DEPLOYMENT GUIDE:

Configuring FatPipe v 9.1.2 for Use

With Zscaler Internet Access

Revision 2.2
December 2018

4455 South 700 East, Salt Lake City, UT 84107
Tel: (801)281-3434 Fax: (801)281-0317
www.FatPipe.com

4455 South 700 East, Salt Lake City, UT 84107
Tel: (801)281-3434 Fax: (801)281-0317
www.FatPipe.com

For any additional questions regarding FatPIpe – Zscaler deployment, please contact:

FatPipe Technical Support

1 (800) 724-8521 Option 3
+1 (801) 281-3434 Option 3
support@fatpipeinc.com
Skype: fp.support
Web Chat: http://chat.fatpipeinc.com/chat.php

4455 South 700 East, Salt Lake City, UT 84107
Tel: (801)281-3434 Fax: (801)281-0317
www.FatPipe.com

TABLE OF CONTENTS

About Zscaler Internet Access 1

Before You Begin 2

Prerequisites 2

Planning Your FatPipe – Zscaler Integration 2

Connecting to ZIA via GRE (Preferred Method) 3

Create Outbound Policy 3

Create GRE Tunnel to ZIA 5

Connecting to ZIA via IPSec (Required for Dynamic IP Addresses) 7

Create Outbound Policy 7

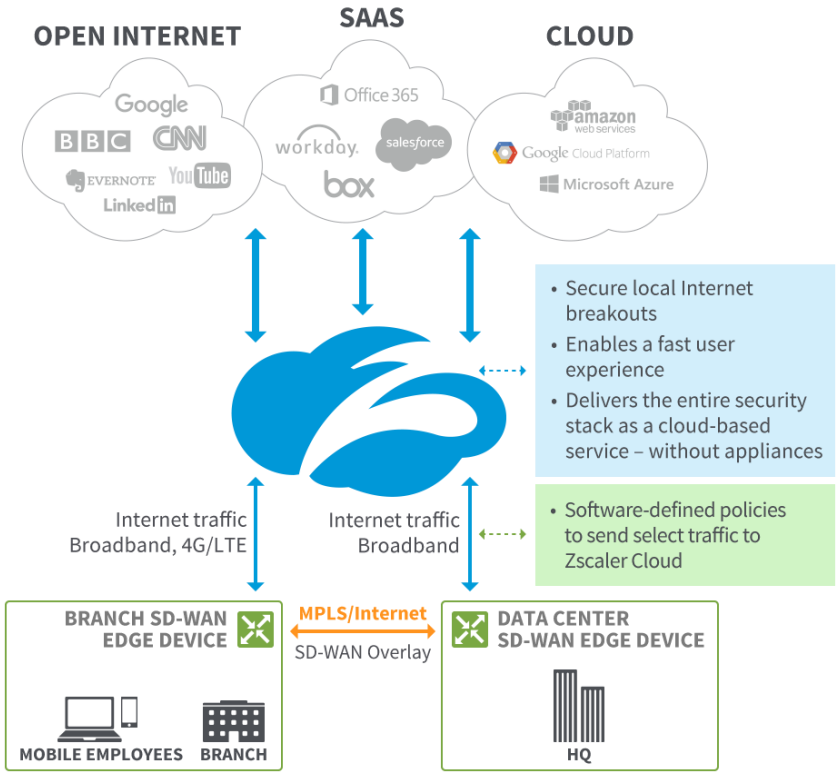
Create IPSec Tunnel to ZIA 10

Validate Configuration 13

Route Test 13

ABOUT ZSCALER INTERNET ACCESS

Zscaler secures direct-to-internet connections and delivers a fast user experience — without backhauling and without the cost and complexity of duplicating the appliance security stack at each location. With Zscaler in combination with your FatPipe SD-WAN can reduce MPLS costs and provide a fast and secure user experience.



BEFORE YOU BEGIN

PREREQUISITES

The following items are required for configuring FatPipe and Zscaler Internet Access integration:

- FatPipe MPVPN, FatPipe IPVPN, or FatPipe SD-WAN appliance running v9.1.2 or later
  - Optional – FatPipe Orchestrator v9.1.2 or later
  - Note: If you have a FatPipe WARP, please contact your FatPipe customer care specialist to upgrade to FatPipe MPVPN.
- Active Zscaler Internet Access Instance
  - Administrator login credentials for this instance

PLANNING YOUR FATPIPE – ZSCALER INTEGRATION

FatPipe supports tunneling traffic to Zscaler Internet Access (ZIA) via two methods.

- **GRE: This is the preferred method.** This requires a static IPv4 address
- **IPSec:** For locations with dynamic IPv4 addressing, IPsec must be used.

Prior to configuring the FatPipe you should decide whether GRE or IPSec tunneling to ZIA is appropriate for the location you are deploying. FatPipe routes traffic to ZIA via an outbound policy for all traffic (0.0.0.0 or *). The ZIA policy should be the last policy on your outbound policy list. FatPipe will route ALL traffic not matching a higher policy in the list to ZIA for further firewalling.

- **NOTE: ANY OUTBOUND POLICY BELOW THE ZIA (0.0.0.0 or *) POLICY WILL NOT BE FOLLOWED**

Before configuring FatPipe to integrate with Zscaler, verify the following:

1. Ensure access to an active Zscaler subscription for Zscaler Internet Access.

2. Choose a root FQDN for the Zscaler subscription account that will be used for credentials for each site or Service Center (ex: @mycompanydomain.com). If this FQDN is not yet registered and authorized in the Zscaler account, open a ticket with Zscaler and request that FQDN be added to the account:
   a. https://help.zscaler.com/submit-ticket

3. Create a comprehensive list of all the Zscaler Enforcement Nodes (ZEN) VPN Host names you wish to be used by all sites and/or Service Centers.

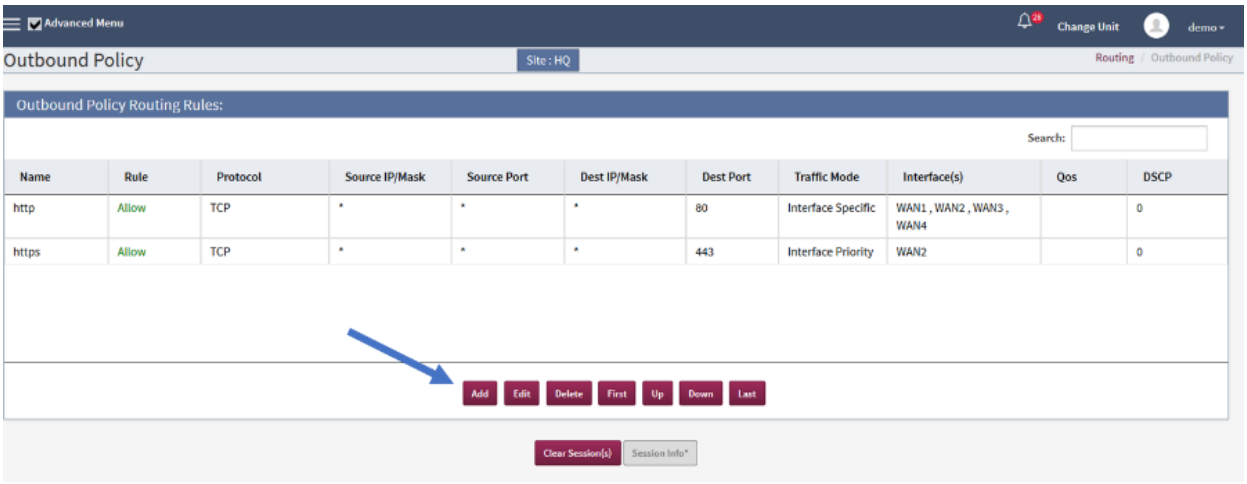
4. The full list of available hostnames can be obtained for each Zscaler environment by using the corresponding URL:
   a. https://ips.zscaler.net/cenr
   b. https://ips.zscalerone.net/cenr
   c. https://ips.zscalertwo.net/cenr
   d. https://ips.zscalerthree.net/cenr/
   e. https://ips.zscalerbeta.net/cenr

CONNECTING TO ZIA VIA GRE (PREFERRED METHOD)

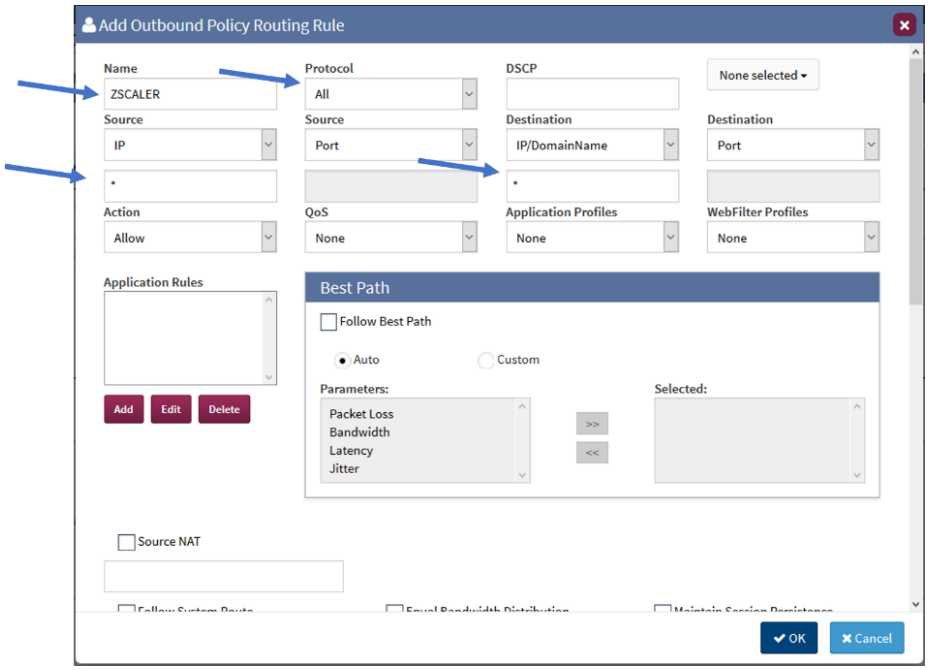
To route traffic to ZIA via GRE, you will need to create an outbound policy for to determine what traffic to route to ZIA and build the GRE tunnel to ZIA.

CREATE OUTBOUND POLICY

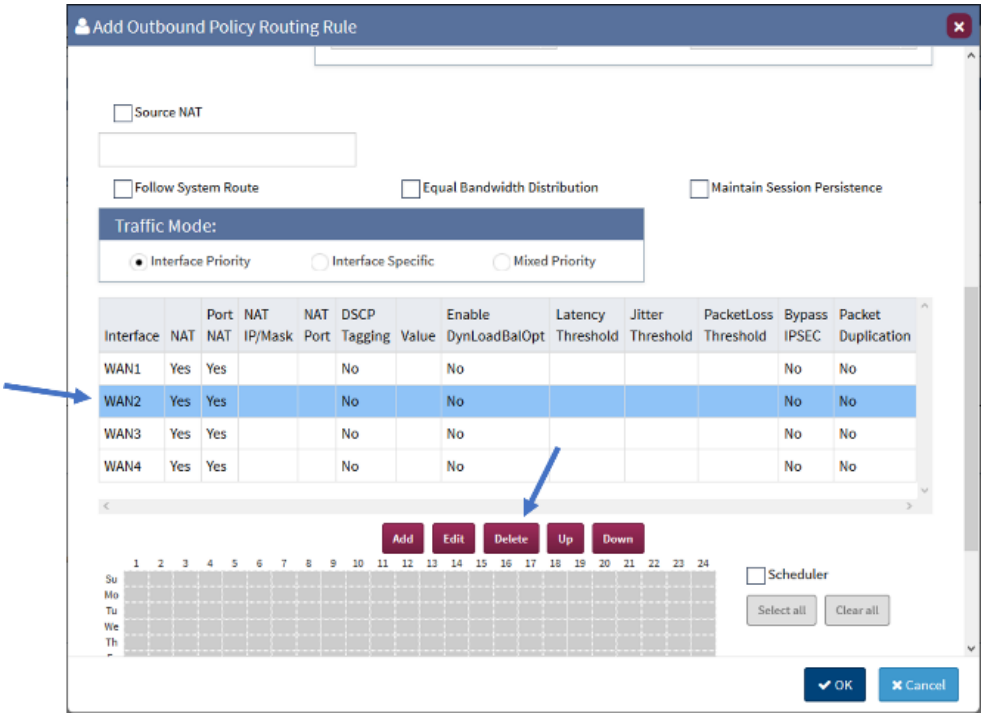
1. Select “Outbound Policy” from the “Routing” section, then select “Add”
    a. NOTE – “Advanced Menu” must be checked to have “Routing” section visible.



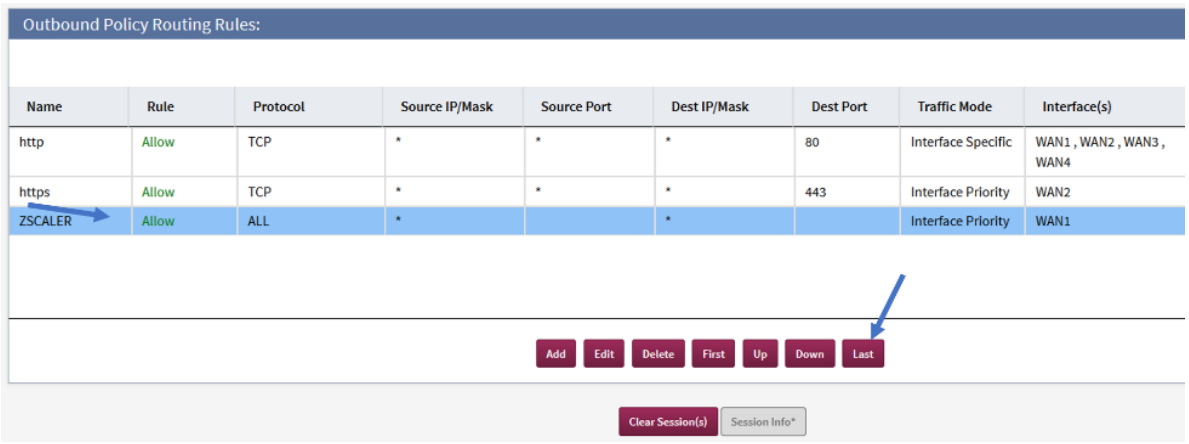
2. Fill in traffic identification parameters in the new Outbound Policy
    a. Name the Outbound Policy
    b. Select Protocol = “All”
    c. Source select “IP”, and fill in the wildcard “*” for all source IPs
    d. Destination select “IP/DomainName”, and fill in the wildcard “*” for all source IPs



3. Remove Outbound Interfaces that will not be used to forward traffic to ZIA
    a. Select WAN Interface(s) to remove one at a time
    b. Select “Delete”
    c. NOTE: This will remove the WAN Interface from this rule only.



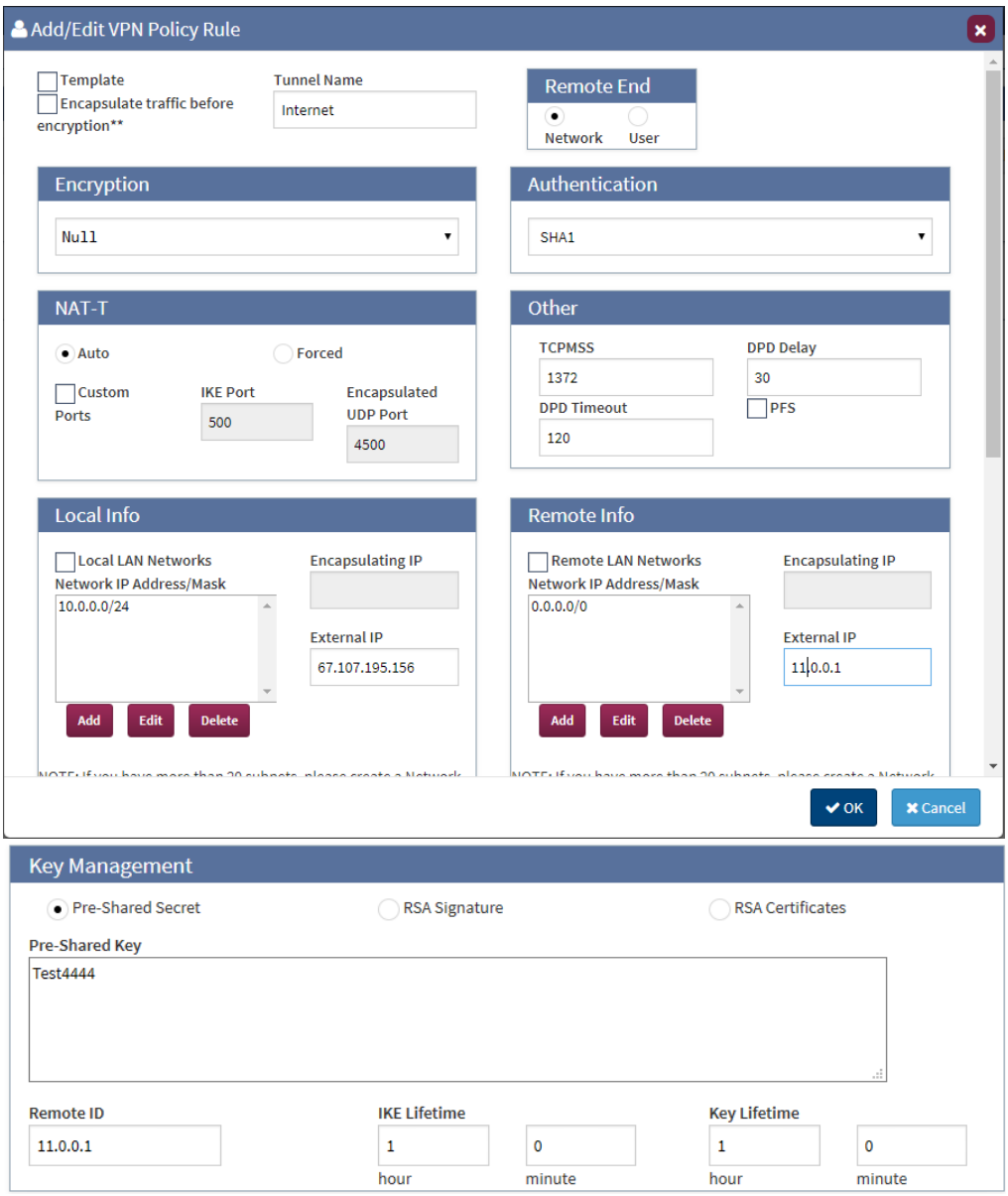
4. Select “OK” to save the Outbound Policy
5. This Outbound Policy should **ALWAYS** be the last policy in the Outbound Policy Routing Rules list. If it is not move it to the bottom of the list
    a. Select the Policy
    b. Select “Last”



6. Remember to save you changes.

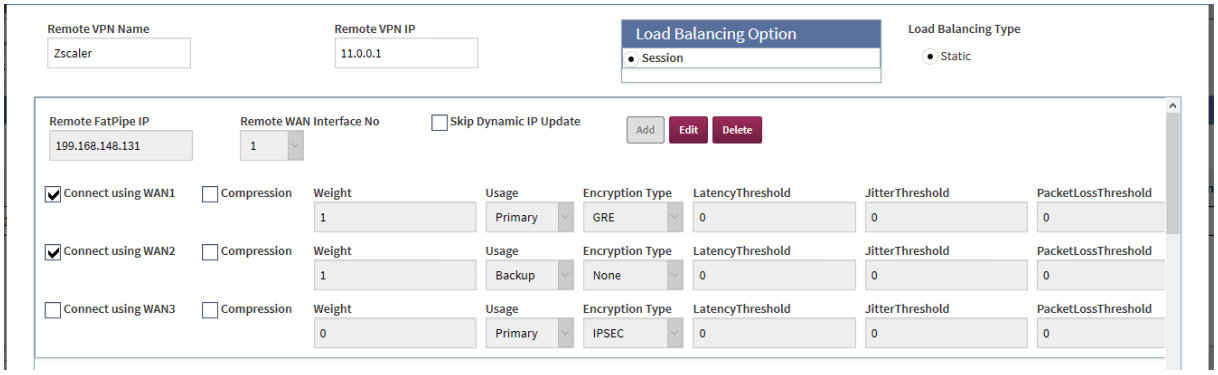
CREATE GRE TUNNEL TO ZIA

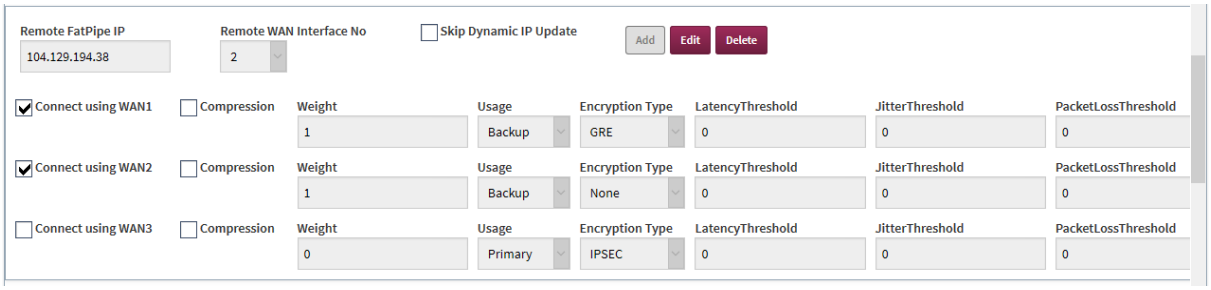
1. Select “VPN” from the “Routing” section, then select “Add”
2. Configure VPN.
    a. Since we are using GRE remote host should be a non-routable IP address



3. Create MPSec paths to ZIA.
    a. Select “MPSec” within the “Routing” section, then “Add”
        i. Name the MPSec Rule (Remote Network name)
        ii. Input Remote VPN IP Address
            1. 11.0.0.1(Matches fake peer in VPN policy)
        iii. Confirm Session Load Balancing in selected
        iv. Select OK

4. Add Paths to the ZIA
    a. Select “Add”, next to the first window
        i. Input “Remote FatPipe IP”
            1. This is the Assign IP address from Zscaler of your Primary GRE Tunnel
        ii. Remote WAN Interface No = 1(This will not be used)
        iii. Check “GRE”
            1. Select Usage = Primary
            2. Second path for backup Internet select backup and none for encryption.
    b. Select “Add”, next to the second window
        i. Input “Remote FatPipe IP”
            1. This is the Assign IP address from Zscaler of your Backup GRE Tunnel
        ii. Remote WAN Interface No = 2(This will not be used)
        iii. Check “GRE” for first path and none for second.
        iv. Select Usage = Backup for both paths.
    c. Select “OK” at the bottom of the “Add Path” window
    d. Select “Save” at the bottom of the configuration interface.



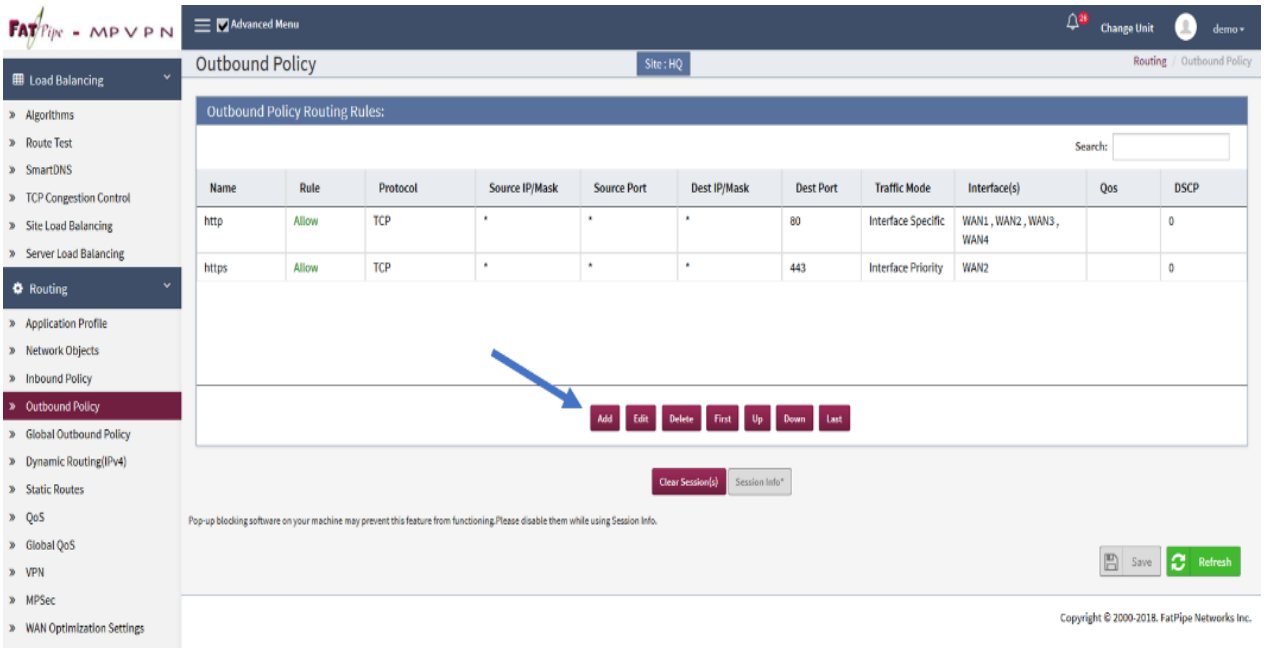


CONNECTING TO ZIA VIA IPSEC (REQUIRED FOR DYNAMIC IP ADDRESSES)

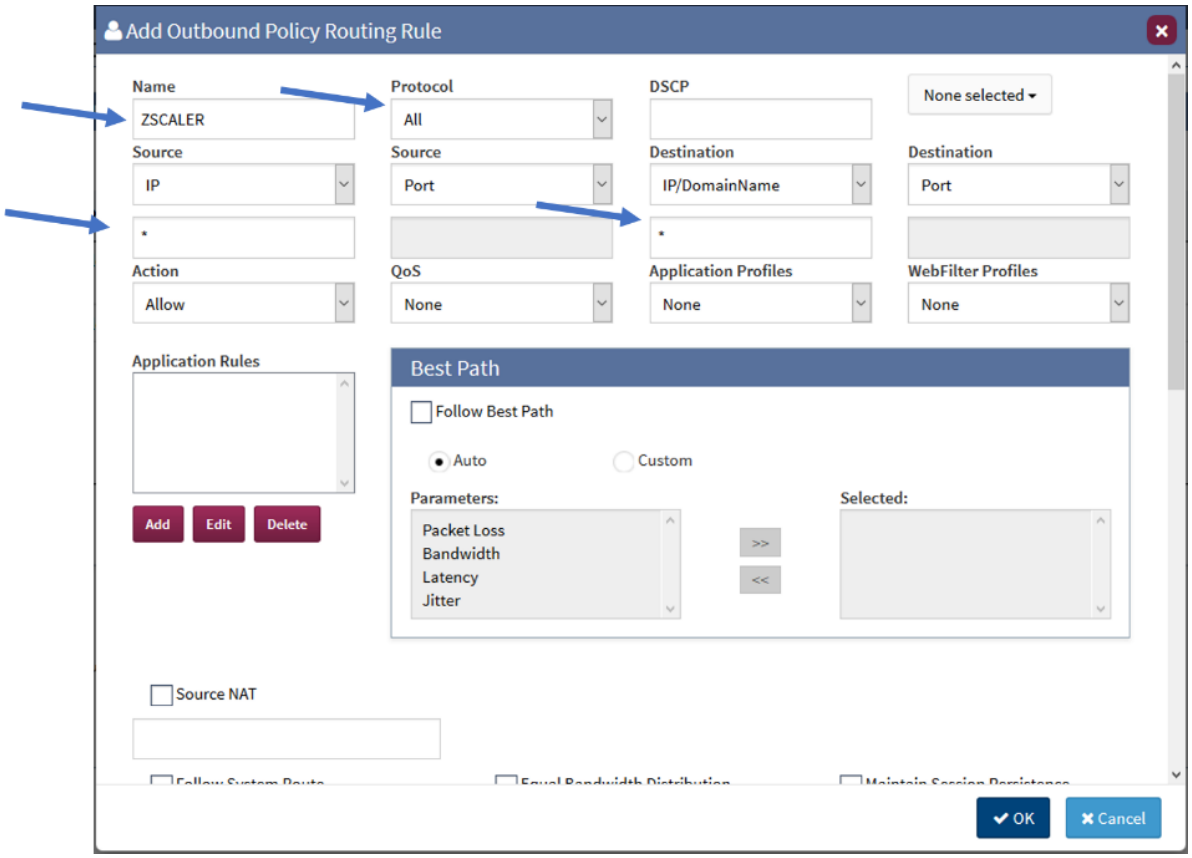
To route traffic to ZIA via IPSec, you will need to create an outbound policy for to determine what traffic to route to ZIA and build the IPSec tunnel to ZIA.

CREATE OUTBOUND POLICY

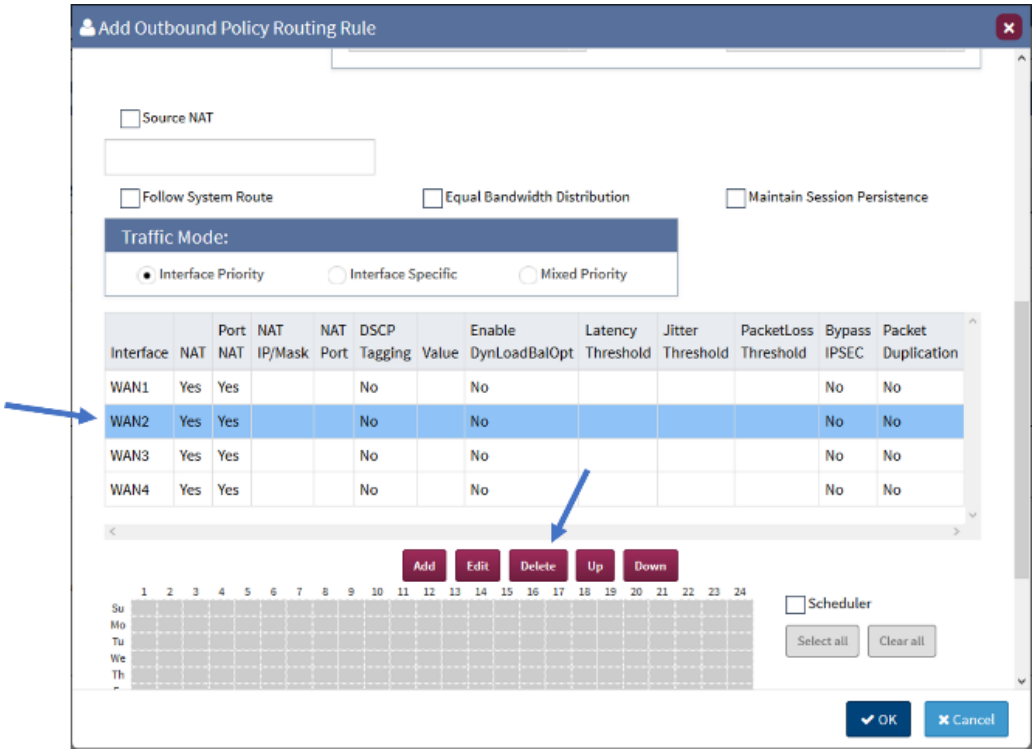
1. Select “Outbound Policy” from the “Routing” section, then select “Add”
    a. NOTE – “Advanced Menu” must be checked to have “Routing” section visible.



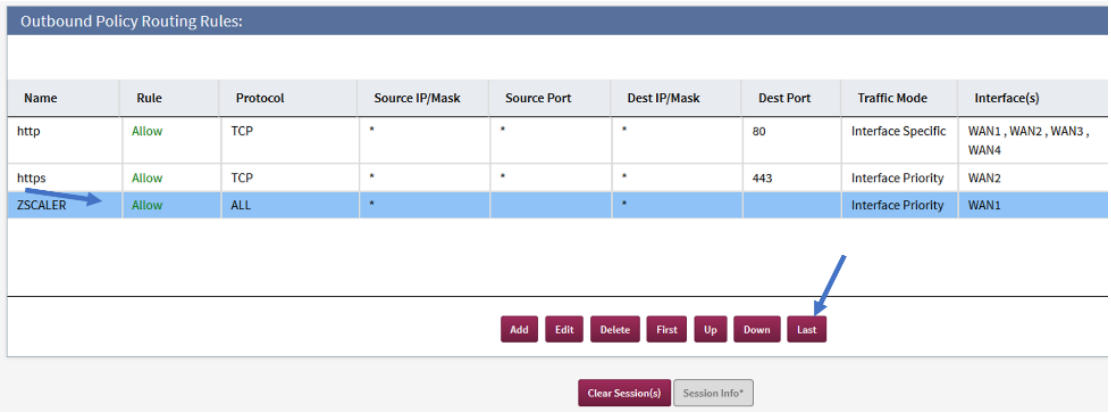
2. Fill in traffic identification parameters in the new Outbound Policy
    a. Name the Outbound Policy
    b. Select Protocol = “All”
    c. Source select “IP”, and fill in the wildcard “*” for all source IPs
    d. Destination select “IP/DomainName”, and fill in the wildcard “*” for all source IPs



3. Remove Outbound Interfaces that will not be used to forward traffic to ZIA
    a. Select WAN Interface(s) to remove one at a time
    b. Select “Delete”
    c. NOTE: This will remove the WAN Interface from this rule only.



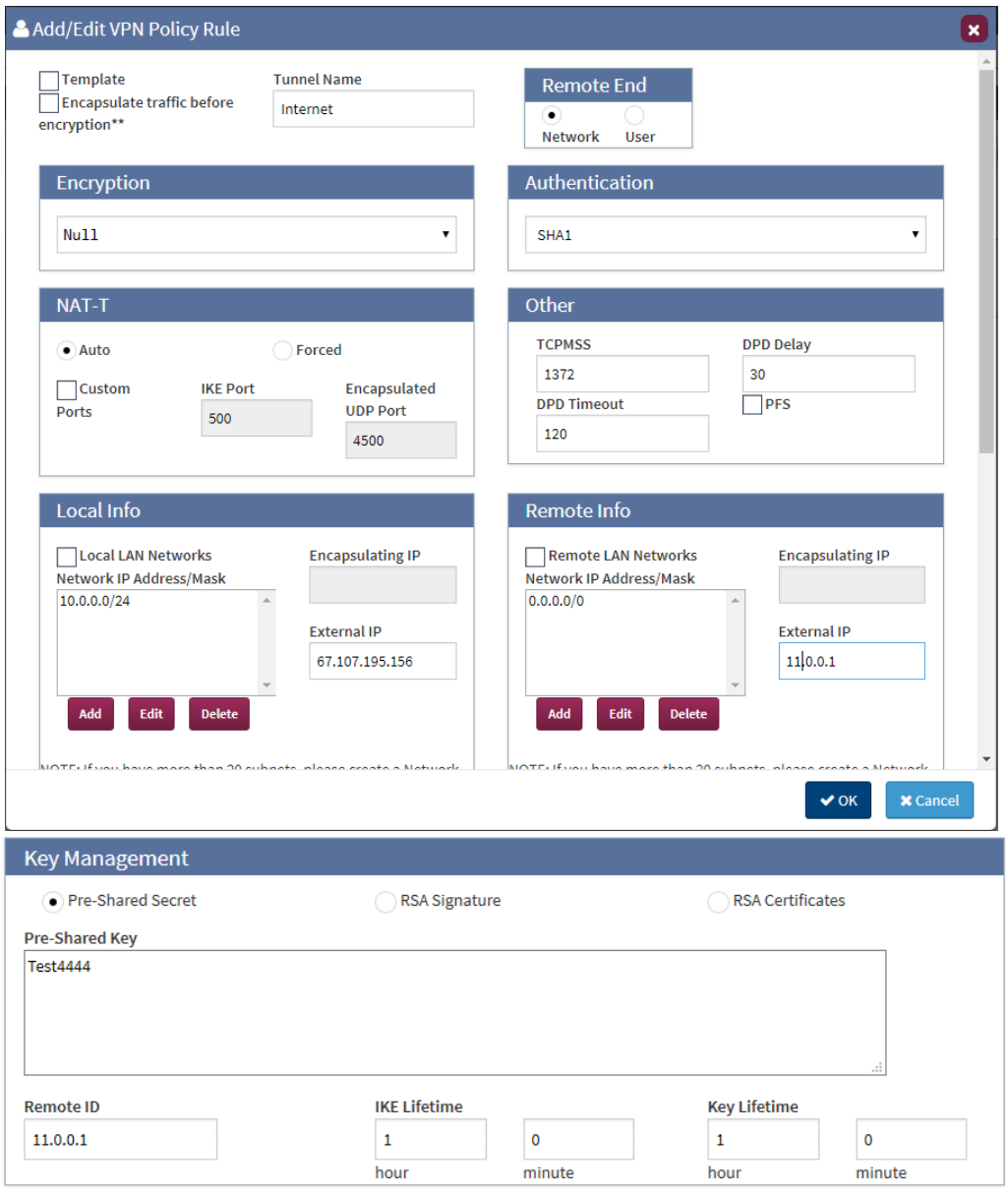
4. Select “OK” to save the Outbound Policy
5. This Outbound Policy should **<u>ALWAYS</u>** be the last policy in the Outbound Policy Routing Rules list. If it is not move it to the bottom of the list
    a. Select the Policy
    b. Select “Last”



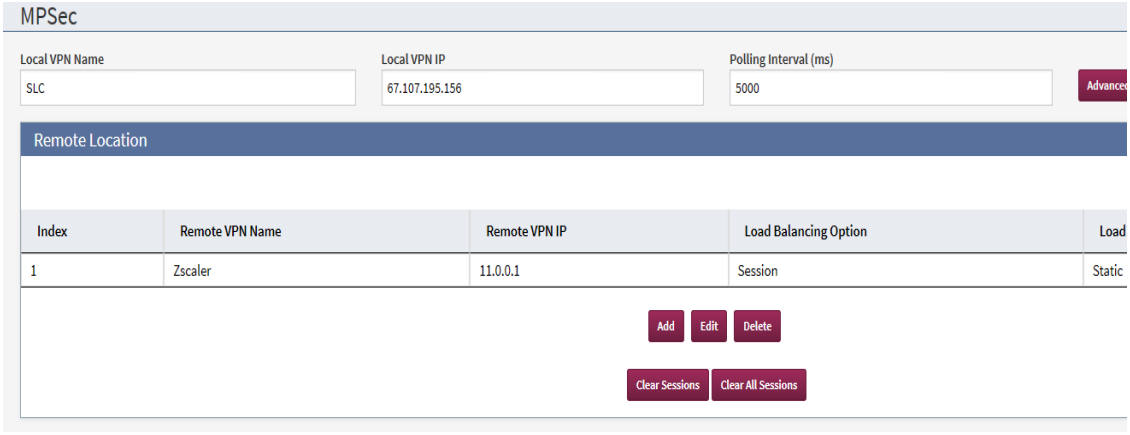
6. Remember to save your changes Create IPSec Tunnel to ZIA

CREATE IPSEC TUNNEL TO ZIA

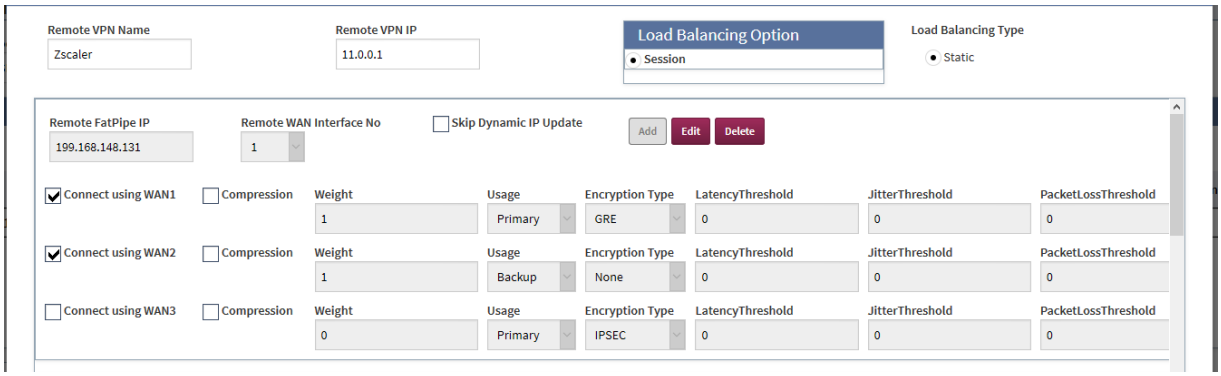
1. Select “VPN” from the “Routing” section, then select “Add”
2. Configure VPN.
    a. Since we are using VPN remote host should be the Zscaler VPN IP address

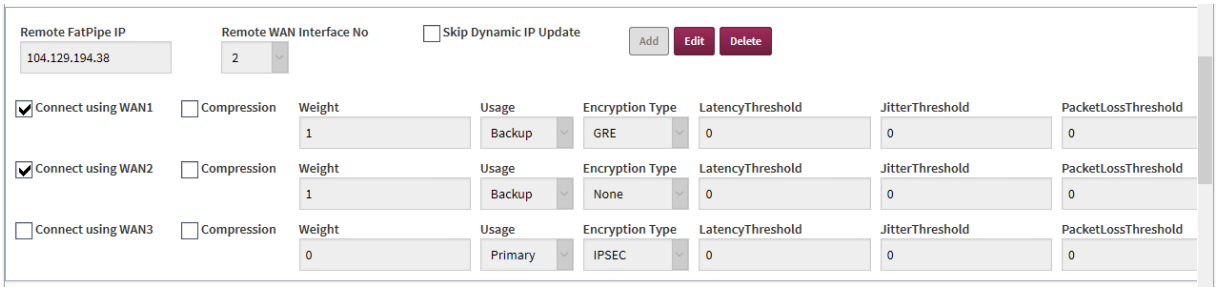


3. Create MPSec paths to ZIA.
    a. Select “MPSec” within the “Routing” section, then “Add”
        i. Name the MPSec Rule (Remote Network name)
        ii. Input Remote VPN IP Address
            1. (Matches peer in VPN policy)
        iii. Confirm Session Load Balancing in selected
        iv. Select OK



4. Add Paths to the ZIA
    a. Select “Add”, next to the first window
        i. Input “Remote FatPipe IP”
            1. This is the Assign IP address from Zscaler of your Primary VPN Tunnel
        ii. Remote WAN Interface No = 1(This will not be used)
        iii. Check “IPSec”
            1. Select Usage = Primary
            2. Second path for backup Internet select backup and none for encryption.
    b. Select “Add”, next to the second window
        i. Input “Remote FatPipe IP”
            1. This is the Assign IP address from Zscaler of your Backup VPN Tunnel
        ii. Remote WAN Interface No = 2(This will not be used)
        iii. Check “IPSec” for first path and none for second.
        iv. Select Usage = Backup for both paths.
    c. Select “OK” at the bottom of the “Add Path” window
    d. Select “Save” at the bottom of the configuration interface.

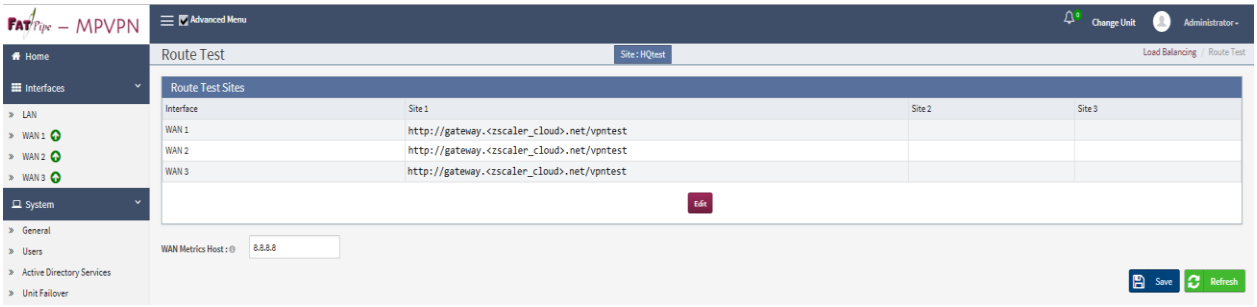




VALIDATE CONFIGURATION

ROUTE TEST

1. Select “Route Test” under “Load Balancing” tab
2. Select WAN1 and click “Edit”
3. Enter the URL as show in the screenshot below
4. Configure the same for all the required WAN interfaces
5. Click “Save”



Note: <zscaler_cloud> IP to be confirmed by Zscaler

Once you have configured FatPipe to direct traffic to ZIA, you can confirm the traffic is actually traversing Zscaler.

1. Open a browser and navigate to:

   https://ip.zscaler.com

2. This screen will confirm your session is actually traversing Zscaler.