Cisco ASA 5505
MDS BYOG Integration Guide

CONTENTS

INTRODUCTION

Congratulations on your sale of MyDigitalShield, using the BYOG option.

This guide is written specifically for the **Cisco ASA 5505 (9.0(1))**. 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 Cisco ASA gateway.

ASSUMPTIONS

- This guide was developed to provide configuration information of the Cisco ASA 5505 gateway specifically for the setup of the IPSEC tunnel to the MDS Cloud.
- The configuration was tested using the Cisco ASA 5505 (9.0(1))
- Cisco ASA access via the Cisco ASDM client is available (The configuration was tested using Cisco ASDM 7.1)
- This guide is NOT intended to be a full configuration guide for the Cisco ASA gateway
- Responsibility of the management of the Cisco ASA 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:

- The local public IP address/subnet
- Local LAN network/subnet
- The MDS Cloud 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.

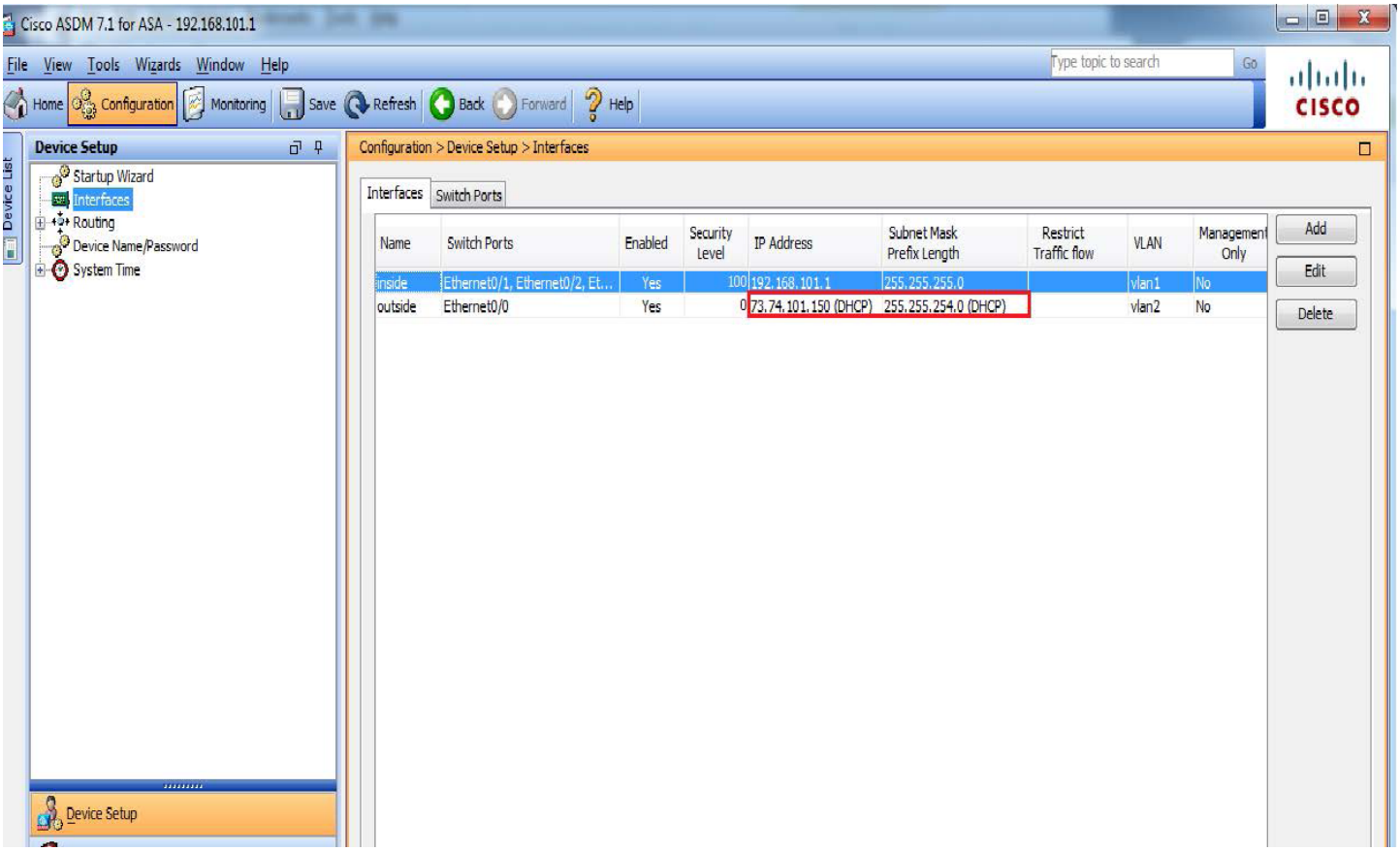
1. **Local Public IP:** The local Public IP address/subnet mask that your customer's ISP provides. You can find this address following the instructions in the IPSEC Configuration section below.
2. **Local LAN Network:** This is the network address that is being used on your customer's LAN.
3. **Cloud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

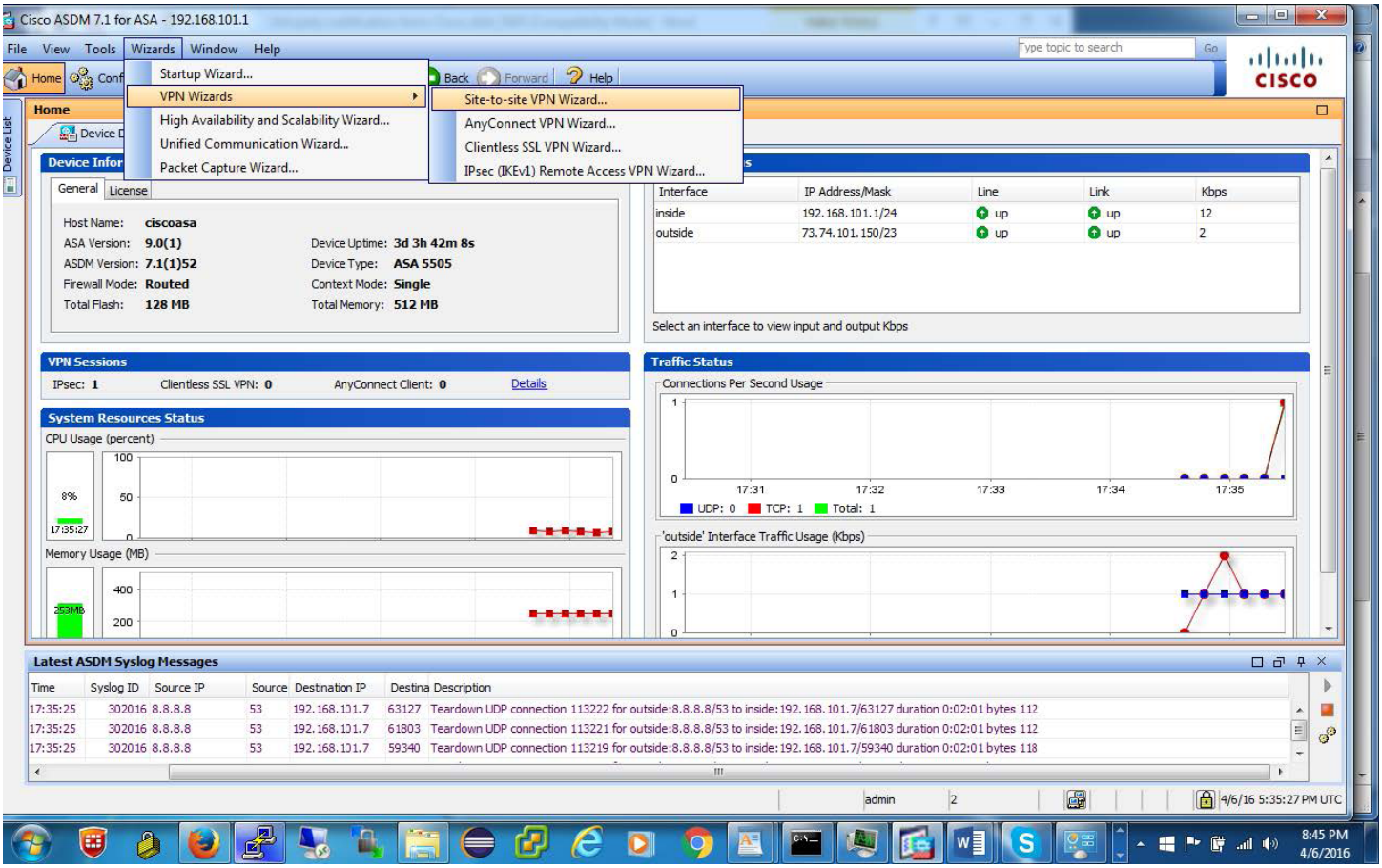
Network	**IP**	**Reference Sample**
Local Public IP: (x.x.x.x/mask)		73.74.101.150
Local LAN Network (x.x.x.x/mask)		192.168.101.0/24
Cloud Public IP (x.x.x.x)		66.163.23.209

IPSEC CONFIGURATION

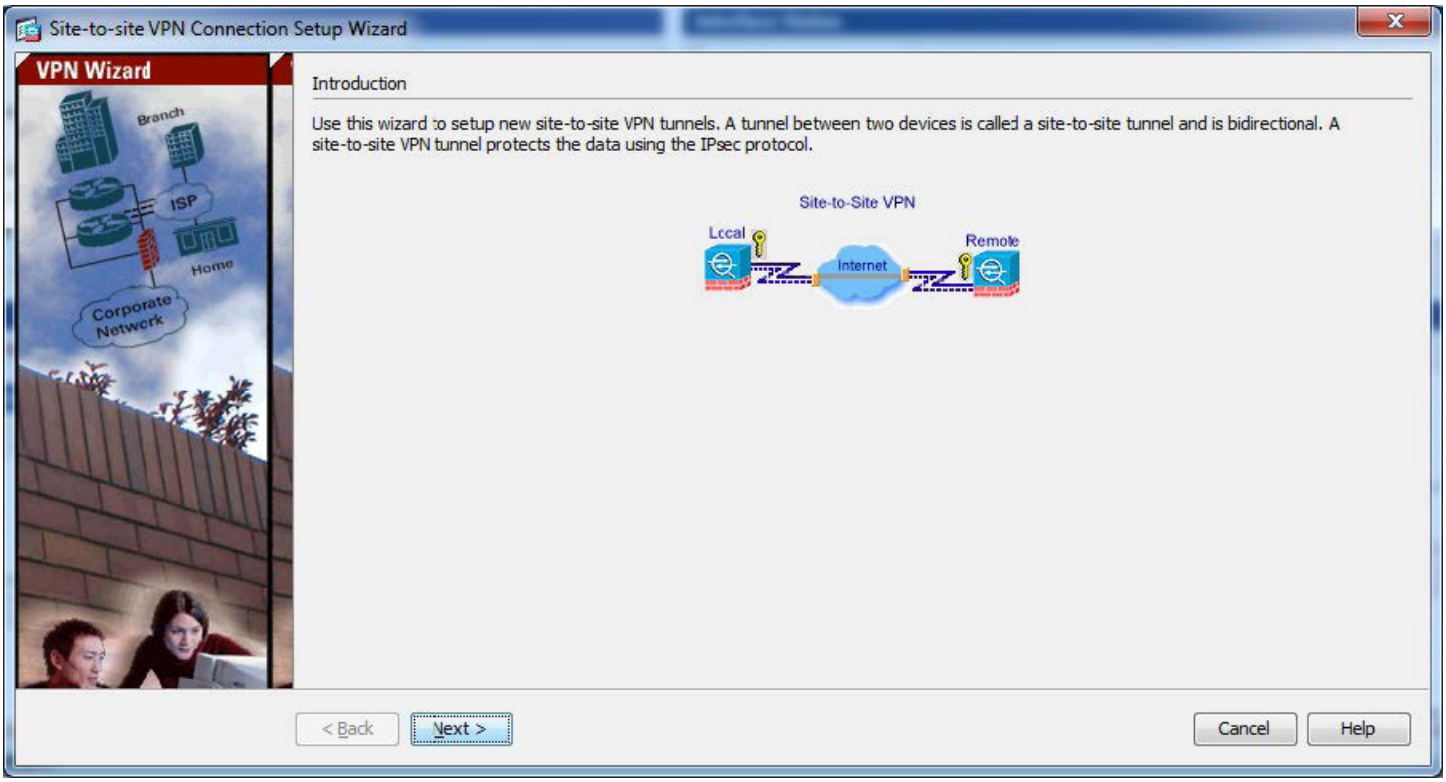
Login to the Cisco ASA using the Cisco ASDM web interface.
You can find your Local Public IP and subnet mask by going into the **Configuration** > **Device Setup** > **Interfaces** section:



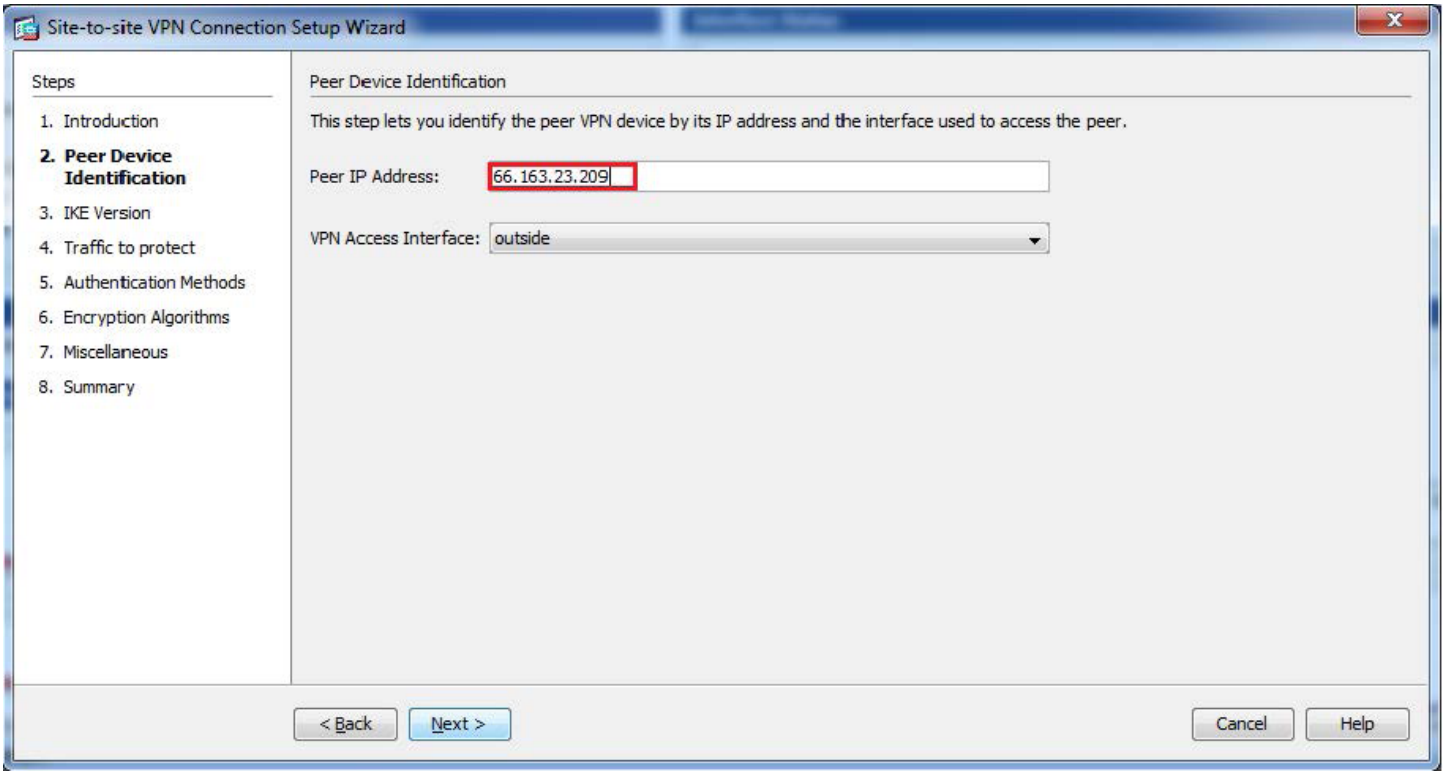
Once you have recorded your local IP information (Interface Name: outside), then from the top menu, click **Wizards** -> **VPN Wizards** -> **Sitesto-site VPN Wizard** to add a new tunnel



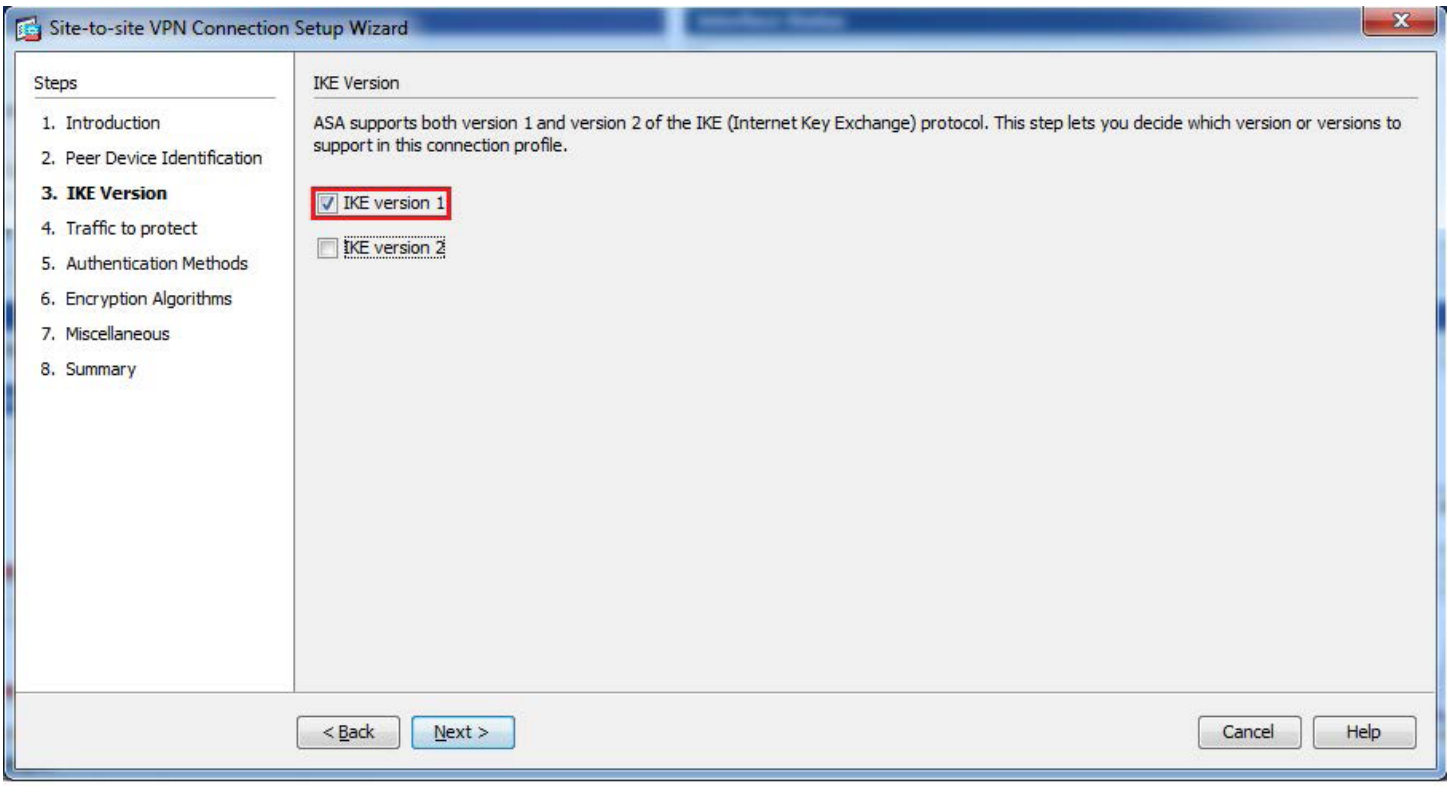
The following screen will be presented, click Next> to create a Site-to-Site VPN.



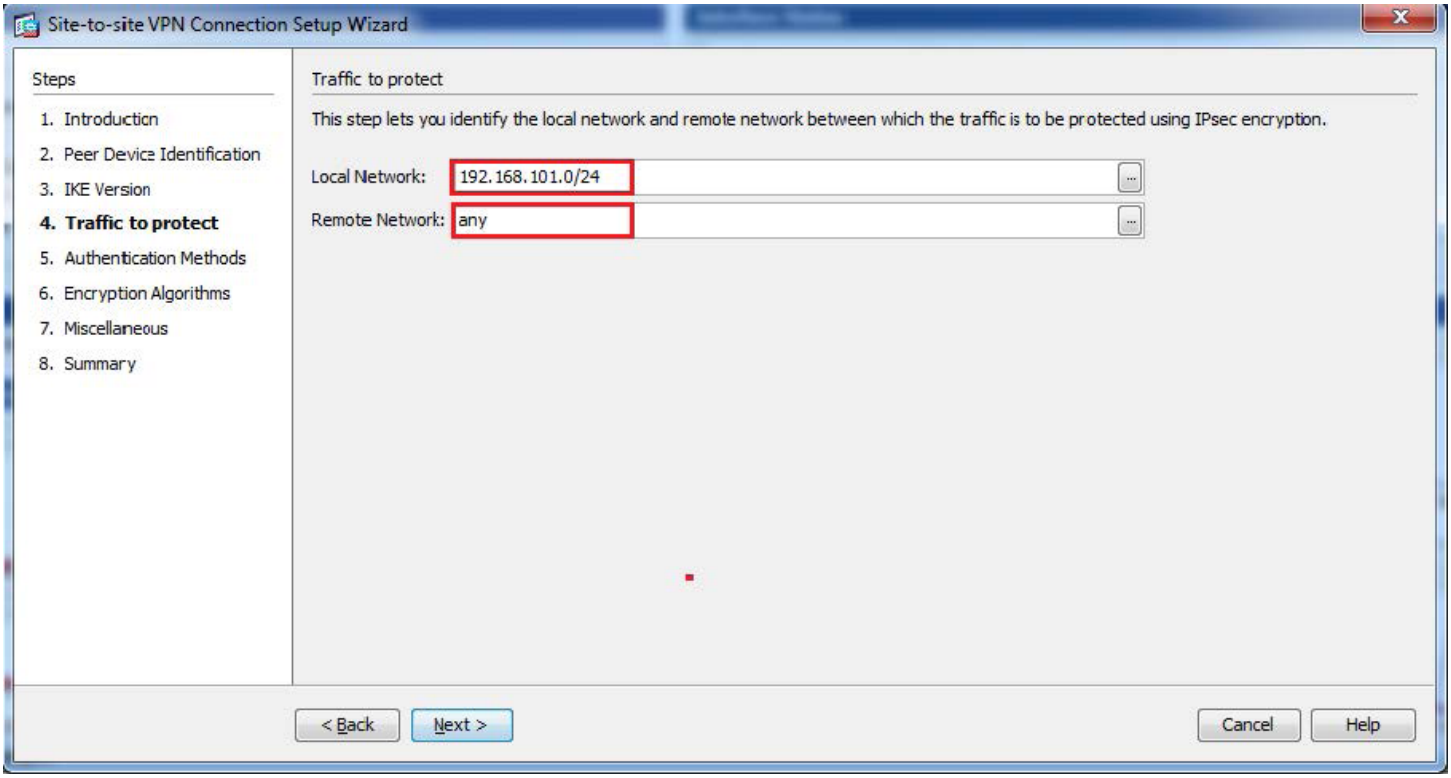
Enter the Cloud Public IP in the Peer IP address field as shown in the screenshot below, click Next> to continue.



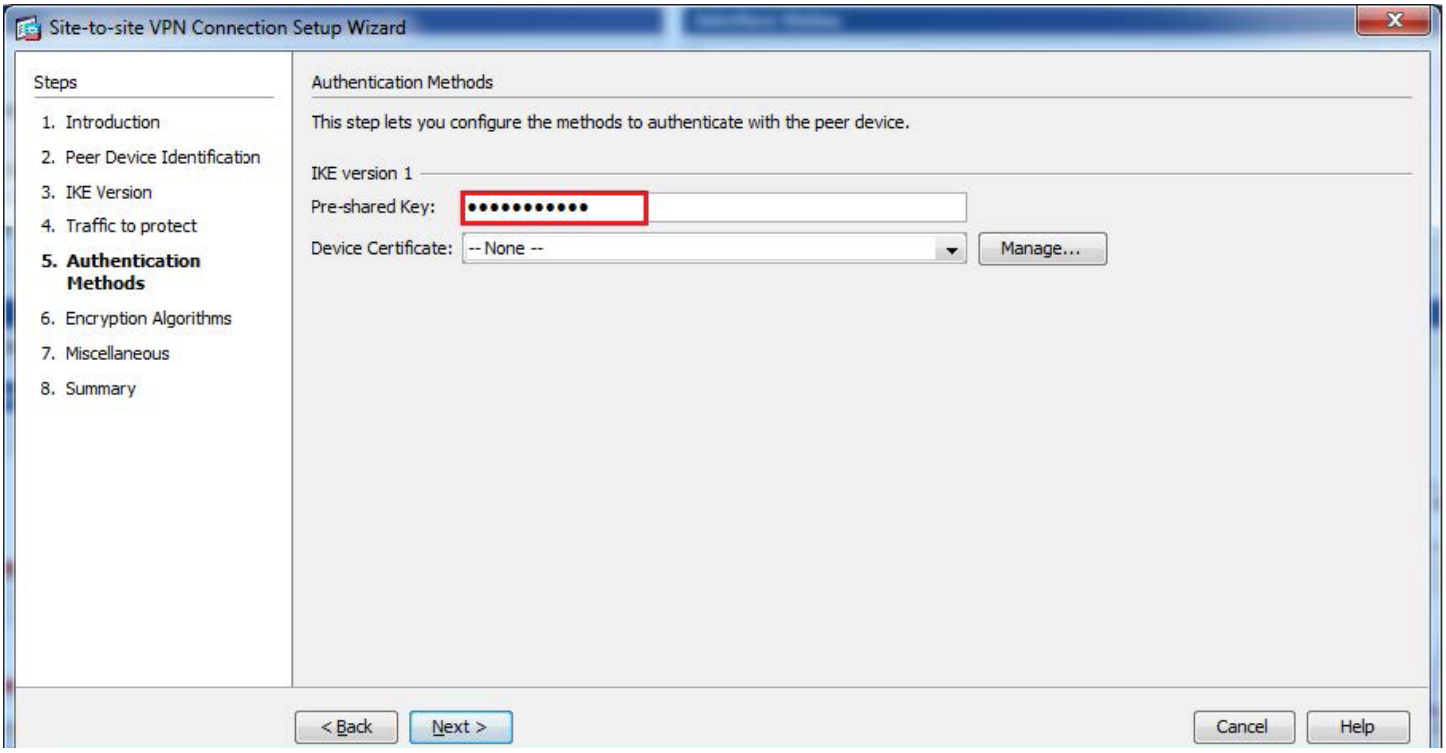
Check IKE version 1, as shown in the screenshot below and click Next> to continue.



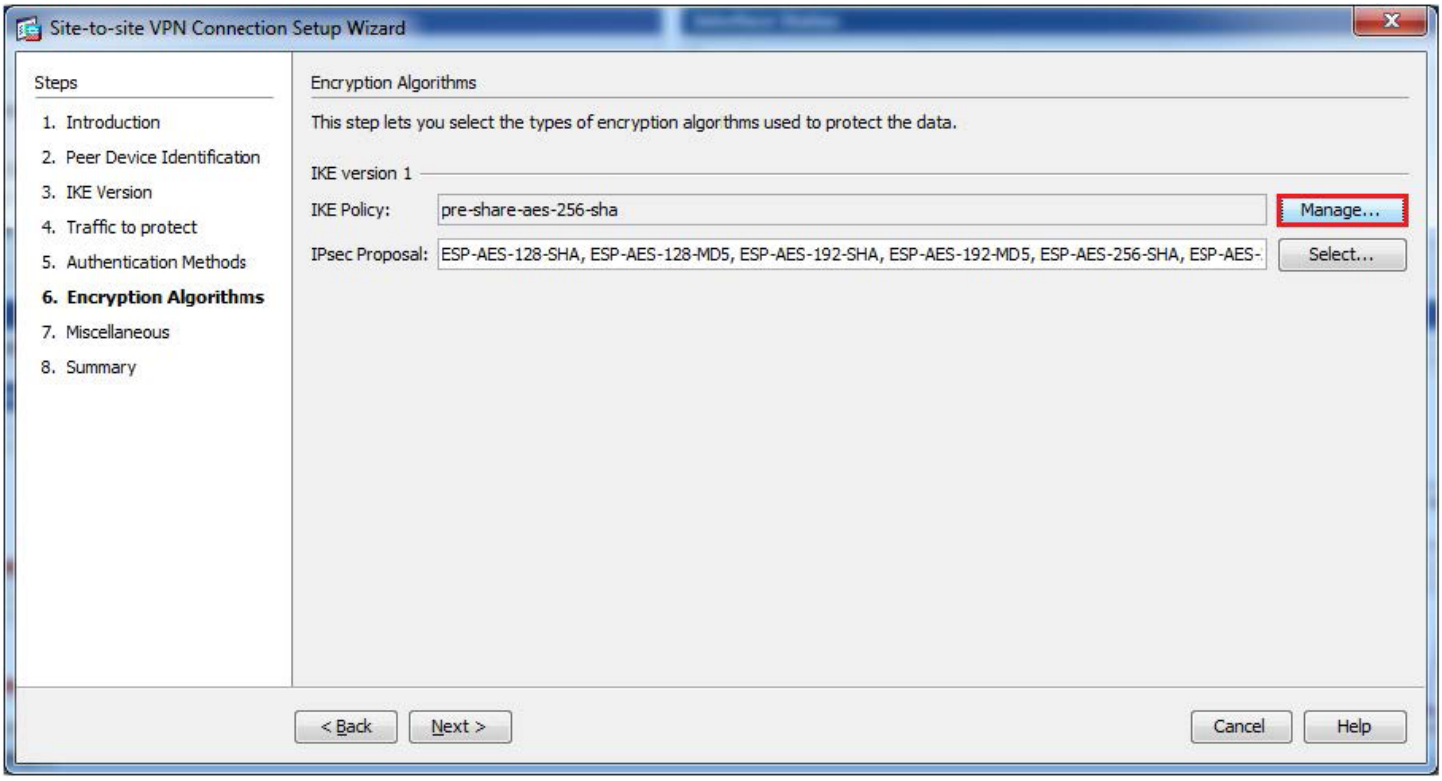
Enter your Local LAN network in the Local Network field and your remote network (if conencting to the Internet, “any” should be used). Once those two blanks are filled in, click Next> to continue.



Now enter your Pre-shared Key in the available field as shown below. The Pre-shared key MUST be the same on the Cisco ASA as the MDS endpoint. Once complete, click Next> to continue.

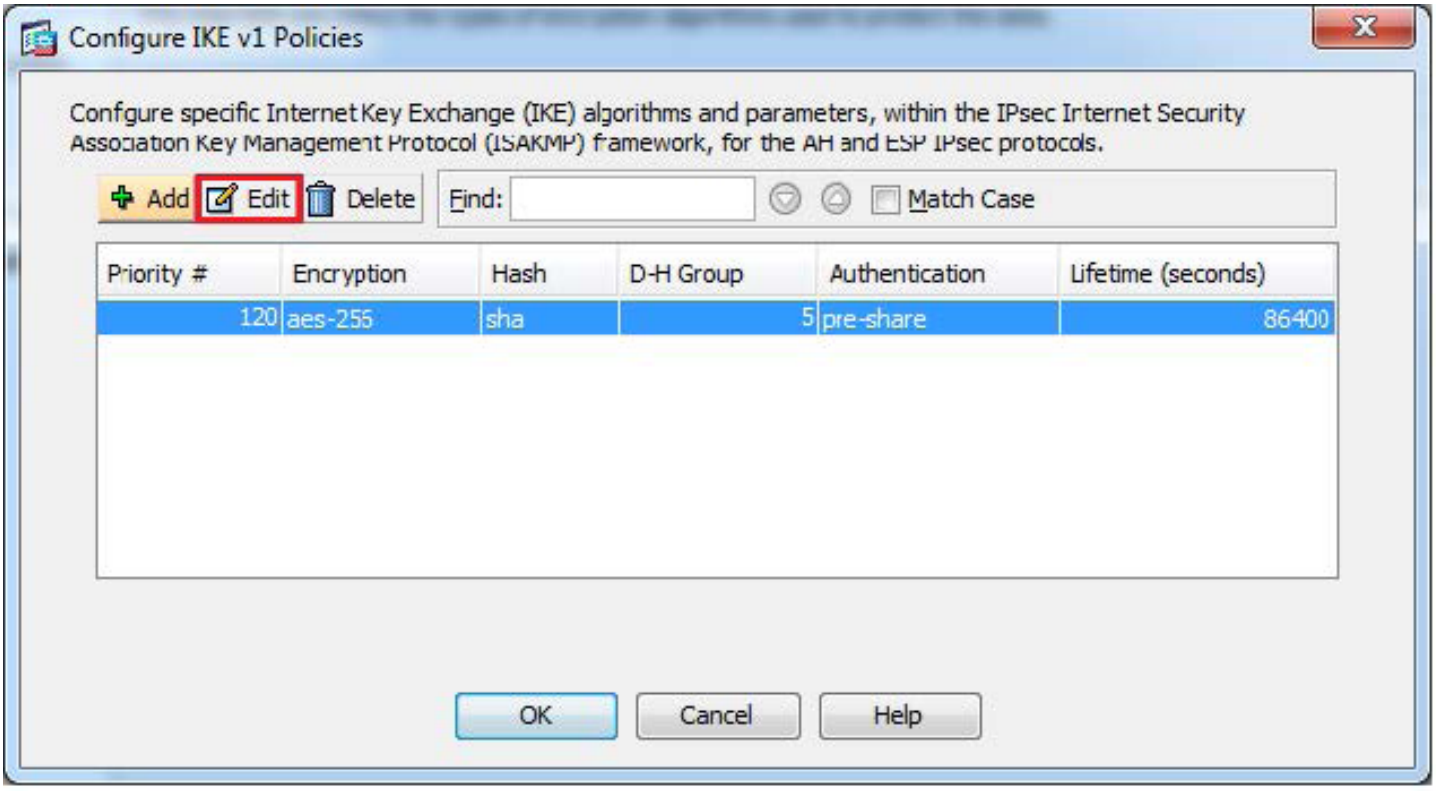


To select your Encryption Algorithms, select Manage as shown in the screenshot below.

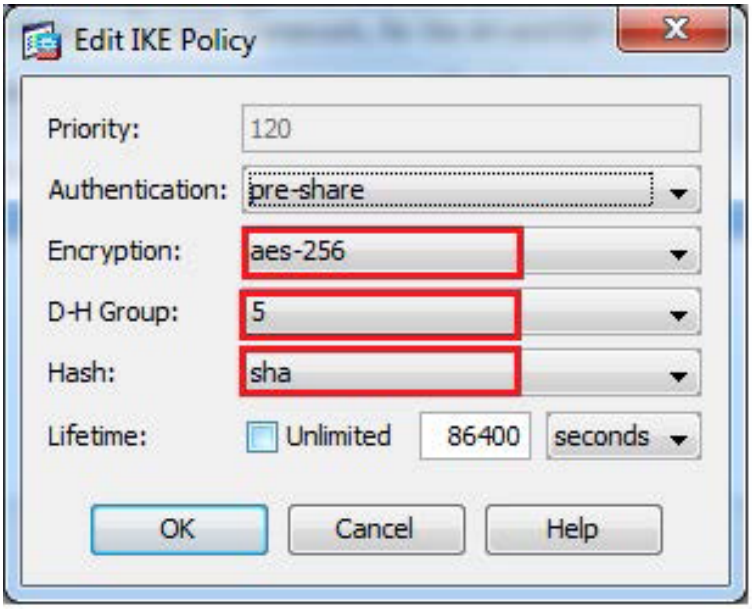


You will get a warning message as shown below. If this is your first IPsec tunnel you can continue. If not, you'll most likely want to stick with the IKE policy already set.

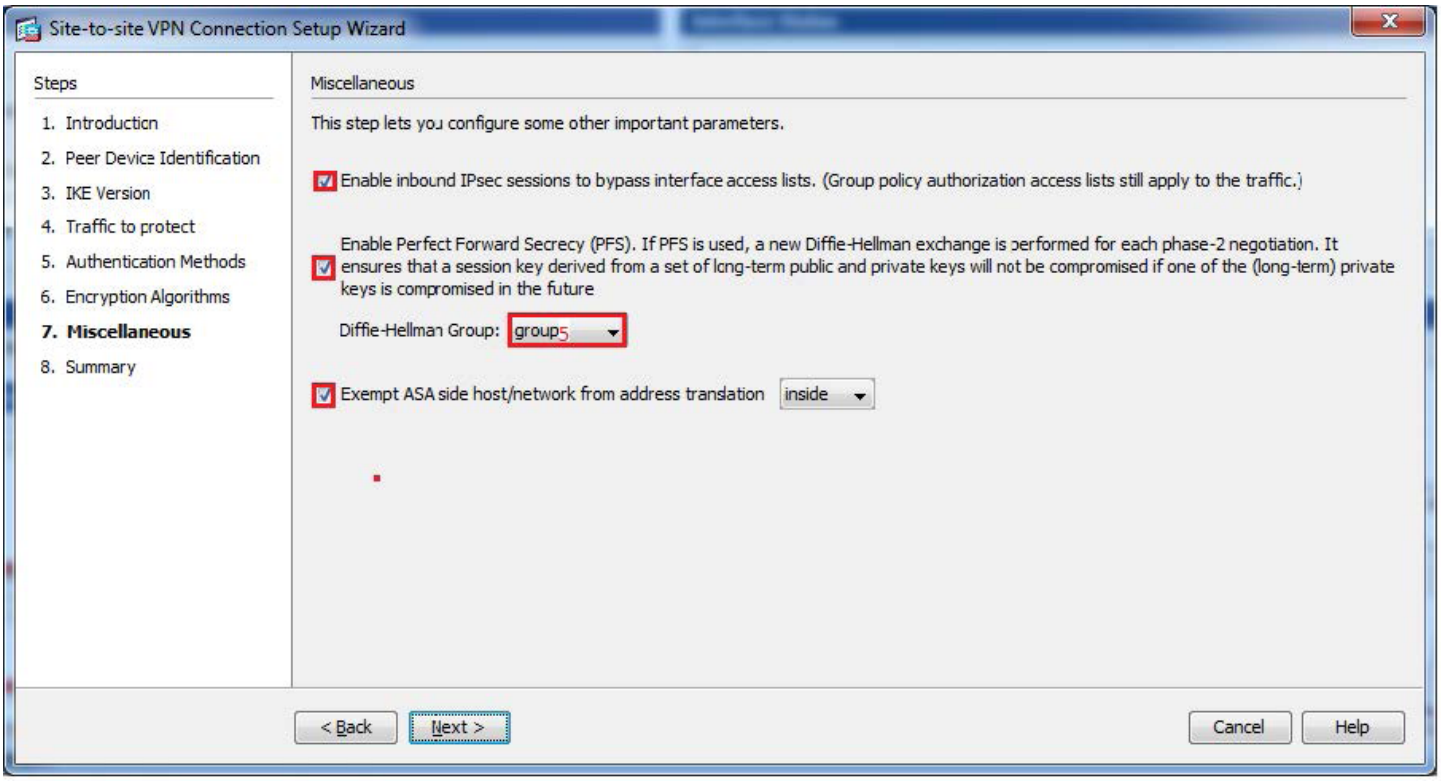
If you are selecting your IKE policy, select edit on the screen shown below.



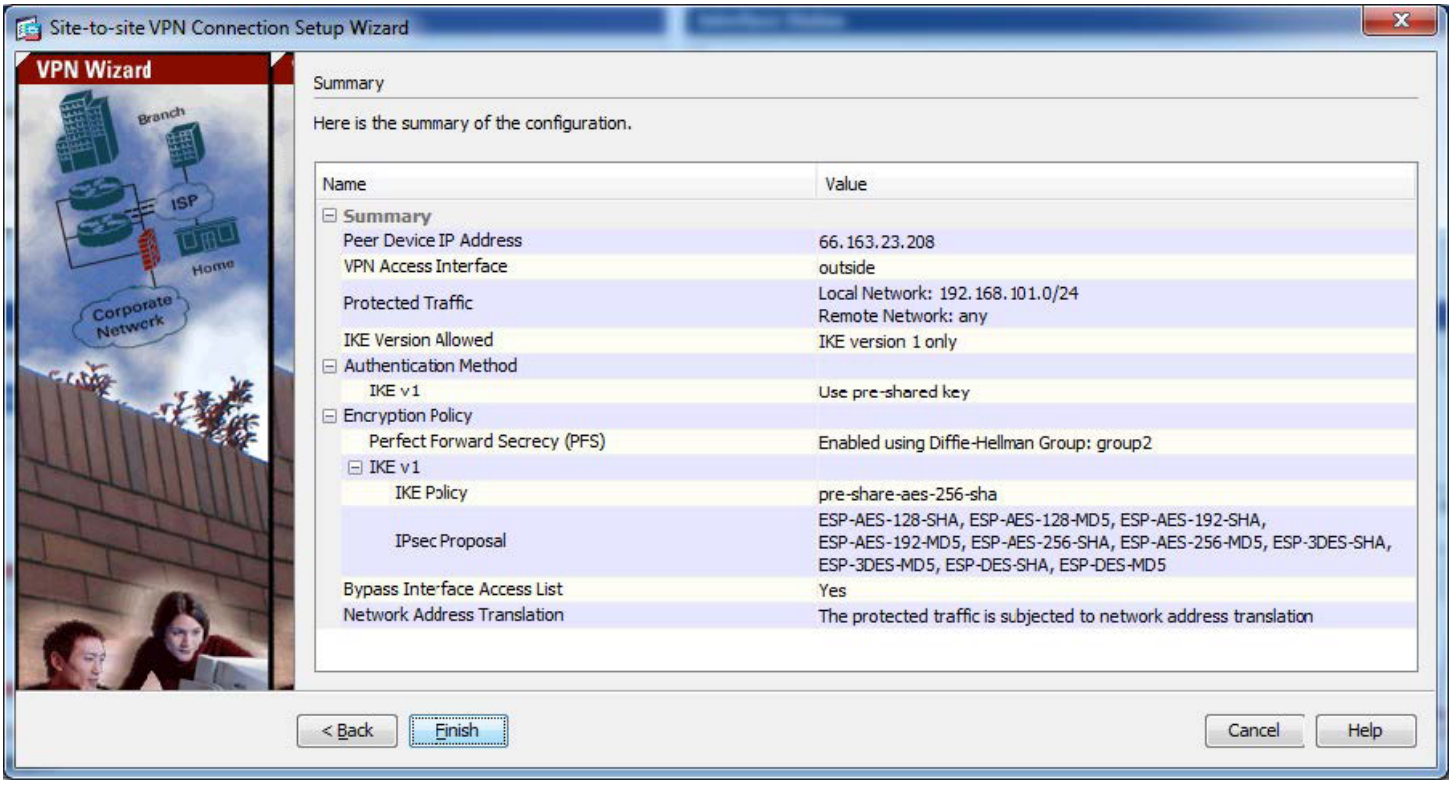
Now you can select the Encryption, D-H Group and Hash, you desire. Once complete, click OK to return back to the previous screen. Click OK once more to return to the Encryption Alogriths selection screen, then Next> to continue.



Once presented with the screen illustrated below, check all three miscellaneous options and change the Diffie-Hellman Group from “Group 2” to “Group 5”. Click Next to continue.

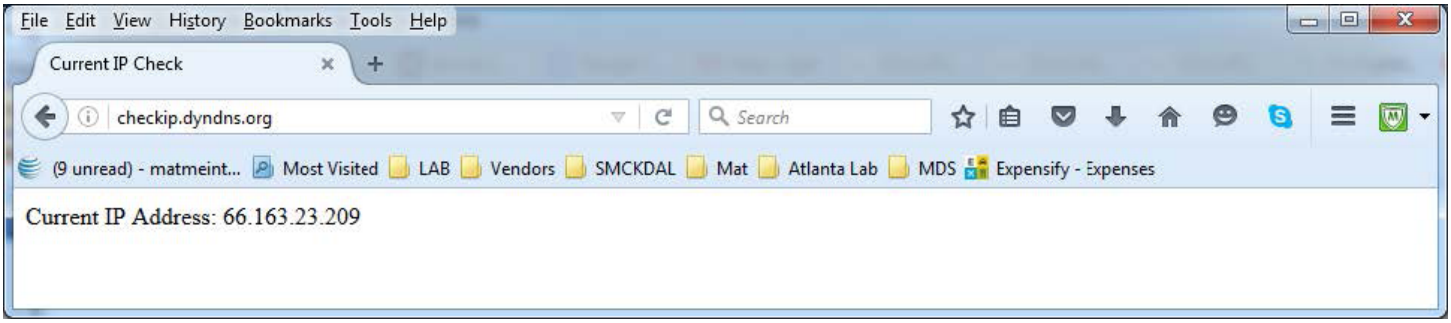


Finally, you will be presented with a Summary screen. If all of the values look correct, click Finish to complete the Site-to-site VPN tunnel configuration.



VALIDATE TRAFFIC TO MDS

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



VALIDATE MDS WEB BLOCK

Access EICAR AV download page:
http://www.eicar.org/download/eicar.com