Watchguard T30
MDS 3rd Party Integration

CONTENTS

Introduction 3
Assumptions 3
What You Will Need 4
IPSEC Configuration 6
Phase2 Proposals 11
Tunnel Configuration 12
VPN Status Verification 15
Traffic Verification and MDS Web Block 16

INTRODUCTION

Congratulations on your sale of My Digital Shield, using the option to configure existing device(s) to use tunneling protocol.

This guide is written specifically for the **Watchguard Firebox_T30**. It can be used as a reference guide to configure the IPSEC tunnel, which will provide the connection to the MDS cloud.

This guide documents configuration of the Firebox_T30.

ASSUMPTIONS

- **This guide was developed to provide configuration information of the Firebox_T30 gateway specifically for the setup of the IPSEC tunnel to the MDS Cloud.**
- **The configuration was tested using the Firebox_T30 11.10.5.B492938.**
- **This guide is NOT intended to be a full configuration guide for the Firebox_T30.**
- **Responsibility for the management of the Firebox_T30 gateway is not assumed by MyDigitalShield.**
- **The Firebox_T30 should have at least one External and one Trusted interface. This guide does not cover the configuration of ports to be in bridge mode.**
- **The partner should have activated the Firebox T30 in the Watchguard Support site. IPSEC configuration cannot be achieved without activation. To activate, visit http://www.watchguard.com/wgrd-support/overview.**

WHAT YOU WILL NEED

- Any browser such as Firefox, Internet Explorer or Chrome is needed to configure the router.
- The following IP address information:
  - The local public IP address/subnet.
  - The local public IP GW address (your customer's default gateway address).
  - Local LAN network/subnet.
  - The MDS Cloud IP address assigned to you.

In this document, the term "Local" refers to a configuration or IP address at your customer's site. "Cloud" refers to the MyDigitalShield node.

1. **Local Public IP:** The local Public IP address/subnet mask that your customer's ISP provides.
2. **Local Public GW:** The gateway IP address provided by the customer's ISP.
3. **Local LAN Network:** This is the network address that is being used on your customer's LAN.
4. **Cloud Public IP:** This is the address assigned to you by MyDigitalShield. It is the remote IP address at the MDS Node that the IPSEC tunnel will terminate on.

Fill in the middle column of the following table for reference throughout this guide. To map IP addresses that are used in this guide, values in the "Reference Sample" column are used.

Network	IP	Reference Sample
Local Public IP: (x.x.x.x/mask)		24.14.85.102/23
Local Public GW (x.x.x.x)		24.14.84.1
Local LAN Network (x.x.x.x/mask)		192.168.1.0/24
Cloud Public IP (x.x.x.x)		199.91.85.19

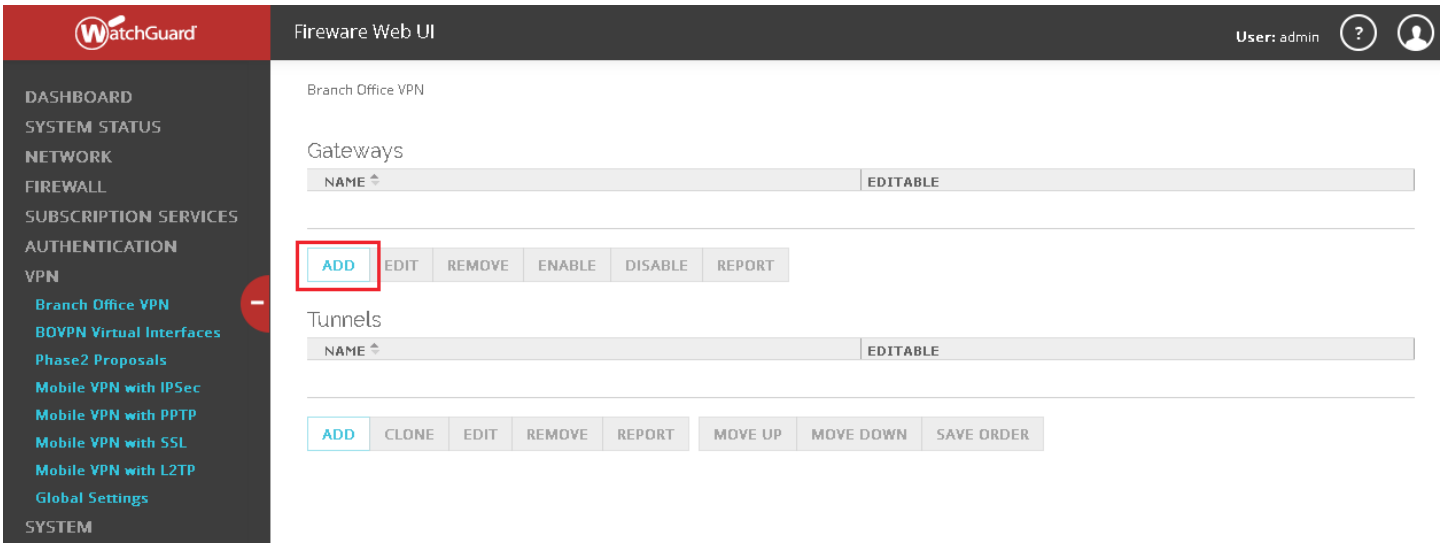
Please reference the sample configuration from the MDS Portal:

IPSEC CONFIGURATION

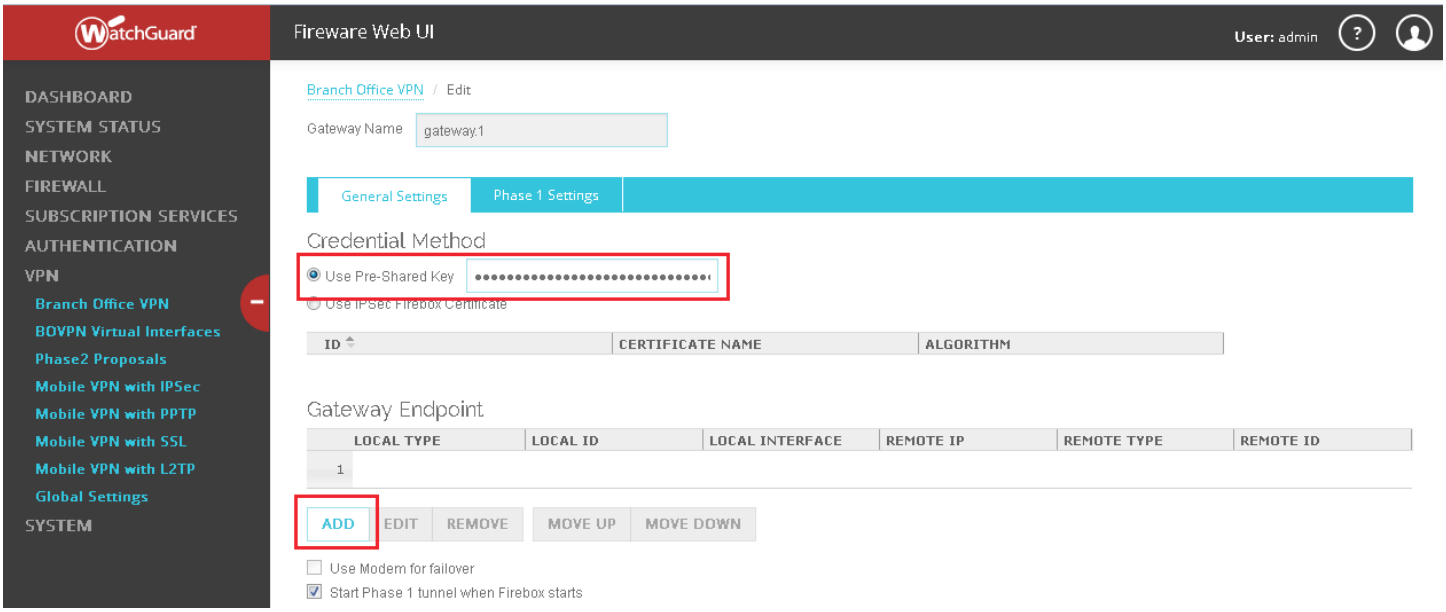
Login to the router using the credentials created during activation.

On the Dashboard click **VPN > Branch Office VPN**.

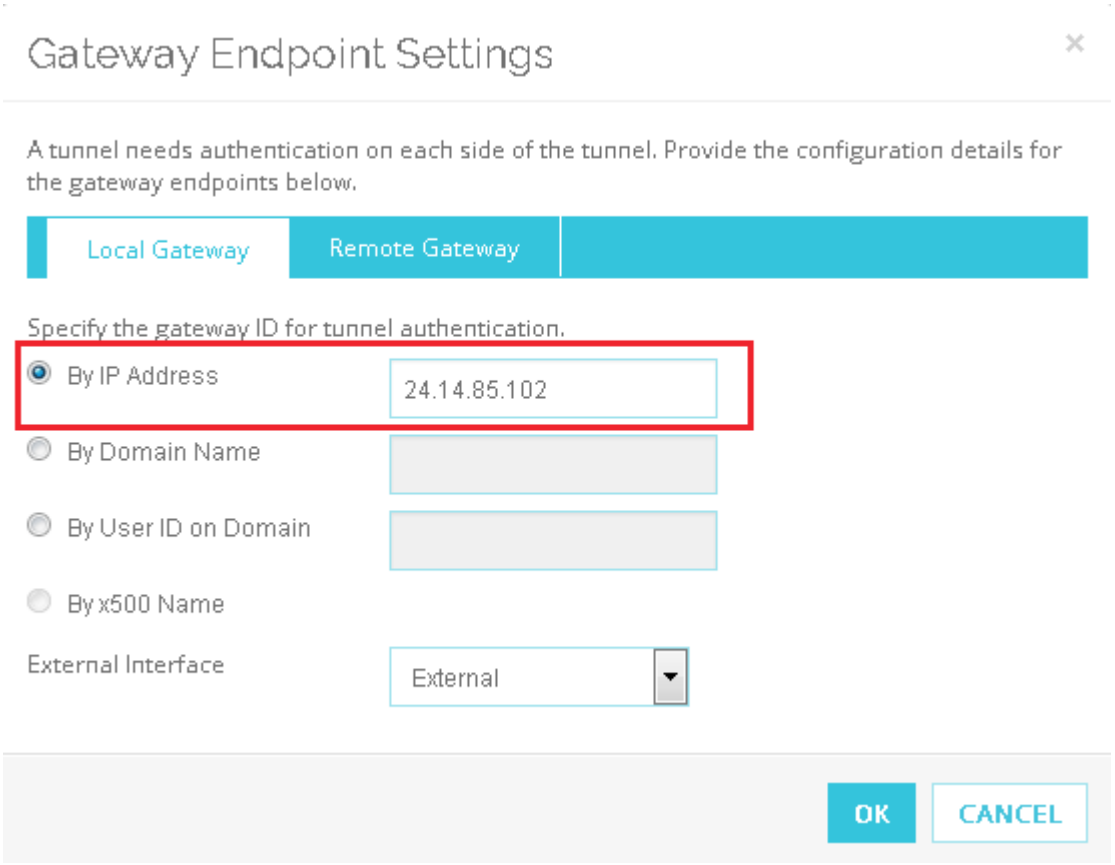
On the Gateway section Click **Add**.



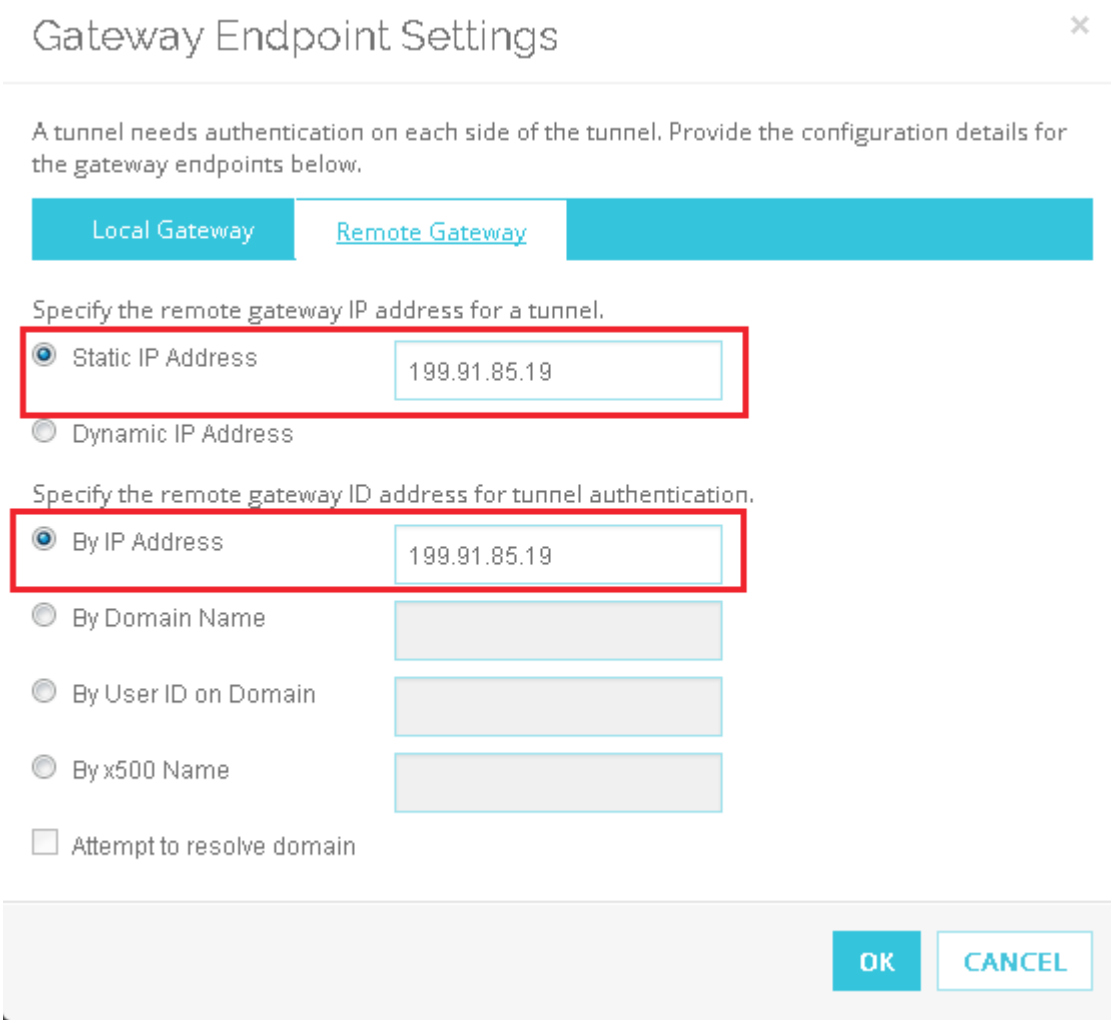
Click the "**Use Pre-Shared Key**" radio button and enter the Preshared Key you defined in the MDS Portal. Click **Add** in the **Gateway Endpoint** section so you can enter the Local and Remote IP.



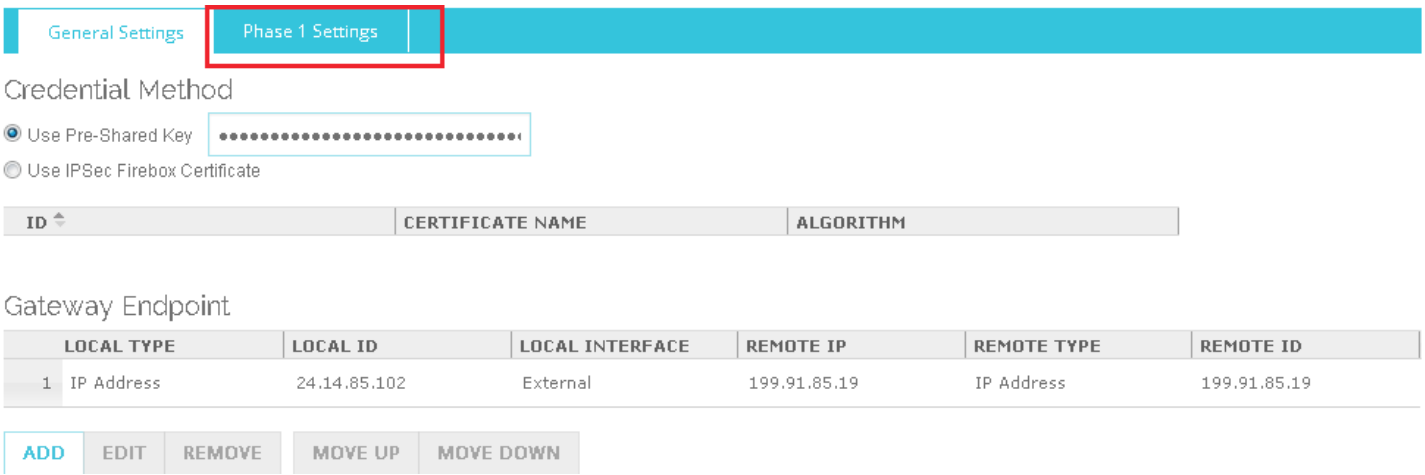
Under Gateway Endpoint Settings in the **Local Gateway** Tab, enter the **Local Public IP**.



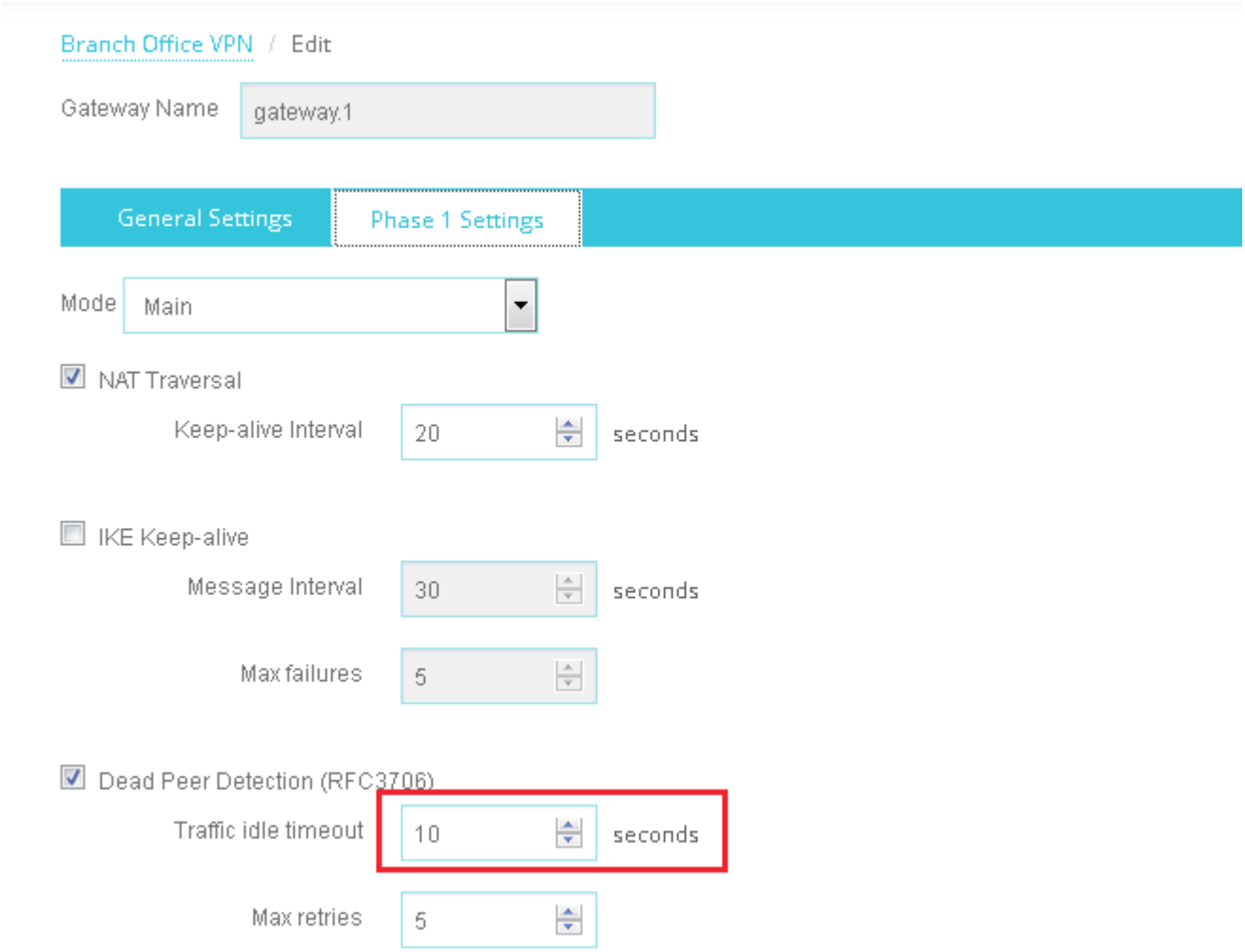
On the **Remote Gateway** tab enter the **Cloud Public IP** in the field provided. Then Click **OK**.



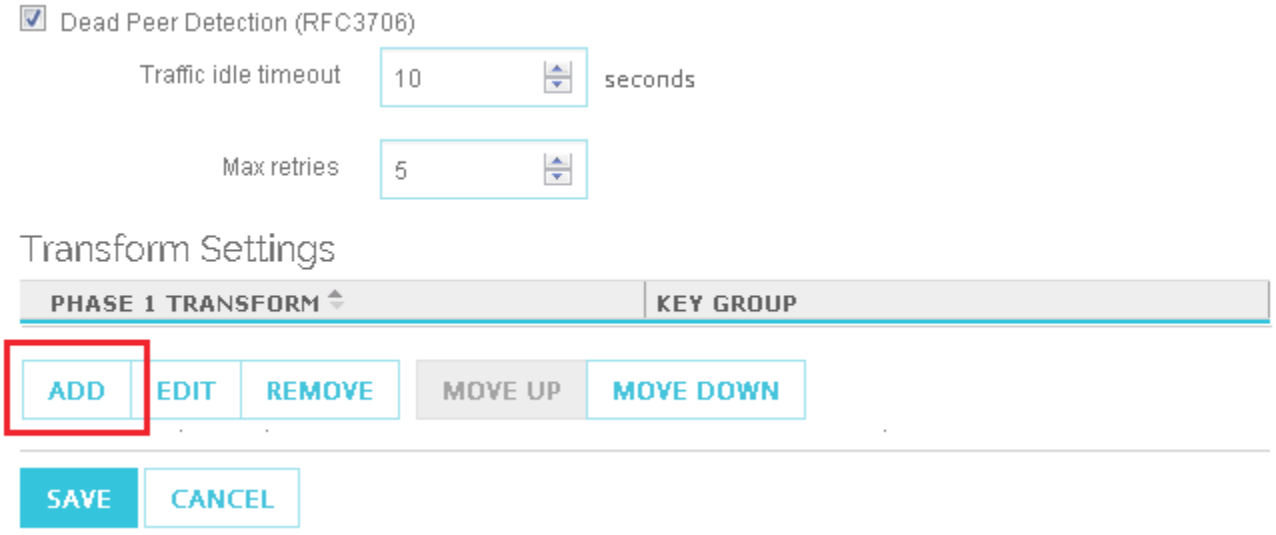
Click on **Phase1 Settings.**



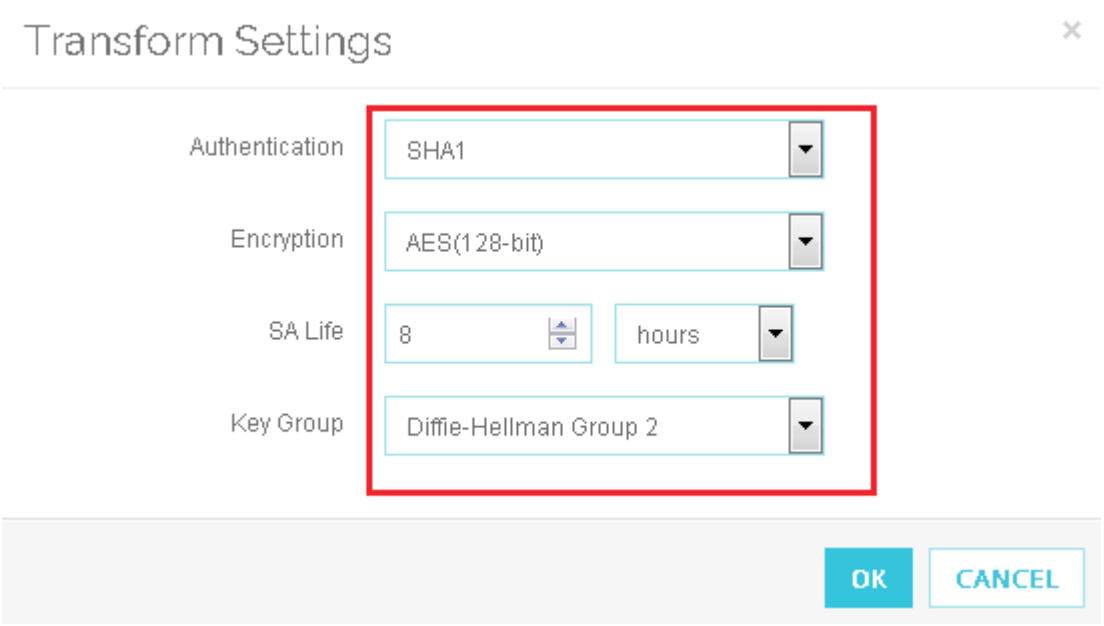
Set **Dead Peer Detection** to 10 seconds.



Click **ADD** under **Phase1 Transform** Settings.

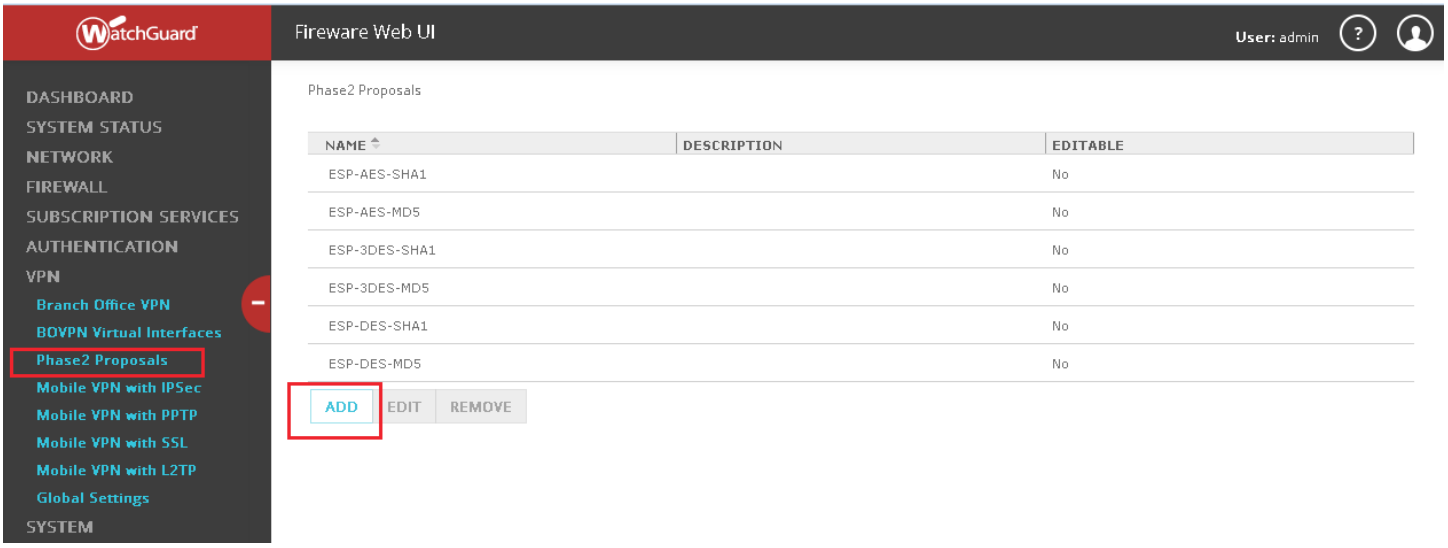


Select the appropriate values as shown below then click **OK**.

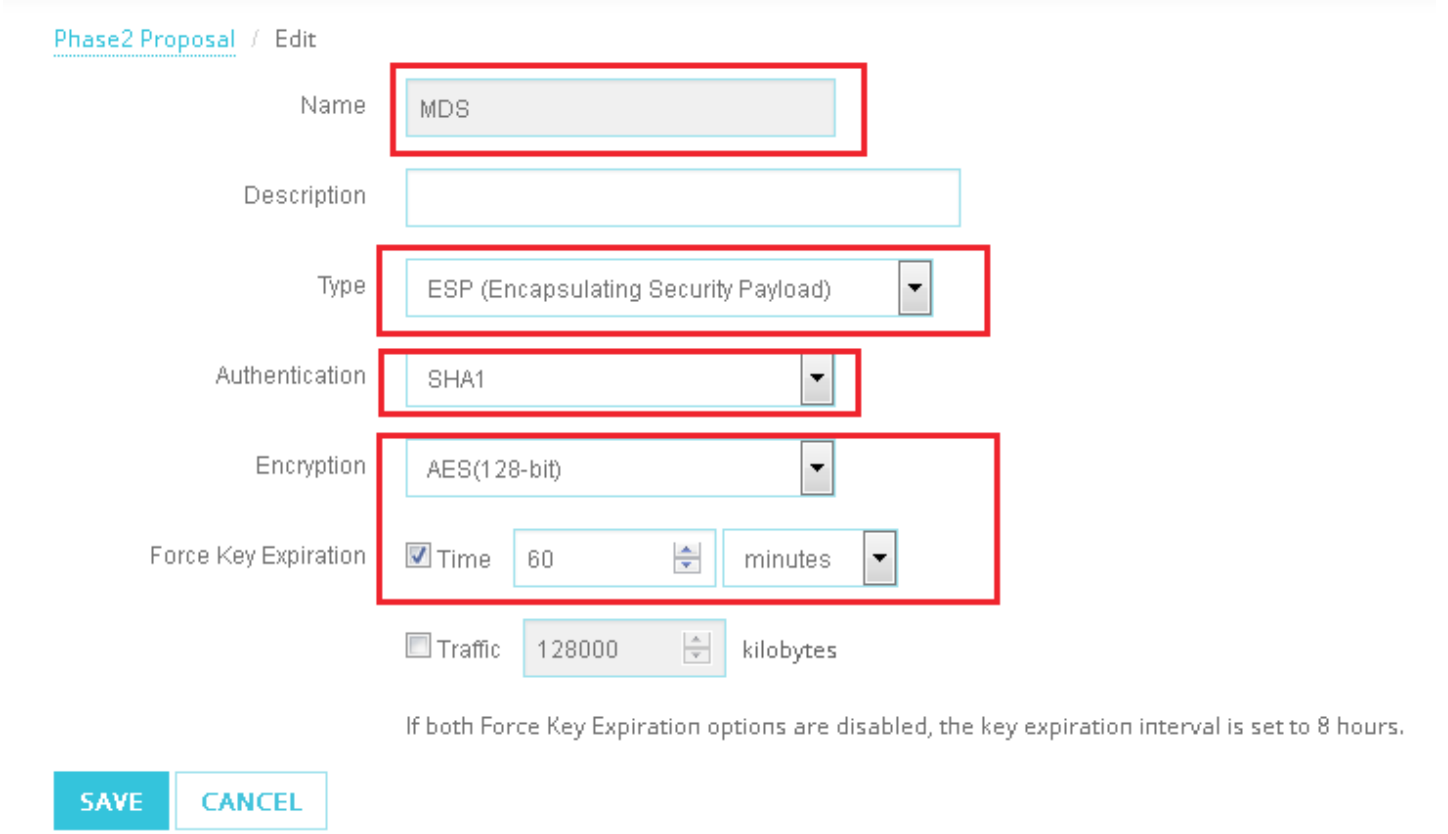


PHASE2 PROPOSALS

Click **Phase2 Proposals** and Click **ADD**.

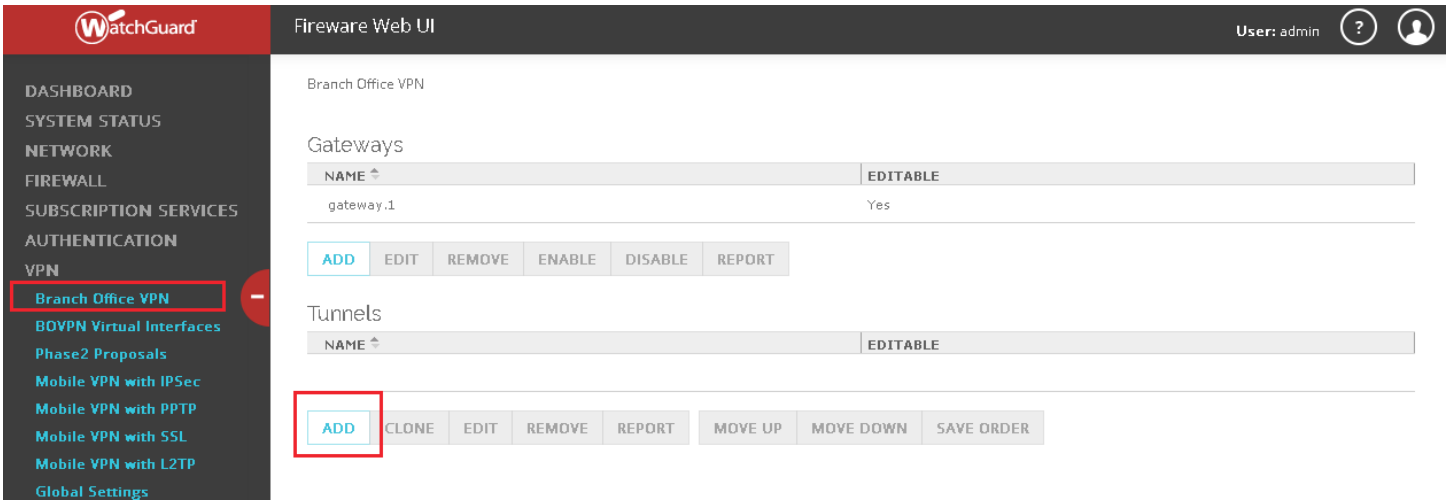


Set the Phase2 Proposal **Name** to MDS. Select the appropriate values as shown below then click **SAVE**.

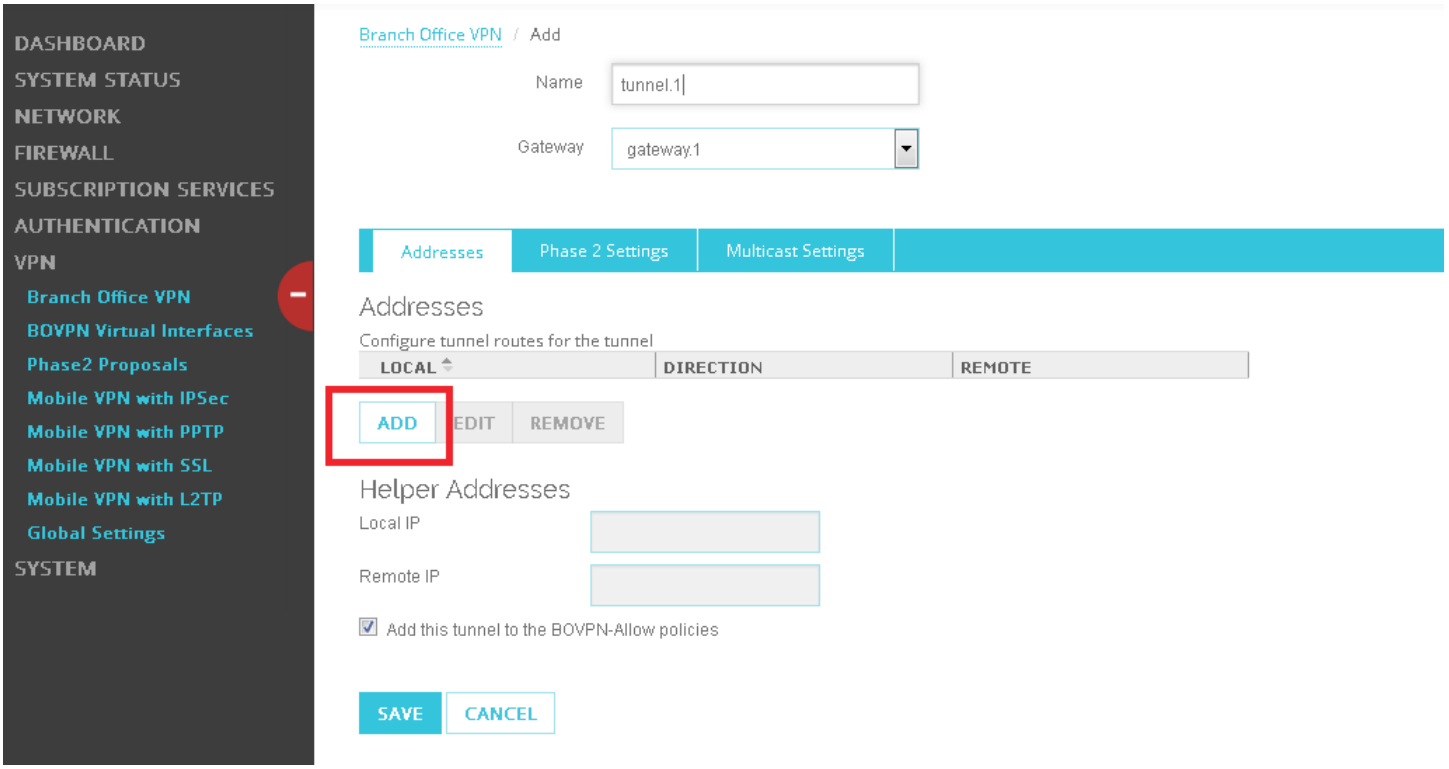


TUNNEL CONFIGURATION

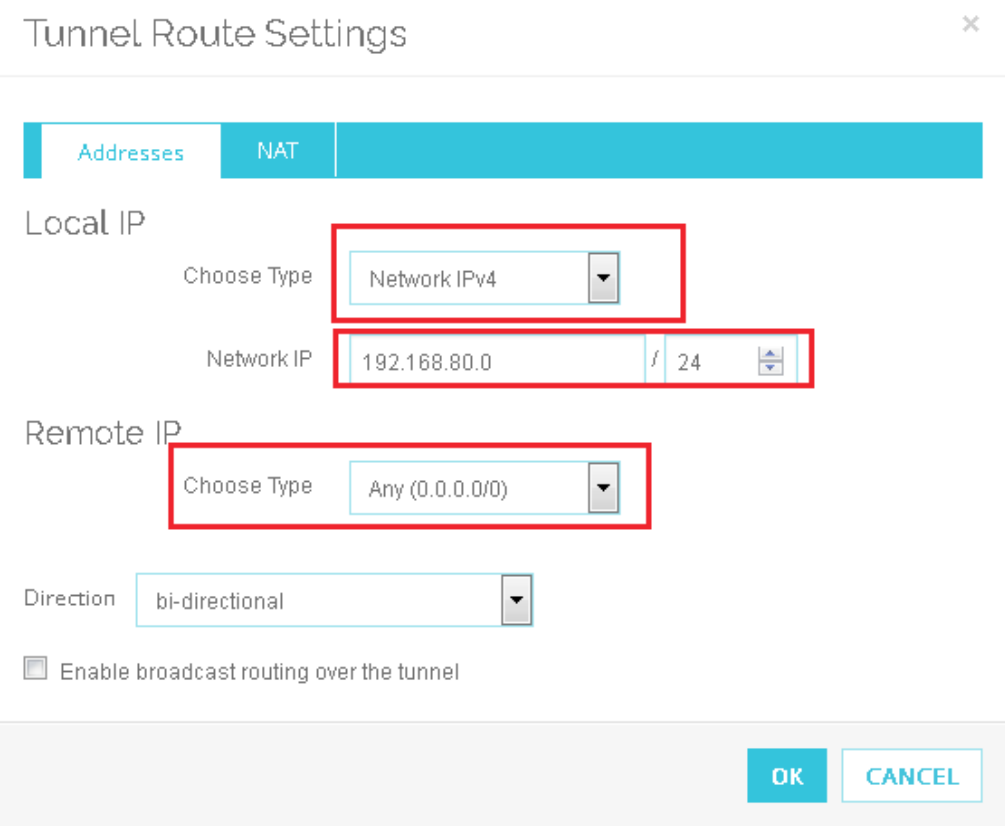
Select **Branch Office VPN**.
Under the **Tunnels** Section, Click **ADD**.



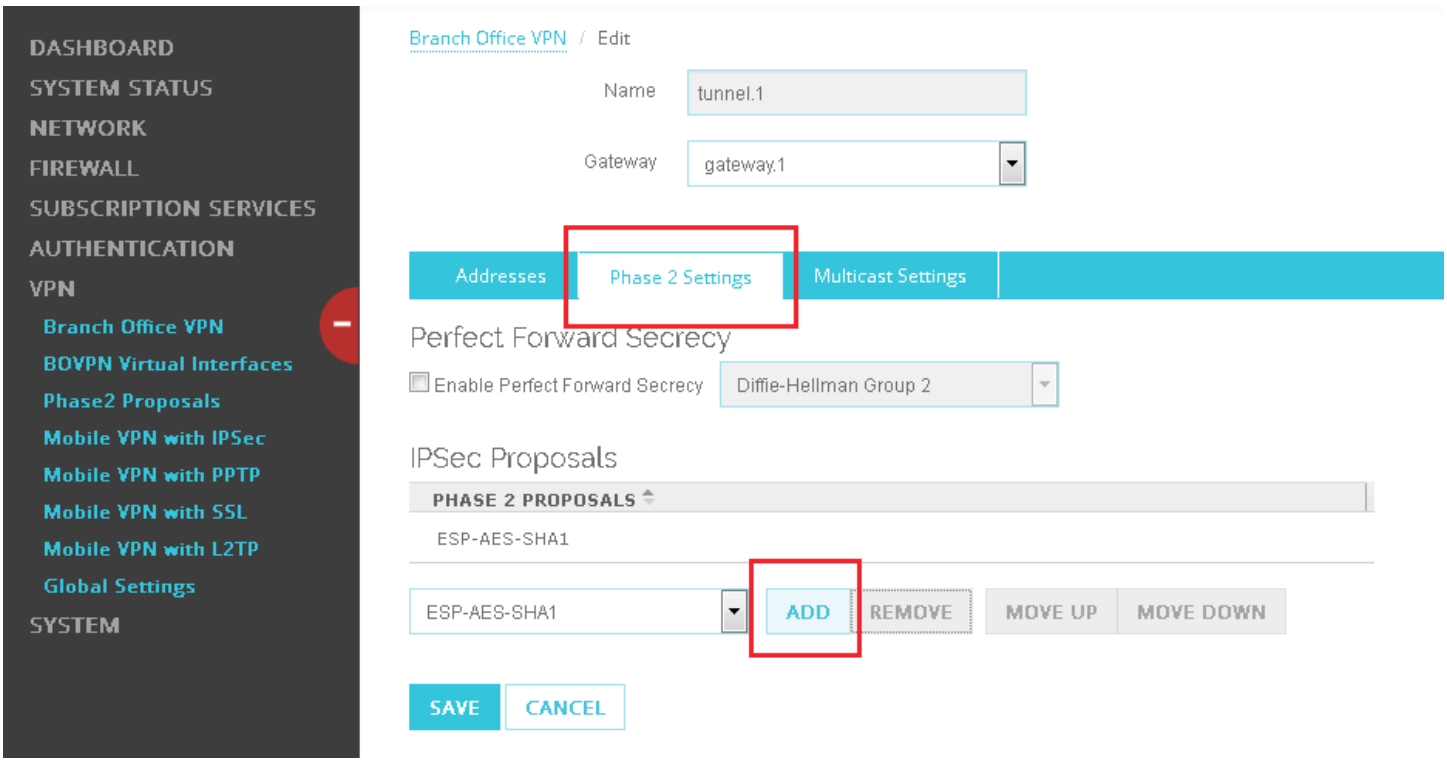
Click **ADD**.



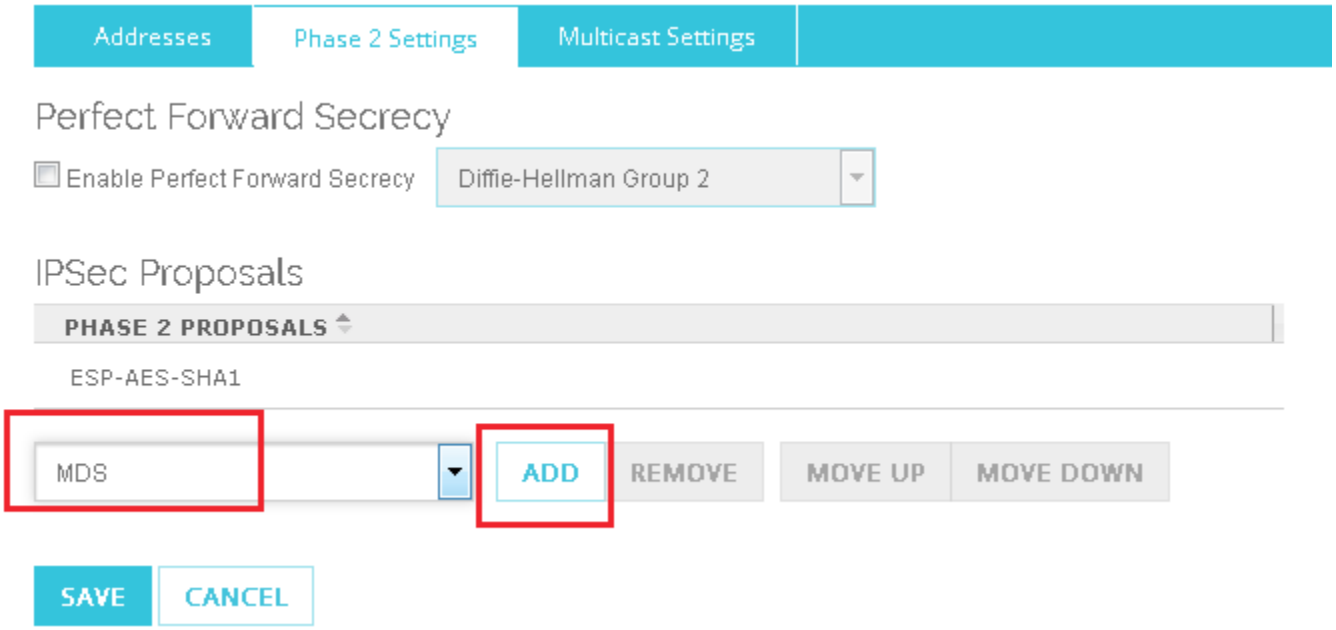
Fill in the Local LAN network type (IPv4). Enter the **Local LAN Network** and the CIDR notation for the mask in the **Network IP** selection. Select **Any** for the remote IP then select **OK**.



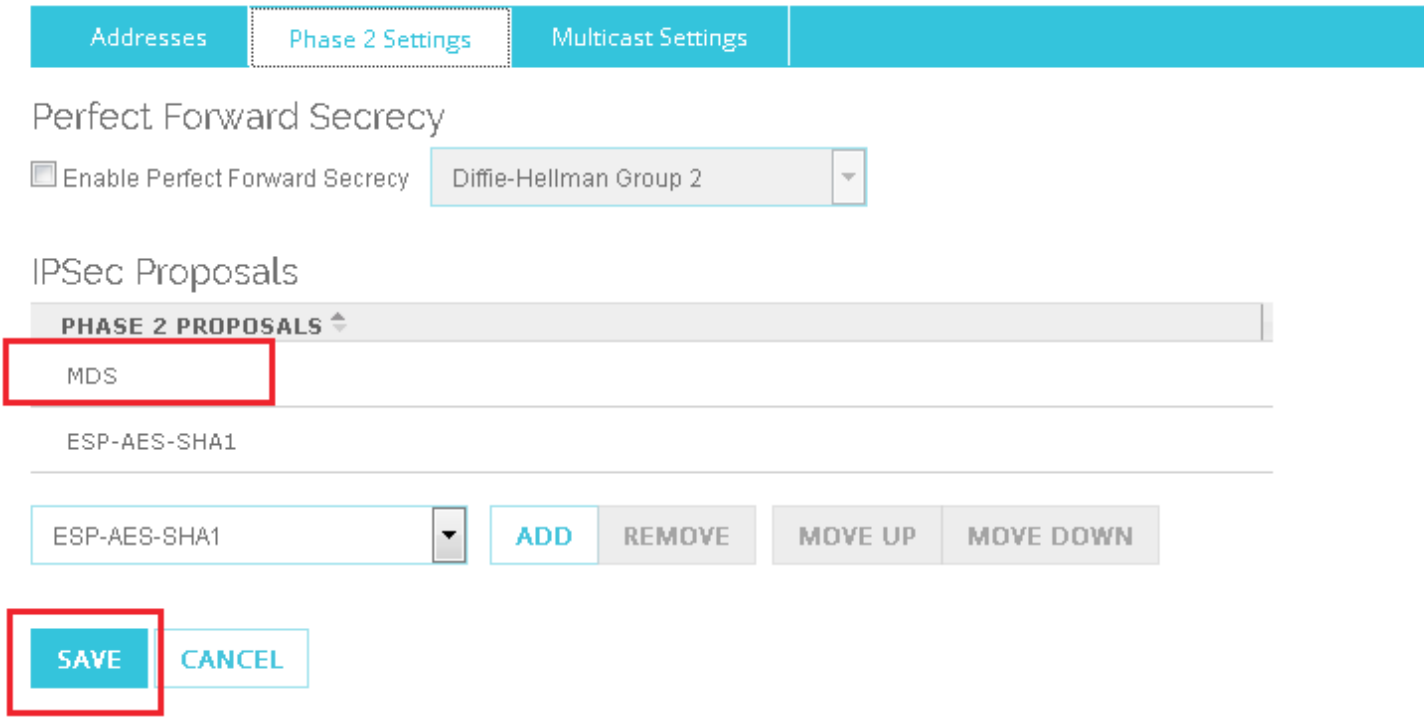
Click **Phase 2 Settings** tab then click **ADD** to add the MDS Phase 2 Proposals settings.



Select **MDS**.

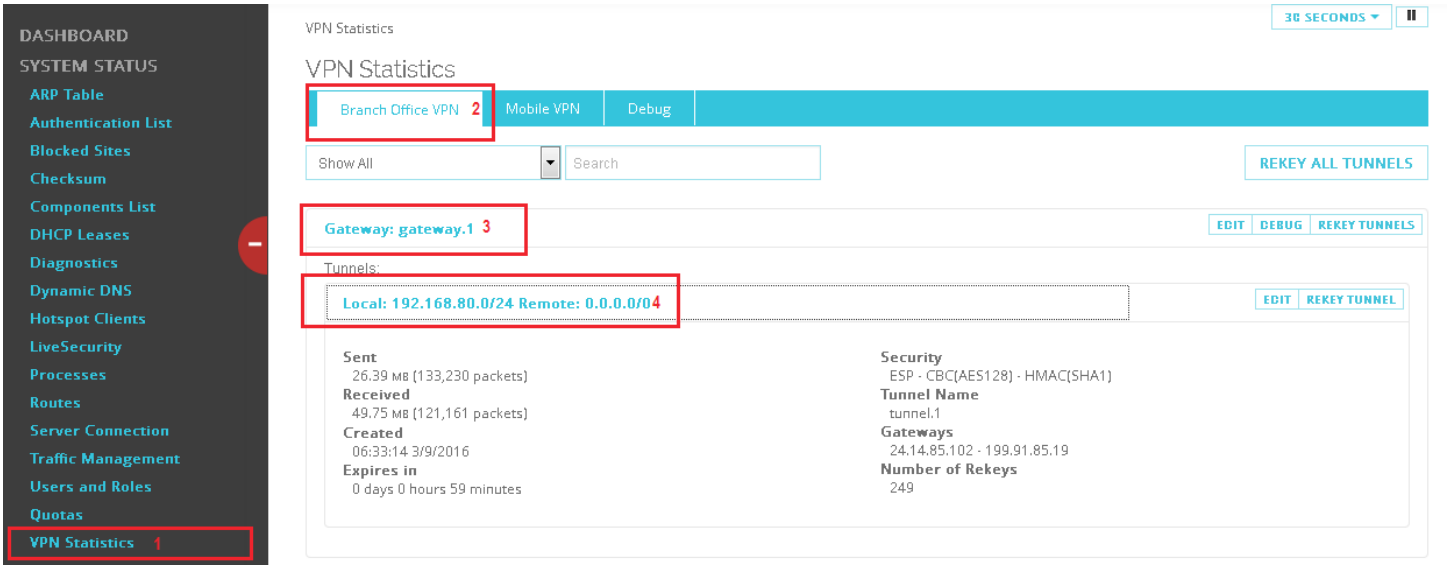


Make sure **MDS** is the first selection in **PHASE 2 PROPOSALS**, then Click **SAVE**.



VPN STATUS VERIFICATION

Under the Dashboard Menu, select **VPN Statistics**. Click **Branch Office VPN** tab, then the **Gateway**. Click the tunnel to show the current status of the VPN connection. The **Sent** and **Received** counters should increase. If the **Received** counter is zero, the VPN is not established. Check the configuration again.



TRAFFIC VERIFICATION AND MDS WEB BLOCK

From a local computer that is connected to the Local LAN network, open up the browser and go to **checkip.dyndns.org**. The Public IP should reflect the MDS node.

Browse to **http://www.eicar.org/download/eicar.com** to validate successful block.