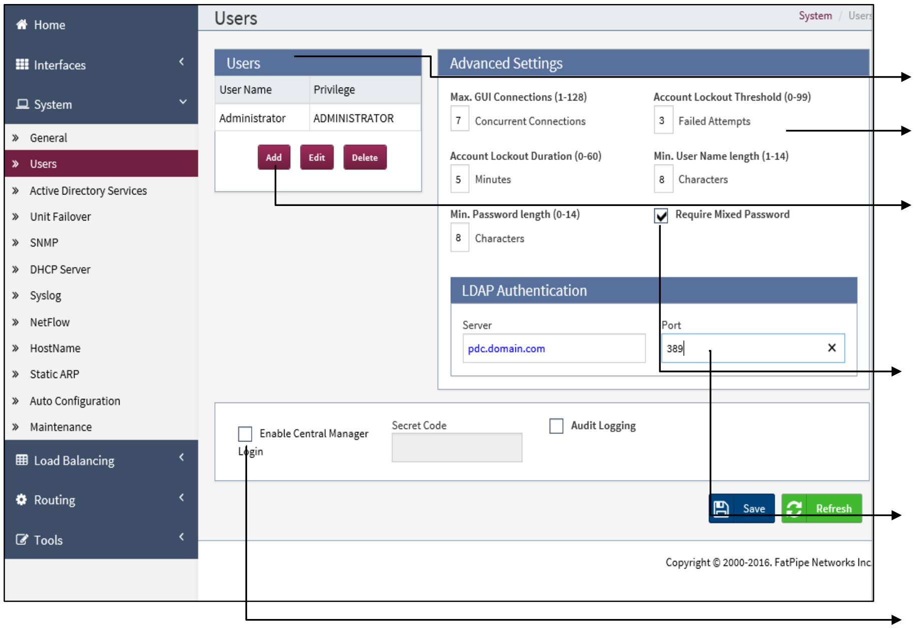
Check this box to synchronize with an external time server.

Uncheck this box to use the default time servers.

Input the time server hostname or IP.

USER CONFIGURATION

Used to configure various Administrative tasks



Users

User Name	Privilege
Administrator	ADMINISTRATOR

Advanced Settings

Max. GUI Connections (1-128): 7 Concurrent Connections

Account Lockout Threshold (0-99): 3 Failed Attempts

Account Lockout Duration (0-60): 5 Minutes

Min. User Name length (1-14): 8 Characters

Min. Password length (0-14): 8 Characters

☑ Require Mixed Password

LDAP Authentication

Server: pdc.domain.com

Port: 389

□ Enable Central Manager Login

Secret Code

□ Audit Logging

Copyright © 2000-2016. FatPipe Networks Inc

Manage User accounts and access privileges (more Info…)

Account policy settings (more Info…)

Specify username and password(more Info…)

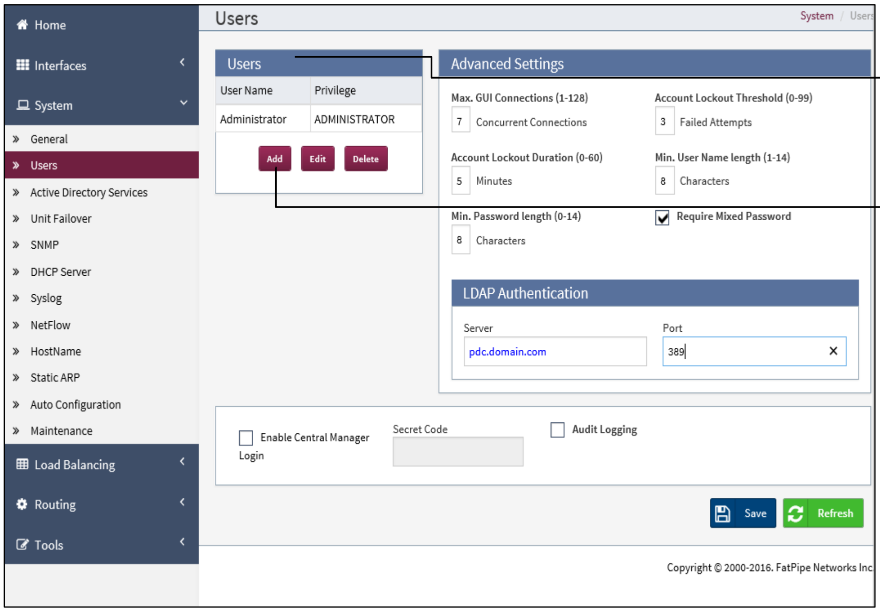
Permits to give a mixed password(more Info…)

Enter the LDAP server's IP address and port information (more Info…)

This provides access to the Central Manager Software (more Info…)

USER CONFIGURATION

Used to configure various Administrative tasks



Users

User Name	Privilege
Administrator	ADMINISTRATOR

Advanced Settings

Max. GUI Connections (1-128): 7 Concurrent Connections

Account Lockout Threshold (0-99): 3 Failed Attempts

Account Lockout Duration (0-60): 5 Minutes

Min. User Name length (1-14): 8 Characters

Min. Password length (0-14): 8 Characters

☑ Require Mixed Password

LDAP Authentication

Server: pdc.domain.com

Port: 389

□ Enable Central Manager Login

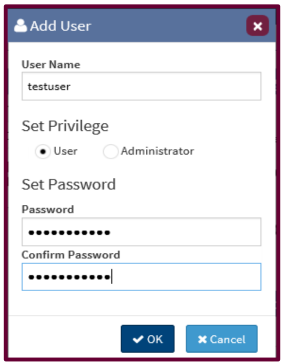
Secret Code:

□ Audit Logging

Copyright © 2000-2016. FatPipe Networks Inc

Manage User accounts and access privileges

Specify username and password



Add User

User Name: testuser

Set Privilege

● User ○ Administrator

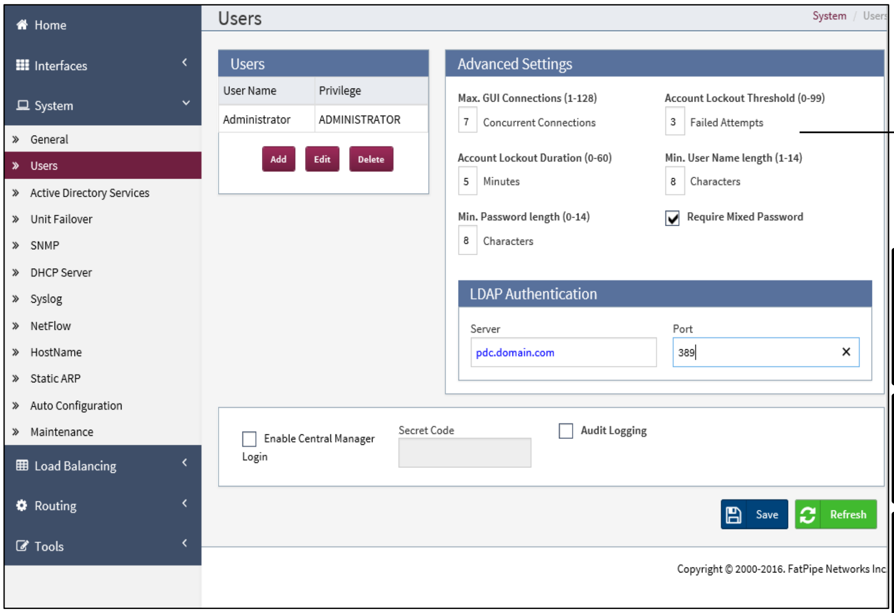
Set Password

Password: •••••••••••

Confirm Password: •••••••••••

USER CONFIGURATION

Used to configure various Administrative tasks



Users

User Name	Privilege
Administrator	ADMINISTRATOR

Advanced Settings

Max. GUI Connections (1-128): 7 Concurrent Connections

Account Lockout Threshold (0-99): 3 Failed Attempts

Account Lockout Duration (0-60): 5 Minutes

Min. User Name length (1-14): 8 Characters

Min. Password length (0-14): 8 Characters

☑ Require Mixed Password

LDAP Authentication

Server: pdc.domain.com

Port: 389

□ Enable Central Manager Login

Secret Code:

□ Audit Logging

Copyright © 2000-2016. FatPipe Networks Inc

Account policy settings

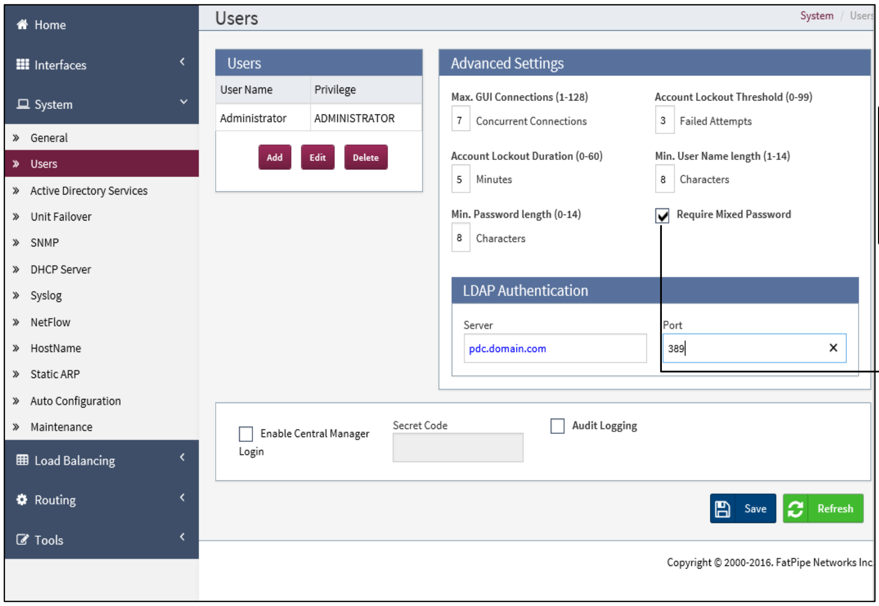
Maximum GUI Connections, sets the limit on the number of concurrent connections that are allowed to the remote management interface.

Account Lockout Threshold specifies the number of failed login attempts allowed before locking out the user.

Account Lockout Duration specifies the number of minutes before a user can attempt to login again after being locked out.

USER CONFIGURATION

Used to configure various Administrative tasks



Users

User Name	Privilege
Administrator	ADMINISTRATOR

Advanced Settings

Max. GUI Connections (1-128): 7 Concurrent Connections

Account Lockout Threshold (0-99): 3 Failed Attempts

Account Lockout Duration (0-60): 5 Minutes

Min. User Name length (1-14): 8 Characters

Min. Password length (0-14): 8 Characters

☑ Require Mixed Password

LDAP Authentication

Server: pdc.domain.com

Port: 389

☐ Enable Central Manager Login

Secret Code

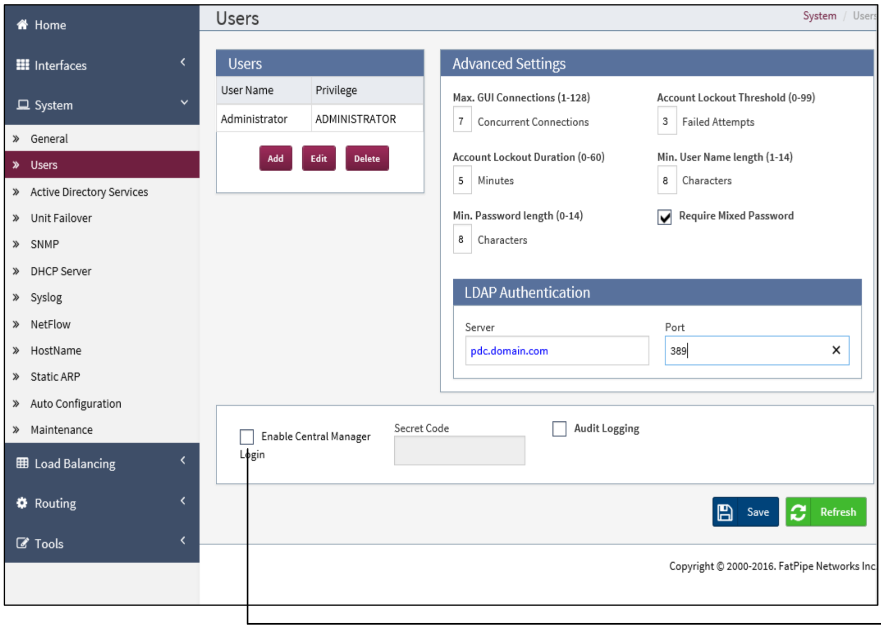
☐ Audit Logging

Will enable complex password checking. Passwords for new user accounts must contain a mix of letters, numbers, and special characters when this is enabled.

Permits to give a mixed password

USER CONFIGURATION

Used to configure various Administrative tasks



Users

User Name	Privilege
Administrator	ADMINISTRATOR

Advanced Settings

Max. GUI Connections (1-128): 7 Concurrent Connections

Account Lockout Threshold (0-99): 3 Failed Attempts

Account Lockout Duration (0-60): 5 Minutes

Min. User Name length (1-14): 8 Characters

Min. Password length (0-14): 8 Characters

☑ Require Mixed Password

LDAP Authentication

Server: pdc.domain.com

Port: 389

☐ Enable Central Manager Login

Secret Code

☐ Audit Logging

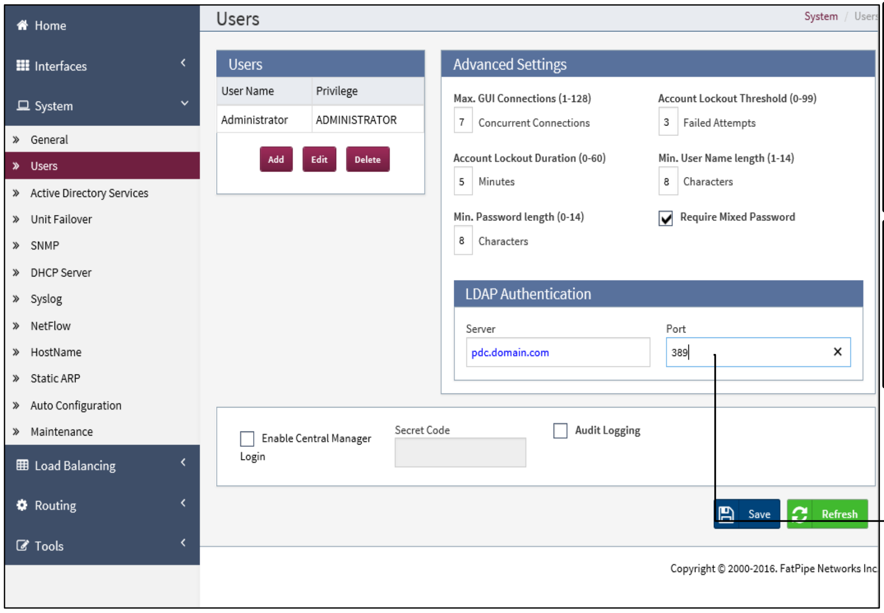
Copyright © 2000-2016. FatPipe Networks Inc.

The FatPipe Central Manager Platform is a adjunct used separately to manage multiple FatPipes enterprise wide via one interface.

This provides access to the Central Manager Software

USER CONFIGURATION

Used to configure various Administrative tasks



Users

User Name	Privilege
Administrator	ADMINISTRATOR

Advanced Settings

Max. GUI Connections (1-128): 7 Concurrent Connections

Account Lockout Threshold (0-99): 3 Failed Attempts

Account Lockout Duration (0-60): 5 Minutes

Min. User Name length (1-14): 8 Characters

Min. Password length (0-14): 8 Characters

☑ Require Mixed Password

LDAP Authentication

Server: pdc.domain.com

Port: 389

□ Enable Central Manager Login

Secret Code

□ Audit Logging

Copyright © 2000-2016. FatPipe Networks Inc

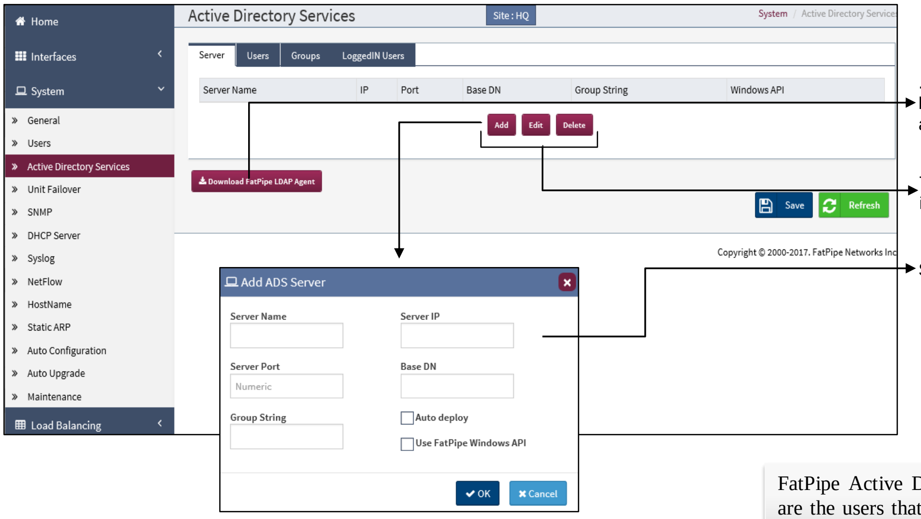
FatPipe uses Transport Layer Security technology to ensure confidential data exchange between the LDAP server and the FatPipe in order to protect sensitive information, including the usernames, passwords and privileges.

FatPipe offers two secure protocols: TLS and SSLv3. TLS is an upgraded version of SSLv3. TLS is used by default. The SSLv3 is only used when TLS is not functional on the server.

Enter the LDAP server's IP address and port information

Active Directory Services

Used to create profiles for Users



Active Directory Services

Server Name	IP	Port	Base DN	Group String	Windows API

Copyright © 2000-2017. FatPipe Networks Inc

Add ADS Server

Server Name

Server IP

Server Port: Numeric

Base DN

Group String

□ Auto deploy

□ Use FatPipe Windows API

.exe file to download into computer for having user name and passwords assigned to users.

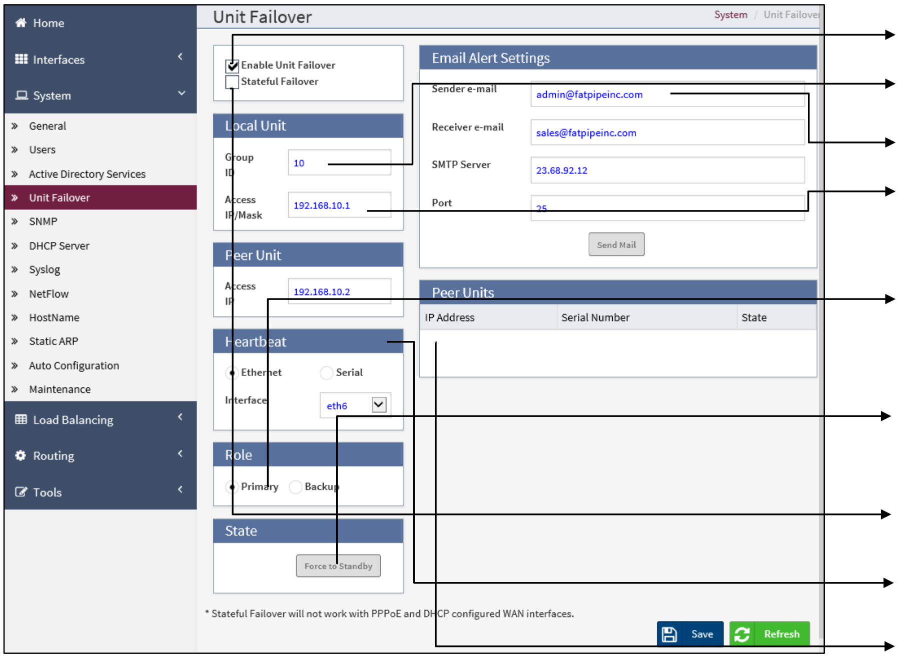
To add, edit or delete ADS server information

Specify information about ADS server

FatPipe Active Directories works to define who are the users that can access FatPipe UI and can login using their existing credentials instead of creating new user name and password for each and every user.

UNIT FAILOVER CONFIGURATION

Used to configure Unit Failover



Unit Failover

☑ Enable Unit Failover
□ Stateful Failover

Local Unit

Group ID: 10
Access IP/Mask: 192.168.10.1

Peer Unit

Access IP: 192.168.10.2

Heartbeat

● Ethernet ○ Serial
Interface: eth6

Role

● Primary ○ Backup

State

Email Alert Settings

Sender e-mail: admin@fatpipeinc.com
Receiver e-mail: sales@fatpipeinc.com
SMTP Server: 23.68.92.12
Port: 25

Peer Units

IP Address	Serial Number	State

* Stateful Failover will not work with PPPoE and DHCP configured WAN interfaces.

Select this to enable unit failover. (more Info…)

Specify the failover group the unit belongs to. (more Info…)

Provide Email to get alerts. (more Info…)

Specify the Access IP for heartbeat / config syncing between peers. (more Info…)

Specify the preferred role of the unit, which only applies when both units are powered ON at the same time. (more Info…)

Forces a Switch of Activity between the 2 peered boxes in HA for maintenance purposes.

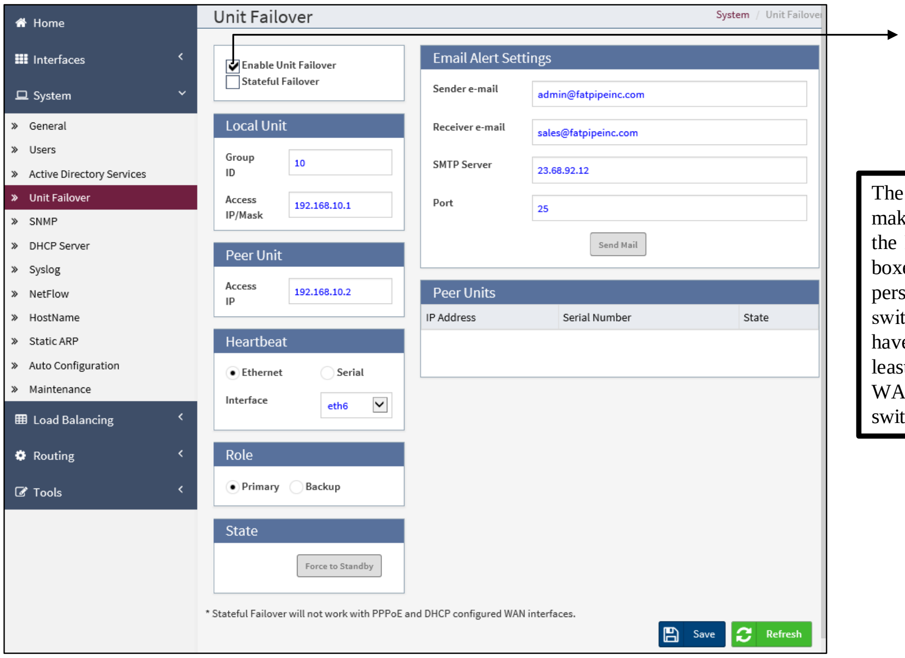
Enable Stateful Failover to seamlessly failover sessions from Active unit to Standby unit (more Info…)

Choose Ethernet or Serial Interface to exchange heartbeat packets (more Info…)

Displays which unit is backup (more Info…)

UNIT FAILOVER CONFIGURATION

Used to configure Unit Failover



Unit Failover

☑ Enable Unit Failover
□ Stateful Failover

Local Unit

Group ID: 10
Access IP/Mask: 192.168.10.1

Peer Unit

Access IP: 192.168.10.2

Heartbeat

● Ethernet ○ Serial
Interface: eth6

Role

● Primary ○ Backup

State

Email Alert Settings

Sender e-mail: admin@fatpipeinc.com
Receiver e-mail: sales@fatpipeinc.com
SMTP Server: 23.68.92.12
Port: 25

Peer Units

IP Address	Serial Number	State

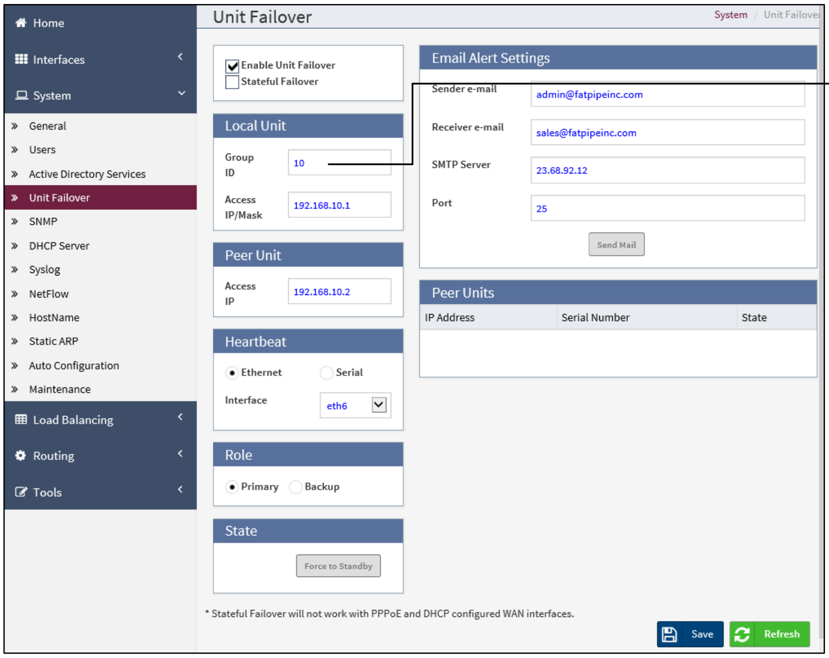
* Stateful Failover will not work with PPPoE and DHCP configured WAN interfaces.

Select this to enable unit failover.

The physical setup consists of making each network segment on the Fatpipe common between the 2 boxes from an electrical ethernet perspective using separate switches/VLAN's (I.E. LAN would have its own switch/VLAN with at least 3 ports having membership, WAN1 would have its own switch/VLAN with 3 ports, etc.)

UNIT FAILOVER CONFIGURATION

Used to configure Unit Failover



Unit Failover

☑ Enable Unit Failover
☐ Stateful Failover

Local Unit

Group ID: 10
Access IP/Mask: 192.168.10.1

Peer Unit

Access IP: 192.168.10.2

Heartbeat

● Ethernet ○ Serial
Interface: eth6

Role

● Primary ○ Backup

State

Email Alert Settings

Sender e-mail: admin@fatpipeinc.com
Receiver e-mail: sales@fatpipeinc.com
SMTP Server: 23.68.92.12
Port: 25

Peer Units

IP Address	Serial Number	State

* Stateful Failover will not work with PPPoE and DHCP configured WAN interfaces.

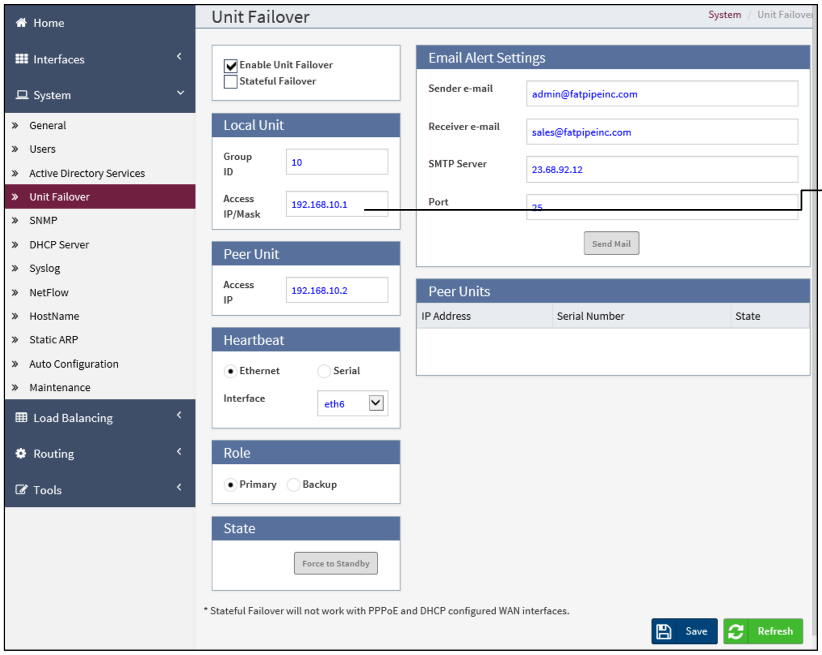
Specify the failover group the unit belongs to.

The Group ID uniquely identifies the failover group. Both of your failover units must use the same Group ID.

Valid range is 1-255.

UNIT FAILOVER CONFIGURATION

Used to configure Unit Failover


Unit Failover

☑ Enable Unit Failover
☐ Stateful Failover

Local Unit

Group ID: 10
Access IP/Mask: 192.168.10.1

Peer Unit

Access IP: 192.168.10.2

Heartbeat

● Ethernet ○ Serial
Interface: eth6

Role

● Primary ○ Backup

State

Email Alert Settings

Sender e-mail: admin@fatpipeinc.com
Receiver e-mail: sales@fatpipeinc.com
SMTP Server: 23.68.92.12
Port: 25

Peer Units

IP Address	Serial Number	State

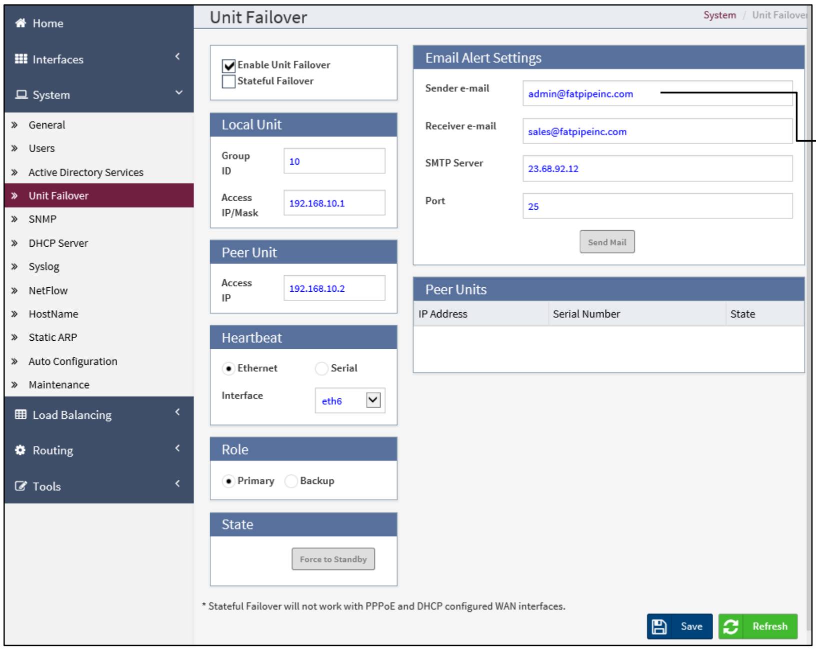
* Stateful Failover will not work with PPPoE and DHCP configured WAN interfaces.

Specify the Access IP for heartbeat / config syncing between peers.

Access IP/Mask uniquely identifies each unit in a private subnet common to both units and will be used to access the unit when in Standby mode.

UNIT FAILOVER CONFIGURATION

Used to configure Unit Failover



Unit Failover

☑ Enable Unit Failover
☐ Stateful Failover

Local Unit

Group ID	10
Access IP/Mask	192.168.10.1

Peer Unit

Access IP	192.168.10.2

Heartbeat

● Ethernet ○ Serial

Interface: eth6

Role

● Primary ○ Backup

State

Force to Standby

Email Alert Settings

Sender e-mail	admin@fatpipeinc.com
Receiver e-mail	sales@fatpipeinc.com
SMTP Server	23.68.92.12
Port	25

Send Mail

Peer Units

IP Address	Serial Number	State

* Stateful Failover will not work with PPPoE and DHCP configured WAN interfaces.

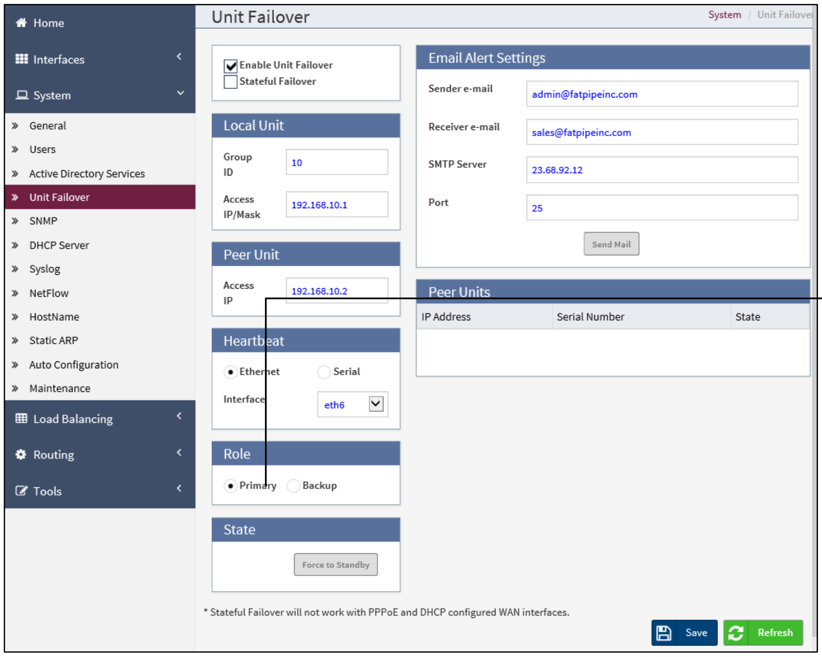
Save Refresh

Provide Email to get alerts.

Email Alert Settings allows you to specify email information so an email can be sent whenever failover occurs. This email will be sent from the box assuming the active role.

UNIT FAILOVER CONFIGURATION

Used to configure Unit Failover



Unit Failover

☑ Enable Unit Failover
☐ Stateful Failover

Local Unit

Group ID	10
Access IP/Mask	192.168.10.1

Peer Unit

Access IP	192.168.10.2

Heartbeat

● Ethernet ○ Serial

Interface: eth6

Role

● Primary ○ Backup

State

Force to Standby

Email Alert Settings

Sender e-mail	admin@fatpipeinc.com
Receiver e-mail	sales@fatpipeinc.com
SMTP Server	23.68.92.12
Port	25

Send Mail

Peer Units

IP Address	Serial Number	State

* Stateful Failover will not work with PPPoE and DHCP configured WAN interfaces.

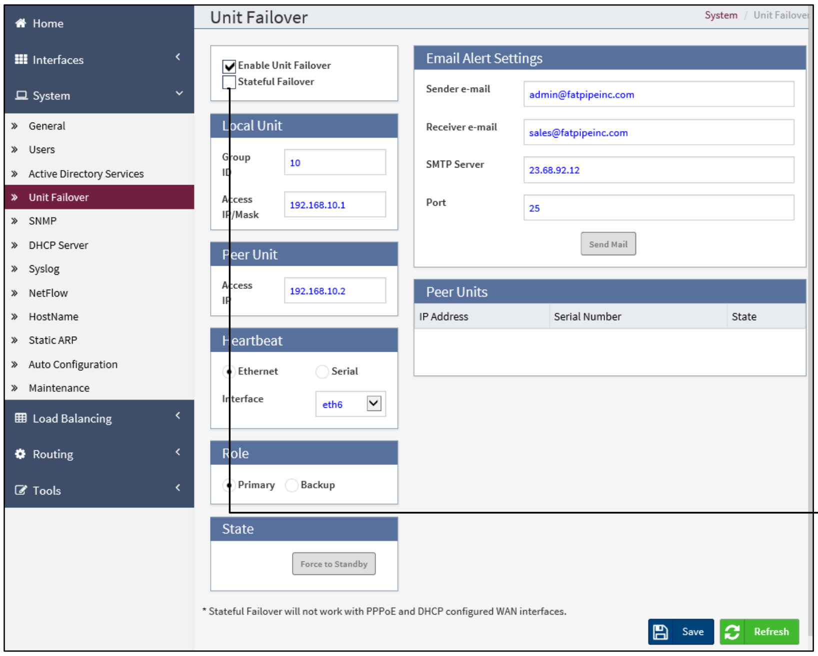
Save Refresh

Specify the preferred role of the unit, which only applies when both units are powered ON at the same time.

One unit will be set as Primary and the other as Backup. The role only applies when both units are powered on at the same time. The unit marked as Primary will go to the Active state and the unit marked as Backup will go to the Standby state.

UNIT FAILOVER CONFIGURATION

Used to configure Unit Failover



Unit Failover

☑ Enable Unit Failover
□ Stateful Failover

Local Unit

Group ID	10
Access IP/Mask	192.168.10.1

Peer Unit

Access IP	192.168.10.2

Heartbeat

● Ethernet ○ Serial

Interface: eth6

Role

● Primary ○ Backup

State

Force to Standby

Email Alert Settings

Sender e-mail	admin@fatpipeinc.com
Receiver e-mail	sales@fatpipeinc.com
SMTP Server	23.68.92.12
Port	25

Send Mail

Peer Units

IP Address	Serial Number	State

* Stateful Failover will not work with PPPoE and DHCP configured WAN interfaces.

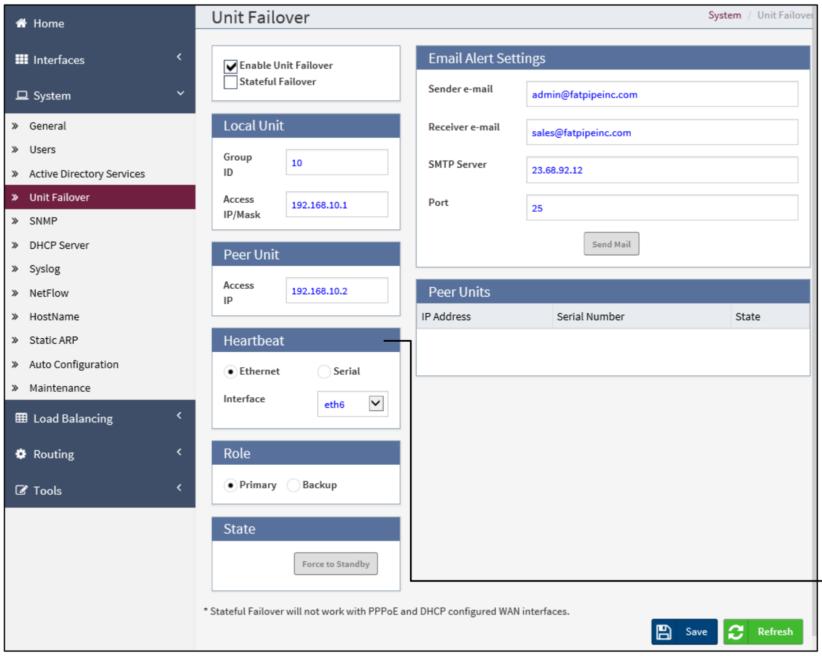
Save Refresh

Enable Stateful Failover to ensure all sessions from the Active units are failed over transparently to the Standby unit in case of failure of Active unit.

Enable Stateful Failover to seamlessly failover sessions from Active unit to Standby unit

UNIT FAILOVER CONFIGURATION

Used to configure Unit Failover



Unit Failover

☑ Enable Unit Failover
□ Stateful Failover

Local Unit: Group ID 10; Access IP/Mask 192.168.10.1

Peer Unit: Access IP 192.168.10.2

Heartbeat: ● Ethernet ○ Serial; Interface eth6

Role: ● Primary ○ Backup

State: Force to Standby

Email Alert Settings: Sender e-mail admin@fatpipeinc.com; Receiver e-mail sales@fatpipeinc.com; SMTP Server 23.68.92.12; Port 25; Send Mail

Peer Units: IP Address | Serial Number | State

* Stateful Failover will not work with PPPoE and DHCP configured WAN interfaces.

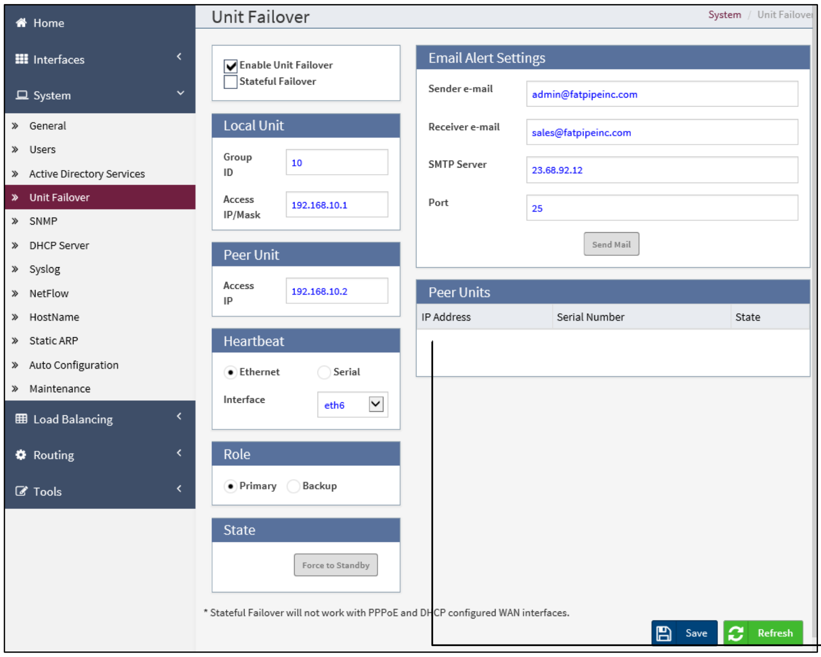
Save Refresh

This option indicates the physical interface that heartbeats traverse. Choose Ethernet to exchange the heartbeat packets over the Ethernet interface. Choose Serial to exchange the heartbeat packets over the Serial interface.

Choose Ethernet or Serial Interface to exchange heartbeat packets

UNIT FAILOVER CONFIGURATION

Used to configure Unit Failover



Unit Failover

☑ Enable Unit Failover
☐ Stateful Failover

Local Unit

Group ID: 10
Access IP/Mask: 192.168.10.1

Peer Unit

Access IP: 192.168.10.2

Heartbeat

● Ethernet ○ Serial
Interface: eth6

Role

● Primary ○ Backup

State

Email Alert Settings

Sender e-mail: admin@fatpipeinc.com
Receiver e-mail: sales@fatpipeinc.com
SMTP Server: 23.68.92.12
Port: 25

Peer Units

IP Address	Serial Number	State

* Stateful Failover will not work with PPPoE and DHCP configured WAN interfaces.

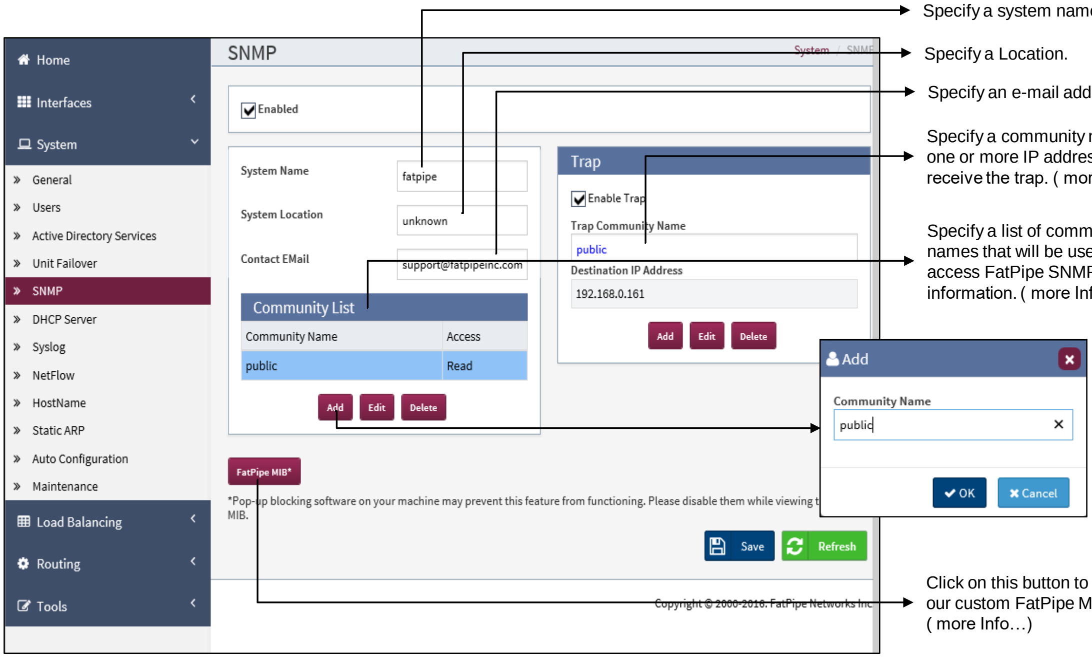
The Peer Unit shows details about the inactive box.

The IP address of the backup unit is the Access IP. Serial Number is the Serial Number of the Peer Unit. The State could be displayed as "Up," "Backup," or "Down." If it is marked as Down, it means the unit is no longer detected.

Displays which unit is backup

SNMP TOOL

Used to setup and manage SNMP



SNMP

☑ Enabled

System Name: fatpipe
System Location: unknown
Contact EMail: support@fatpipeinc.com

Community List

Community Name	Access
public	Read

Trap

☑ Enable Trap
Trap Community Name: public
Destination IP Address: 192.168.0.161

Add

Community Name: public

*Pop-up blocking software on your machine may prevent this feature from functioning. Please disable them while viewing t MIB.

Copyright © 2000-2016. FatPipe Networks Inc

Specify a system name.

Specify a Location.

Specify an e-mail address.

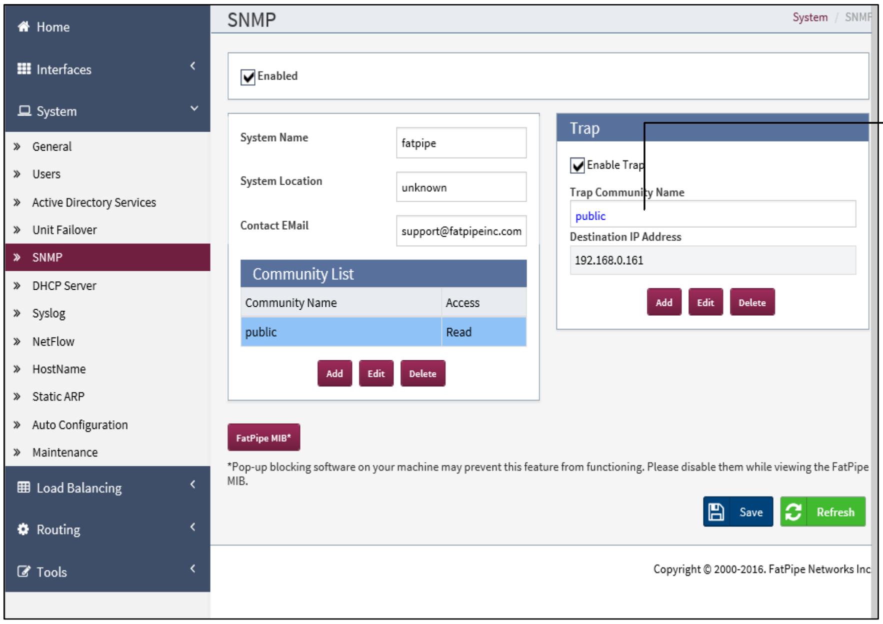
Specify a community name and one or more IP addresses that will receive the trap. (more Info…)

Specify a list of community names that will be used to access FatPipe SNMP information. (more Info…)

Click on this button to download our custom FatPipe MIB. (more Info…)

SNMP TOOL

Used to setup and manage SNMP



SNMP

☑ Enabled

System Name: fatpipe

System Location: unknown

Contact EMail: support@fatpipeinc.com

Community List

Community Name	Access
public	Read

Trap

☑ Enable Trap

Trap Community Name: public

Destination IP Address: 192.168.0.161

*Pop-up blocking software on your machine may prevent this feature from functioning. Please disable them while viewing the FatPipe MIB.

Copyright © 2000-2016. FatPipe Networks Inc

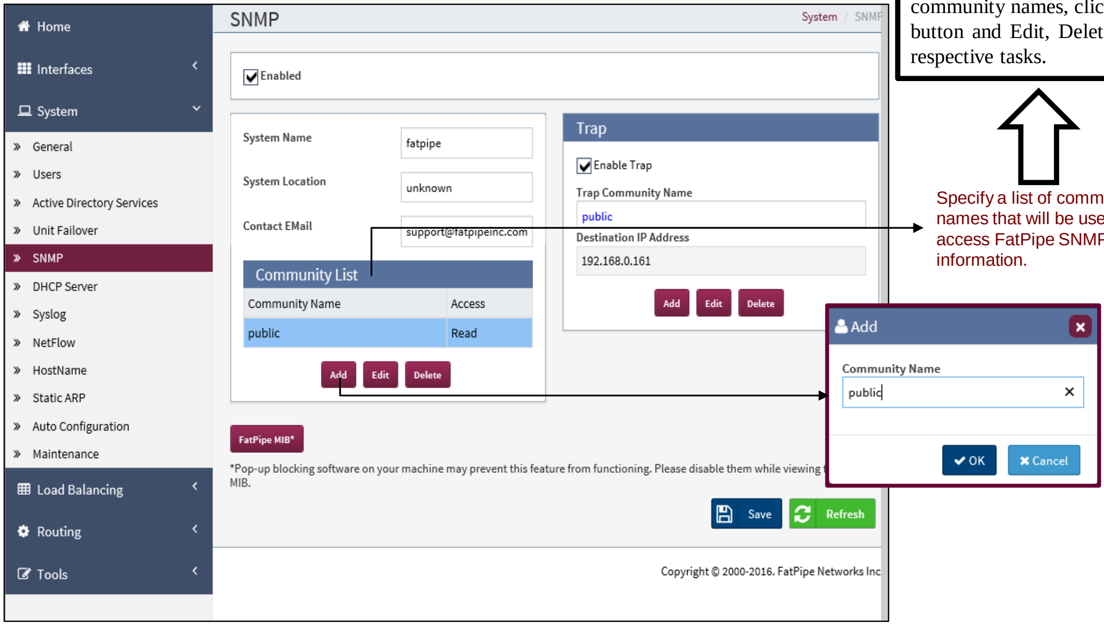
Specify a community name and one or more IP addresses that will receive the trap.

The Fatpipe will send an SNMP trap to alert you when there is a off normal condition. Community name and one or more IP addresses of a network management platform that will receive the trap must be specified

SNMP TOOL

Used to setup and manage SNMP

The community List has a default community name, “public,” with read only access available. To add community names, click on the Add button and Edit, Delete to perform respective tasks.



SNMP

☑ Enabled

System Name: fatpipe

System Location: unknown

Contact EMail: support@fatpipeinc.com

Community List

Community Name	Access
public	Read

Trap

☑ Enable Trap

Trap Community Name: public

Destination IP Address: 192.168.0.161

*Pop-up blocking software on your machine may prevent this feature from functioning. Please disable them while viewing the MIB.

Copyright © 2000-2016. FatPipe Networks Inc

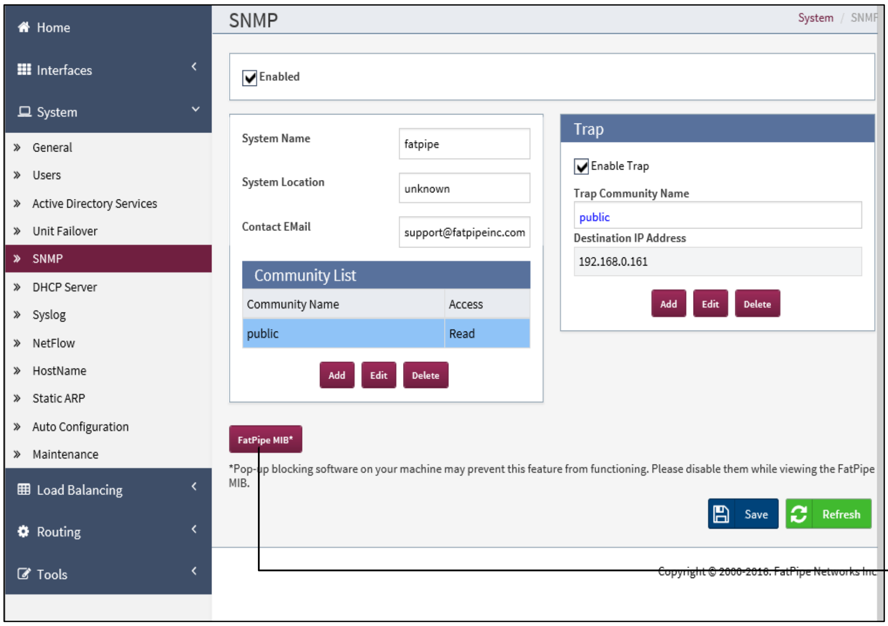
Add

Community Name: public

Specify a list of community names that will be used to access FatPipe SNMP information.

SNMP TOOL

Used to setup and manage SNMP



SNMP

☑ Enabled

System Name: fatpipe

System Location: unknown

Contact EMail: support@fatpipeinc.com

Community List

Community Name	Access
public	Read

Trap

☑ Enable Trap

Trap Community Name: public

Destination IP Address: 192.168.0.161

*Pop-up blocking software on your machine may prevent this feature from functioning. Please disable them while viewing the FatPipe MIB.

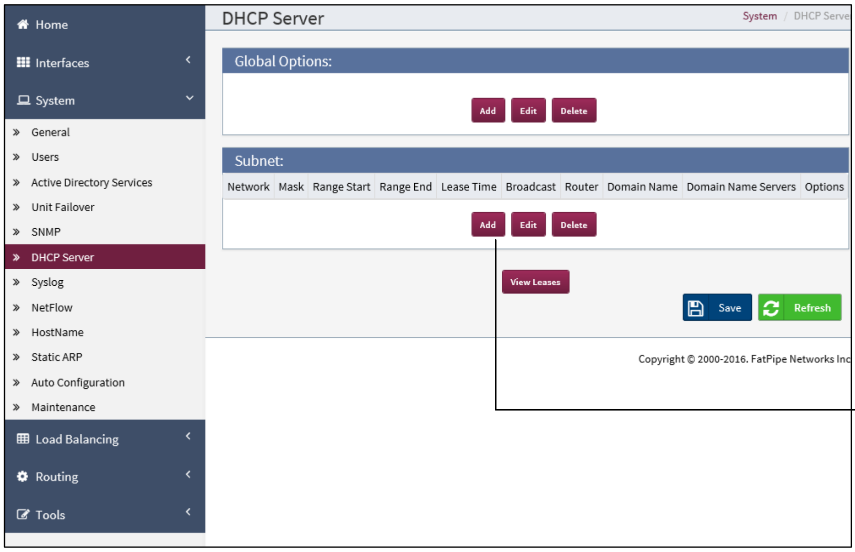
Copyright © 2000-2016. FatPipe Networks Inc

This MIB can be imported into your local SNMP based network management platform, where you can configure how your platform interoperates with the Fatpipe.

Click on this button to download our custom FatPipe MIB.

DHCP SERVER

Used to setup and manage DHCP server



DHCP Server

Global Options:

Subnet:

Network	Mask	Range Start	Range End	Lease Time	Broadcast	Router	Domain Name	Domain Name Servers	Options

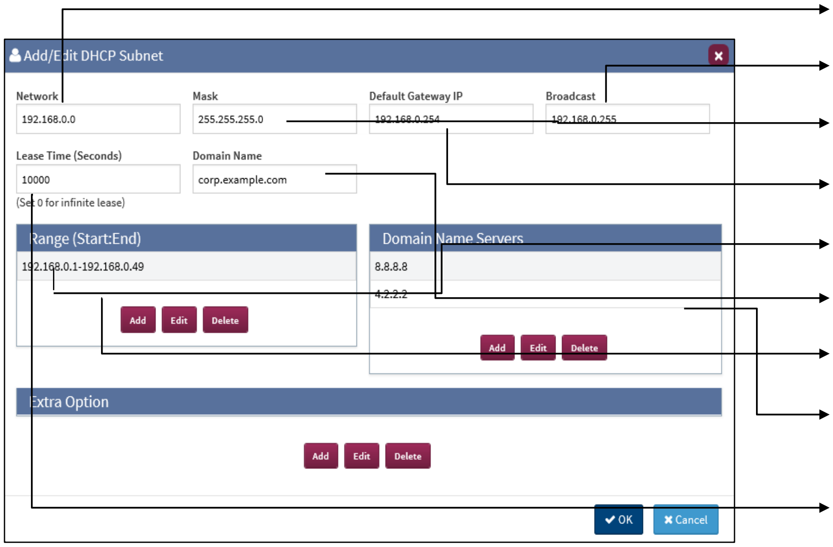
Copyright © 2000-2016. FatPipe Networks Inc

FatPipe DHCP server allows you to configure the built-in DHCP Server to assign IP addresses to devices on your local area network (LAN).

To add a DHCP subnet

DHCP SERVER

Add and manage DHCP server



Add/Edit DHCP Subnet

Network	Mask	Default Gateway IP	Broadcast
192.168.0.0	255.255.255.0	192.168.0.254	192.168.0.255

Lease Time (Seconds): 10000

(Set 0 for infinite lease)

Domain Name: corp.example.com

Range (Start:End)

192.168.0.1-192.168.0.49

Domain Name Servers

8.8.8.8

4.2.2.2

Network address of subnet that DHCP will assign from

Broadcast IP of this subnet

Subnet mask of the this network

Gateway IP address to be assigned

The starting IP address for the DHCP range to be assigned

Domain name given.

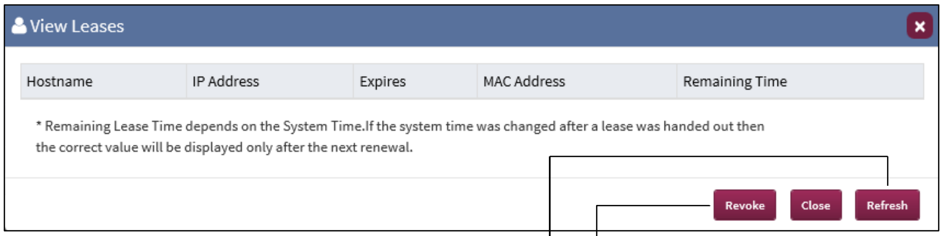
The last IP for the DHCP range to be assigned.

IP address of the preferred DNS servers in hierarchical order.

The amount of time a DHCP client may have an IP address before it is required to renew the lease.

DHCP SERVER

Used to view Leases



View Leases

Hostname	IP Address	Expires	MAC Address	Remaining Time

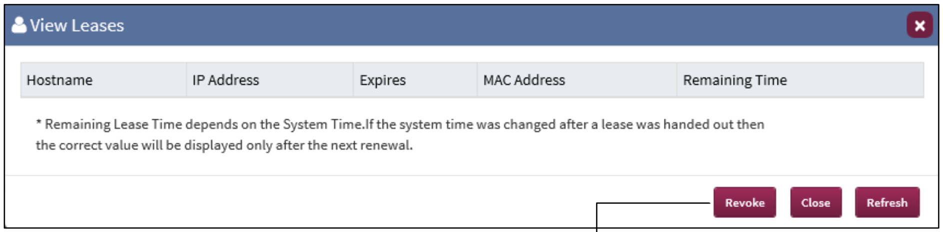
* Remaining Lease Time depends on the System Time.If the system time was changed after a lease was handed out then the correct value will be displayed only after the next renewal.

The Revoke button is used to cancel the lease for a specific LAN device, and releases the entry from the lease table (more Info…)

Click Refresh button to update the View Lease table

DHCP SERVER

Used to view Leases



Hostname	IP Address	Expires	MAC Address	Remaining Time

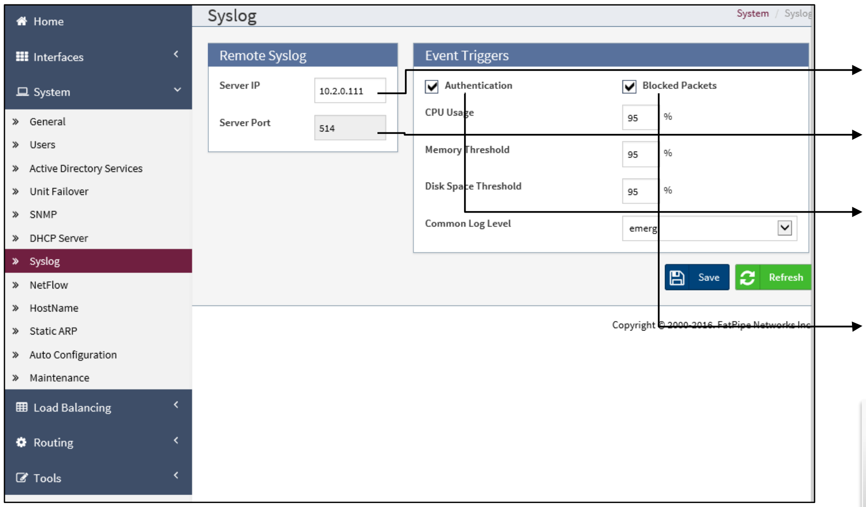
* Remaining Lease Time depends on the System Time.If the system time was changed after a lease was handed out then the correct value will be displayed only after the next renewal.

The Revoke button is used to cancel the lease for a specific LAN device, and releases the entry from the lease table

Use the Revoke button for maintenance purposes or if the device no longer needs the leased IP address.

SYSLOG

Used to Configure Syslog Server



Server IP: 10.2.0.111

Server Port: 514

☑ Authentication ☑ Blocked Packets

CPU Usage: 95 %

Memory Threshold: 95 %

Disk Space Threshold: 95 %

Common Log Level: emerg

Copyright © 2000-2016. FatPipe Networks Inc.

The IP of the host that the Fatpipe will send Syslog flows to (more Info…)

The remote syslog server port number (more Info…)

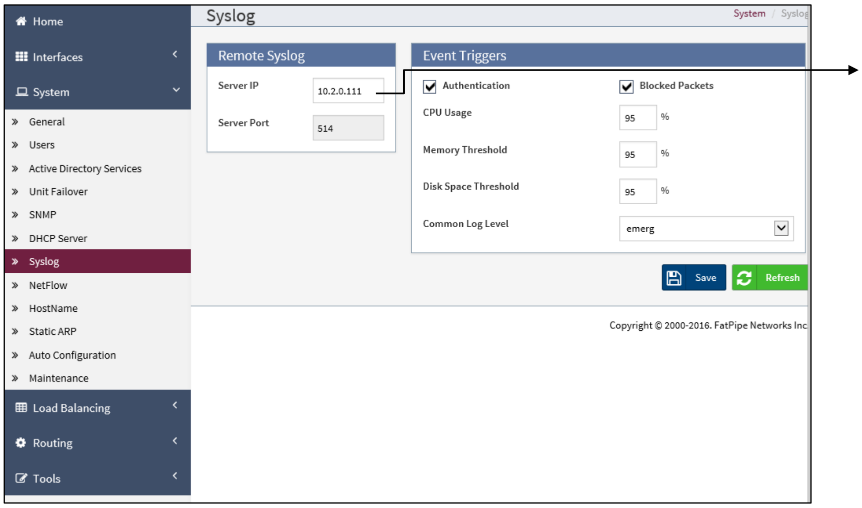
If this is enabled, a log message will be sent to syslog server giving information about the login and logout time of a user to a particular IP

If this is enabled, a log message will be sent to syslog server giving the information about the packets source, destination and type that are being dropped by the FatPipe via policies

Syslog is a standard for forwarding log messages in an IP network. In order to take advantage of this feature, a running syslog server on a host reachable from the FatPipe is necessary.

SYSLOG

Used to Configure Syslog Server



Server IP 10.2.0.111

Server Port 514

☑ Authentication ☑ Blocked Packets

CPU Usage 95 %

Memory Threshold 95 %

Disk Space Threshold 95 %

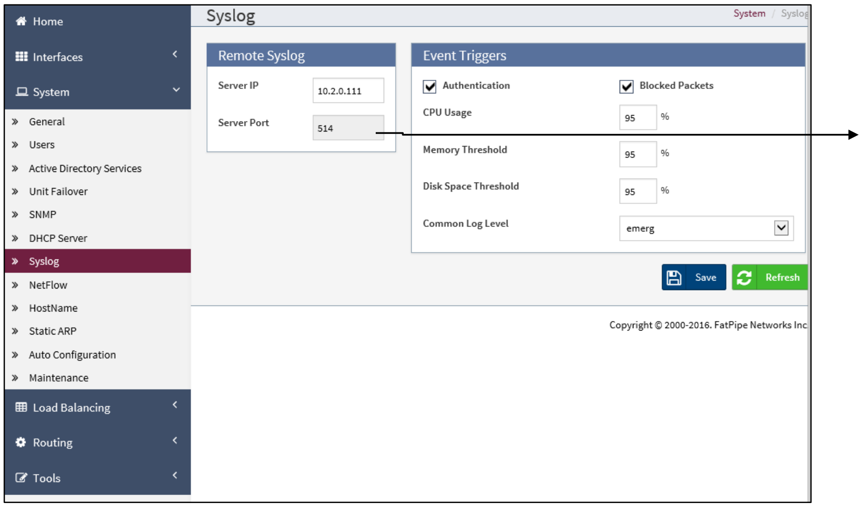
Common Log Level emerg

Copyright © 2000-2016. FatPipe Networks Inc

The IP of the host that the Fatpipe will send Syslog flows to

SYSLOG

Used to Configure Syslog Server



Server IP 10.2.0.111

Server Port 514

☑ Authentication ☑ Blocked Packets

CPU Usage 95 %

Memory Threshold 95 %

Disk Space Threshold 95 %

Common Log Level emerg

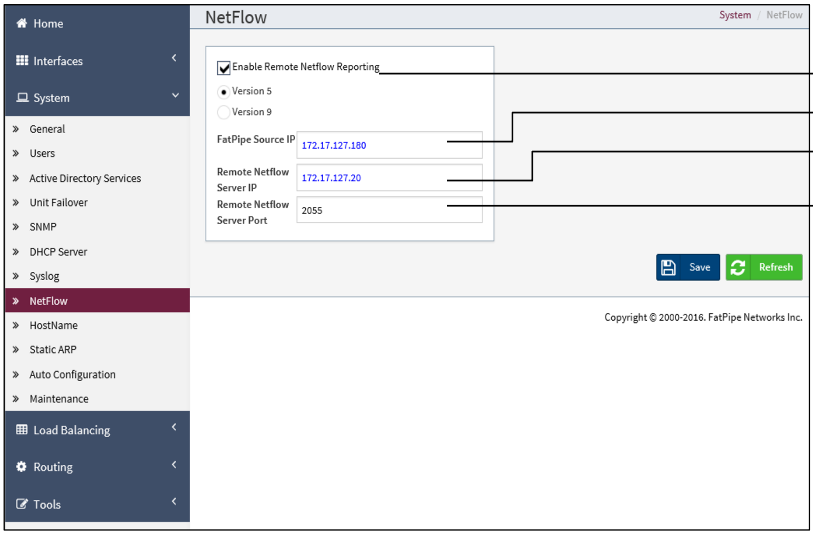
Copyright © 2000-2016. FatPipe Networks Inc

The remote syslog server port number

NETFLOW

Used to Configure NetFlow

FatPipe NetFlow allows you to export traffic statistics using Netflow protocol.



NetFlow

☑ Enable Remote Netflow Reporting

● Version 5

○ Version 9

FatPipe Source IP	172.17.127.180
Remote Netflow Server IP	172.17.127.20
Remote Netflow Server Port	2055

Copyright © 2000-2016. FatPipe Networks Inc.

Enable NetFlow

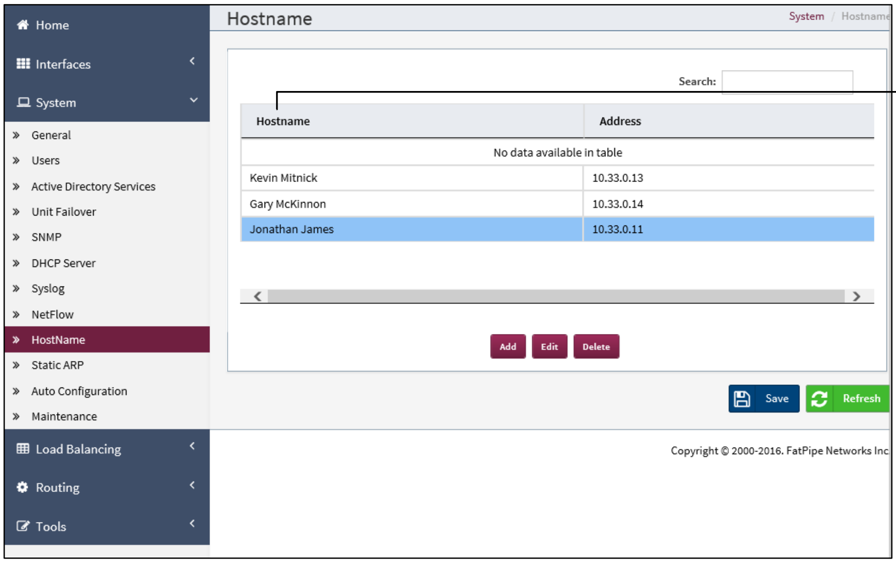
FatPipe Source IP

NetFlow Flow collector IP

Remote NetFlow server port number

HOSTNAME

Used to Configure Hostnames with IP addresses



Hostname

Hostname	Address
No data available in table	
Kevin Mitnick	10.33.0.13
Gary McKinnon	10.33.0.14
Jonathan James	10.33.0.11

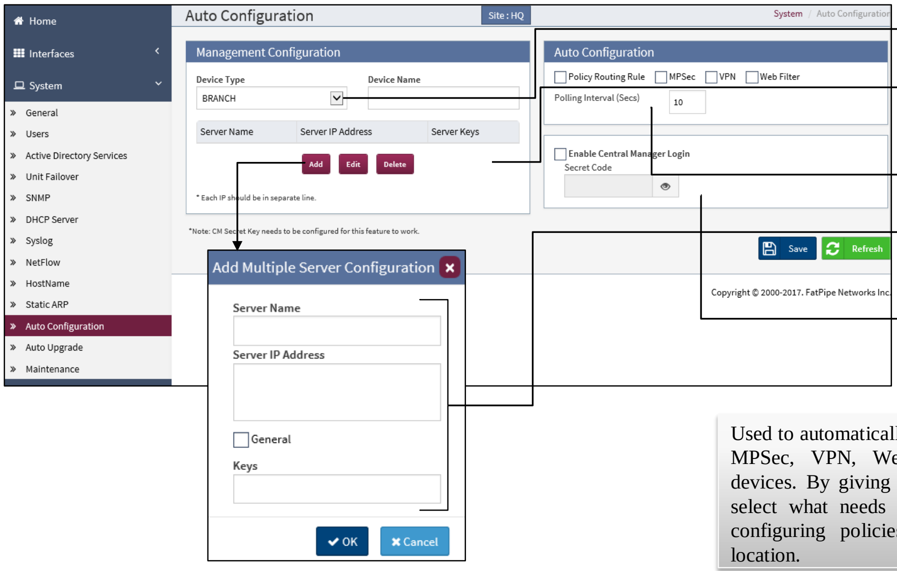
Copyright © 2000-2016. FatPipe Networks Inc

Enter Hostnames in your LAN and their IP addresses. These Hostnames will be displayed in addition to the IP addresses in 'Traffic Logging Info'

.exe file to download into computer for having user name and passwords assigned to users.

AUTO CONFIGURATION

Used to configure policies between two locations



Select devices from the added list

Add FatPipe device from other location.

To have the features configured automatically.

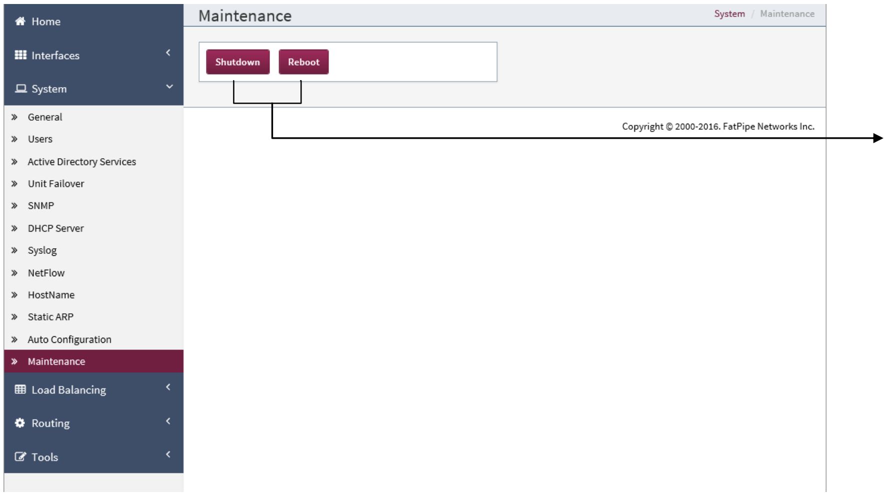
DR site FatPipe credentials

Enable Central Manager login with Secrete Code.

Used to automatically configure Policy Routing Rules, MPSec, VPN, Web Filter between two FatPipe devices. By giving DR site FatPipe information and select what needs to be configured, we can avoid configuring policies manually at each and every location.

REBOOT / SHUTDOWN

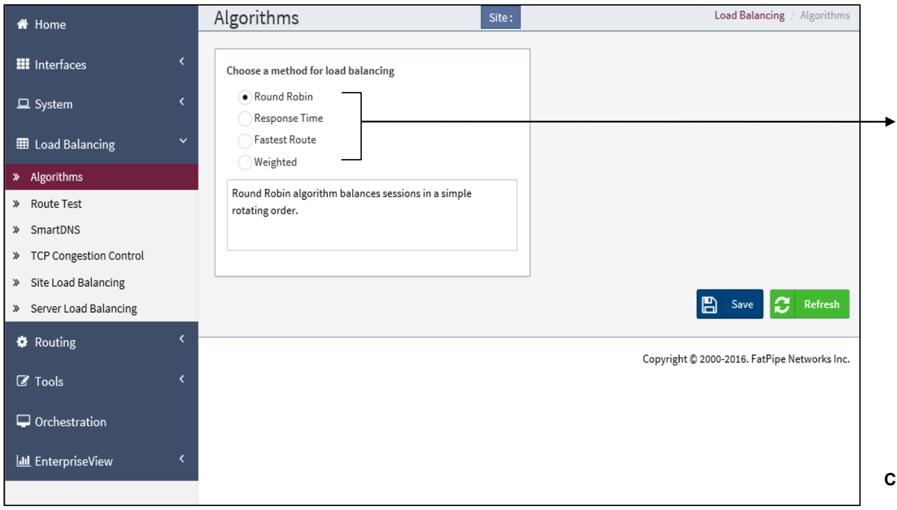
Used to reboot or shutdown the system



Select to do an immediate reboot or shutdown

LOAD BALANCING CONFIGURATION

Used to specify a method for Load Balancing



Algorithms

Choose a method for load balancing

- ● Round Robin
- ○ Response Time
- ○ Fastest Route
- ○ Weighted

Round Robin algorithm balances sessions in a simple rotating order.

Copyright © 2000-2016. FatPipe Networks Inc.

Four methods of Load Balancing:

Round Robin

Response Time

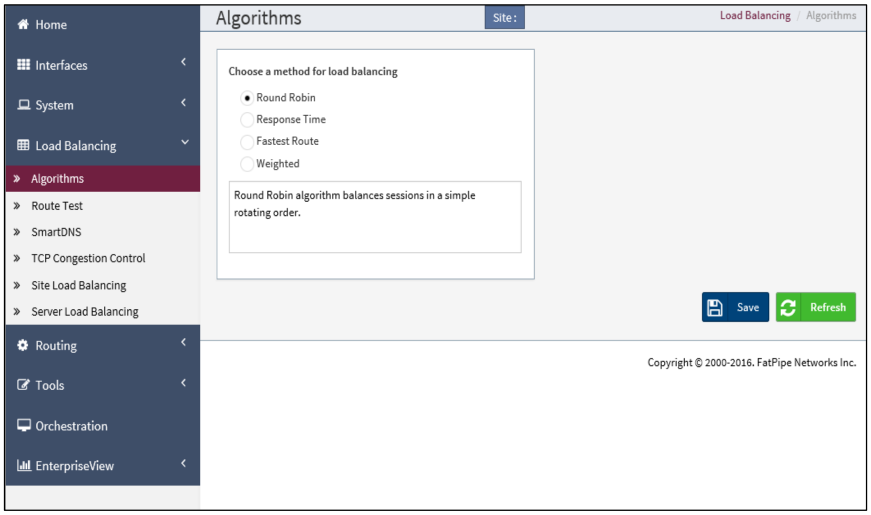
Fastest Route

Weighted

Click on each method for more Info…

LOAD BALANCING CONFIGURATION

Used to specify a method for Load Balancing



Algorithms

Choose a method for load balancing

- ● Round Robin
- ○ Response Time
- ○ Fastest Route
- ○ Weighted

Round Robin algorithm balances sessions in a simple rotating order.

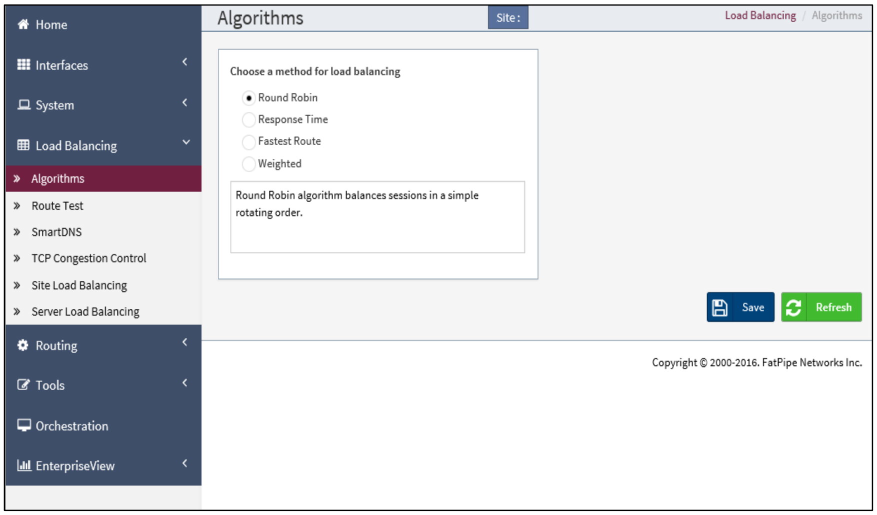
Copyright © 2000-2016. FatPipe Networks Inc.

Round Robin

Round Robin configures FatPipe MPVPN to send sessions down links in rotating order. This method is recommended for similar speed connections to the Internet, even if the connections are not of the same ISP (e.g. two similar speed fractional T1s and a DSL line).

LOAD BALANCING CONFIGURATION

Used to specify a method for Load Balancing



Choose a method for load balancing

- ● Round Robin
- ○ Response Time
- ○ Fastest Route
- ○ Weighted

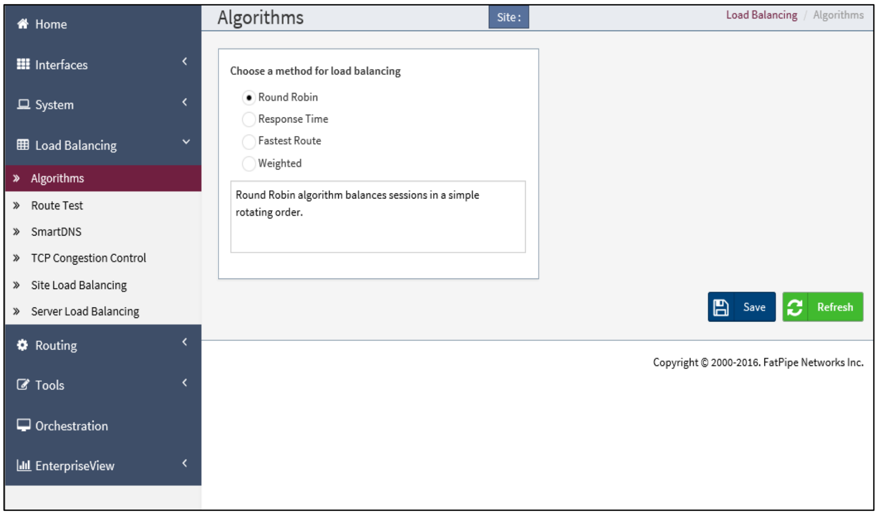
Round Robin algorithm balances sessions in a simple rotating order.

Response Time

Response Time will balance traffic based on each link's average response time for Internet requests. This method is recommended for unequal speed connections. The link with the smallest syn/syn-ack time delta will be used more often with Response Time.

LOAD BALANCING CONFIGURATION

Used to specify a method for Load Balancing



Choose a method for load balancing

- ● Round Robin
- ○ Response Time
- ○ Fastest Route
- ○ Weighted

Round Robin algorithm balances sessions in a simple rotating order.

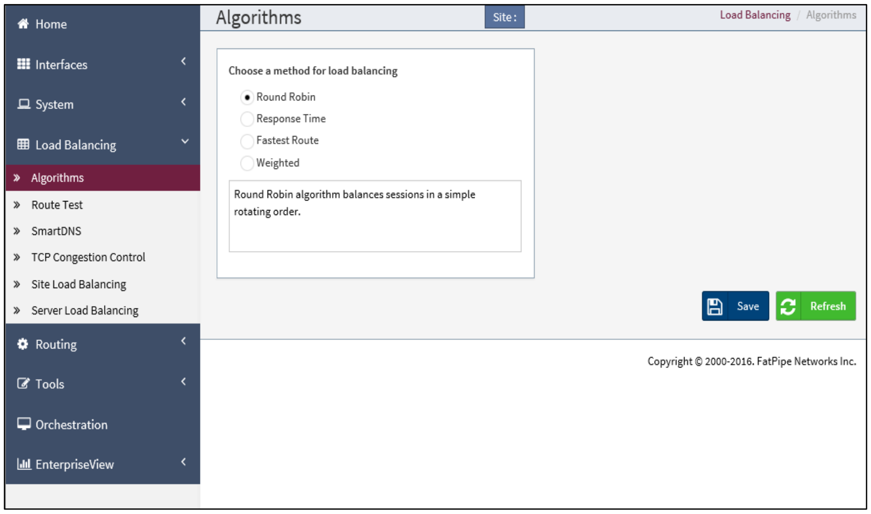
Fastest Route

Fastest Route will balance traffic on a per-destination host basis.

Syn packets get sent out of all interfaces, which ever interface's syn-ack "wins the race back" will get used here.

LOAD BALANCING CONFIGURATION

Used to specify a method for Load Balancing



Choose a method for load balancing

- ● Round Robin
- ○ Response Time
- ○ Fastest Route
- ○ Weighted

Round Robin algorithm balances sessions in a simple rotating order.

Copyright © 2000-2016. FatPipe Networks Inc.

Weighted

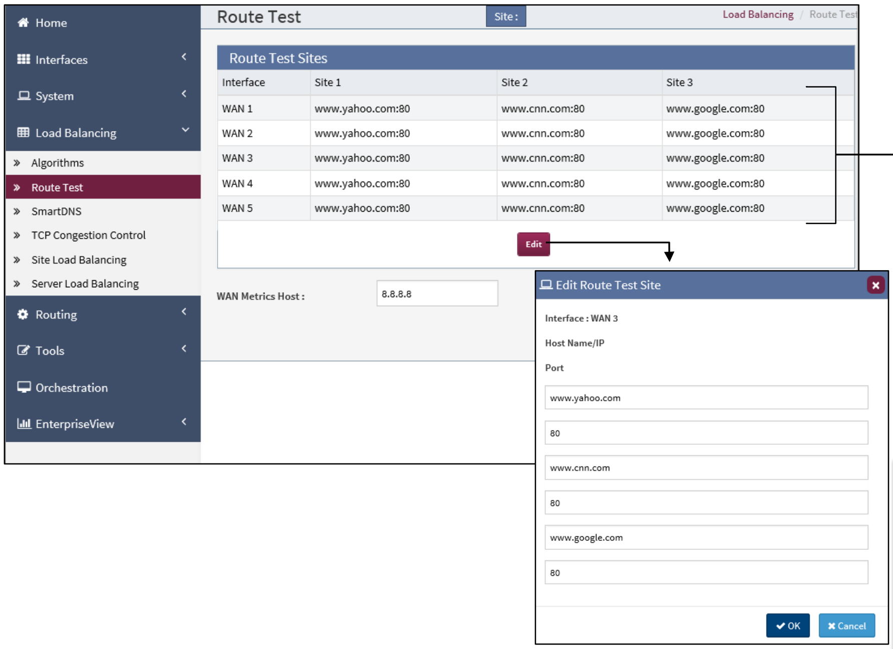
⇩

Weighted will balance traffic on a arbitrary percentage rise basis in comparison from 1 interface to another (opposite of costing)

If you were wanting to weight based on available bandwidth & had a 1.5mb T1; a 7mb DSL link; and a 50mb cable link you could weight 1, 7 , and 50 accordingly.

ROUTE TEST CONFIGURATION

Used to test the availability of the Internet (WAN) connections



Route Test Sites

Interface	Site 1	Site 2	Site 3
WAN 1	www.yahoo.com:80	www.cnn.com:80	www.google.com:80
WAN 2	www.yahoo.com:80	www.cnn.com:80	www.google.com:80
WAN 3	www.yahoo.com:80	www.cnn.com:80	www.google.com:80
WAN 4	www.yahoo.com:80	www.cnn.com:80	www.google.com:80
WAN 5	www.yahoo.com:80	www.cnn.com:80	www.google.com:80

WAN Metrics Host : 8.8.8.8

Edit Route Test Site

Interface : WAN 3

Host Name/IP

Port

www.yahoo.com

80

www.cnn.com

80

www.google.com

80

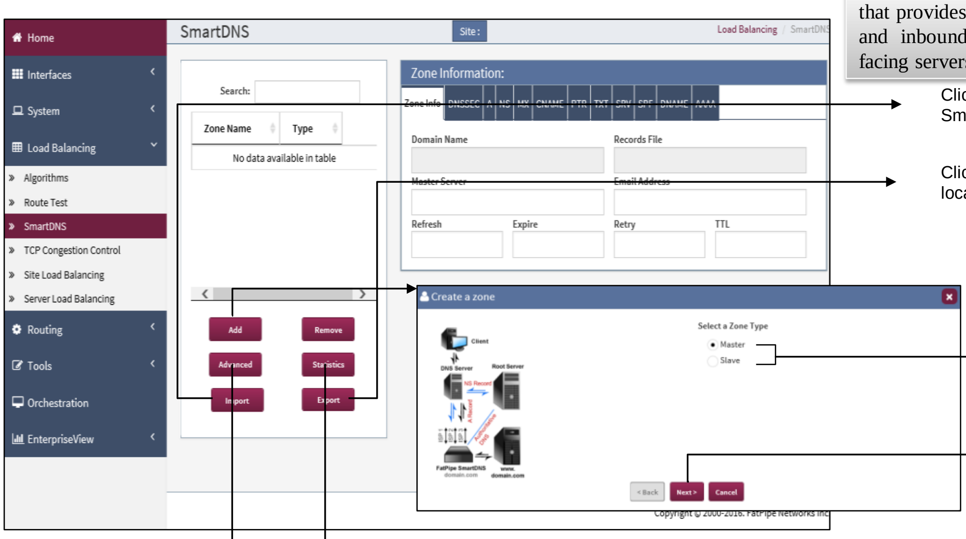
Add the details about the interface to all Sites

FatPipe MPVPN tests connections to the router, to the Internet Service Provider, and to a maximum of three user-specified sites on the Internet. Each site can be specified using a domain name or an IP address.

SMARTDNS CONFIGURATION

SmartDNS with master zone information

SmartDNS is a patented technology that provides inbound load balancing and inbound redundancy to public facing servers in the LAN.



No data available in table

● Master
○ Slave

Copyright © 2000-2016. FatPipe Networks Inc

Click to Import zone files to SmartDNS

Click to export DNS zone files locally

Select the option Master

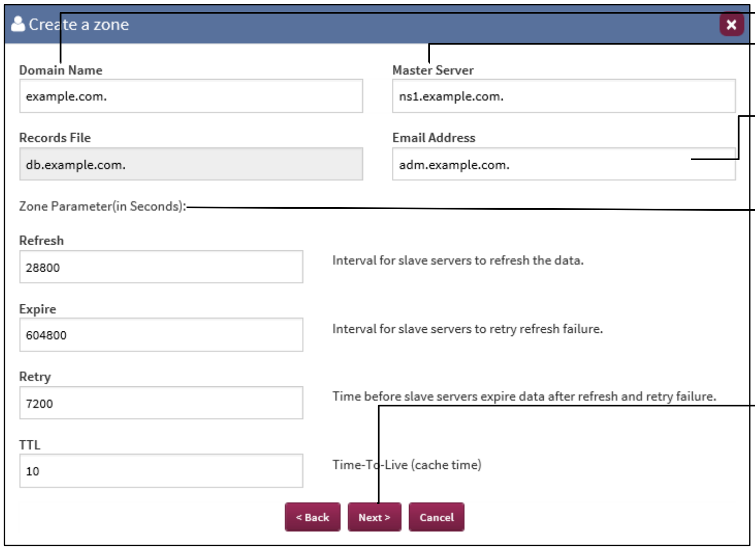
To create a master zone

View the record of SmartDNS statistics for all the zones

Click to configure advanced settings

SMARTDNS CONFIGURATION

Domain Name, Master Server, Email Address information for master zone



Domain Name: example.com.

Master Server: ns1.example.com.

Records File: db.example.com.

Email Address: adm.example.com.

Zone Parameter(in Seconds):

Refresh: 28800 — Interval for slave servers to refresh the data.

Expire: 604800 — Interval for slave servers to retry refresh failure.

Retry: 7200 — Time before slave servers expire data after refresh and retry failure.

TTL: 10 — Time-To-Live (cache time)

Zone name

Primary Name Server

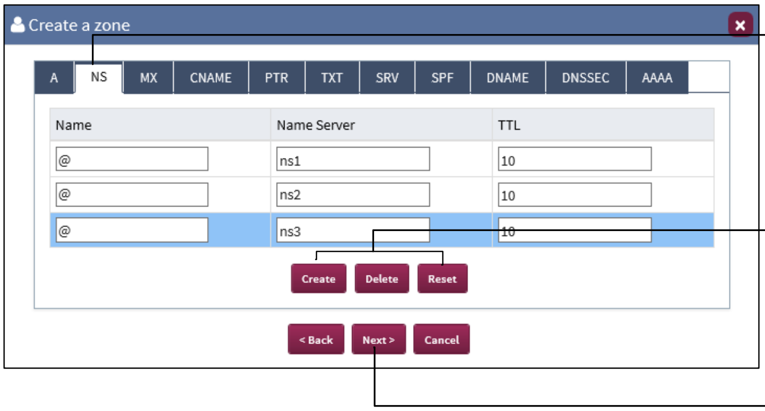
Administrative Contact

SOA values for your zone (rarely do you need to change the defaults)

To add the record information for master zone

SMARTDNS CONFIGURATION

Create record information for master zone



Name	Name Server	TTL
@	ns1	10
@	ns2	10
@	ns3	10

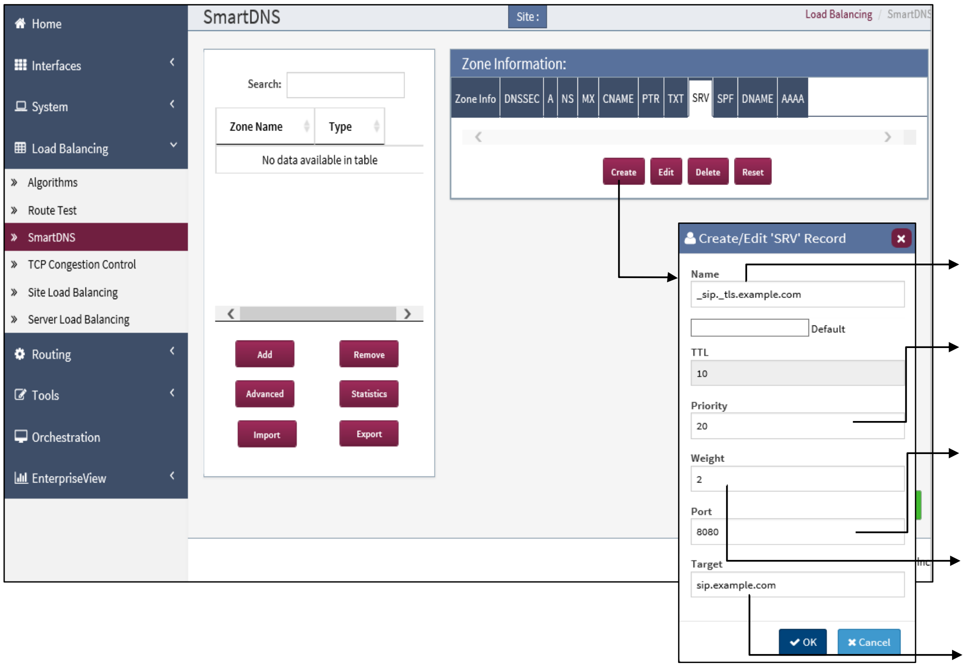
Click on any one of these buttons, to configure different types of records for master zone

Add/Edit or delete record information

To show SmartDNS configuration with master zone record information

SMARTDNS CONFIGURATION

Create record information for master zone



Name: _sip._tls.example.com

Default

TTL: 10

Priority: 20

Weight: 2

Port: 8080

Target: sip.example.com

Enter the host name

Priority determines in what order the client should use which serverif there is more than one SRV record for a given service

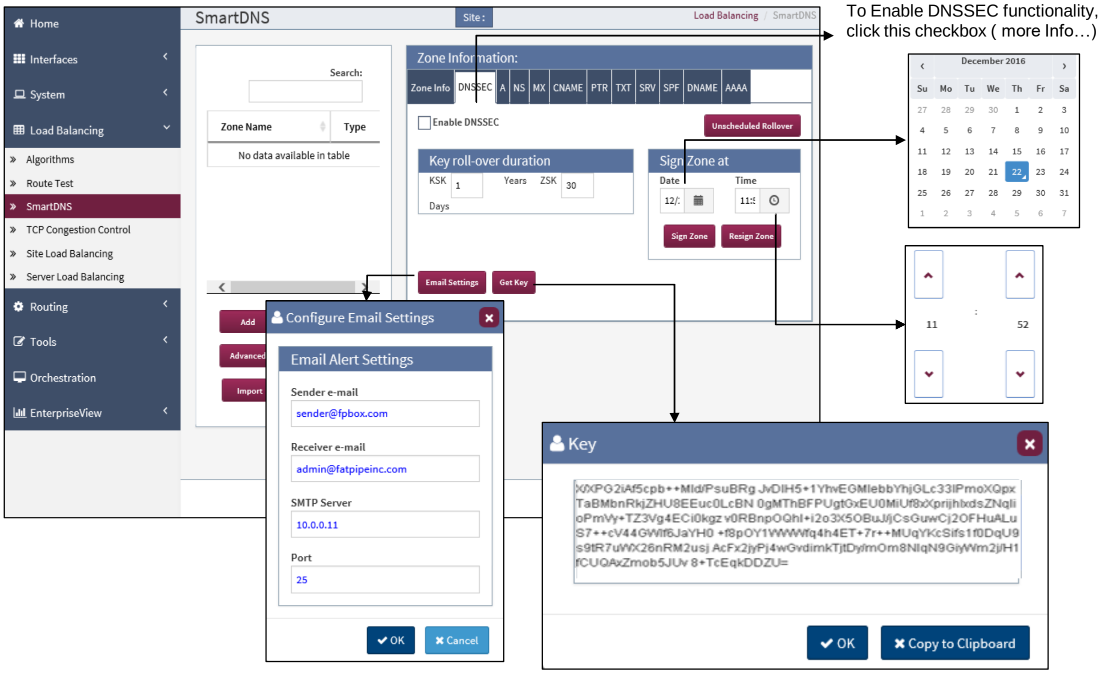
Port determines the number , the service is run through on the machine providing it

If 2 SRV records exist for the same service at the same priority, traffic will be directed to them in proportion to the weight

Target host this traffic should go to

SMARTDNS CONFIGURATION

Using DNSSEC to secure master zone



KSK 1 Years, ZSK 30 Days

Sign Zone at: Date 12/: Time 11:!

Su	Mo	Tu	We	Th	Fr	Sa
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

11 : 52

Sender e-mail: sender@fpbox.com

Receiver e-mail: admin@fatpipeinc.com

SMTP Server: 10.0.0.11

Port: 25

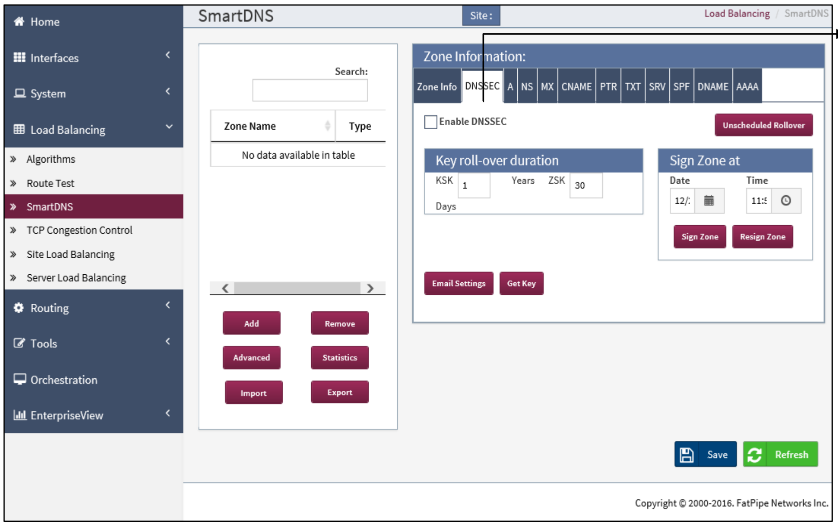
X/XPG2iAf5cpb++Mld/PsuBRg JvDIH5+1YhvEGMlebbYhjGLc33lPmoXQpx
TaBMbnRkjZHU8EEuc0LcBN 0gMThBFPUgtGxEU0MiUf8xXprijhlxdsZNqli
oPmVy+TZ3Vg4ECi0kgz v0RBnpOQhl+i2o3X5OBuJ/jCsGuwCj2OFHuALu
S7++cV44GWlf6JaYH0 +f8pOY1WWWfq4h4ET+7r++MUqYKcSifs1f0DqU9
s9tR7uWX26nRM2usj AcFx2jyPj4wGvdimkTjtDy/mOm8NlqN9GiyWm2j/H1
fCUQAxZmob5JUv 8+TcEqkDDZU=

To Enable DNSSEC functionality, click this checkbox (more Info…)

Click on each box for more Info…

SMARTDNS CONFIGURATION

Using DNSSEC to secure master zone



KSK 1 Years, ZSK 30 Days

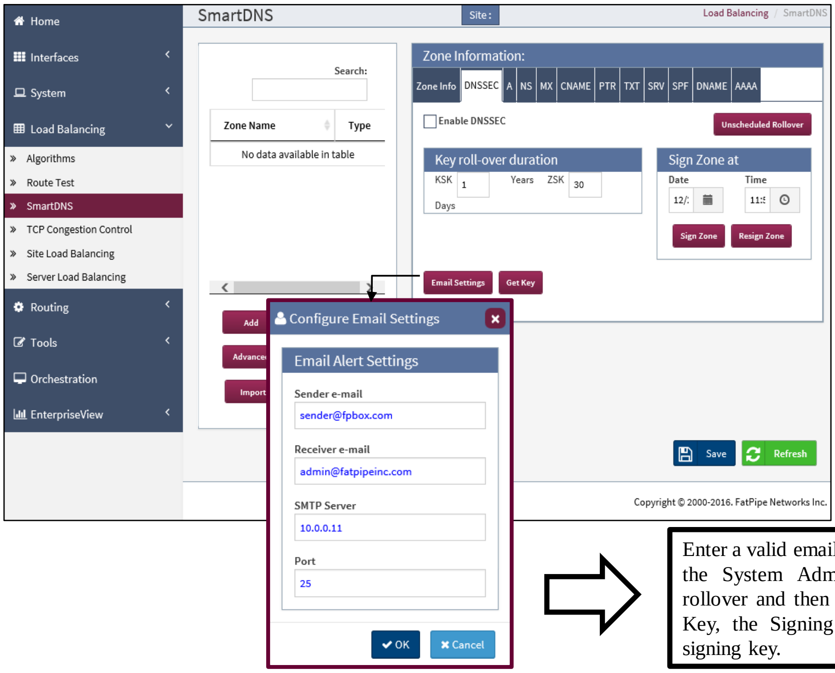
To Enable DNSSEC functionality, click this checkbox

The Domain Name System Security Extensions (DNSSEC) deals with cache poisoning and a set of other DNS vulnerabilities such as "Man in the Middle“ attacks and data modification in authoritative servers. Its major objective is to provide the ability to validate the authenticity and integrity of DNS messages in such a way that tampering with the DNS information anywhere in the DNS system can be detected.

Enter the KSK rollover duration in years (by default it is 1 year). Enter ZSK rollover duration in days - usually it is 90 days.

SMARTDNS CONFIGURATION

Using DNSSEC to secure master zone



□ Enable DNSSEC

Key roll-over duration: KSK 1 Years, ZSK 30 Days

Sign Zone at: Date 12/: Time 11:!

Sender e-mail: sender@fpbox.com

Receiver e-mail: admin@fatpipeinc.com

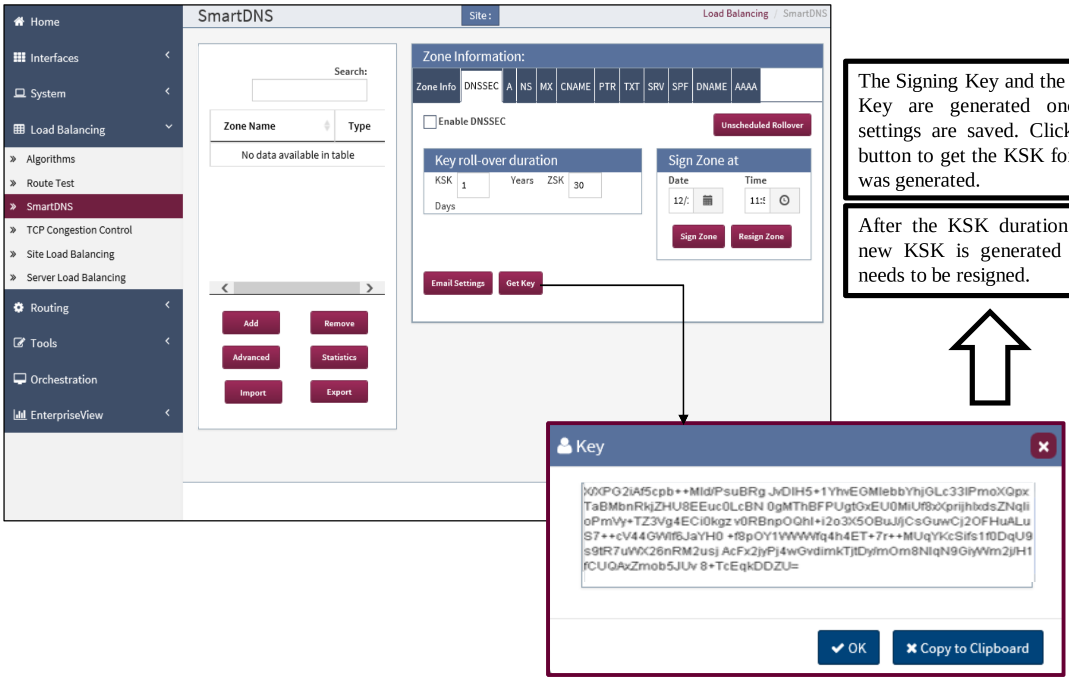
SMTP Server: 10.0.0.11

Port: 25

Enter a valid email address to notify the System Administrator about the rollover and then Save to generate the Key, the Signing Key and the Zone signing key.

SMARTDNS CONFIGURATION

Using DNSSEC to secure master zone



□ Enable DNSSEC

Key roll-over duration: KSK 1 Years, ZSK 30 Days

Sign Zone at: Date 12/: Time 11:!

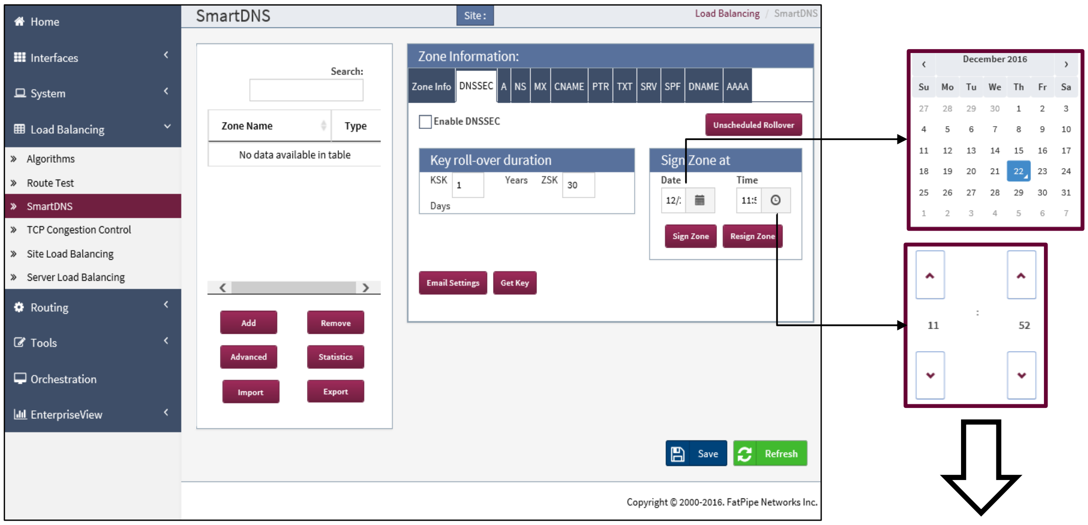
X/XPG2iAf5cpb++Mld/PsuBRg JvDIH5+1YhvEGMlebbYhjGLc33IPmoXQpx
TaBMbnRkjZHU8EEuc0LcBN 0gMThBFPUgtGxEU0MiUf8xXprijhlxdsZNqli
oPmVy+TZ3Vg4ECi0kgz v0RBnpOQhl+i2o3X5OBuJ/jCsGuwCj2OFHuALu
S7++cV44GWlf6JaYH0 +f8pOY1WWWfq4h4ET+7r++MUqYKcSifs1f0DqU9
s9tR7uWX26nRM2usj AcFx2jyPj4wGvdimkTjtDy/mOm8NIqN9GiyWm2j/H1
fCUQAxZmob5JUv 8+TcEqkDDZU=

The Signing Key and the Zone signing Key are generated once the email settings are saved. Click on Get Key button to get the KSK for the zone that was generated.

After the KSK duration is expired, a new KSK is generated and the zone needs to be resigned.

SMARTDNS CONFIGURATION

Using DNSSEC to secure master zone



☐ Enable DNSSEC

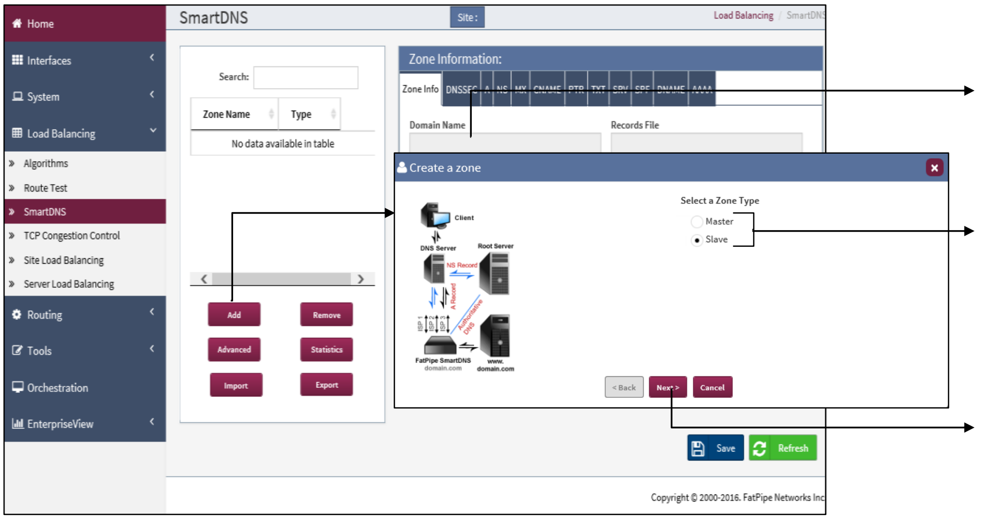
Key roll-over duration: KSK 1 Years, ZSK 30 Days

Sign Zone at: Date 12/: Time 11:5

To sign the zone, select the date and time and click the Sign Zone button. The zone signing will happen at the date and time specified

SMARTDNS CONFIGURATION

SmartDNS with slave zone information



Select a Zone Type

○ Master

● Slave

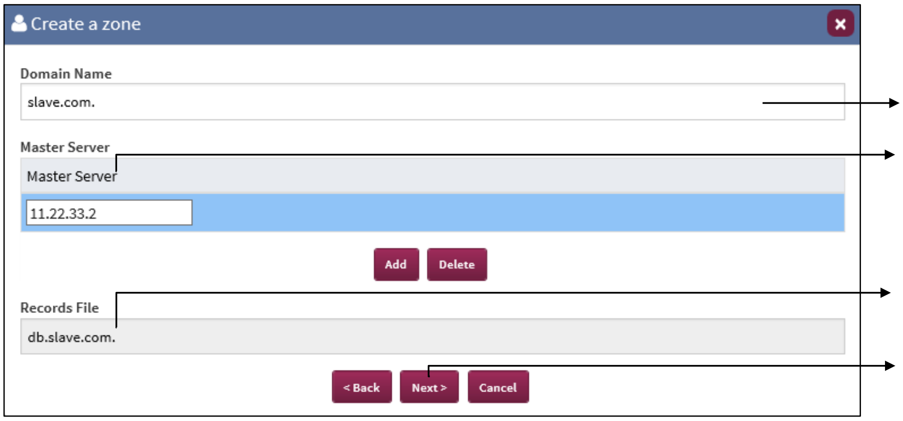
Primary Name Server

Select the option Slave

To create a slave zone

SMARTDNS CONFIGURATION

Domain Name, Master Server IP address and Records File information for slave zone



Domain Name: slave.com.

Master Server: 11.22.33.2

Records File: db.slave.com.

Domain name for the zone

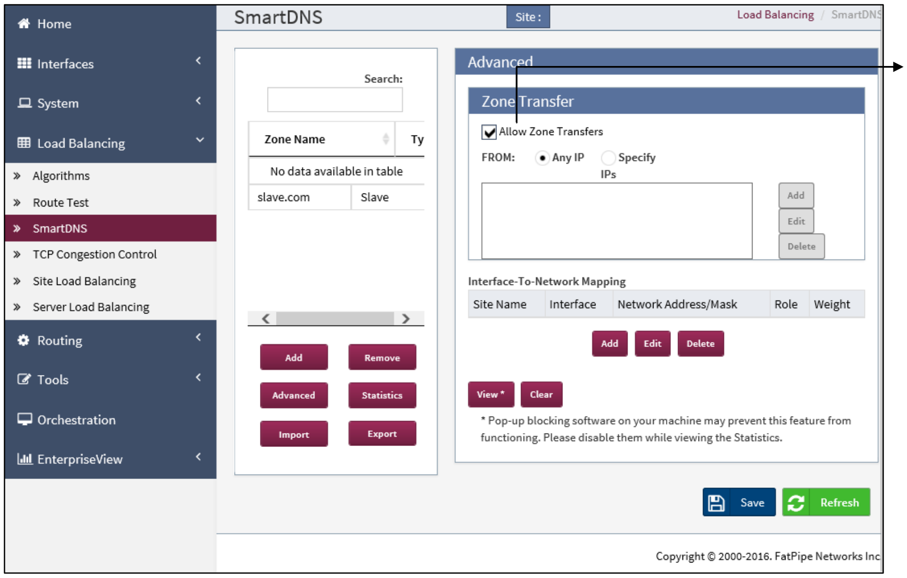
Master Server IP address

Records file information

To show SmartDNS configuration with slave zone record information

SMARTDNS CONFIGURATION

Zone transfers information



Zone Name	Ty
No data available in table	
slave.com	Slave

☑ Allow Zone Transfers

FROM: ● Any IP ○ Specify IPs

Interface-To-Network Mapping

Site Name	Interface	Network Address/Mask	Role	Weight

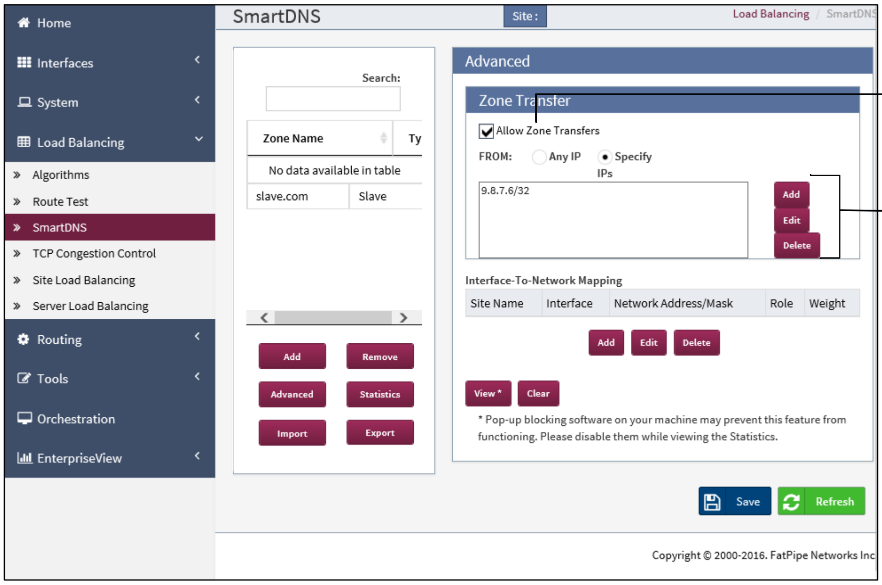
* Pop-up blocking software on your machine may prevent this feature from functioning. Please disable them while viewing the Statistics.

Copyright © 2000-2016. FatPipe Networks Inc

If you have slave servers that will initiate zone transfers, then enable “Allow Zone Transfers”. If you want to allow zone transfers from any IP in the internet, choose “Any IP”

SMARTDNS CONFIGURATION

Zone transfers information



Zone Name	Ty
No data available in table	
slave.com	Slave

☑ Allow Zone Transfers

FROM: ○ Any IP ● Specify IPs

9.8.7.6/32

Site Name	Interface	Network Address/Mask	Role	Weight

* Pop-up blocking software on your machine may prevent this feature from functioning. Please disable them while viewing the Statistics.

Copyright © 2000-2016. FatPipe Networks Inc.

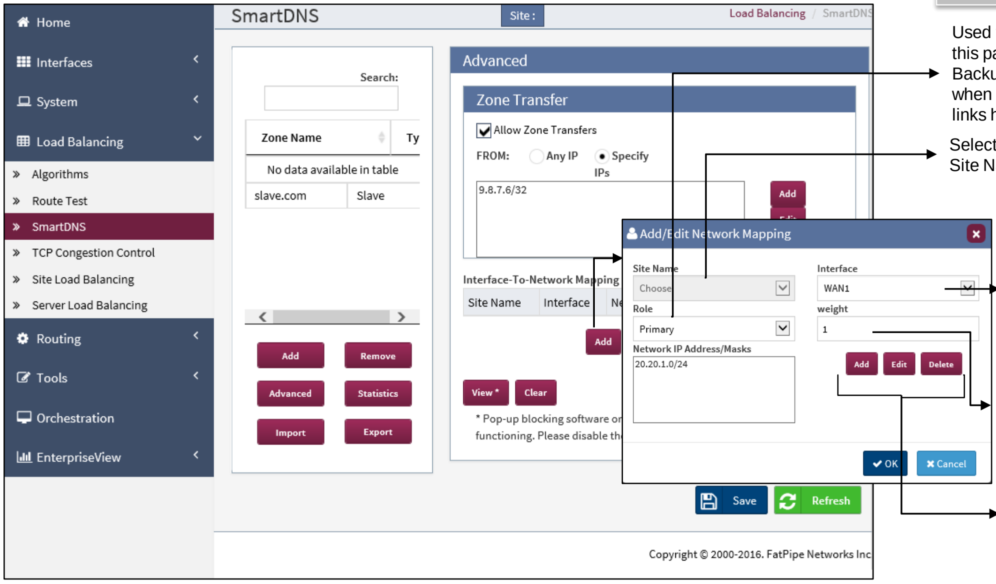
Create an ACL for only specific IP's to be able to perform zone transfers

Add/Edit/Delete IPs from which zone transfer should be allowed

SMARTDNS CONFIGURATION

The mappings are used as a filtering table, so when a WAN link takes a hit, effected addresses can be filtered off before we advertise them

Interface-To-Network Mappings



Zone Name	Ty
No data available in table	
slave.com	Slave

☑ Allow Zone Transfers

FROM: ○ Any IP ● Specify IPs

9.8.7.6/32

Site Name: Choose

Interface: WAN1

Role: Primary

weight: 1

Network IP Address/Masks: 20.20.1.0/24

* Pop-up blocking software on your machine may prevent this feature from functioning. Please disable th

Copyright © 2000-2016. FatPipe Networks Inc.

Used to assign a role to this particular mapping; Backup links only get used when all of the primary links have gone down

Select the particular Site Name

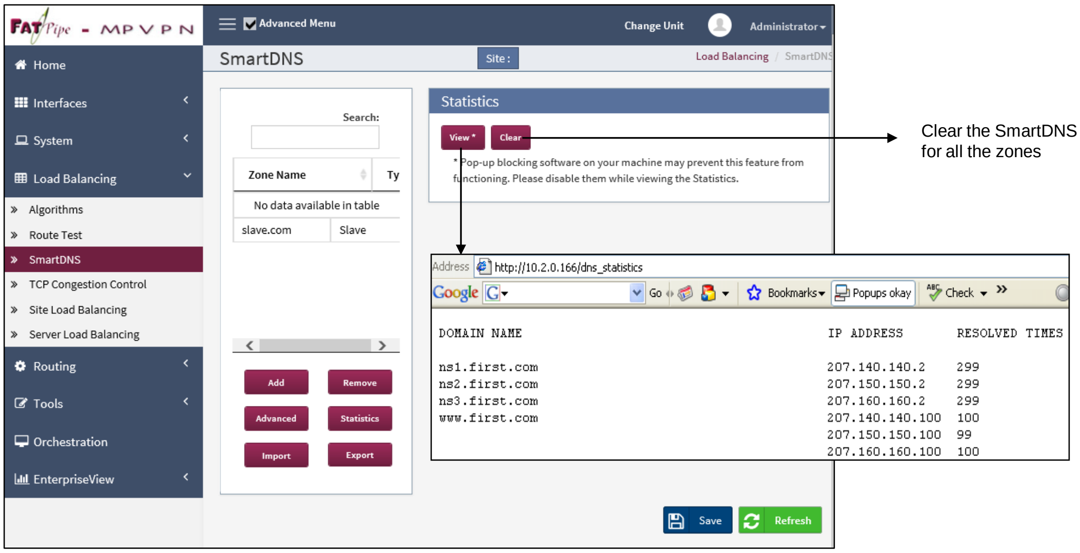
Used to correlate a physical interface to a subnet

Weight affects balancing & how often IPs from this link are handed out in DNS requests

Add/Edit IP Address/Mask

SMARTDNS CONFIGURATION

Used to view SMARTDNS Statistics



Zone Name	Ty
No data available in table	
slave.com	Slave

* Pop-up blocking software on your machine may prevent this feature from functioning. Please disable them while viewing the Statistics.

http://10.2.0.166/dns_statistics

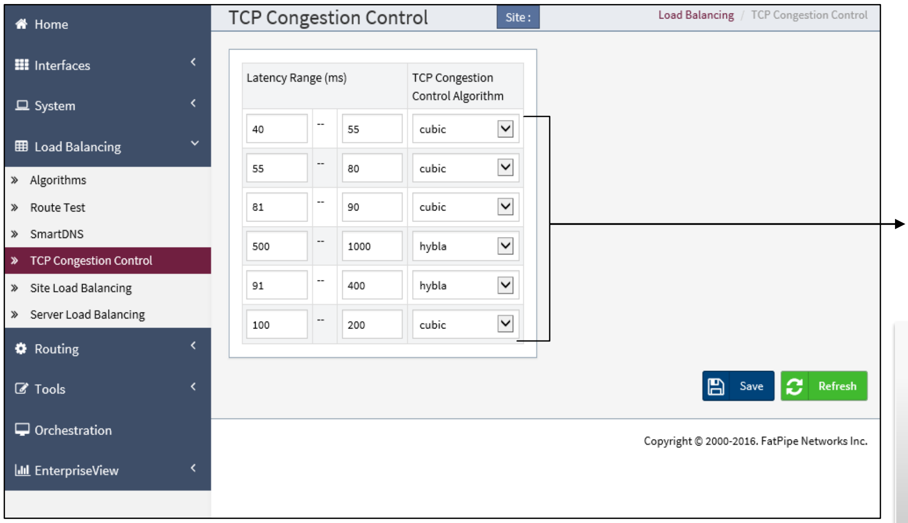
```
DOMAIN NAME                               IP ADDRESS       RESOLVED TIMES

ns1.first.com                             207.140.140.2    299
ns2.first.com                             207.150.150.2    299
ns3.first.com                             207.160.160.2    299
www.first.com                             207.140.140.100  100
                                          207.150.150.100  99
                                          207.160.160.100  100
```

Clear the SmartDNS statistics for all the zones

TCP CONGESTION CONTROL

Used to configure TCP Congestion Control



Latency Range (ms)			TCP Congestion Control Algorithm
40	--	55	cubic
55	--	80	cubic
81	--	90	cubic
500	--	1000	hybla
91	--	400	hybla
100	--	200	cubic

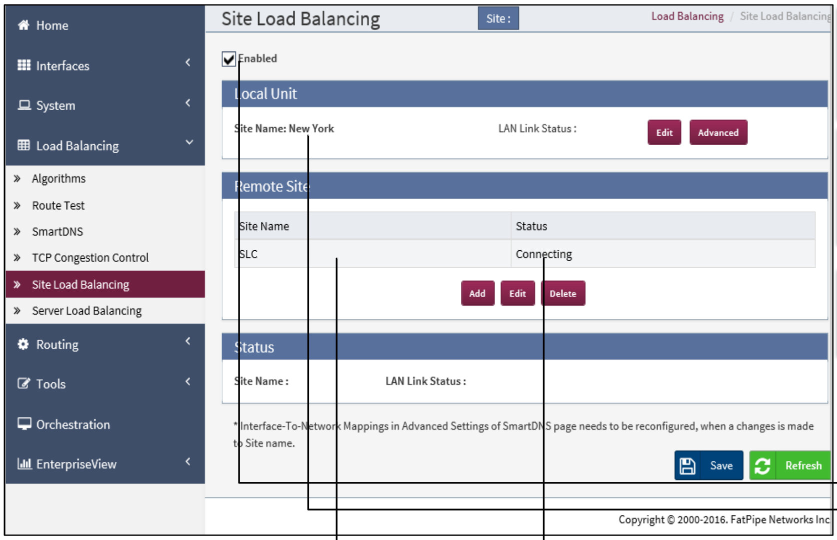
Copyright © 2000-2016. FatPipe Networks Inc.

Specify the congestion control algorithms

With FatPipe's TCP Congestion Control feature, you can select the Congestion Avoidance Algorithm for different network latency ranges. Use the FatPipe defined Congestion Control Algorithms listed. By default, the latency ranges and Congestion Control Algorithms mapped to those is defined by FatPipe.

SITE LOAD BALANCING

Used to configure Site Load Balancing



Site Load Balancing

☑ Enabled

Local Unit

Site Name: New York   LAN Link Status :

Remote Site

Site Name	Status
SLC	Connecting

Status

Site Name :   LAN Link Status :

*Interface-To-Network Mappings in Advanced Settings of SmartDNS page needs to be reconfigured, when a changes is made to Site name.

Copyright © 2000-2016. FatPipe Networks Inc.

Using site load balancing, SmartDNS gains a replication facility for DNS zones, changes, and a location abstraction for balancing

Site Load Balancing allows for Site Failover between servers located in geographically separate locations that have a shared/replicated storage substrate

Site Load Balancing can provide distributed balancing utilizing all links available at each site.

Select to enable Site load balancing

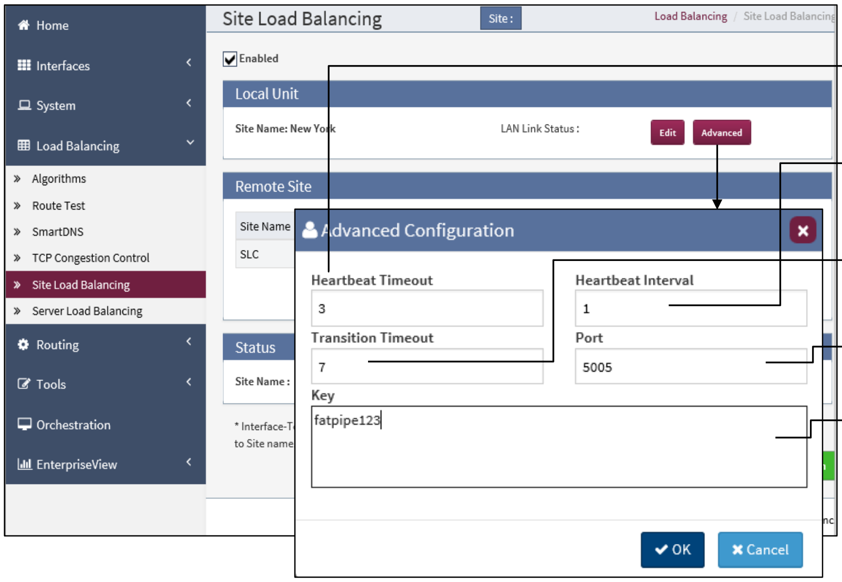
Enter the local site name

Displays the link status of all interface in both site

Select the remote site name

SITE LOAD BALANCING

Used to configure Site Load Balancing



Site Load Balancing

☑ Enabled

Local Unit

Site Name: New York   LAN Link Status :

Site Name
SLC

Site Name :

* Interface-T
to Site name

Advanced Configuration

Heartbeat Timeout: 3

Heartbeat Interval: 1

Transition Timeout: 7

Port: 5005

Key: fatpipe123

Specifies the time to wait for a heartbeat a peer before determining that the connection to the peer is lost

Time interval between two heartbeats sent from this unit to other peers.

Time interval after a line has failed during which connectivity problems will be ignored.

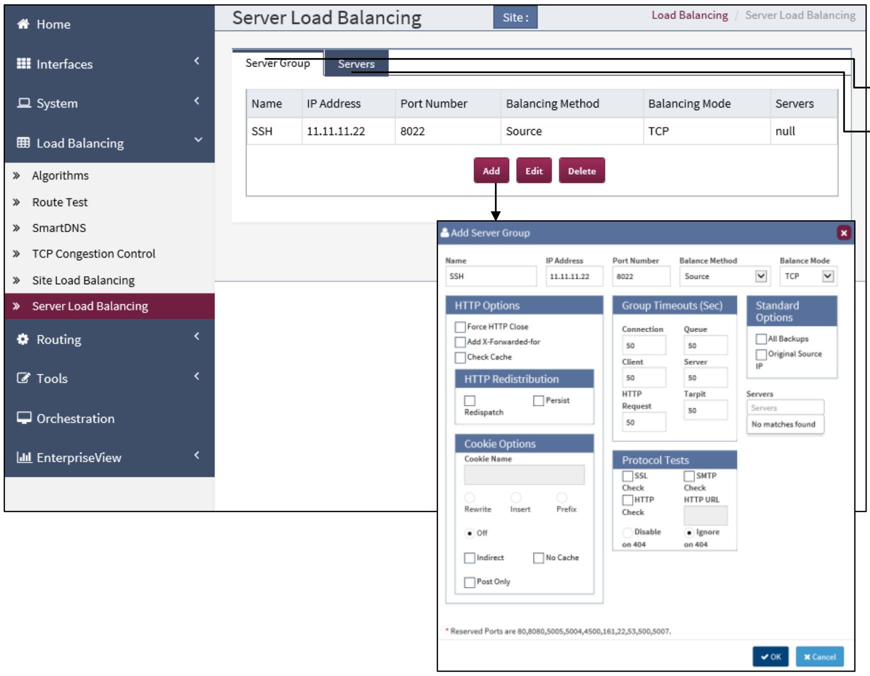
The port number used for communication between peers.

The Secret Key used for securing the communication between peers.

The heartbeat is a small network packet sent periodically between peers. It keeps each peer updated with the status of other peers.

SERVER LOAD BALANCING

Used to configure Server Load Balancing



Name	IP Address	Port Number	Balancing Method	Balancing Mode	Servers
SSH	11.11.11.22	8022	Source	TCP	null

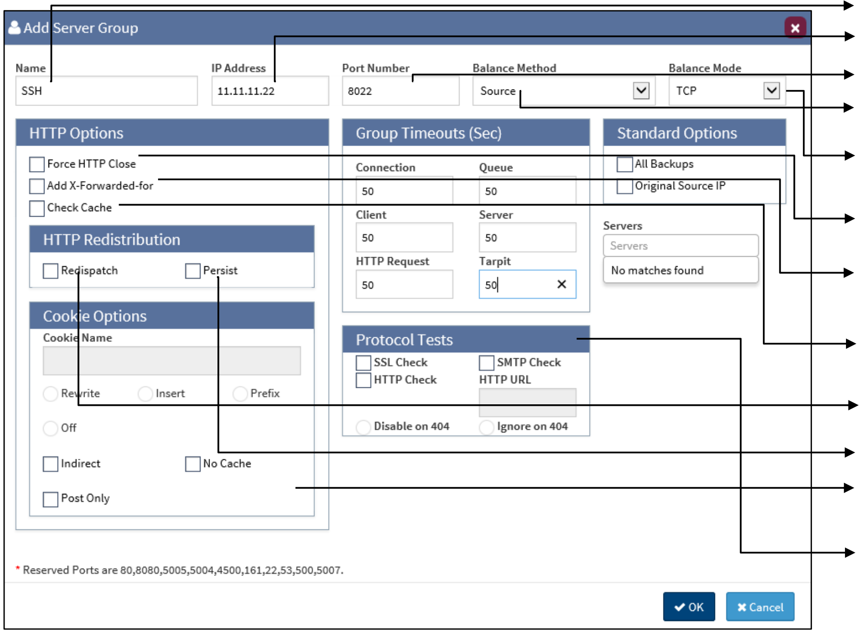
To create and manage Server groups

To create and manage Servers

Server Load Balancing provides a scalable model for any number of servers, server groups and inbound connections. It allows to seamlessly integrating servers into your architecture without any downtime.

SERVER LOAD BALANCING

Used to configure Server Load Balancing



Add Server Group

Name: SSH

IP Address: 11.11.11.22

Port Number: 8022

Balance Method: Source

Balance Mode: TCP

HTTP Options
- □ Force HTTP Close
- □ Add X-Forwarded-for
- □ Check Cache

HTTP Redistribution
- □ Redispatch
- □ Persist

Cookie Options

Cookie Name

○ Rewrite ○ Insert ○ Prefix

○ Off

□ Indirect □ No Cache

□ Post Only

Group Timeouts (Sec)

Connection: 50

Queue: 50

Client: 50

Server: 50

HTTP Request: 50

Tarpit: 50

Protocol Tests
- □ SSL Check
- □ SMTP Check
- □ HTTP Check

HTTP URL

○ Disable on 404 ○ Ignore on 404

Standard Options
- □ All Backups
- □ Original Source IP

Servers

No matches found

* Reserved Ports are 80,8080,5005,5004,4500,161,22,53,500,5007.

Specify the name for the server group

Specify the IP address of the server group

Specify the Port # used for this application

Select the Balance Method

Select the Balance Mode

Enabling this flag ensures that the HTTP connection is closed after each response.

Add 'X-Forwarded-For' header to the requests sent to servers

Enable deep inspection of all server responses for strict compliance with HTTP specification in terms of cache ability.

Ensures session redistribution in case of connection failure.

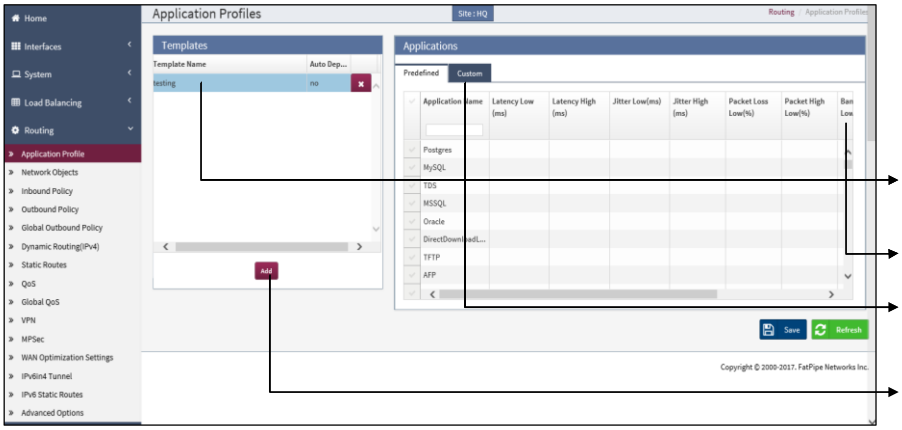
Ensures forced persistence on servers that are down.

Cookie configuration

Server sanity validation

APPLICATION PROFILE

Used to define line conditions for Policy Routing Rules



Template Name	Auto Dep...
testing	no

Application Name	Latency Low (ms)	Latency High (ms)	Jitter Low(ms)	Jitter High (ms)	Packet Loss Low(%)	Packet High Low(%)	Ban Low
Postgres							
MySQL							
TDS							
MSSQL							
Oracle							
DirectDownloadL...							
TFTP							
AFP							

Copyright © 2000-2017. FatPipe Networks Inc.

Name to be given for any specific template

Line conditions

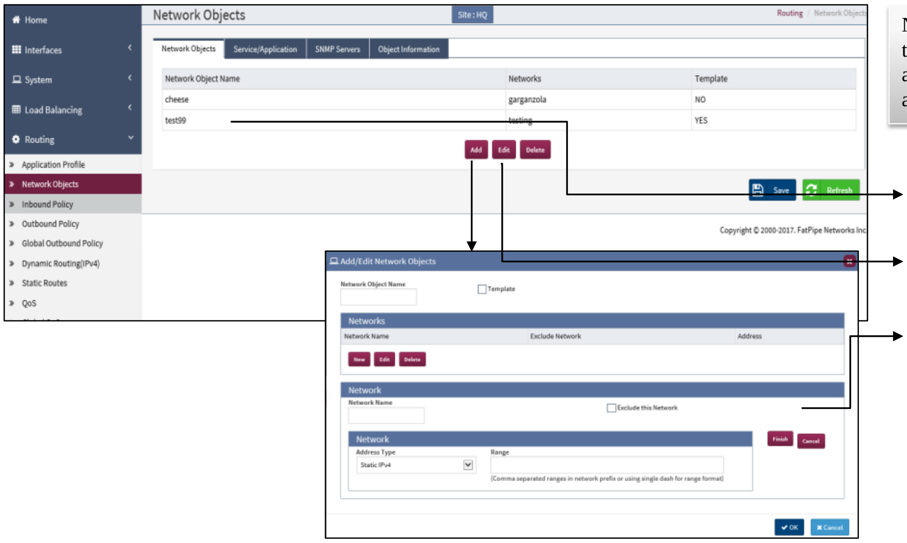
Used to define an Application name

To add a new template name

Application Profile feature on FatPipe can be used to define several line conditions with separate template name and can be used where ever required in Policy Routing Rules

NETWORK OBJECTS

Used to replace IP addresses without re-entering the whole data



Network Object Name	Networks	Template
cheese	garganzola	NO
test99	testing	YES

Network Name	Exclude Network	Address

(Comma separated ranges in network prefix or using single dash for range format)

Copyright © 2000-2017. FatPipe Networks Inc.

Name to be given for a Network Object

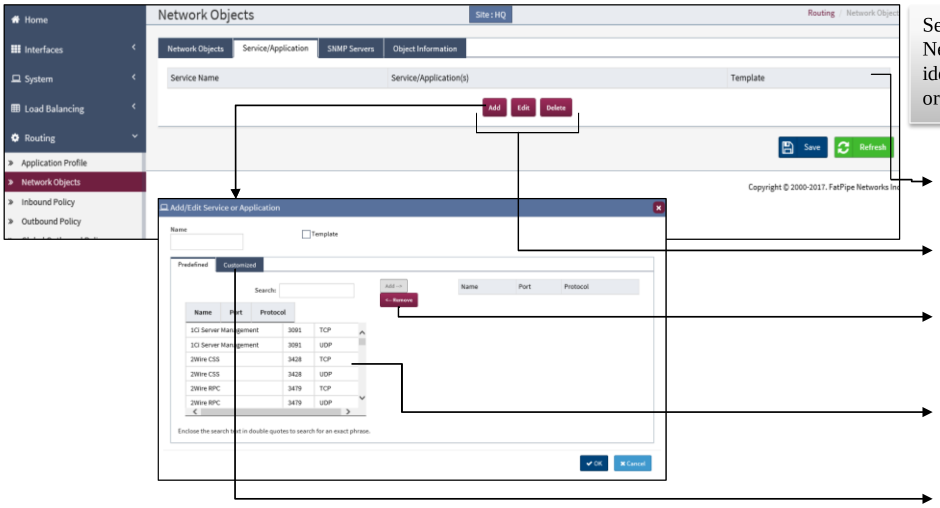
To add, edit or delete a Network Object.

To add a new network to the list of networks existing.

Network Objects makes it easy to replace existing private IP addresses with new private IP addresses

NETWORK OBJECTS

Used to replace IP addresses without re-entering the whole data



Service or Application in Network Objects is used to identify using port number used or protocol

Details about the service

To add, edit or delete a Network Object.

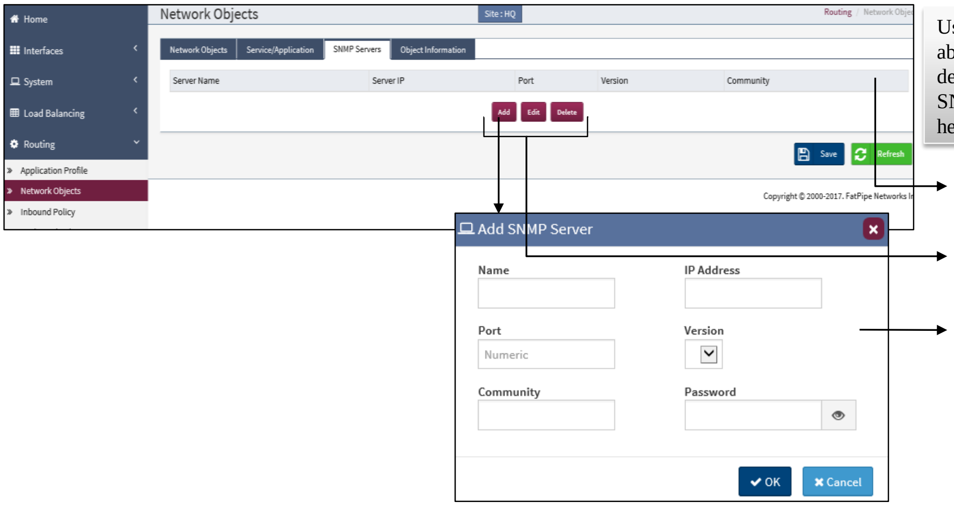
To add or remove pre-existing applications

Select a pre-existing application with port number and protocol

Used to add Service Name manually, select protocol and enter port number

NETWORK OBJECTS

Used to replace IP addresses without re-entering the whole data



Used to gather information about routes from other SNMP devices in the network. All the SNMP servers can be added here.

Details about the service

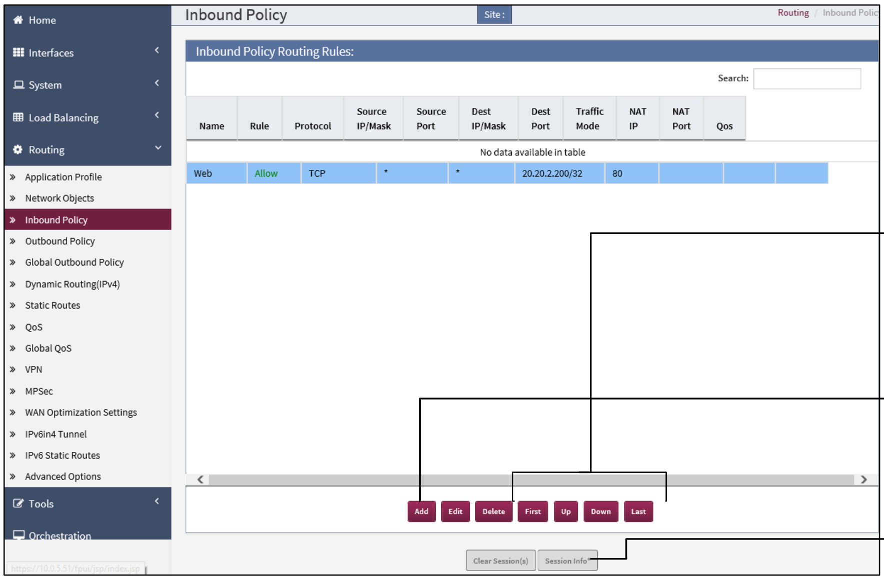
To add, edit or delete an SNMP server details

To add SNMP server details on FatPipe

INBOUND POLICY CONFIGURATION

Used to direct inbound traffic based on specific criteria

Inbound Policies are used to:
- •Allow traffic from the WAN to the LAN
- •Build inbound NAT's from one subnet to another
- •Build inbound ACL's
- •Route traffic from 1 WAN to another



Inbound Policy

Inbound Policy Routing Rules:

Name	Rule	Protocol	Source IP/Mask	Source Port	Dest IP/Mask	Dest Port	Traffic Mode	NAT IP	NAT Port	Qos
No data available in table										
Web	Allow	TCP	*	*	20.20.2.200/32	80				

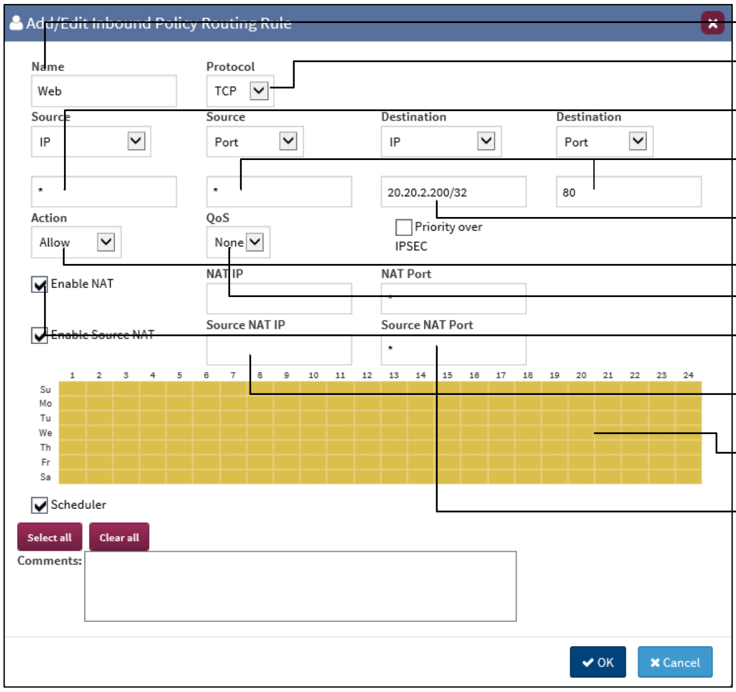
Policies get processed top down, these buttons are used to modify policy order

To add a new inbound policy routing rule

View all sessions that match the selected inbound policy rule

INBOUND POLICY CONFIGURATION

Add Inbound Policy rule based on specific criteria



Add/Edit Inbound Policy Routing Rule

Name: Web

Protocol: TCP

Source: IP — *

Source: Port — *

Destination: IP — 20.20.2.200/32

Destination: Port — 80

Action: Allow

QoS: None

□ Priority over IPSEC

☑ Enable NAT

NAT IP:

NAT Port: *

☑ Enable Source NAT

Source NAT IP:

Source NAT Port: *

☑ Scheduler

Comments:

Give each rule a unique name. (more Info…)

Choose an IP protocol from the list (more Info…)

Specify a source IP and mask (more Info…)

Specify a port number or range(more Info…)

Specify a destination IP and mask (more Info…)

Choose "Allow" or "Deny“ (more Info…)

Choose a pre-defined QoS rule (more Info…)

Check this box if you want to NAT traffic that matches this rule

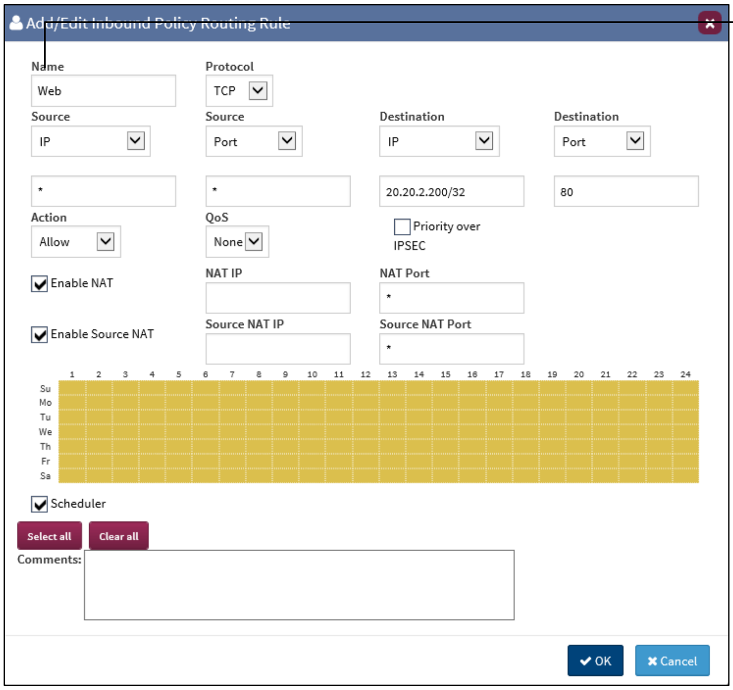
Specify a source IP and mask (more Info…)

Select the day of week & time of day the policy is to be implemented (more Info…)

Specify the port number the traffic will be mapped to (more Info…)

INBOUND POLICY CONFIGURATION

Add Inbound Policy rule based on specific criteria



Add/Edit Inbound Policy Routing Rule

Name: Web

Protocol: TCP

Source: IP

Source: Port

Destination: IP

Destination: Port

*

*

20.20.2.200/32

80

Action: Allow

QoS: None

□ Priority over IPSEC

☑ Enable NAT

NAT IP:

NAT Port: *

☑ Enable Source NAT

Source NAT IP:

Source NAT Port: *

☑ Scheduler

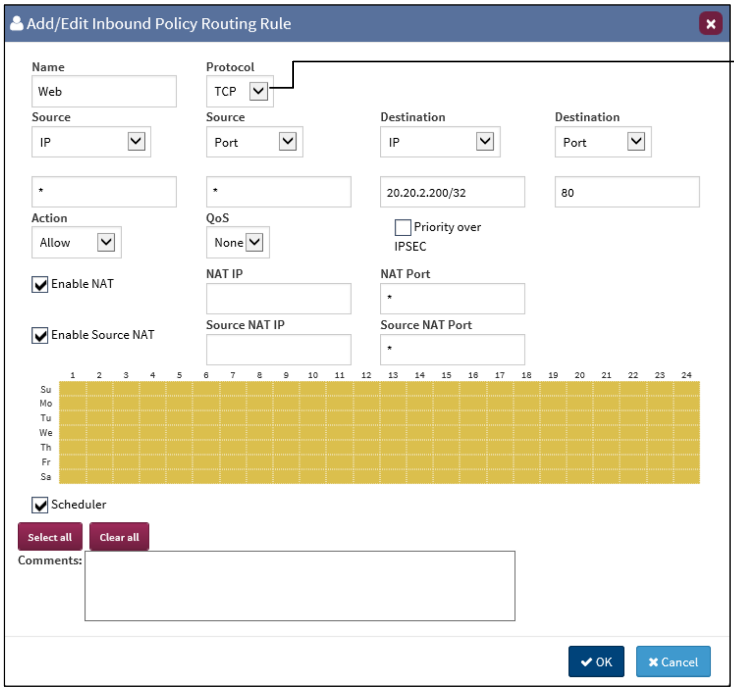
Comments:

Give each rule a unique name.

Use this to identify the purpose of the rule.

INBOUND POLICY CONFIGURATION

Add Inbound Policy rule based on specific criteria



Add/Edit Inbound Policy Routing Rule

Name: Web

Protocol: TCP

Source: IP

Source: Port

Destination: IP

Destination: Port

*

*

20.20.2.200/32

80

Action: Allow

QoS: None

□ Priority over IPSEC

☑ Enable NAT

NAT IP:

NAT Port: *

☑ Enable Source NAT

Source NAT IP:

Source NAT Port: *

☑ Scheduler

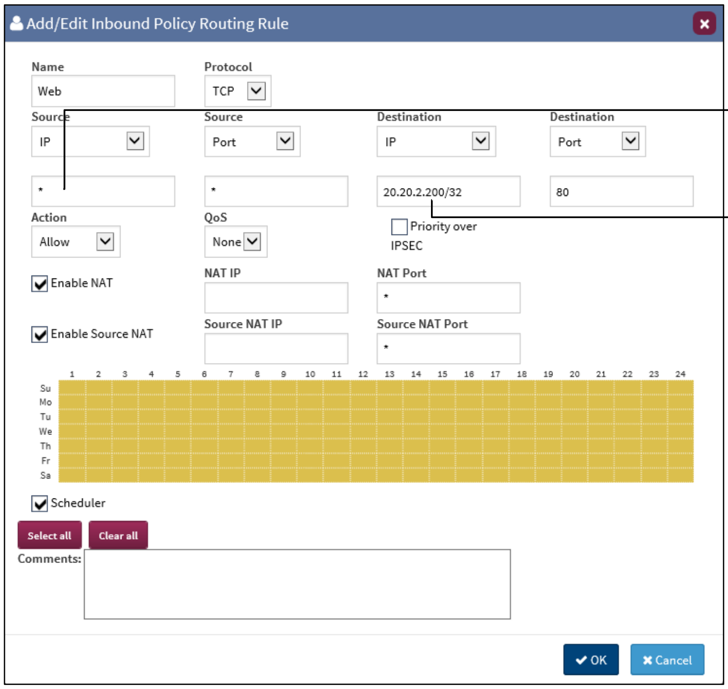
Comments:

Choose an IP protocol from the list

Choose from ALL, TCP, UDP, ICMP, GRE, ESP, AH. ALL will match all protocols. Port numbers only apply when using TCP or UDP.

INBOUND POLICY CONFIGURATION

Add Inbound Policy rule based on specific criteria



Add/Edit Inbound Policy Routing Rule

Name: Web
Protocol: TCP

Source: IP
Source: Port
Destination: IP
Destination: Port

*
*
20.20.2.200/32
80

Action: Allow
QoS: None
□ Priority over IPSEC

☑ Enable NAT
NAT IP:
NAT Port: *

☑ Enable Source NAT
Source NAT IP:
Source NAT Port: *

☑ Scheduler

Comments:

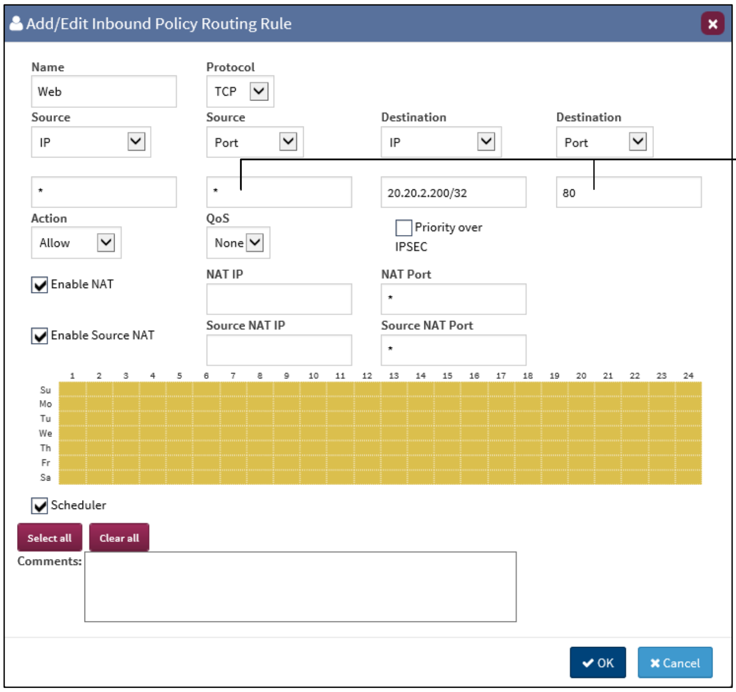
Specify a source IP and mask

Specify a destination IP and mask

If you want to match a single IP, use a /32 mask. If you want to match an entire subnet, use the network number with the network mask. If you want to match any IP, use an asterisk (*). MPVPN will display asterisk (*) as 0.0.0.0/0 meaning all IP's.

INBOUND POLICY CONFIGURATION

Add Inbound Policy rule based on specific criteria



Add/Edit Inbound Policy Routing Rule

Name: Web
Protocol: TCP

Source: IP
Source: Port
Destination: IP
Destination: Port

*
*
20.20.2.200/32
80

Action: Allow
QoS: None
□ Priority over IPSEC

☑ Enable NAT
NAT IP:
NAT Port: *

☑ Enable Source NAT
Source NAT IP:
Source NAT Port: *

☑ Scheduler

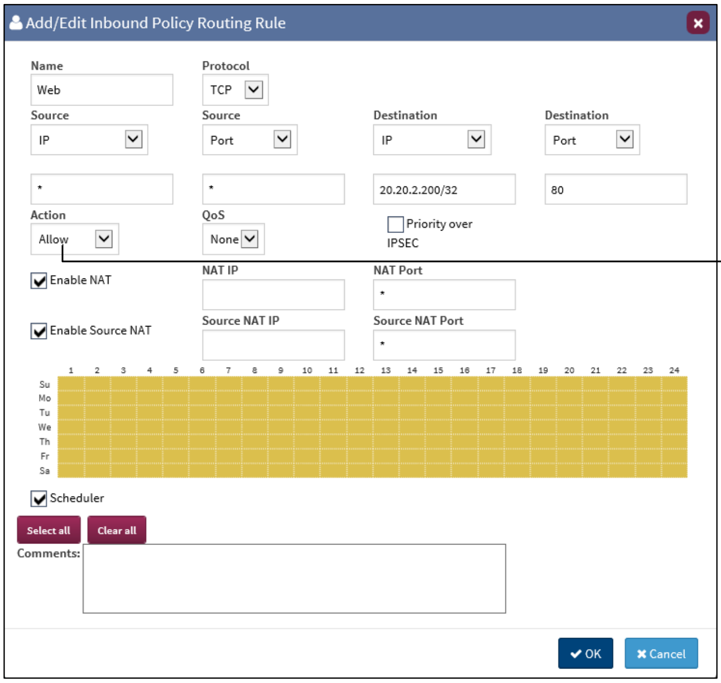
Comments:

Specify a port number or a port range

Port range should be separated by a hyphen (e.g., 1-1023). If you want to match any port number, use an asterisk (*).

INBOUND POLICY CONFIGURATION

Add Inbound Policy rule based on specific criteria



Add/Edit Inbound Policy Routing Rule

Name: Web

Protocol: TCP

Source: IP

Source: Port

Destination: IP

Destination: Port

*

*

20.20.2.200/32

80

Action: Allow

QoS: None

☐ Priority over IPSEC

☑ Enable NAT

NAT IP:

NAT Port: *

☑ Enable Source NAT

Source NAT IP:

Source NAT Port: *

☑ Scheduler

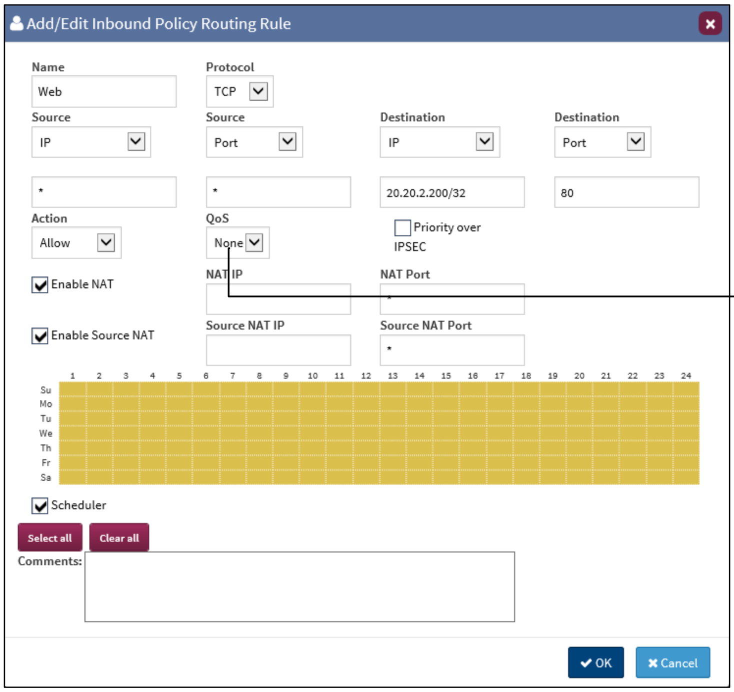
Comments:

Choose "Allow" or "Deny"

"Allow" to allow traffic that matches the rule and "Deny" to deny traffic that matches the rule.

INBOUND POLICY CONFIGURATION

Add Inbound Policy rule based on specific criteria



Add/Edit Inbound Policy Routing Rule

Name: Web

Protocol: TCP

Source: IP

Source: Port

Destination: IP

Destination: Port

*

*

20.20.2.200/32

80

Action: Allow

QoS: None

☐ Priority over IPSEC

☑ Enable NAT

NAT IP:

NAT Port: *

☑ Enable Source NAT

Source NAT IP:

Source NAT Port: *

☑ Scheduler

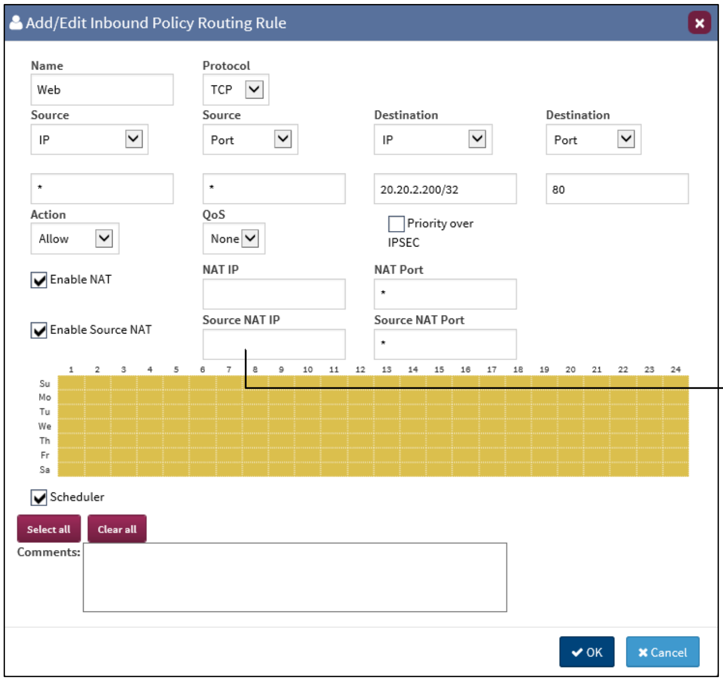
Comments:

Choose a pre-defined QoS rule

QoS rule will apply to the traffic matched by this policy route rule. QoS is a feature add-on. The default is “None.”

INBOUND POLICY CONFIGURATION

Add Inbound Policy rule based on specific criteria



Add/Edit Inbound Policy Routing Rule

Name: Web

Protocol: TCP

Source: IP — *

Source: Port — *

Destination: IP — 20.20.2.200/32

Destination: Port — 80

Action: Allow

QoS: None

☐ Priority over IPSEC

☑ Enable NAT

NAT IP:

NAT Port: *

☑ Enable Source NAT

Source NAT IP:

Source NAT Port: *

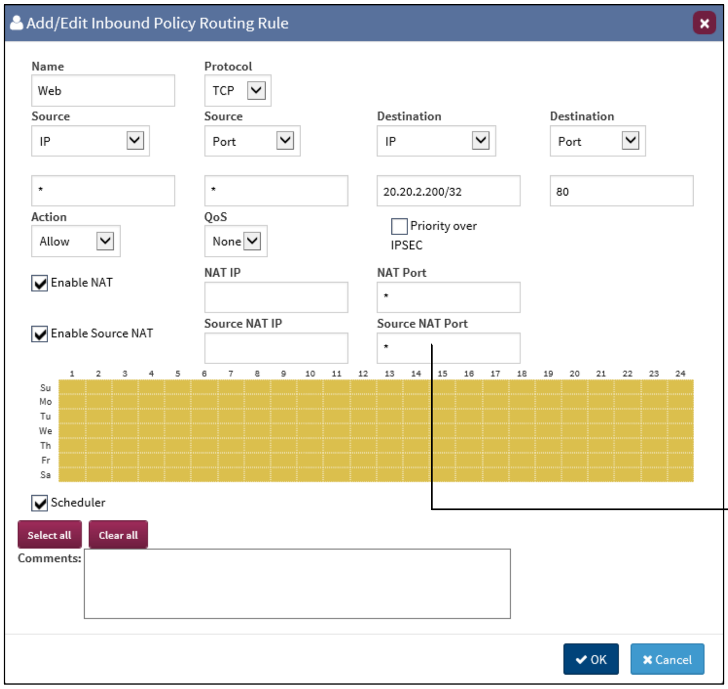
☑ Scheduler

Comments:

Specify destination IP

INBOUND POLICY CONFIGURATION

Add Inbound Policy rule based on specific criteria



Add/Edit Inbound Policy Routing Rule

Name: Web

Protocol: TCP

Source: IP — *

Source: Port — *

Destination: IP — 20.20.2.200/32

Destination: Port — 80

Action: Allow

QoS: None

☐ Priority over IPSEC

☑ Enable NAT

NAT IP:

NAT Port: *

☑ Enable Source NAT

Source NAT IP:

Source NAT Port: *

☑ Scheduler

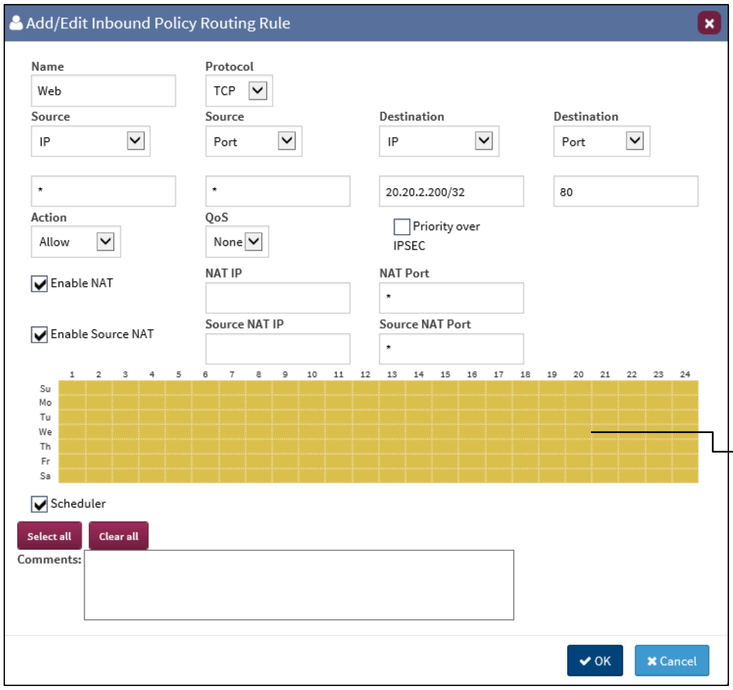
Comments:

If you want to map all ports, use an asterisk (*). If NAT is not selected, then the rule will default to Pass Through, which means that MPVPN simply forwards traffic matching the rule.

Specify the port number the traffic will be mapped to

INBOUND POLICY CONFIGURATION

Add Inbound Policy rule based on specific criteria



Add/Edit Inbound Policy Routing Rule

Name	Web
Protocol	TCP
Source	IP
	*
Source	Port
	*
Destination	IP
	20.20.2.200/32
Destination	Port
	80
Action	Allow
QoS	None
□ Priority over IPSEC	
☑ Enable NAT	
NAT IP	
NAT Port	*
☑ Enable Source NAT	
Source NAT IP	
Source NAT Port	*

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Su	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Mo	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Tu	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
We	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Th	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Fr	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Sa	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

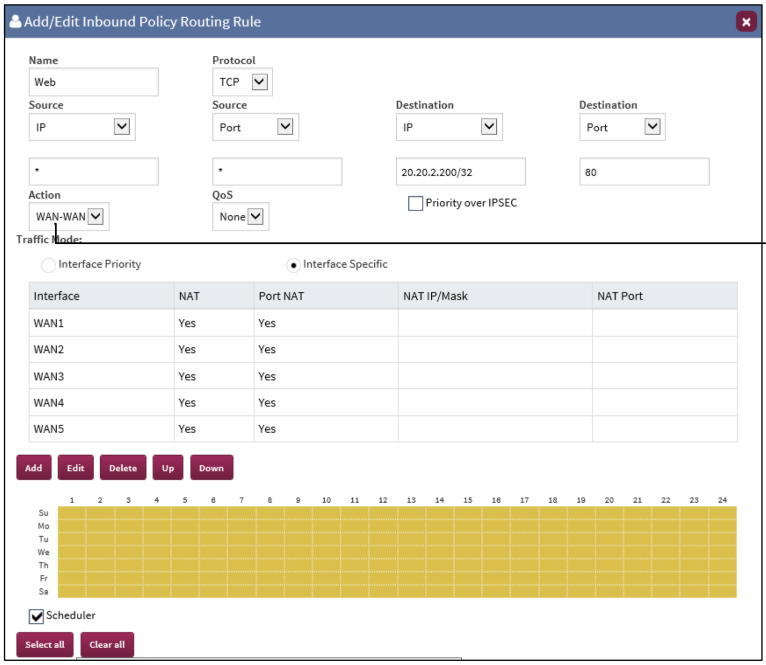
☑ Scheduler

If you want a particular rule to be followed, including QoS rules, during a specific period, then it can be scheduled using the scheduler.

Select the day of week & time of day the policy is to be implemented

INBOUND POLICY CONFIGURATION

WAN-WAN Routing



Add/Edit Inbound Policy Routing Rule

Name	Web
Protocol	TCP
Source	IP
	*
Source	Port
	*
Destination	IP
	20.20.2.200/32
Destination	Port
	80
Action	WAN-WAN
QoS	None
□ Priority over IPSEC	
Traffic Mode:	○ Interface Priority ● Interface Specific

Interface	NAT	Port NAT	NAT IP/Mask	NAT Port
WAN1	Yes	Yes		
WAN2	Yes	Yes		
WAN3	Yes	Yes		
WAN4	Yes	Yes		
WAN5	Yes	Yes		

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Su	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Mo	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Tu	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
We	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Th	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Fr	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Sa	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

☑ Scheduler

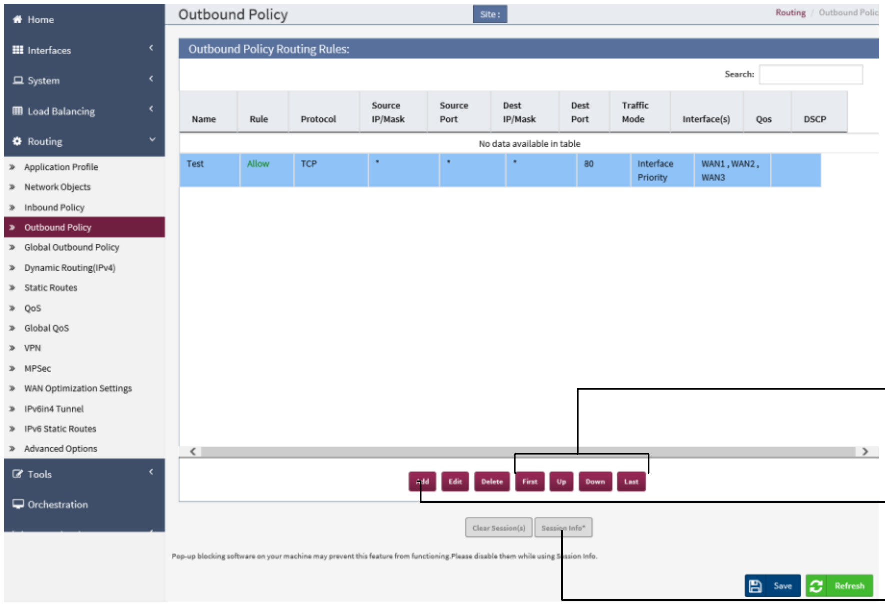
The rule has to be configured in Outbound Policy Routing fashion, but the source subnet should be that of remote network, whose traffic would reach FatPipe through a WAN interface

WAN-WAN action serves as an outbound policy route for the traffic matching the inbound rule

This traffic is routed to destinations using other WAN interfaces. The destination subnet will be * in case the traffic is routed to the Internet or another network in CIDR notation.

OUTBOUND POLICY CONFIGURATION

Used to direct Outbound traffic based on specific criteria



Outbound Policy Routing Rules:

Name	Rule	Protocol	Source IP/Mask	Source Port	Dest IP/Mask	Dest Port	Traffic Mode	Interface(s)	Qos	DSCP
No data available in table										
Test	Allow	TCP	*	*	*	80	Interface Priority	WAN1 , WAN2 , WAN3		

Pop-up blocking software on your machine may prevent this feature from functioning.Please disable them while using Session Info.

By default, all internet bound traffic from the LAN gets balanced & NAT'd to the IP of the interface its destined to leave on. Outbound policies get used when you have certain traffic constraints you either:

- •Don't want to balance
- •Don't want to NAT
- •Want to get creative with balancing and/or NATing

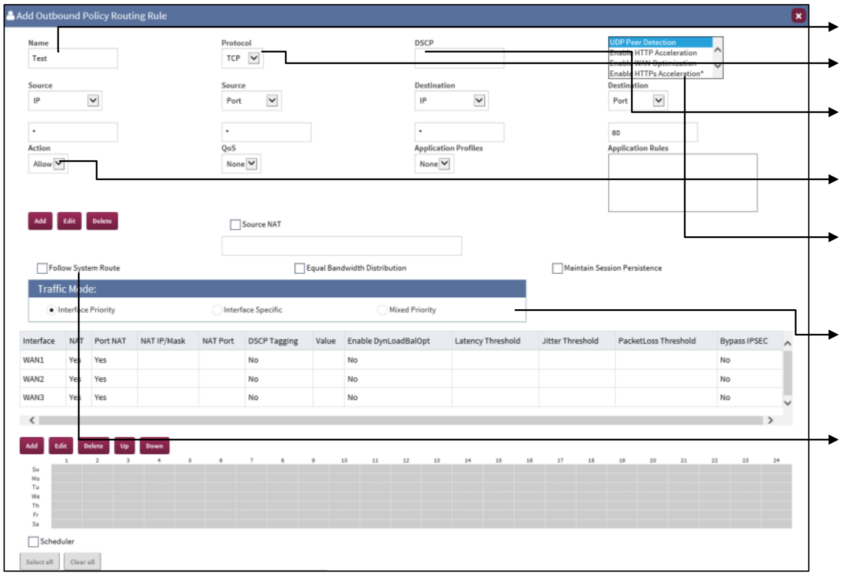
Use these buttons to change the order of the rules

To add a new outbound policy routing rule

View all sessions that match the selected inbound policy rule

OUTBOUND POLICY CONFIGURATION

Add Outbound Policy rule based on specific criteria



Name: Test
Protocol: TCP
DSCP:
Source: IP — *
Source: Port — *
Destination: IP — *
Destination: Port — 80
Action: Allow
QoS: None
Application Profiles: None
Application Rules:

□ Source NAT

□ Follow System Route □ Equal Bandwidth Distribution □ Maintain Session Persistence

Traffic Mode:

● Interface Priority ○ Interface Specific ○ Mixed Priority

Interface	NAT	Port NAT	NAT IP/Mask	NAT Port	DSCP Tagging	Value	Enable DynLoadBalOpt	Latency Threshold	Jitter Threshold	PacketLoss Threshold	Bypass IPSEC
WAN1	Yes	Yes			No		No				No
WAN2	Yes	Yes			No		No				No
WAN3	Yes	Yes			No		No				No

□ Scheduler

Give each rule a unique name to identify the purpose of the rule

Choose protocol from the dropdown

Specify the DSCP tag that is being delivered to the FatPipe from the LAN segment (more Info…)

Choose Allow to allow traffic that matches the rule

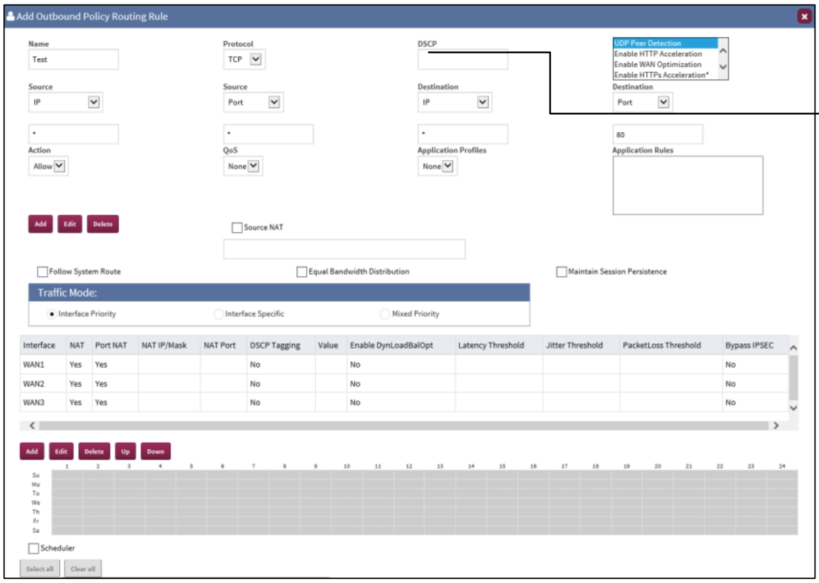
Select these for HTTPs Acceleration, WAN Optimization and UDP Aggregation (more Info…)

Interface Priority directs traffic out the first listed link, using the WAN interface order you specify. Interface Specific Mode load balances the traffic based on the Load Balancing Algorithm between the line(s) chosen in the WAN list.

In the event that this traffic pattern is governed by a static route, this option takes precedence over default Load balancing behavior

OUTBOUND POLICY CONFIGURATION

Add Outbound Policy rule based on specific criteria



Name: Test
Protocol: TCP
DSCP:
Source: IP — *
Source: Port — *
Destination: IP — *
Destination: Port — 80
Action: Allow
QoS: None
Application Profiles: None
Application Rules:

☐ Source NAT

☐ Follow System Route ☐ Equal Bandwidth Distribution ☐ Maintain Session Persistence

Traffic Mode: ● Interface Priority ○ Interface Specific ○ Mixed Priority

Interface	NAT	Port NAT	NAT IP/Mask	NAT Port	DSCP Tagging	Value	Enable DynLoadBalOpt	Latency Threshold	Jitter Threshold	PacketLoss Threshold	Bypass IPSEC
WAN1	Yes	Yes			No		No				No
WAN2	Yes	Yes			No		No				No
WAN3	Yes	Yes			No		No				No

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Su																								
Mo																								
Tu																								
We																								
Th																								
Fr																								
Sa																								

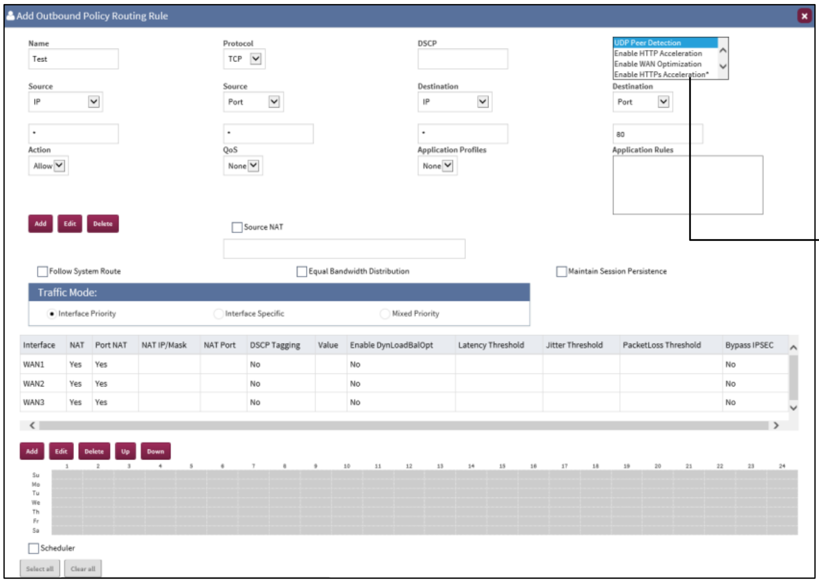
☐ Scheduler

Specify the DSCP tag that is being delivered to the FatPipe from the LAN segment (more Info…)

FatPipe will check the DSCP value in the outgoing packets with the DSCP value that is configured in the outbound policy routing rule. If it matches, then it will follow the actions specified in the policy routing rule. The default value is 0 for untagged packets.

OUTBOUND POLICY CONFIGURATION

Add Outbound Policy rule based on specific criteria



Name: Test
Protocol: TCP
DSCP:
Source: IP — *
Source: Port — *
Destination: IP — *
Destination: Port — 80
Action: Allow
QoS: None
Application Profiles: None
Application Rules:

☐ Source NAT

☐ Follow System Route ☐ Equal Bandwidth Distribution ☐ Maintain Session Persistence

Traffic Mode: ● Interface Priority ○ Interface Specific ○ Mixed Priority

Interface	NAT	Port NAT	NAT IP/Mask	NAT Port	DSCP Tagging	Value	Enable DynLoadBalOpt	Latency Threshold	Jitter Threshold	PacketLoss Threshold	Bypass IPSEC
WAN1	Yes	Yes			No		No				No
WAN2	Yes	Yes			No		No				No
WAN3	Yes	Yes			No		No				No

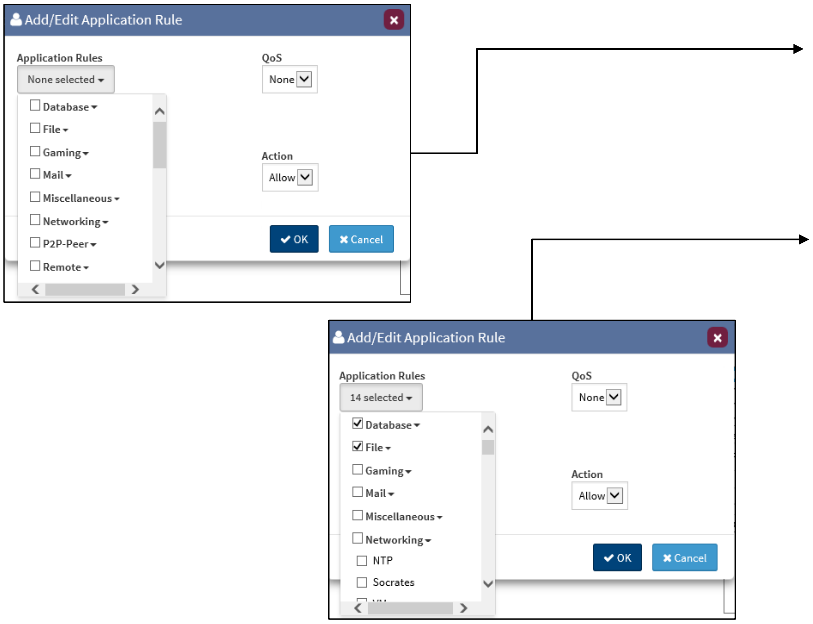
☐ Scheduler

Select these for HTTPs Acceleration, WAN Optimization and UDP Aggregation (more Info…)

- UDP aggregates smaller UDP packets into a bigger UDP packets thereby reducing bandwidth consumption.
- HTTPs Acceleration ensures optimization of SSL based traffic matching this rule.
- WAN Optimization enables WAN DeDup for traffic we can cache.

OUTBOUND POLICY CONFIGURATION

Add and Edit Layer 7 Application for an outbound policy



Add/Edit Application Rule

Application Rules: None selected

- ☐ Database
- ☐ File
- ☐ Gaming
- ☐ Mail
- ☐ Miscellaneous
- ☐ Networking
- ☐ P2P-Peer
- ☐ Remote

QoS: None

Action: Allow

✔ OK ✖ Cancel

Add/Edit Application Rule

Application Rules: 14 selected

- ☑ Database
- ☑ File
- ☐ Gaming
- ☐ Mail
- ☐ Miscellaneous
- ☐ Networking
  - ☐ NTP
  - ☐ Socrates

QoS: None

Action: Allow

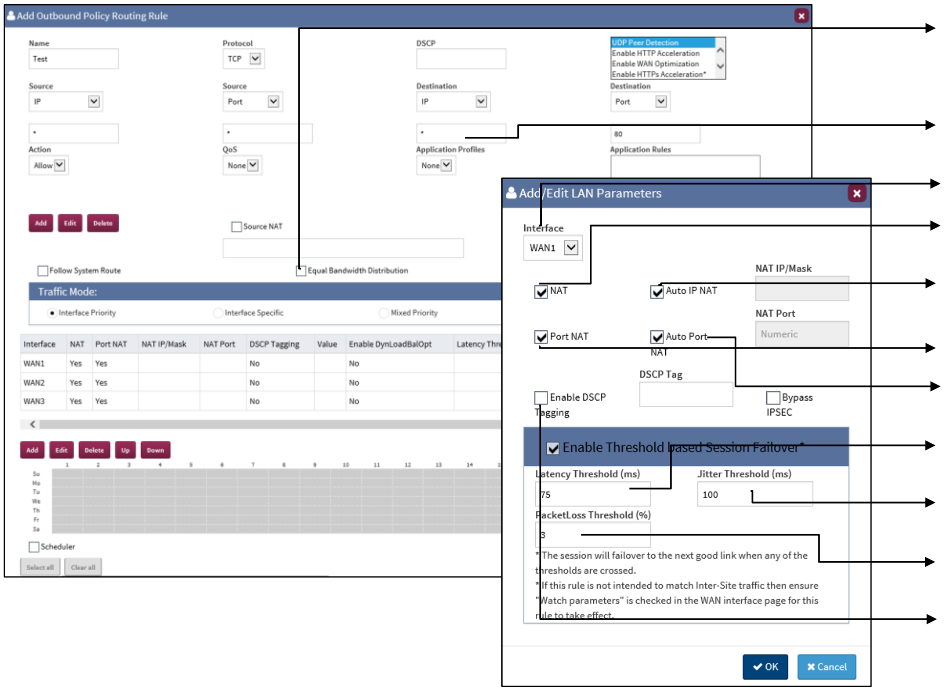
✔ OK ✖ Cancel

Browse through the list of Layer 7 applications listed under different categories. There are 180+ pre-defined applications.

Select one or more Applications from different categories.

OUTBOUND POLICY CONFIGURATION

Add and Edit outbound policy rule WAN Parameters



Add Outbound Policy Routing Rule

Name: Test

Protocol: TCP

DSCP:

UDP Peer Detection
Enable HTTP Acceleration
Enable WAN Optimization
Enable HTTPs Acceleration*

Source: IP — *

Source: Port — *

Destination: IP — *

Destination: Port — 80

Action: Allow

QoS: None

Application Profiles: None

Application Rules:

Add Edit Delete

☐ Source NAT

☐ Follow System Route

☐ Equal Bandwidth Distribution

Traffic Mode:

● Interface Priority ○ Interface Specific ○ Mixed Priority

Interface	NAT	Port NAT	NAT IP/Mask	NAT Port	DSCP Tagging	Value	Enable DynLoadBalOpt	Latency Thre
WAN1	Yes	Yes			No		No	
WAN2	Yes	Yes			No		No	
WAN3	Yes	Yes			No		No	

Add Edit Delete Up Down

☐ Scheduler

Select all Clear all

Add/Edit LAN Parameters

Interface: WAN1

☑ NAT ☑ Auto IP NAT — NAT IP/Mask:

☑ Port NAT ☑ Auto Port NAT — NAT Port: Numeric

☐ Enable DSCP Tagging — DSCP Tag: — ☐ Bypass IPSEC

☑ Enable Threshold based Session Failover*

Latency Threshold (ms): 75

Jitter Threshold (ms): 100

PacketLoss Threshold (%): 3

* The session will failover to the next good link when any of the thresholds are crossed.

* If this rule is not intended to match Inter-Site traffic then ensure "Watch parameters" is checked in the WAN interface page for this rule to take effect.

✔ OK ✖ Cancel

Enable to ensure all matching sessions are provided with equal bandwidth within the selected QoS bandwidth

Type the domain name of destination or the IP address in CIDR notation

Choose a WAN interface

Check this box to NAT traffic for this traffic pattern on this interface

Uncheck to specify an IP other than the IP of the WAN interface

Enable to Port NAT outbound traffic

Disable to configure a customized port

Configure Latency Threshold value for the WAN interface

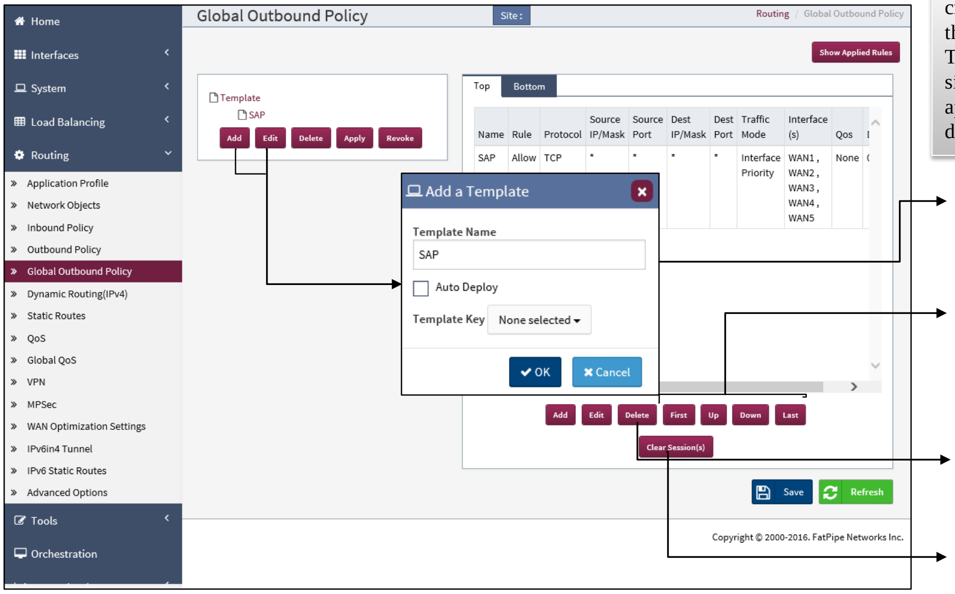
Configure Jitter Threshold value for the WAN interface

Configure Packet Loss Threshold value for the WAN interface.

DSCP NATing

GLOBAL OUTBOUND POLICY CONFIGURATION

This is similar to the Outbound Policy tab except the rules are created and maintained from the Central Manager Console. This rule is used to when a single policy needs to be applied to one or all FatPipe devices across your network.



Template Name: SAP

☐ Auto Deploy

Template Key: None selected

Name	Rule	Protocol	Source IP/Mask	Source Port	Dest IP/Mask	Dest Port	Traffic Mode	Interface (s)	Qos
SAP	Allow	TCP	*	*	*	*	Interface Priority	WAN1 , WAN2 , WAN3 , WAN4 , WAN5	None

Copyright © 2000-2016. FatPipe Networks Inc.

Add / Edit global outbound policy template name

Use these buttons to change the order of the rules for the selected template

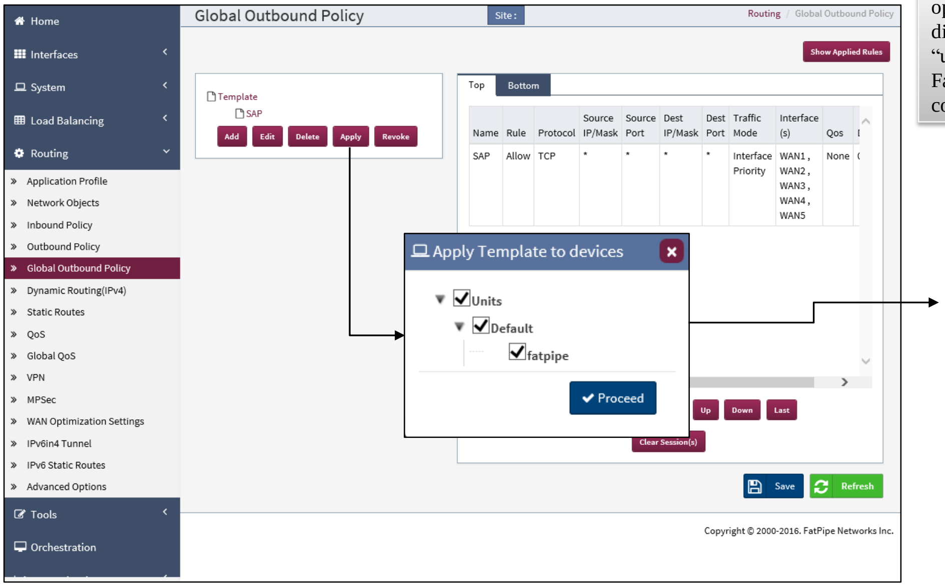
Click to delete a template

Clears sessions matching the selected rule

GLOBAL OUTBOUND POLICY CONFIGURATION

Used to Apply rules for Branch and HQ site FatPipe

Select the units and click on the Proceed button. This will open another pop-up window displaying the "successful" or "unsuccessful" message if the FatPipe is not able to communicate.



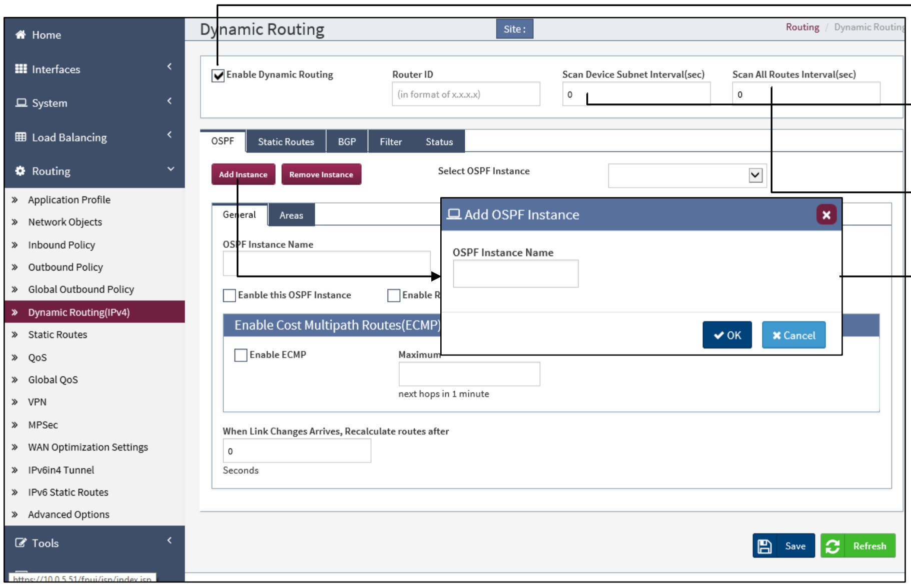
Name	Rule	Protocol	Source IP/Mask	Source Port	Dest IP/Mask	Dest Port	Traffic Mode	Interface (s)	Qos
SAP	Allow	TCP	*	*	*	*	Interface Priority	WAN1 , WAN2 , WAN3 , WAN4 , WAN5	None

- ☑ Units
  - ☑ Default
    - ☑ fatpipe

Copyright © 2000-2016. FatPipe Networks Inc.

Apply the Outbound policy rule from the selected template to all the selected units.

DYNAMIC ROUTING IPv4 CONFIGURATION



Dynamic Routing

☑ Enable Dynamic Routing

Router ID: (in format of x.x.x.x)

Scan Device Subnet Interval(sec): 0

Scan All Routes Interval(sec): 0

Select OSPF Instance

OSPF Instance Name

□ Eanble this OSPF Instance □ Enable R

Enable Cost Multipath Routes(ECMP)

□ Enable ECMP

Maximum

next hops in 1 minute

When Link Changes Arrives, Recalculate routes after

0

Seconds

Add OSPF Instance

OSPF Instance Name

Enable OSPF routing

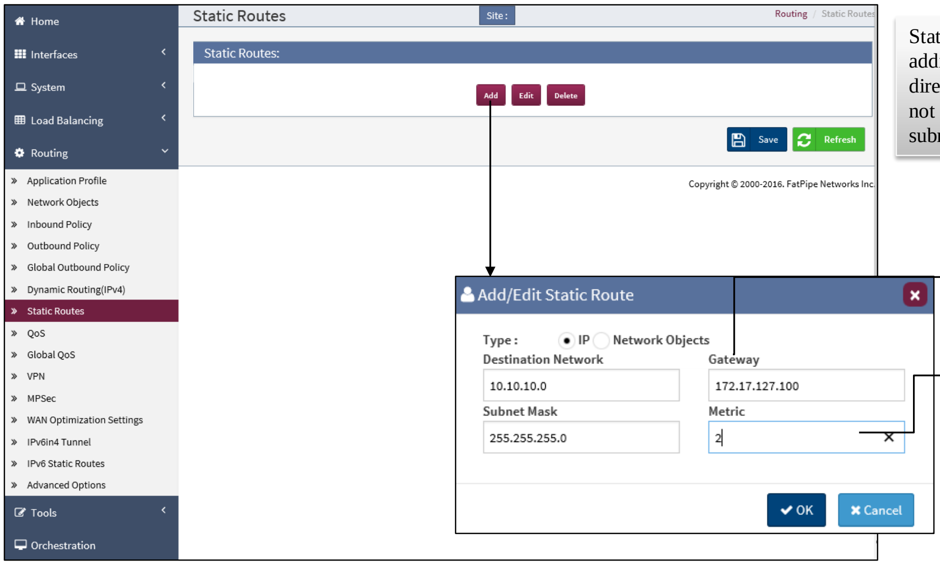
Time in seconds between two scans of the network interface list

Time in seconds between two consecutive scans of the FatPipe routing table

Add an OSPF instance

STATIC ROUTES CONFIGURATION

Used to statically route subnets to a user-defined gateway



Static Routes

Static Routes:

Copyright © 2000-2016. FatPipe Networks Inc.

Add/Edit Static Route

Type : ● IP ○ Network Objects

Destination Network: 10.10.10.0

Gateway: 172.17.127.100

Subnet Mask: 255.255.255.0

Metric: 2

Static Routes are used to route additional subnets that are not directly connected. They are not part of one of the Interface subnets.

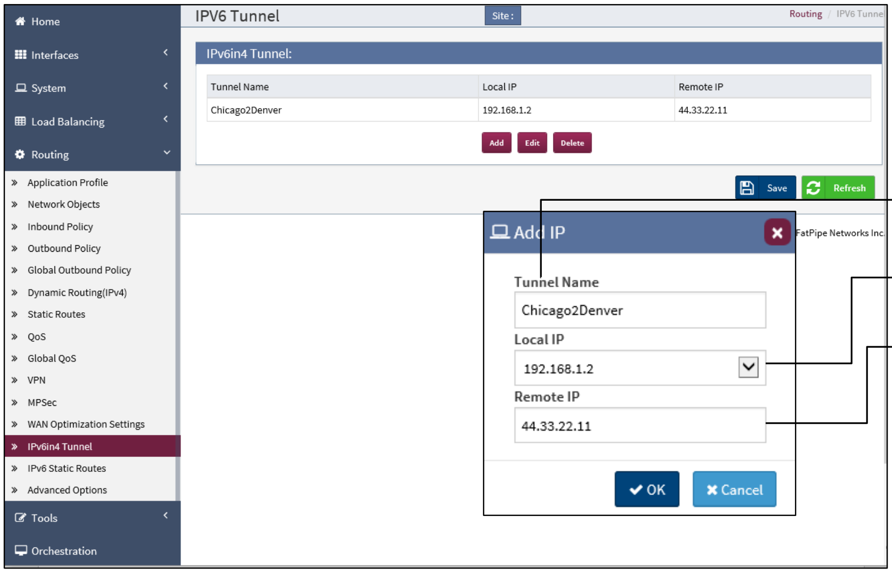
Gateway is typically your firewall or an internal router

Metric, the number of hops to the gateway is typically set to 2

IPv6in4 TUNNEL CONFIGURATION

Add IPv6in4 tunnel

This feature is to encapsulate IPv6 packets within IPv4. This allows the IPv6 packet to be carried across IPv4 routing infrastructures.



IPv6in4 Tunnel:

Tunnel Name	Local IP	Remote IP
Chicago2Denver	192.168.1.2	44.33.22.11

Add IP

Tunnel Name: Chicago2Denver

Local IP: 192.168.1.2

Remote IP: 44.33.22.11

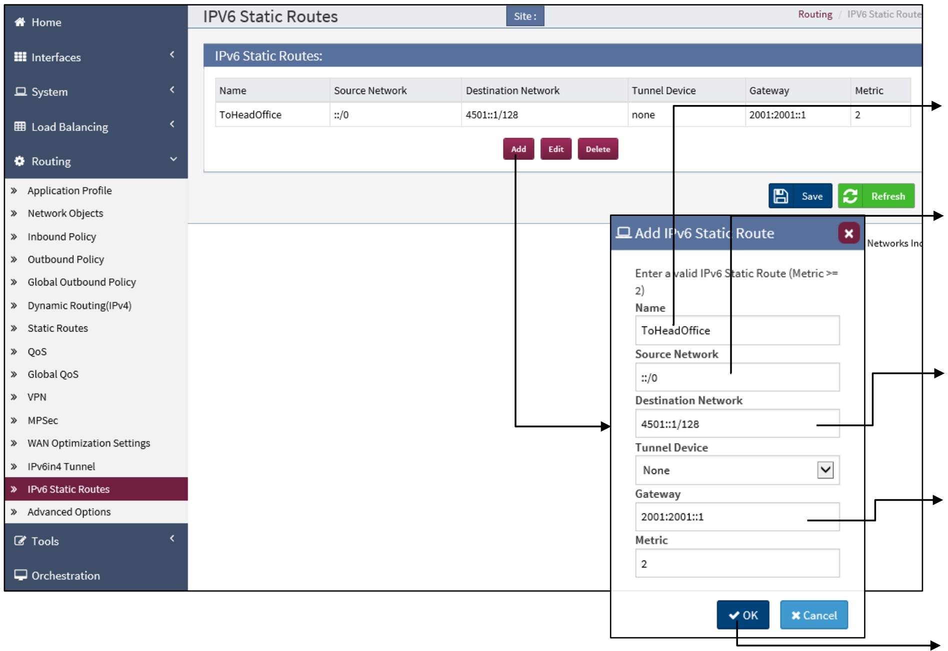
Enter the tunnel name

Select the local IP from the dropdown menu. The list includes all the IPs of the LAN and WAN Interfaces

Enter the remote IP

IPv6 STATIC ROUTES CONFIGURATION

Add IPv6 Static Routes



IPv6 Static Routes:

Name	Source Network	Destination Network	Tunnel Device	Gateway	Metric
ToHeadOffice	::/0	4501::1/128	none	2001:2001::1	2

Add IPv6 Static Route

Enter a valid IPv6 Static Route (Metric >= 2)

Name: ToHeadOffice

Source Network: ::/0

Destination Network: 4501::1/128

Tunnel Device: None

Gateway: 2001:2001::1

Metric: 2

Select the IPv6 tunnel name from the dropdown menu if the traffic is to be routed using the IPv4 node

The source of the IPv6 traffic - the source can be a host address, subnet address, or network address

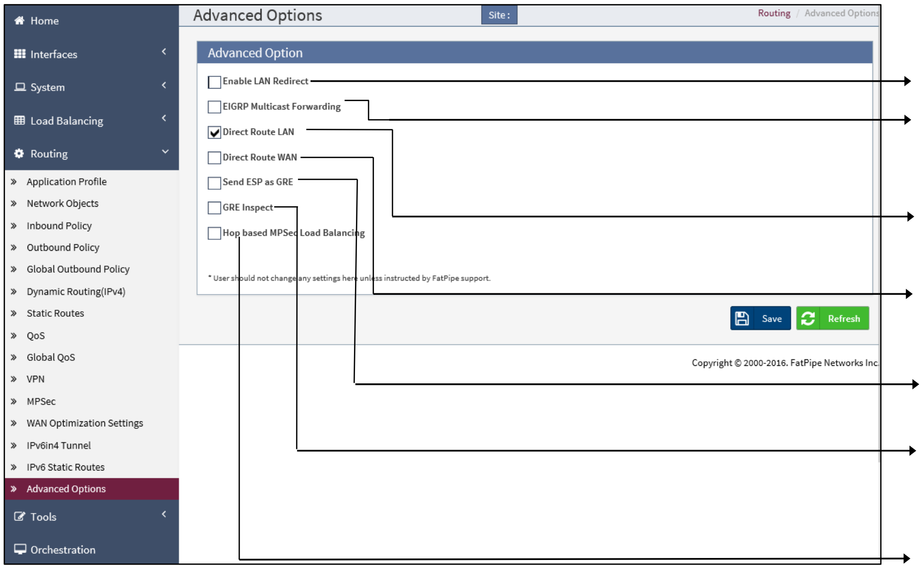
A destination for the IPv6 traffic - the destination can be a host address, subnet address, or network address

The Gateway Is enabled only when a tunnel device is not selected ("None"). The Gateway should belong to one of the local subnets and should be reachable

Specifies the number of hops to the gateway. It is usually 2 hops when using MPVPN

ADVANCED OPTIONS CONFIGURATION

Used to configure advanced options for a specific scenario



□ Enable LAN Redirect

□ EIGRP Multicast Forwarding

☑ Direct Route LAN

□ Direct Route WAN

□ Send ESP as GRE

□ GRE Inspect

□ Hop based MPSec Load Balancing

* User should not change any settings here unless instructed by FatPipe support.

Copyright © 2000-2016. FatPipe Networks Inc.

Enable LAN Redirect when a LAN client wants to access a server in the LAN using its public IP

Enable EIGRP Multicast forwarding when the FatPipe needs to be transparent between two EIGRP end points

Enable Direct Route LAN to route packets directly from LAN to WAN

Enable Direct Route WAN to route packets directly from the LAN to the WAN

Enable Send ESP as GRE to send ESP packets as GRE

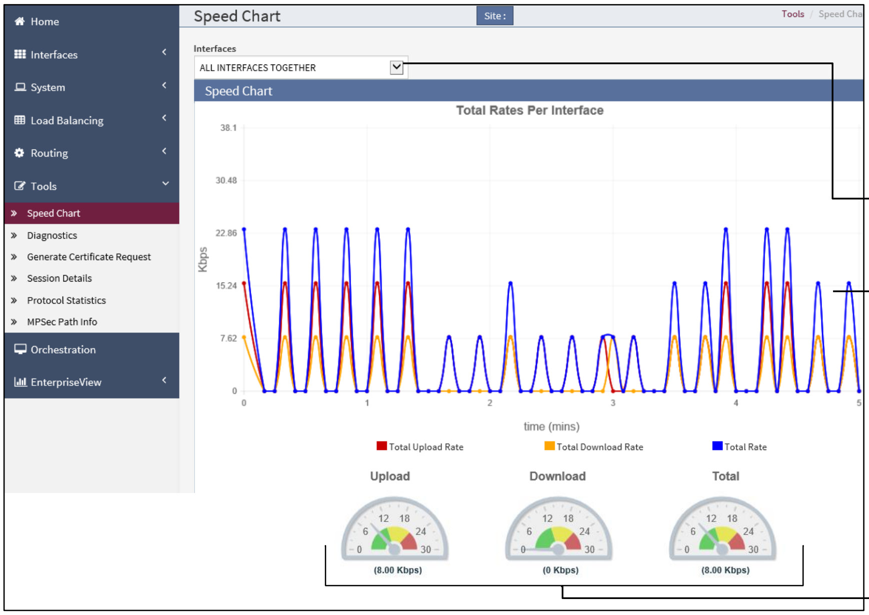
Enable GRE inspection to have policies be able to take action on GRE packet payload

Enable Hop-based MPSec Load balancing to load balance MPSec traffic based on hops

SPEED CHART TOOL

Used to monitor the speed of your WAN connections

Monitor the upload and download or combined speeds of each of the WAN lines independently or in combination by viewing the Speed Chart.



Interfaces: ALL INTERFACES TOGETHER

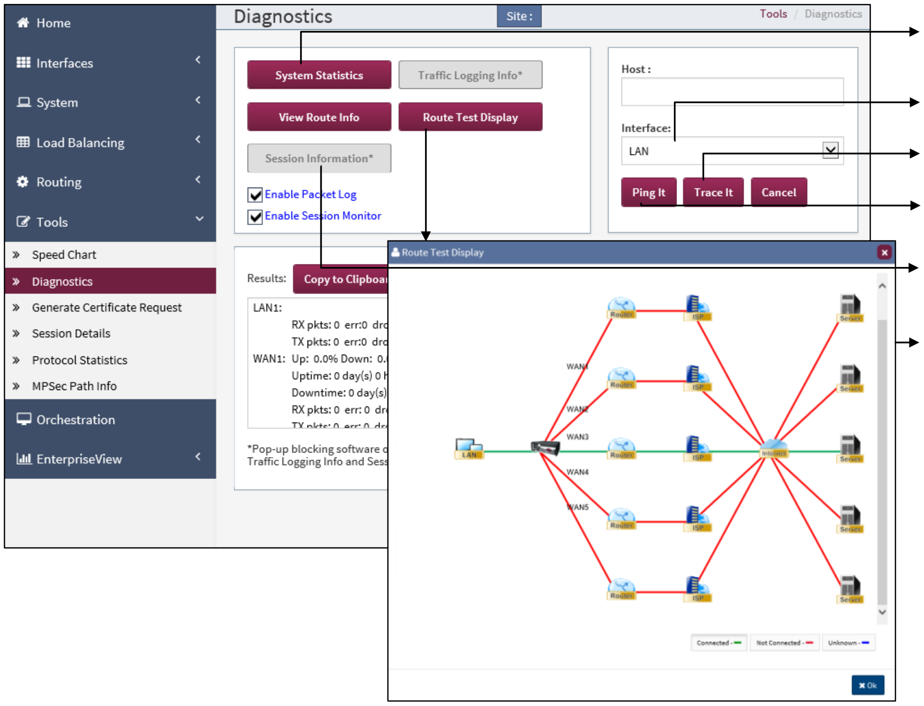
Select the interface that you want to view. WAN1, WAN2, WAN3 or All Interfaces.

Plots real-time bandwidth usage graphically

Displays real-time bandwidth usage numerically

DIAGNOSTIC TOOL

Used to help diagnose and troubleshoot



☑ Enable Packet Log
☑ Enable Session Monitor

Interface: LAN

Ping It
Trace It

```
LAN1:
        RX pkts: 0  err:0  dro
        TX pkts: 0  err:0  dro
WAN1:  Up:  0.0% Down:  0.
        Uptime: 0 day(s) 0 h
        Downtime: 0 day(s)
        RX pkts: 0  err: 0  dro
        TX pkts: 0  err: 0  dro
```

*Pop-up blocking software o
Traffic Logging Info and Sess

Connected - 🟩 Not Connected - 🟥 Unknown - 🟦

View information about system uptime and interface statistics

Select interface to use for ping or trace route

Traceroute on a interface by interface basis

Ping on a interface by interface basis

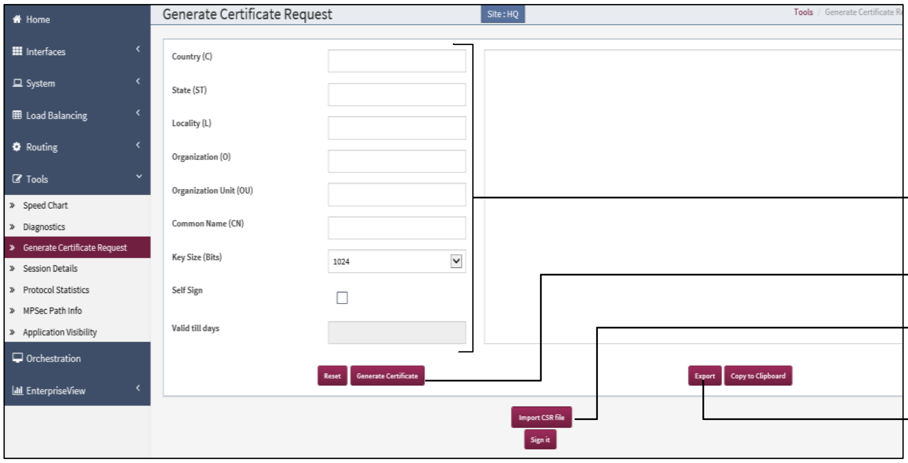
View all the sessions currently running on the unit

View a real-time graphical display of link connectivity validation

GENERATE CERTIFICATE REQUEST

Used to generate certificate for IPSec

Generate Certificate Request will provide a separate certificate for every user instead of having a single generated IPSec key



Country (C)	
State (ST)	
Locality (L)	
Organization (O)	
Organization Unit (OU)	
Common Name (CN)	
Key Size (Bits)	1024
Self Sign	□
Valid till days	

Provide all the credentials to generate Certificate

To get the certificate

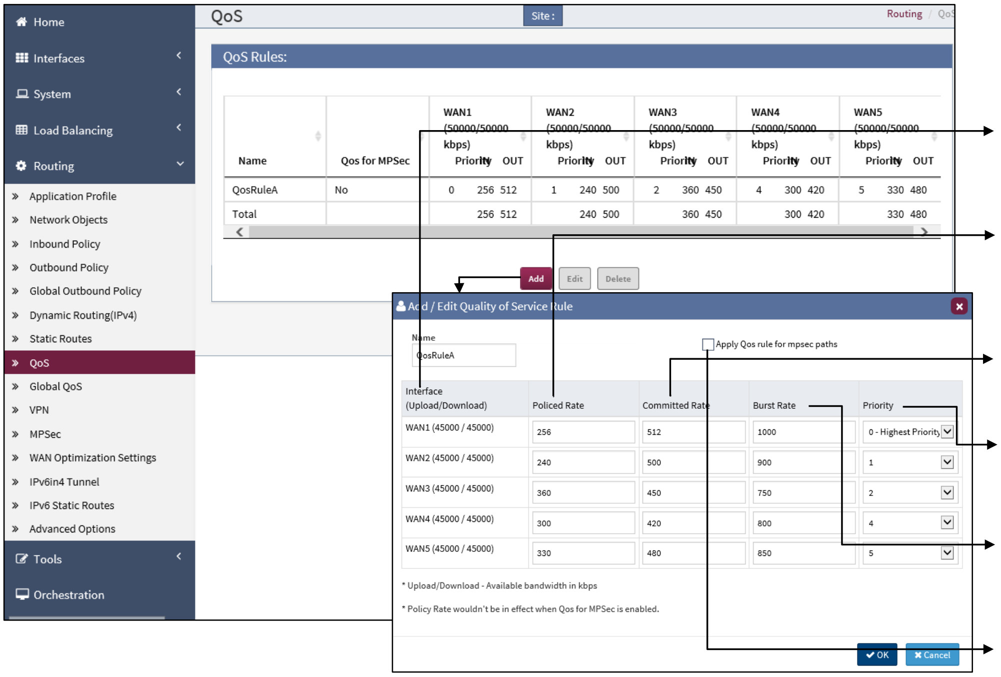
Get CSR info from server and upload on FatPipe

Save the generated certificate to Computer

QUALITY OF SERVICE CONFIGURATION

Used to prioritize your WAN traffic

QoS allows you to prioritize your WAN traffic.



QoS Rules:

Name	Qos for MPSec	WAN1 (50000/50000 kbps) Priority		OUT	WAN2 (50000/50000 kbps) Priority		OUT	WAN3 (50000/50000 kbps) Priority		OUT	WAN4 (50000/50000 kbps) Priority		OUT	WAN5 (50000/50000 kbps) Priority		OUT
QosRuleA	No	0	256	512	1	240	500	2	360	450	4	300	420	5	330	480
Total			256	512		240	500		360	450		300	420		330	480

Add / Edit Quality of Service Rule

Name: QosRuleA

□ Apply Qos rule for mpsec paths

Interface (Upload/Download)	Policed Rate	Committed Rate	Burst Rate	Priority
WAN1 (45000 / 45000)	256	512	1000	0 - Highest Priority
WAN2 (45000 / 45000)	240	500	900	1
WAN3 (45000 / 45000)	360	450	750	2
WAN4 (45000 / 45000)	300	420	800	4
WAN5 (45000 / 45000)	330	480	850	5

* Upload/Download - Available bandwidth in kbps

* Policy Rate wouldn't be in effect when Qos for MPSec is enabled.

This column displays the total amount of bandwidth available on a given interface

The Policed Rate defines what we will try to carve out for incoming bandwidth purposes

Committed rate is the bare minimum amount of bandwidth carved out for a given rule

Specify the priority (precedence level) for this rule

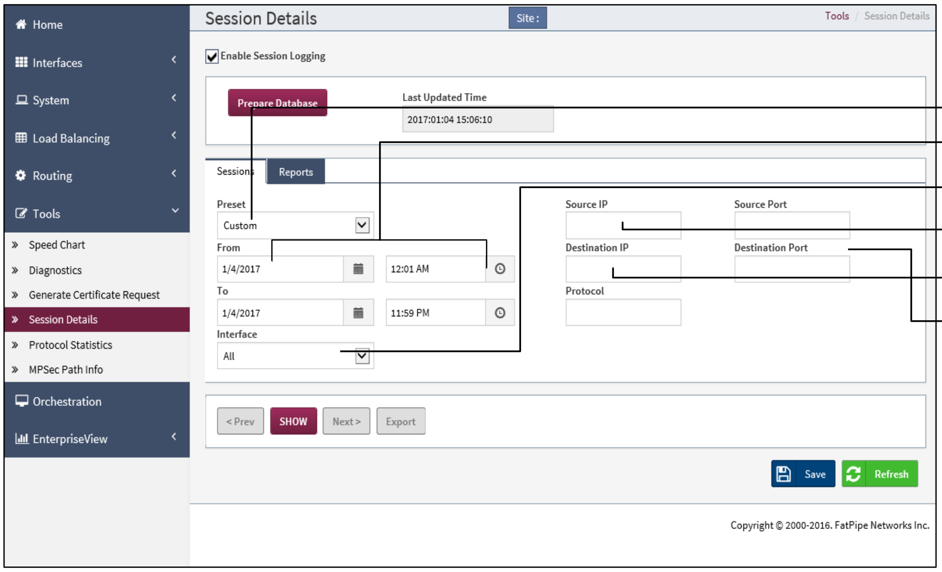
The Burst Rate defines the outbound bandwidth ceiling for this rule

Enable to apply QoS rule to all the MPSec paths automatically

SESSION DETAILS

Used to view Session details

Provides a report on the sessions that flow through the device. You can view all the sessions that flowed through the FatPipe at a given period of time.



☑ Enable Session Logging

Last Updated Time: 2017:01:04 15:06:10

Preset: Custom

From: 1/4/2017 12:01 AM

To: 1/4/2017 11:59 PM

Interface: All

Source IP

Source Port

Destination IP

Destination Port

Protocol

Copyright © 2000-2016. FatPipe Networks Inc.

Choose a preconfigured report from the drop down

Enter a date/time range

Specify an interface

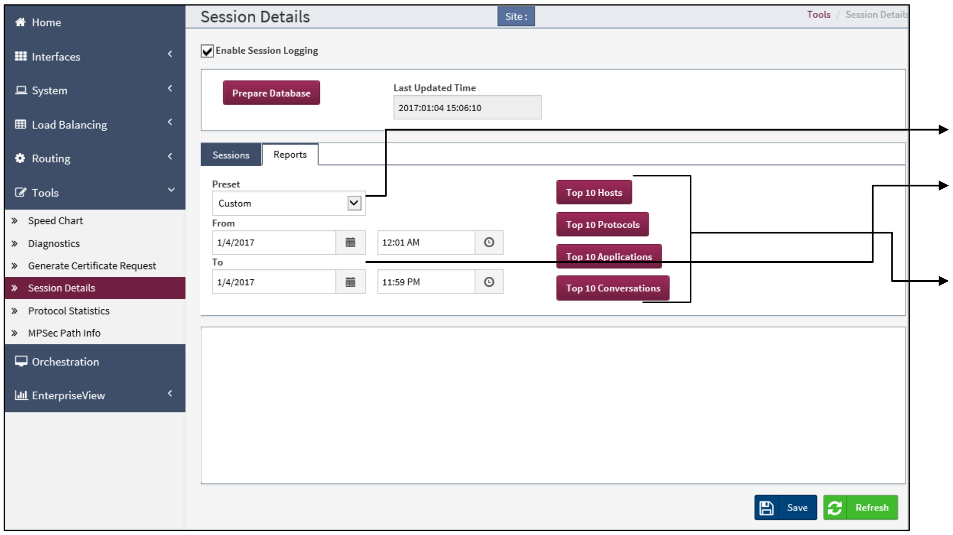
Enter Source IP address

Enter Destination IP address

Enter Source port and Destination port

SESSION REPORTS

Used to view Session reports



Session Details

☑ Enable Session Logging

Last Updated Time: 2017:01:04 15:06:10

Preset: Custom

From: 1/4/2017 12:01 AM

To: 1/4/2017 11:59 PM

Select a preconfigured report

Enter date / time range

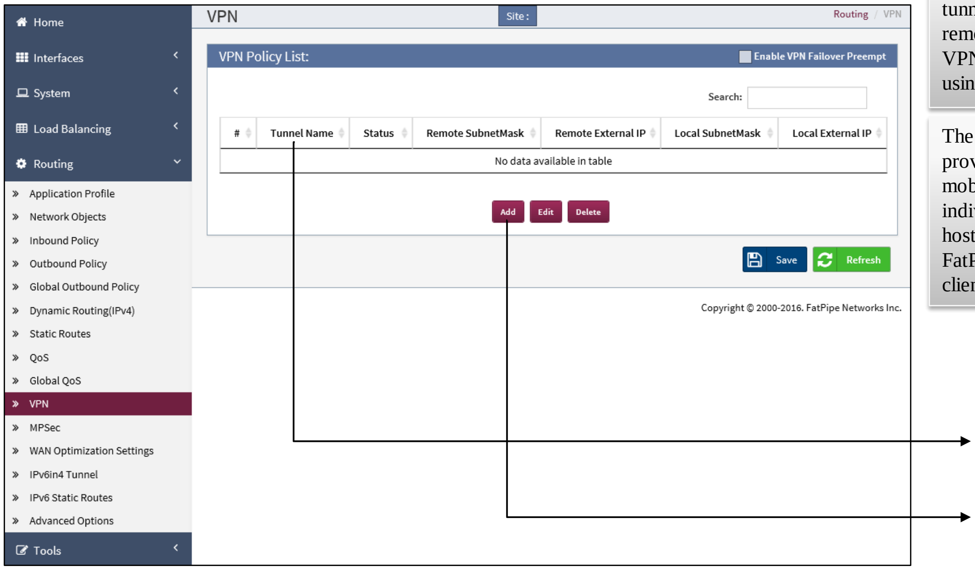
Click to view the different types of Session Reports available.

VPN CONFIGURATION

Used to configure VPN tunnels with standard IPSec VPN peer

FatPipe VPN allows you to create and configure IPSec tunnels between two or more remote networks (site-to-site VPNs) and with remote users using mobile VPN clients.

The Client VPN user feature provides connectivity for mobile VPN clients. It allows individual users to connect to hosts on the LAN behind FatPipe by using a VPN client.



VPN

VPN Policy List:

□ Enable VPN Failover Preempt

#	Tunnel Name	Status	Remote SubnetMask	Remote External IP	Local SubnetMask	Local External IP
No data available in table						

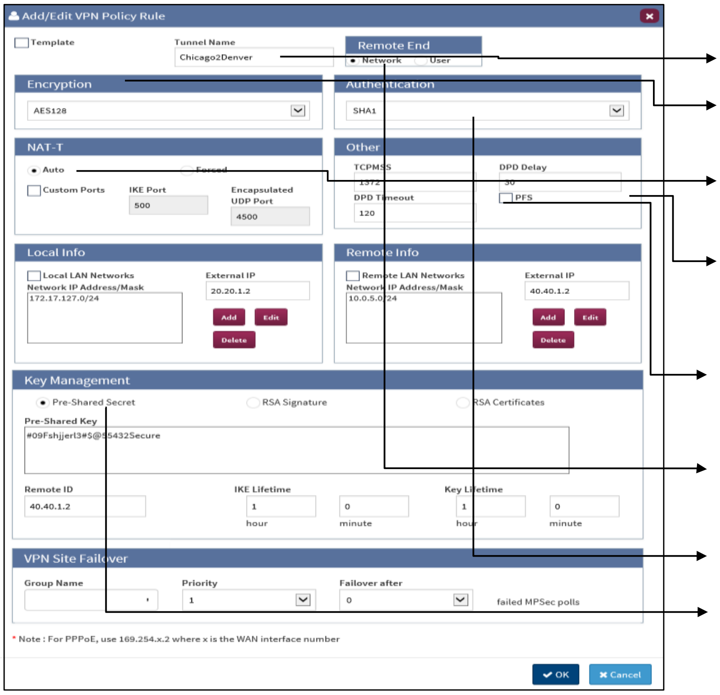
Copyright © 2000-2016. FatPipe Networks Inc.

Specify a unique name for the policy.

To add a new VPN policy rule

VPN CONFIGURATION

Used to configure VPN tunnels with standard IPSec VPN peer



Add/Edit VPN Policy Rule

□ Template

Tunnel Name: Chicago2Denver

Remote End: ● Network ○ User

Encryption: AES128

Authentication: SHA1

NAT-T

● Auto ○ Forced

□ Custom Ports

IKE Port: 500

Encapsulated UDP Port: 4500

Other

TCPMSS: 1372

DPD Delay: 30

DPD Timeout: 120

□ PFS

Local Info

□ Local LAN Networks

Network IP Address/Mask: 172.17.127.0/24

External IP: 20.20.1.2

Remote Info

□ Remote LAN Networks

Network IP Address/Mask: 10.0.5.0/24

External IP: 40.40.1.2

Key Management

● Pre-Shared Secret ○ RSA Signature ○ RSA Certificates

Pre-Shared Key: #09Fshjjerl3#$@55432Secure

Remote ID: 40.40.1.2

IKE Lifetime: 1 hour 0 minute

Key Lifetime: 1 hour 0 minute

VPN Site Failover

Group Name:

Priority: 1

Failover after: 0 failed MPSec polls

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

Enter the name of the tunnel

Select the encryption type you want to use for the policy

Choosing "Auto" mode leaves the VPN devices to negotiate NAT-Traversal

The MSS value helps set the maximum segment size. The size range is from 566 - 1460

By enabling PFS, if someone breaks a key, PFS ensures that the attacker is not able to derive any other key

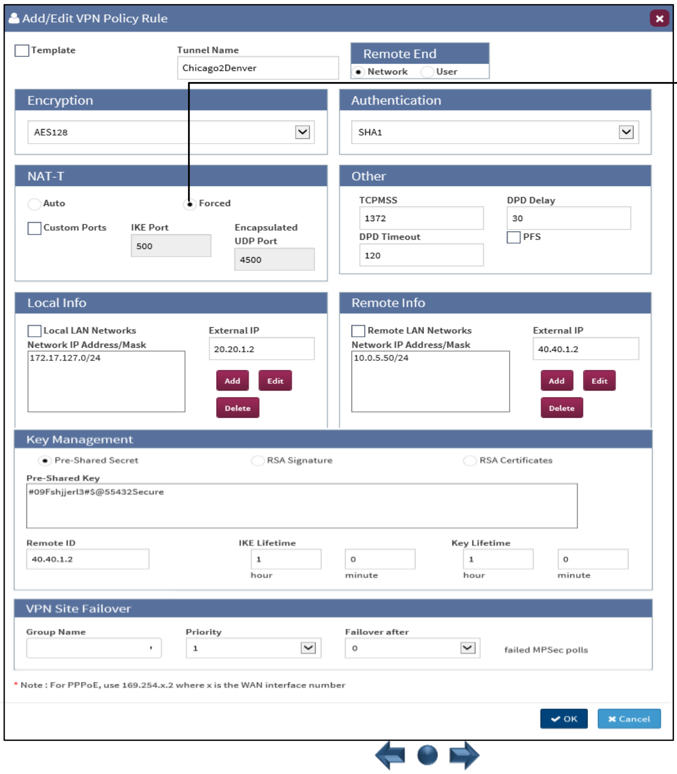
Choose Remote End as 'Network' to create VPN tunnels between two sites

Select the authentication method you want to use for the policy

Configure key'ing

VPN CONFIGURATION

Used to configure VPN tunnels with standard IPSec VPN peer



Add/Edit VPN Policy Rule

□ Template

Tunnel Name: Chicago2Denver

Remote End: ● Network ○ User

Encryption: AES128

Authentication: SHA1

NAT-T

○ Auto ● Forced

□ Custom Ports

IKE Port: 500

Encapsulated UDP Port: 4500

Other

TCPMSS: 1372

DPD Delay: 30

DPD Timeout: 120

□ PFS

Local Info

□ Local LAN Networks

Network IP Address/Mask: 172.17.127.0/24

External IP: 20.20.1.2

Remote Info

□ Remote LAN Networks

Network IP Address/Mask: 10.0.5.50/24

External IP: 40.40.1.2

Key Management

● Pre-Shared Secret ○ RSA Signature ○ RSA Certificates

Pre-Shared Key: #09Fshjjerl3#$@55432Secure

Remote ID: 40.40.1.2

IKE Lifetime: 1 hour 0 minute

Key Lifetime: 1 hour 0 minute

VPN Site Failover

Group Name:

Priority: 1

Failover after: 0 failed MPSec polls

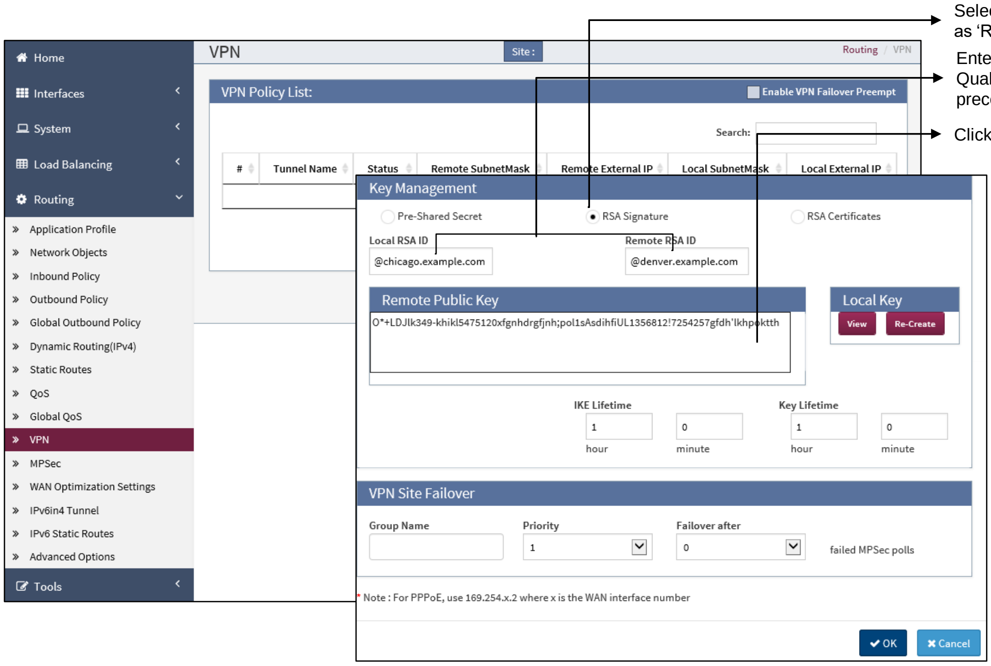
* Note : For PPPoE, use 169.254.x.2 where x is the WAN interface number

NAT-T "Forced" mode will force the VPN devices to encapsulate IPSec packets into UDP packets to solve traversal problems that may occur with intermediate NATing

To configure Forced mode option, select the Forced option, The normal ports for NAT-Traversal are UDP 500 for Key negotiation and UDP 4500 for data exchange. You can change these values by checking the 'Custom Ports' check box which allows you change these values to any valid UDP Port number.

VPN CONFIGURATION

Used to configure VPN tunnels with standard IPSec VPN peer



Key Management

○ Pre-Shared Secret ● RSA Signature ○ RSA Certificates

Local RSA ID: @chicago.example.com

Remote RSA ID: @denver.example.com

Remote Public Key

O*+LDJlk349-khikl5475120xfgnhdrgfjnh;pol1sAsdihfiUL1356812!7254257gfdh'lkhpoktth

Local Key

IKE Lifetime: 1 hour 0 minute

Key Lifetime: 1 hour 0 minute

VPN Site Failover

Group Name:

Priority: 1

Failover after: 0 failed MPSec polls

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

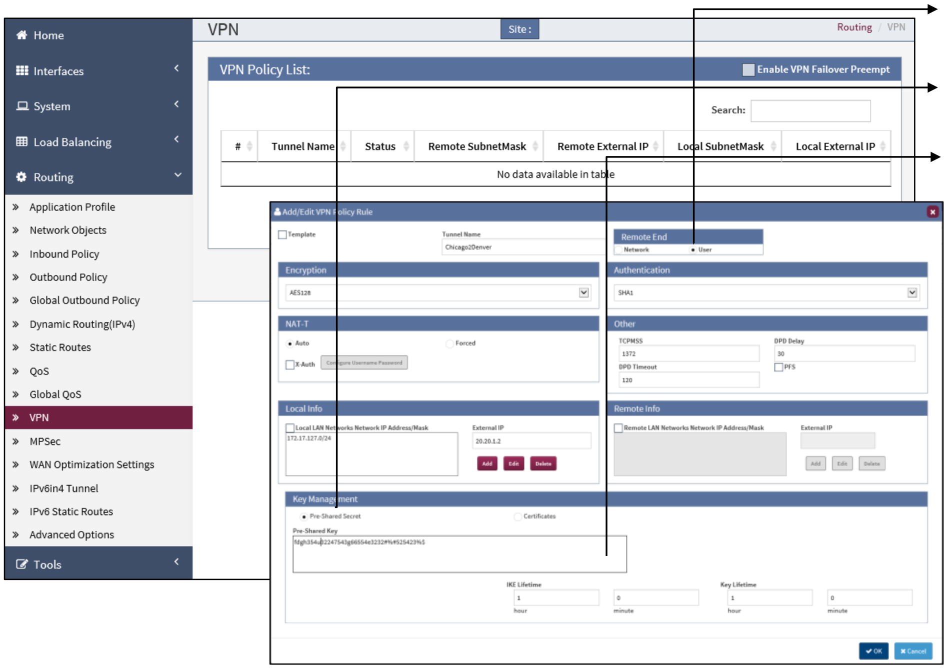
Select Key management as ‘RSA Signature’

Enter RSA ID as a Fully Qualified Domain Name preceded by an @ sign

Click to generate a public key

VPN CONFIGURATION

Used to configure VPN tunnels with standard IPSec VPN peer



No data available in table

□ Template

Tunnel Name: Chicago2Denver

Remote End: ○ Network ● User

Encryption: AES128

Authentication: SHA1

NAT-T: ● Auto ○ Forced

□ X-Auth

Other

TCPMSS: 1372

DPD Delay: 30

DPD Timeout: 120

□ PFS

Local Info

□ Local LAN Networks Network IP Address/Mask: 172.17.127.0/24

External IP: 20.20.1.2

Remote Info

□ Remote LAN Networks Network IP Address/Mask

External IP

Key Management

● Pre-Shared Secret ○ Certificates

Pre-Shared Key: fdgh354u32247543g66554e3232#%#525423%$

IKE Lifetime: 1 hour 0 minute

Key Lifetime: 1 hour 0 minute

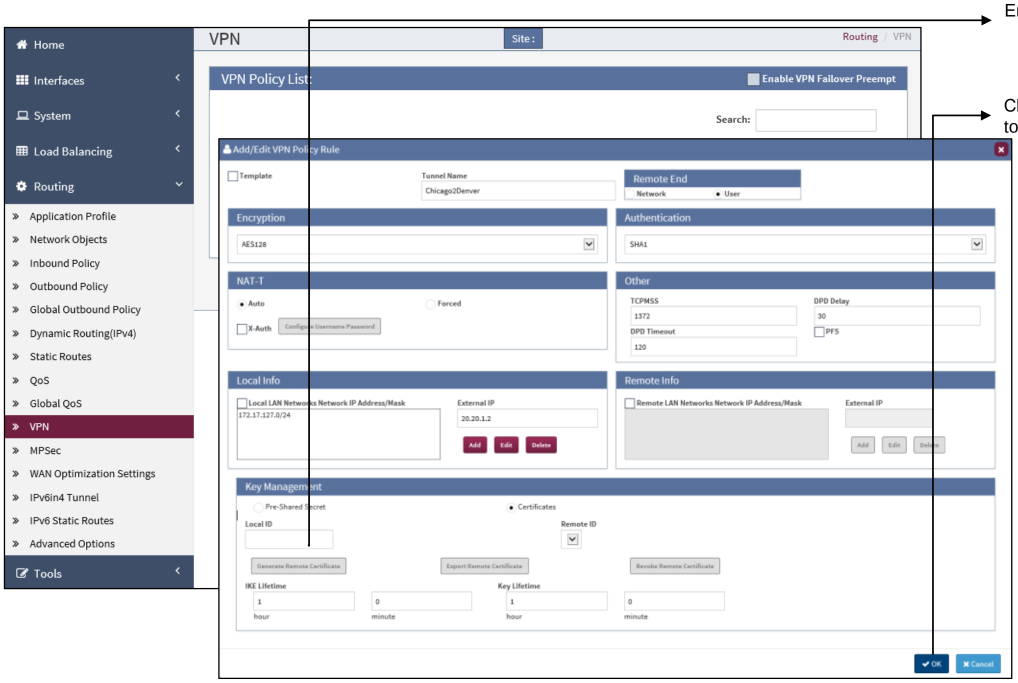
Choose Remote End as ‘User’ to create VPN tunnels with any remote host

Select Key management as ‘pre-shared secret’

Enter pre-shared secret key and this should match the key management type and key used on the VPN peer also

VPN CONFIGURATION

Used to configure VPN tunnels with standard IPSec VPN peer



□ Template

Tunnel Name: Chicago2Denver

Remote End: ○ Network ● User

Encryption: AES128

Authentication: SHA1

NAT-T: ● Auto ○ Forced

□ X-Auth

Other: TCPMSS 1372; DPD Delay 30; DPD Timeout 120; □ PFS

Local Info: □ Local LAN Networks Network IP Address/Mask: 172.17.127.0/24; External IP: 20.20.1.2

Remote Info: □ Remote LAN Networks Network IP Address/Mask; External IP

Key Management: ○ Pre-Shared Secret ● Certificates

Local ID

Remote ID

IKE Lifetime: 1 hour 0 minute

Key Lifetime: 1 hour 0 minute

Enter the “Local ID”

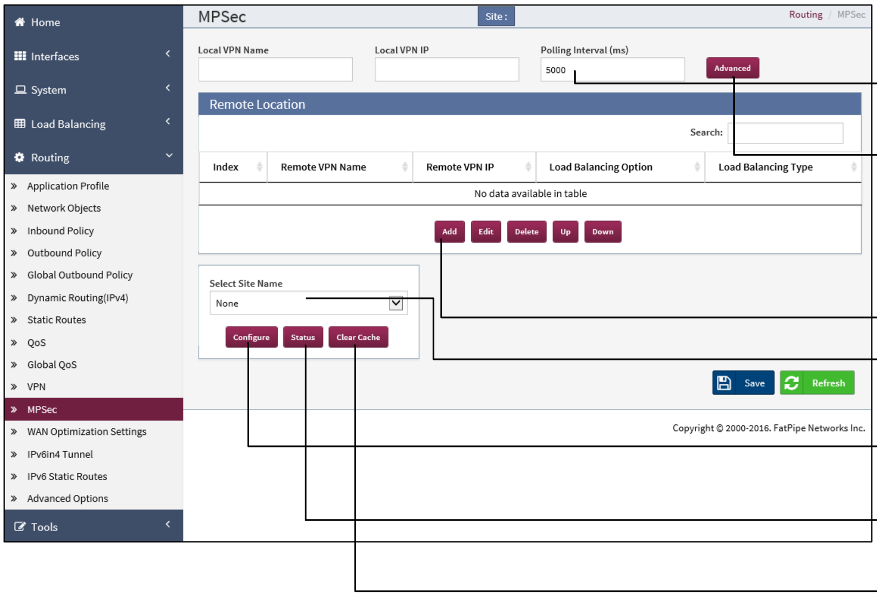
Click the “OK” button to save the VPN entry

The local certificate installed on the FatPipe is created with the Local ID, the Remote ID, and Remote Certificate password. When the certificate is created, it is signed internally by the Fatpipe’s local certificate.

MPSEC CONFIGURATION

Provides security, redundancy & diversity of data transmission over several links. MPSec creates multiple, independent data pathways between two or more locations.

Used to configure about MPSec



Local VPN Name

Local VPN IP

Polling Interval (ms): 5000

Index	Remote VPN Name	Remote VPN IP	Load Balancing Option	Load Balancing Type
No data available in table				

Select Site Name: None

Copyright © 2000-2016. FatPipe Networks Inc.

Specify how often MPSec paths are tested for Up / Down status

Click to view the advanced settings for MPSec paths

Click ‘Add’ to enter the remote location name

Select a remote site

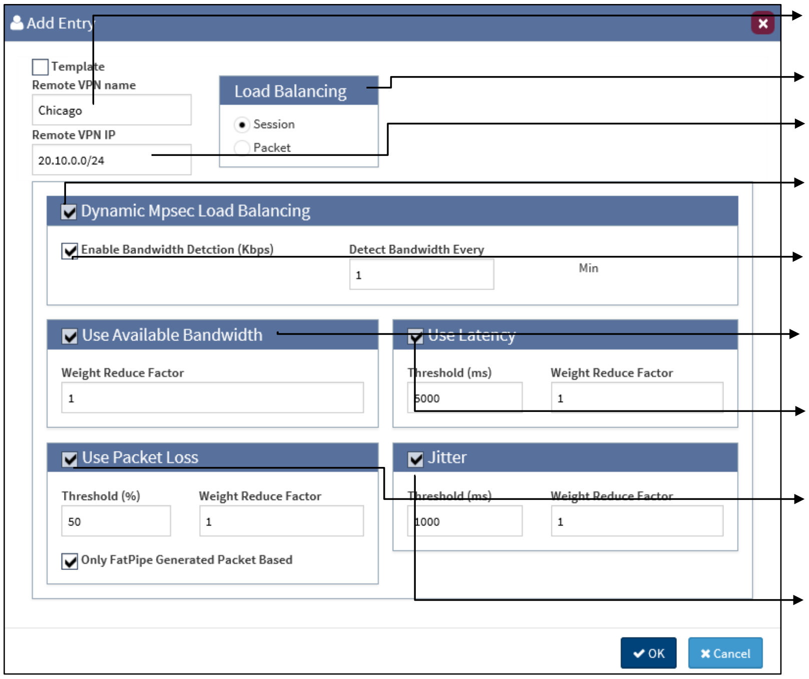
Click ‘Configure’ to modify/add/change path connectivity

Click ‘Status’ to visually show connection status for the selected Site Name

Click to clear the FatPipe WAN Optimization local cache store

MPSEC CONFIGURATION

Used to enter information about Remote Network and view MPSec status



☐ Template

Remote VPN name: Chicago

Remote VPN IP: 20.10.0.0/24

Load Balancing: ● Session ○ Packet

☑ Dynamic Mpsec Load Balancing

☑ Enable Bandwidth Detction (Kbps) — Detect Bandwidth Every: 1 Min

☑ Use Available Bandwidth — Weight Reduce Factor: 1

☑ Use Latency — Threshold (ms): 5000 — Weight Reduce Factor: 1

☑ Use Packet Loss — Threshold (%): 50 — Weight Reduce Factor: 1

☑ Only FatPipe Generated Packet Based

☑ Jitter — Threshold (ms): 1000 — Weight Reduce Factor: 1

Name of the remote site

Select the load balancing option for MPSec traffic

Enter the remote network subnet in CIDR notation

Click to enable Dynamic MPSec Load Balancing using various WAN parameters of the link

Enable to detect bandwidth between two units for all the configured MPSec paths.

Enable to modify the Weight Reducing Factor, up to 10 from 1(by default) for Available Bandwidth

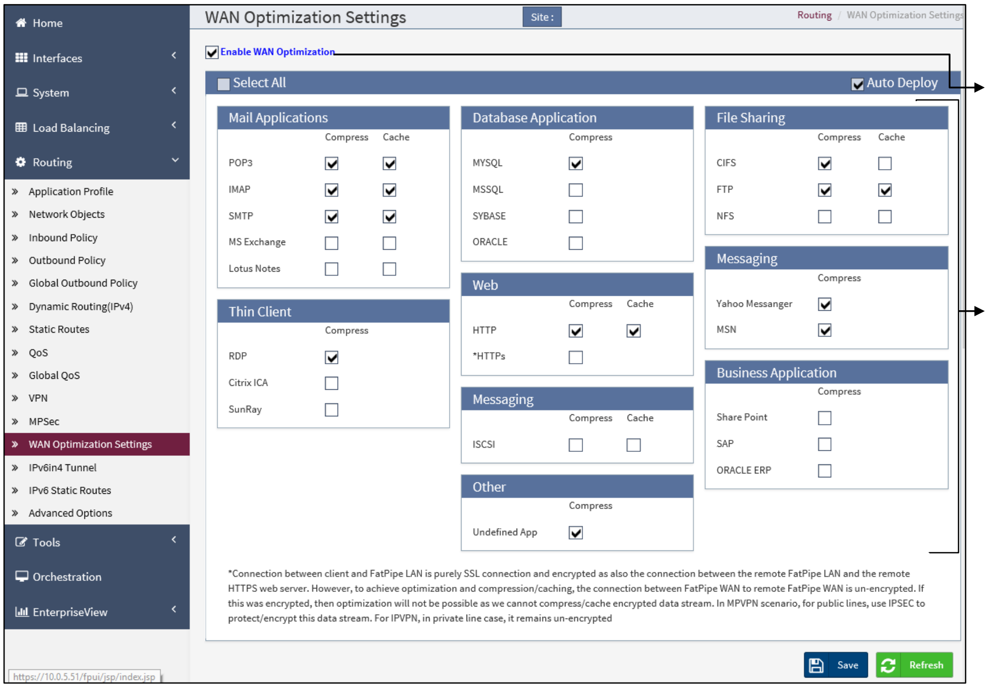
Enable to modify the Weight Reducing Factor and Threshold value for Latency

Enable to modify the Weight Reducing Factor and Threshold value for Packet Loss. Packet Loss is calculated from each MPSec ping interval

Enable to modify the Weight Reducing Factor and Threshold value for Jitter

WAN OPTIMIZATION CONFIGURATION

To configure WAN Optimization for the listed protocols and applications



WAN Optimization Settings

☑ Enable WAN Optimization

☐ Select All — ☑ Auto Deploy

Mail Applications

	Compress	Cache
POP3	☑	☑
IMAP	☑	☑
SMTP	☑	☑
MS Exchange	☐	☐
Lotus Notes	☐	☐

Thin Client

	Compress
RDP	☑
Citrix ICA	☐
SunRay	☐

Database Application

	Compress
MYSQL	☑
MSSQL	☐
SYBASE	☐
ORACLE	☐

Web

	Compress	Cache
HTTP	☑	☑
*HTTPs	☐	

Messaging

	Compress	Cache
ISCSI	☐	☐

Other

	Compress
Undefined App	☑

File Sharing

	Compress	Cache
CIFS	☑	☐
FTP	☑	☑
NFS	☐	☐

Messaging

	Compress
Yahoo Messanger	☑
MSN	☑

Business Application

	Compress
Share Point	☐
SAP	☐
ORACLE ERP	☐

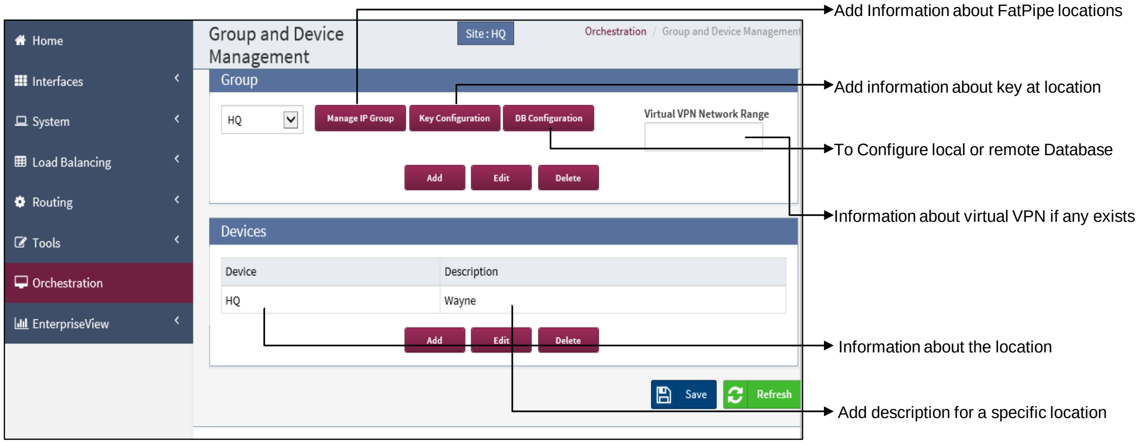
*Connection between client and FatPipe LAN is purely SSL connection and encrypted as also the connection between the remote FatPipe LAN and the remote HTTPS web server. However, to achieve optimization and compression/caching, the connection between FatPipe WAN to remote FatPipe WAN is un-encrypted. If this was encrypted, then optimization will not be possible as we cannot compress/cache encrypted data stream. In MPVPN scenario, for public lines, use IPSEC to protect/encrypt this data stream. For IPVPN, in private line case, it remains un-encrypted

Click to Enable WAN Optimization

Select the protocols to be optimized and then select whether to use Compression only or Caching only or both Compression and Caching to get maximum optimization.

ORCHESTRATION

Used to Manage FatPipes located at different locations



Group: HQ

Virtual VPN Network Range:

Device	Description
HQ	Wayne

Add Information about FatPipe locations

Add information about key at location

To Configure local or remote Database

Information about virtual VPN if any exists

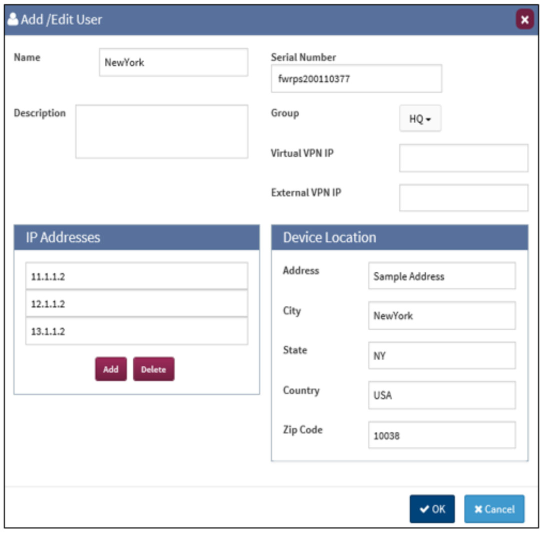
Information about the location

Add description for a specific location

Allows a user to manage all the FatPipe appliances in their network from a single console without the burden of logging into each unit individually. The units can be organized into groups and configured with a secret key for inter unit communication.

ORCHESTRATION

Used to Manage FatPipes located at different locations



Name: NewYork

Serial Number: fwrps200110377

Description:

Group: HQ

Virtual VPN IP:

External VPN IP:

IP Addresses: 11.1.1.2, 12.1.1.2, 13.1.1.2

Address: Sample Address

City: NewYork

State: NY

Country: USA

Zip Code: 10038

Enter a Name for the device, FatPipe Serial Number of the device (Serial Number is case sensitive therefore ensure that the serial number is correct). Enter a relevant description of the device select the group name where it belongs.

To access the GUI of the device WAN IP address are needed. Enter the WAN IP address of the remote device which you want to access. To add an IP address click the Add button under the IP address section. Add all the wan IP address one by one.