Sophos
UTM MDS BYOG Integration Guide

CONTENTS

INTRODUCTION

Congratulations on your sale of MyDigitalShield using the BYOG option.

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

ASSUMPTIONS

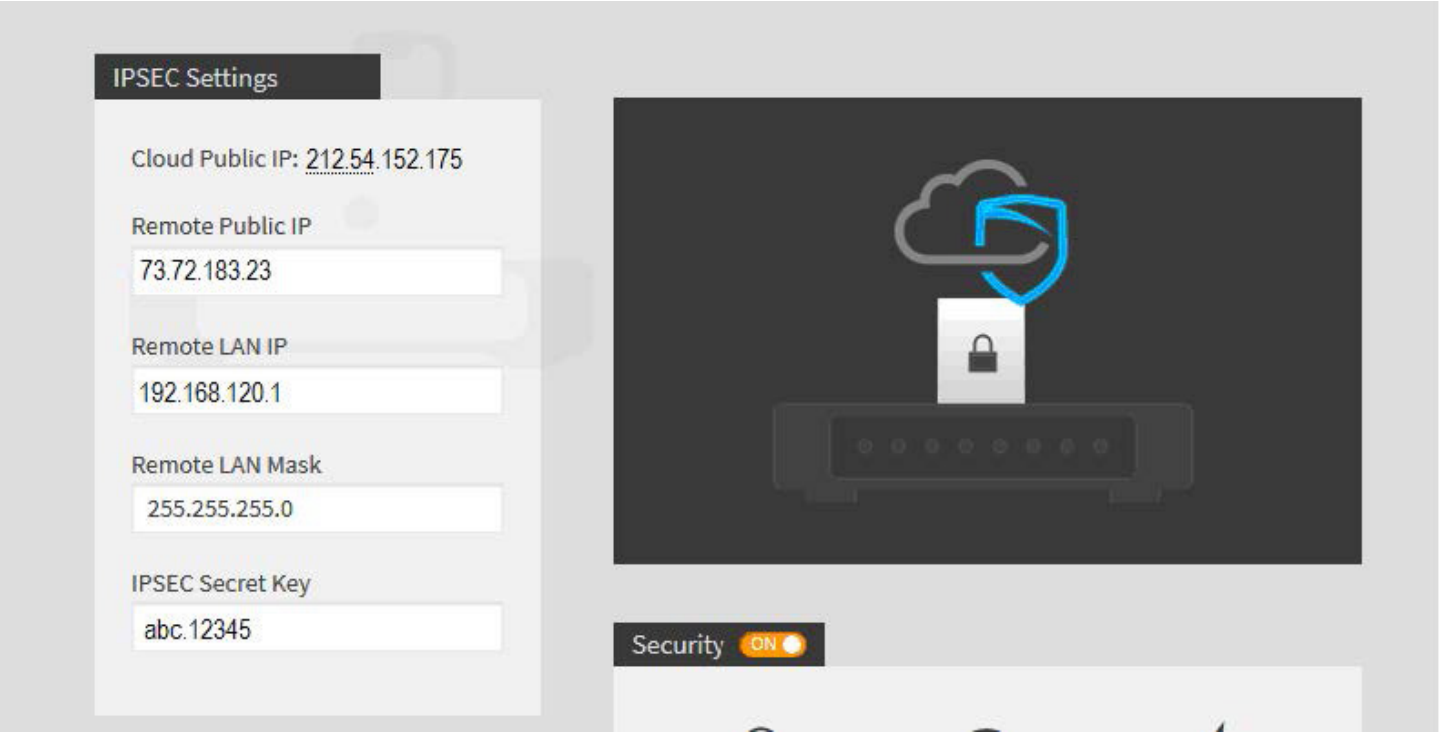
- This guide was developed to provide configuration information of the Sophos UTM gateway specifically for the setup of the IPSEC tunnel to the MDS Cloud.
- The configuration was tested using the Sophos UTM Version 9.400-9.
- This guide is NOT intended to be a full configuration guide for the Sophos gateway
- It is assumed that an Internet port and LAN port are configured and operational.
- Responsibility of the management of the Sophos UTM gateway is not assumed by MyDigitalShield.
- Proceeding to this guide means that the order has been placed in the MyDigitalShield portal.

WHAT YOU WILL NEED

The following IP address information:

- Local Public IP address/subnet.
- Local Public GW address (your customer's default gateway address).
- Local LAN Network/subnet.
- Cloud Public IP address assigned to you during order and activation.
- Preshared key that was defined during setup on the portal.

Please reference the sample configuration from the MDS portal.



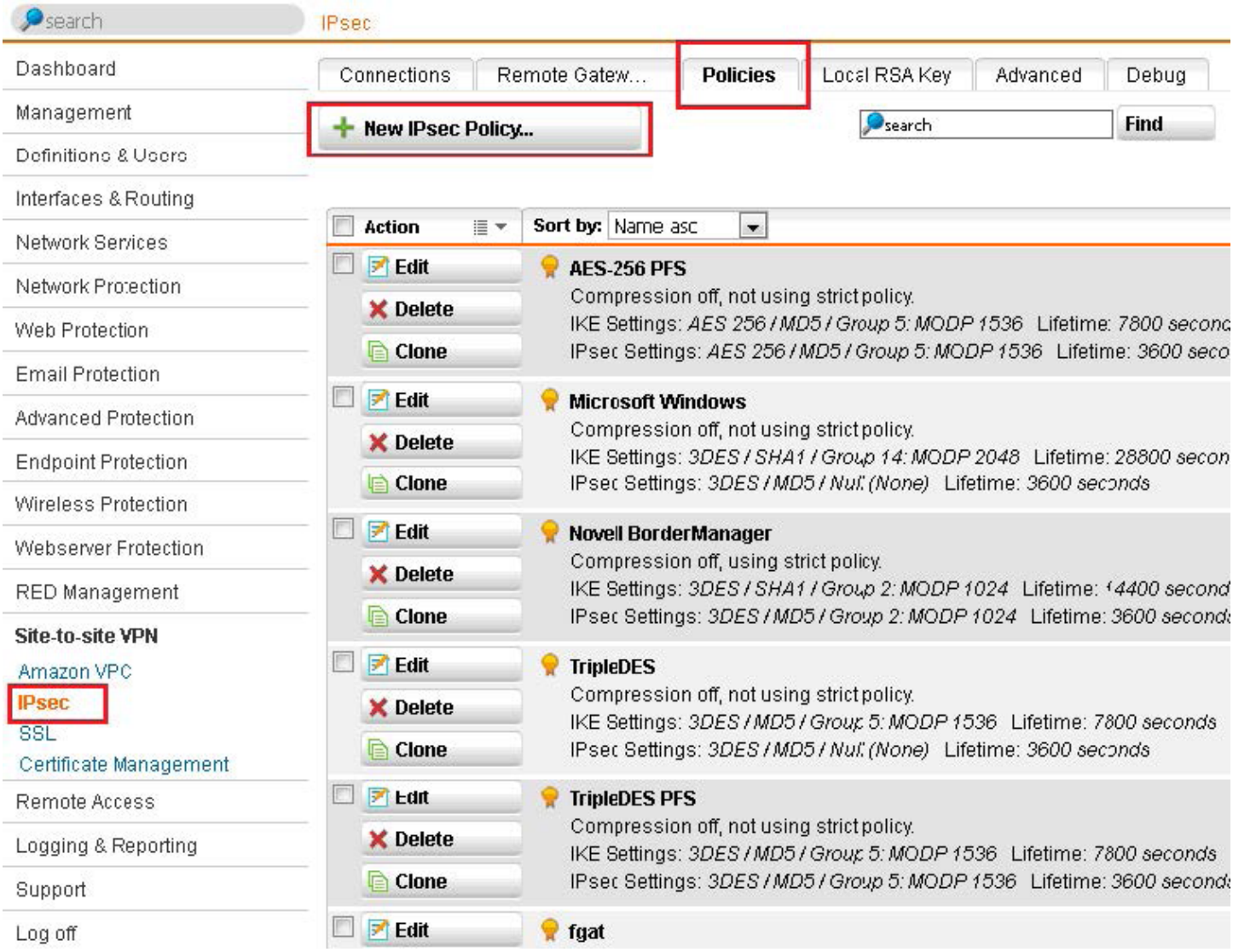
1. **Local Public IP:** The local Public IP address/subnet mask that your customer's ISP provides. You can find this address following the instructions in the IPSEC Configuration section below.
2. **Local LAN Network:** This is the network address that is being used on your customer's LAN.
3. **Cloud 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 throughout this guide, values in the “Reference Sample” column are used.

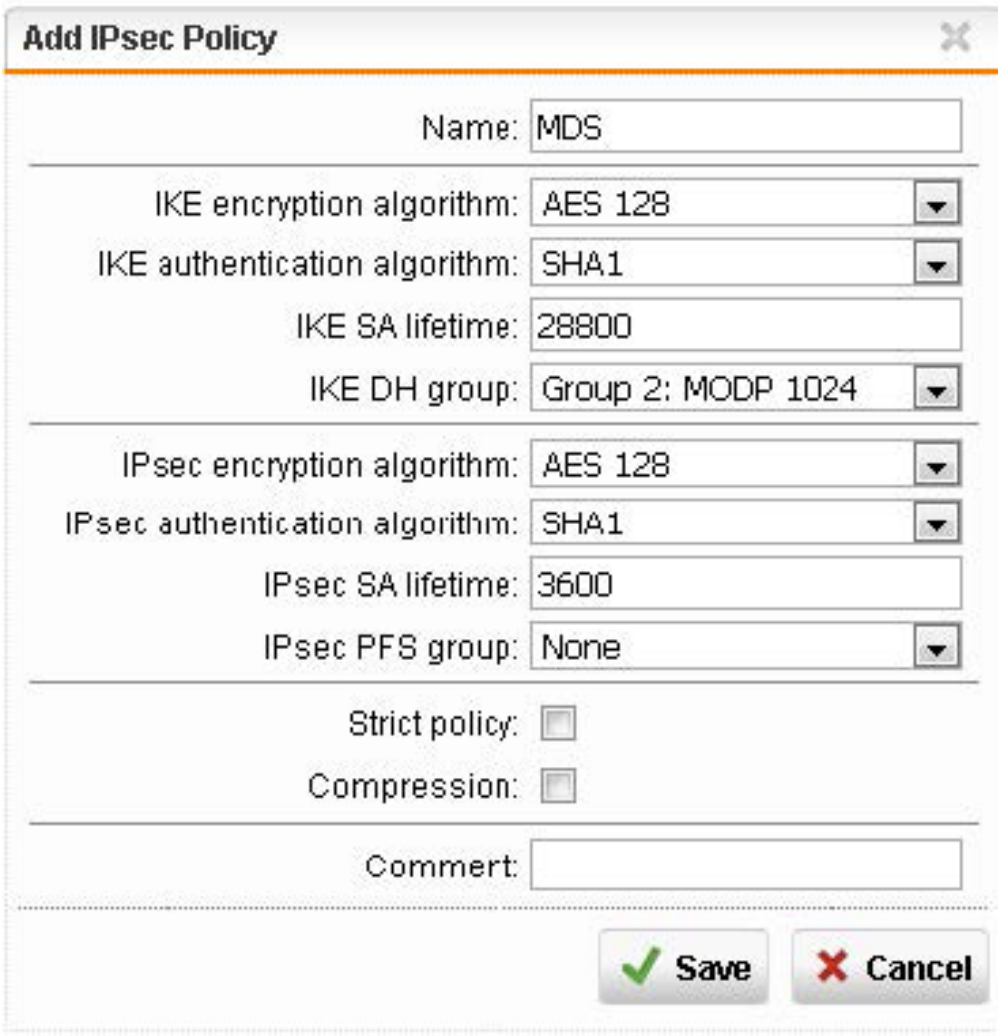
Network	**IP**	**Reference Sample**
Local Public IP: (x.x.x.x/mask)		73.72.183.23/23
Local LAN Network (x.x.x.x/mask)		192.168.120.0/24
Cloud Public IP (x.x.x.x)		212.54.152.175

CONFIGURE THE GATEWAY

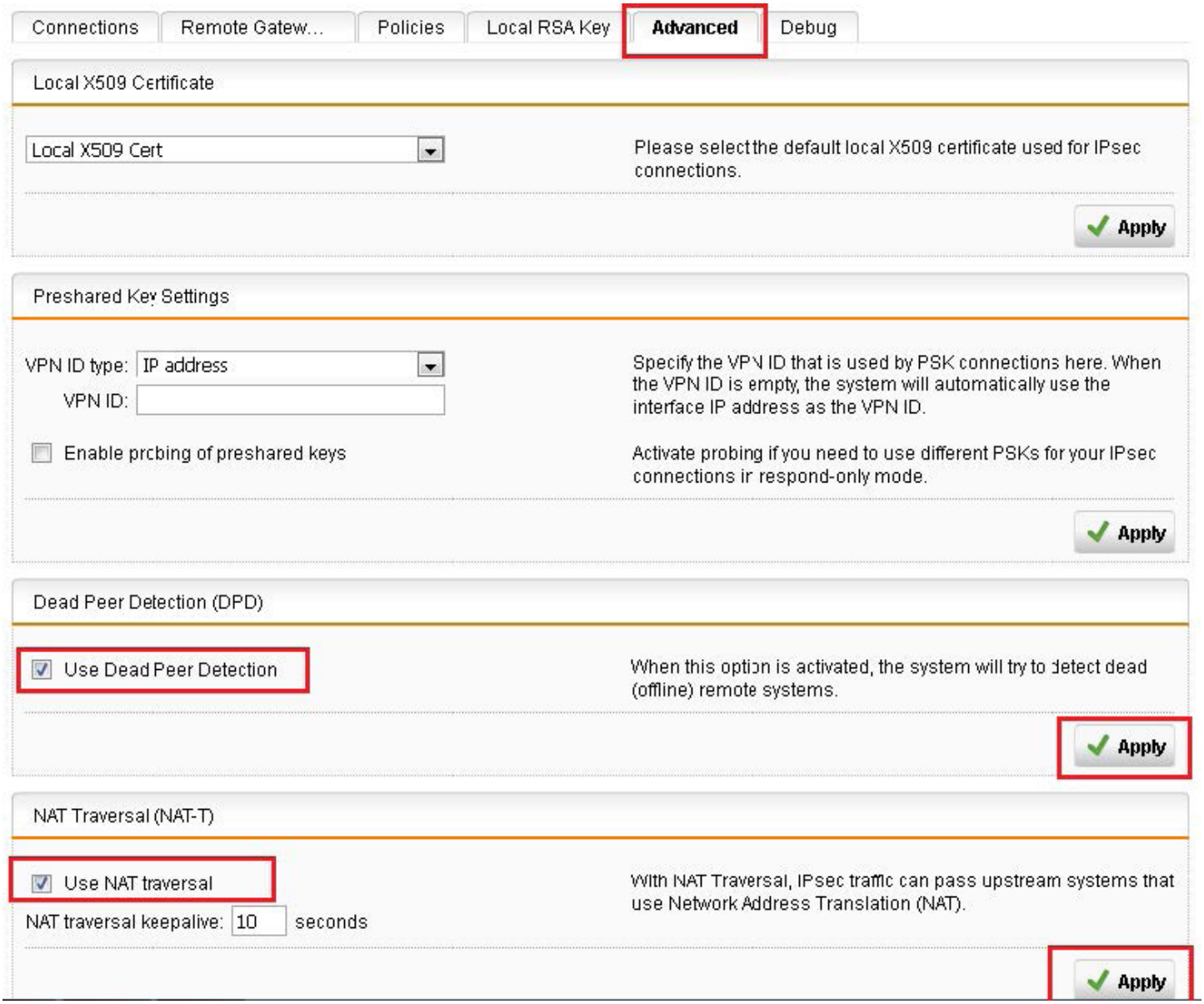
In the left tabs on the main page expand **Site-to-Site VPN** and select **IPsec.** Select the **Policies** tab and click **New IPsec Policy**.



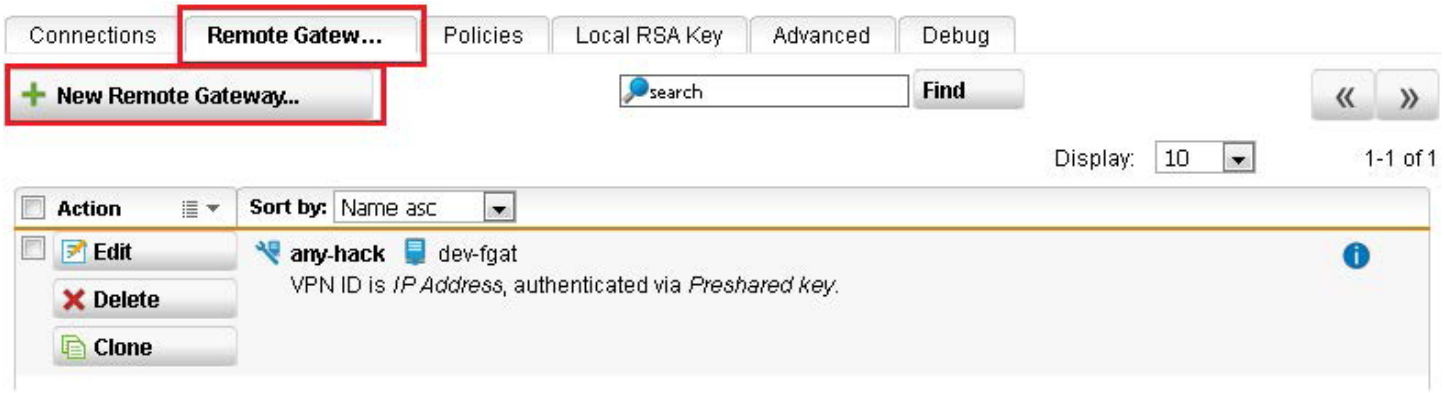
Use the settings from the sample screenshot below:



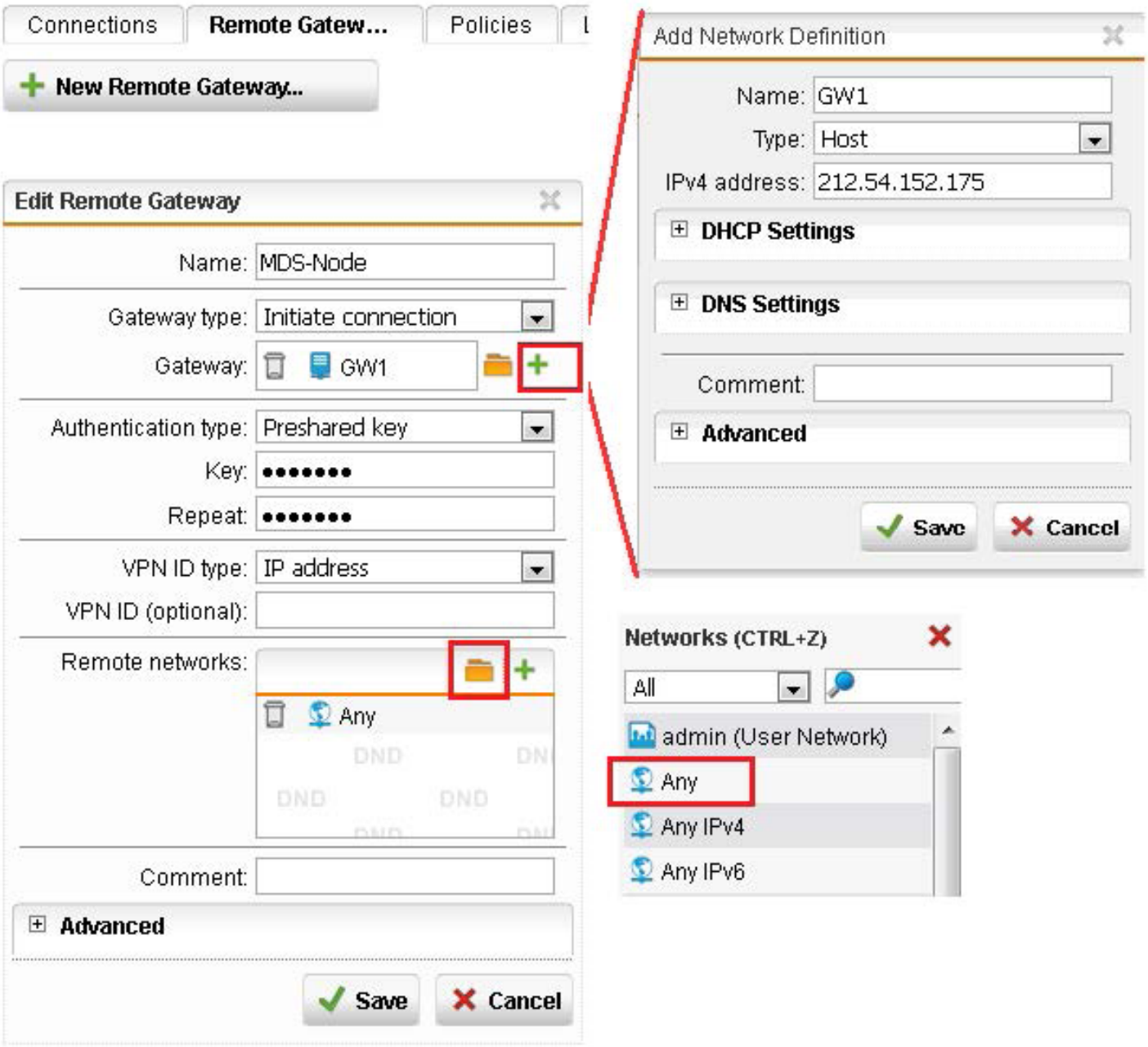
Select the **Advanced** Tab. Enable **Dead Peer Detection** and **NAT Traversal.** Make sure to click **Apply** to save the configuration.



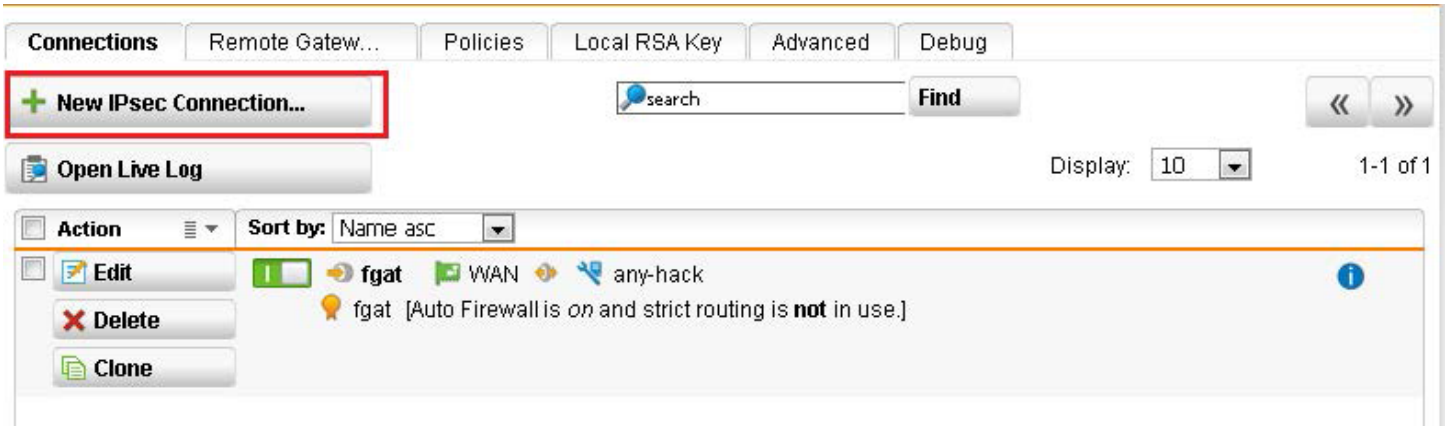
Select the **Remote Gateway** tab and click **New Remote Gateway**.



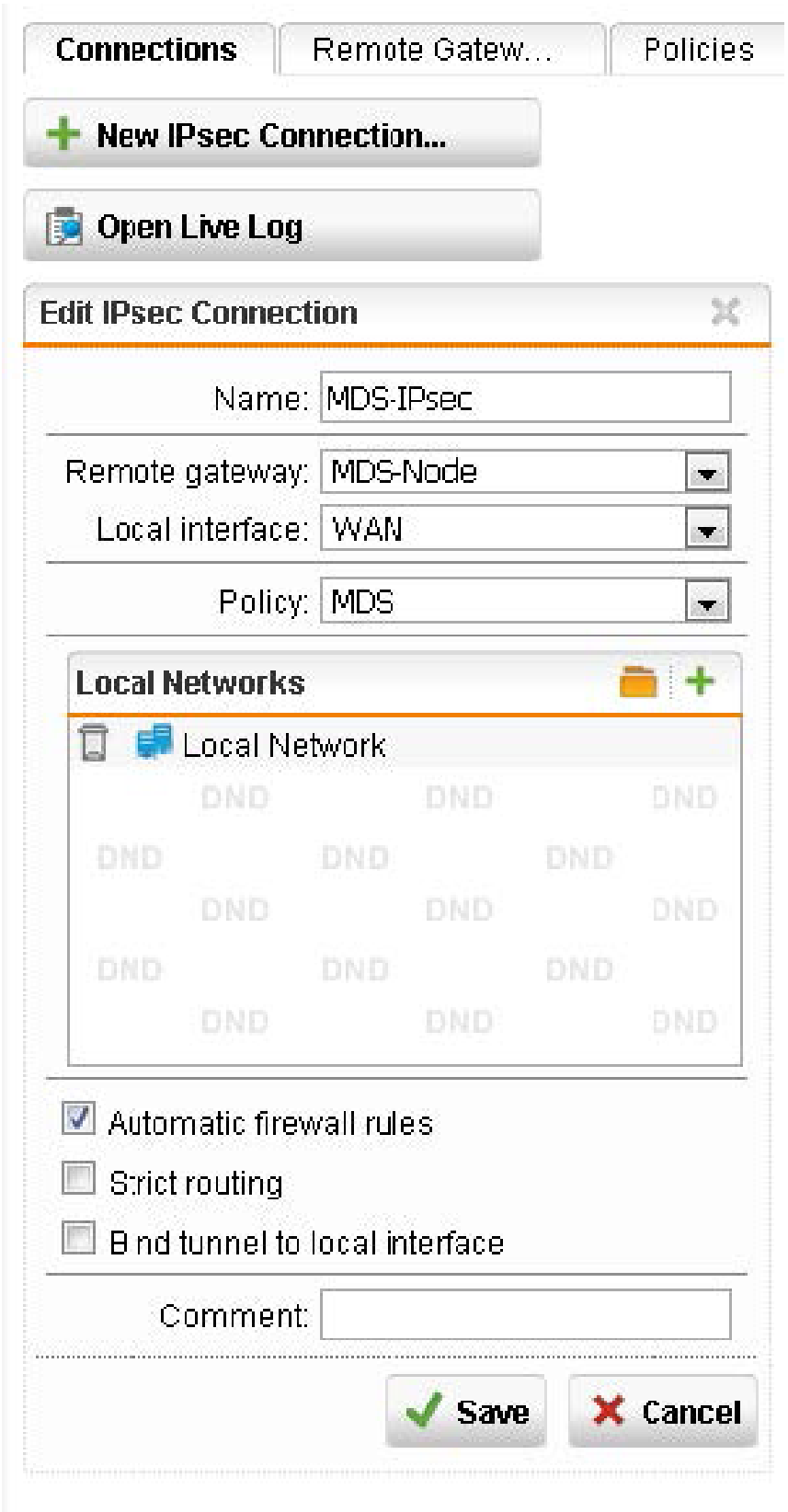
Fill in the IPV4 field with the **Cloud Public IP** address.



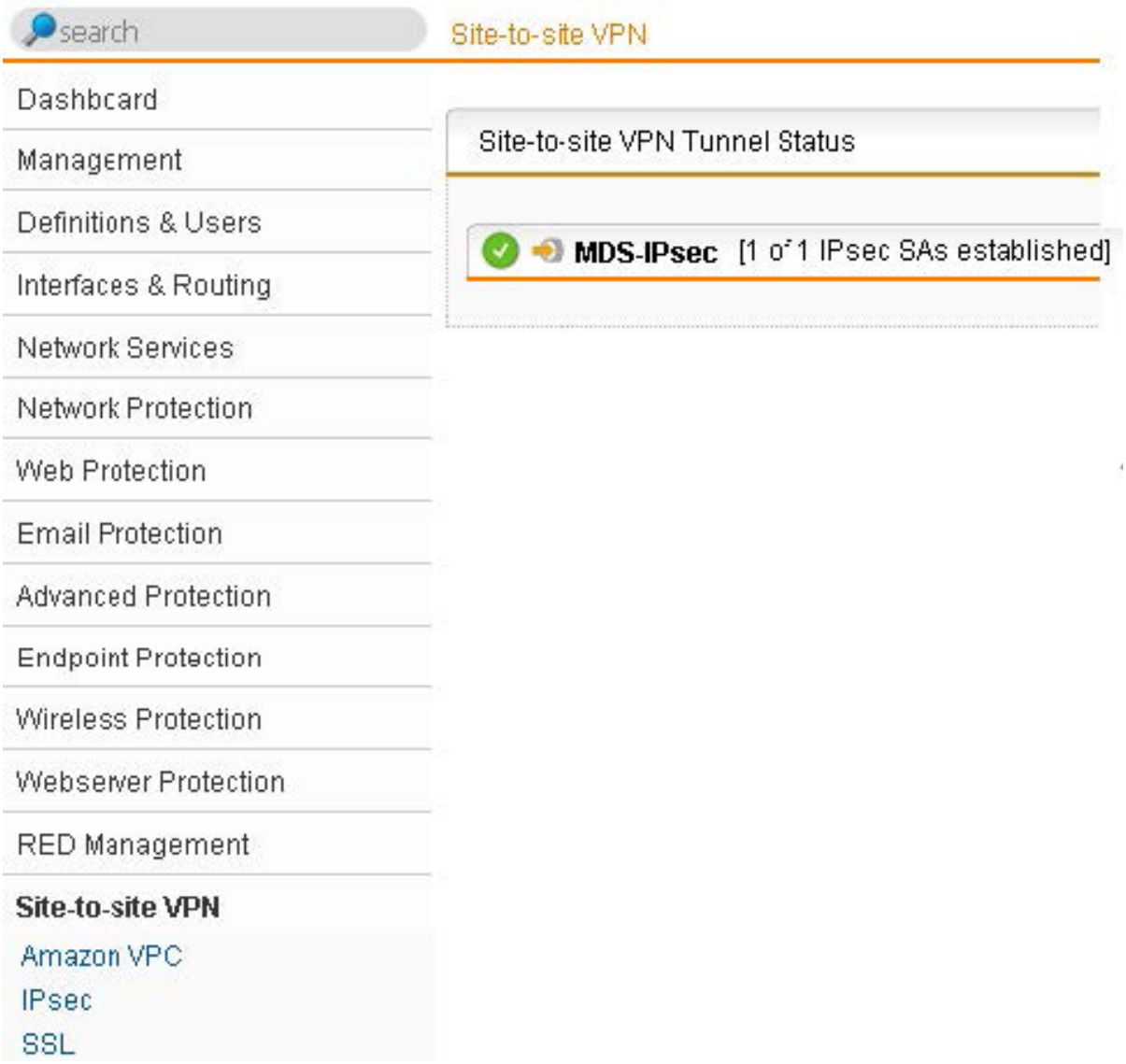
Select the **Connections** tab then click **New IPsec Connection**.



Fill in the appropriate field then click **Save**.

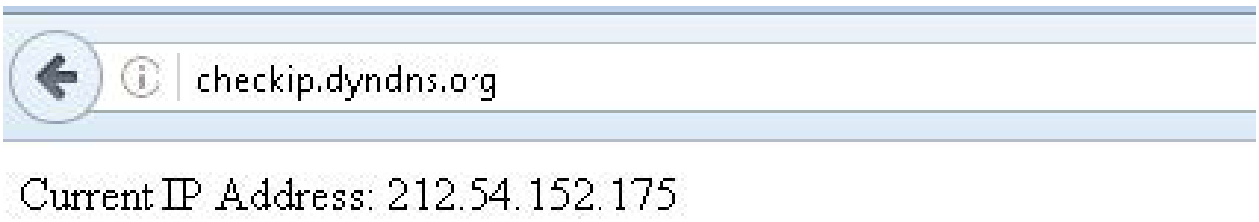


VERIFICATION OF IPSEC TUNNEL



VALIDATE TRAFFIC TO MDS

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



Access a gambling site. For example, try gamblingsites.org.