



**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:



The screenshot displays the 'Network Setup' interface, which is divided into two steps: 'STEP 1' and 'STEP 2'. The current step is 'STEP 2', which is focused on 'IPSEC Settings'. The settings are as follows:

- Cloud Public IP: 199.91.85.19
- Remote Public IP: 24.14.85.102
- Remote LAN IP: 192.168.1.1
- Remote LAN Mask: 255.255.255.0
- IPSEC Secret Key: secure=now

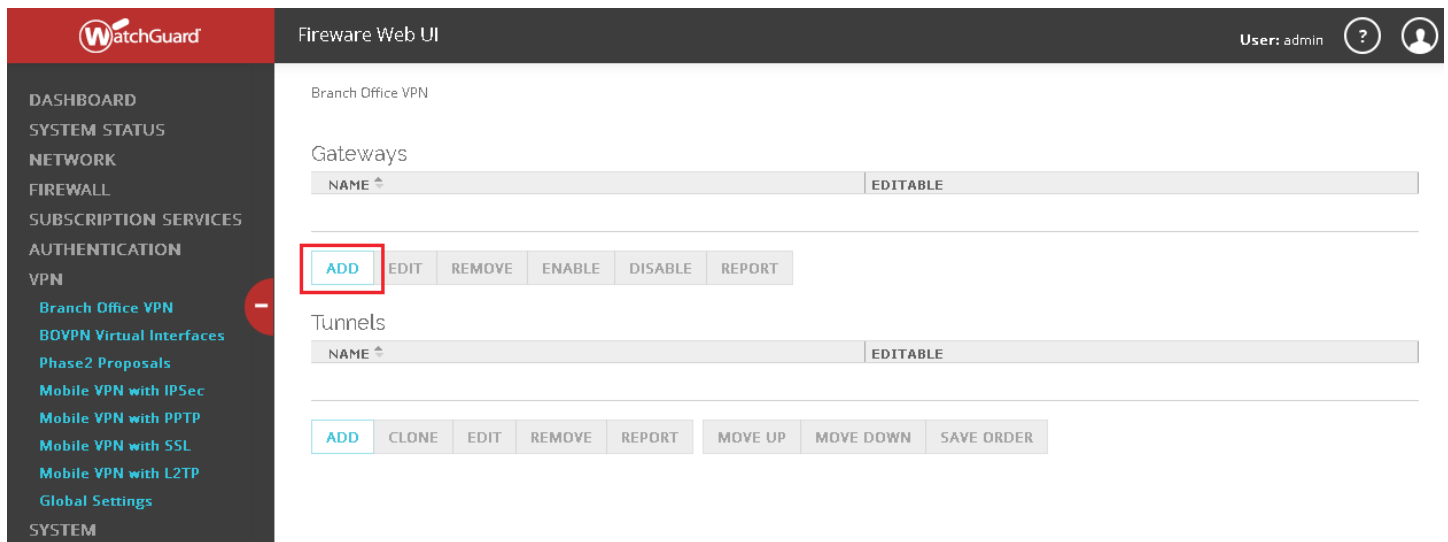
Below the settings, there is a 'Security' toggle switch, which is currently turned 'ON'. To the right of the settings, there is a graphic illustration of a cloud connected to a server rack, with a blue shield icon overlaid on the cloud, symbolizing network security.

IPSEC CONFIGURATION

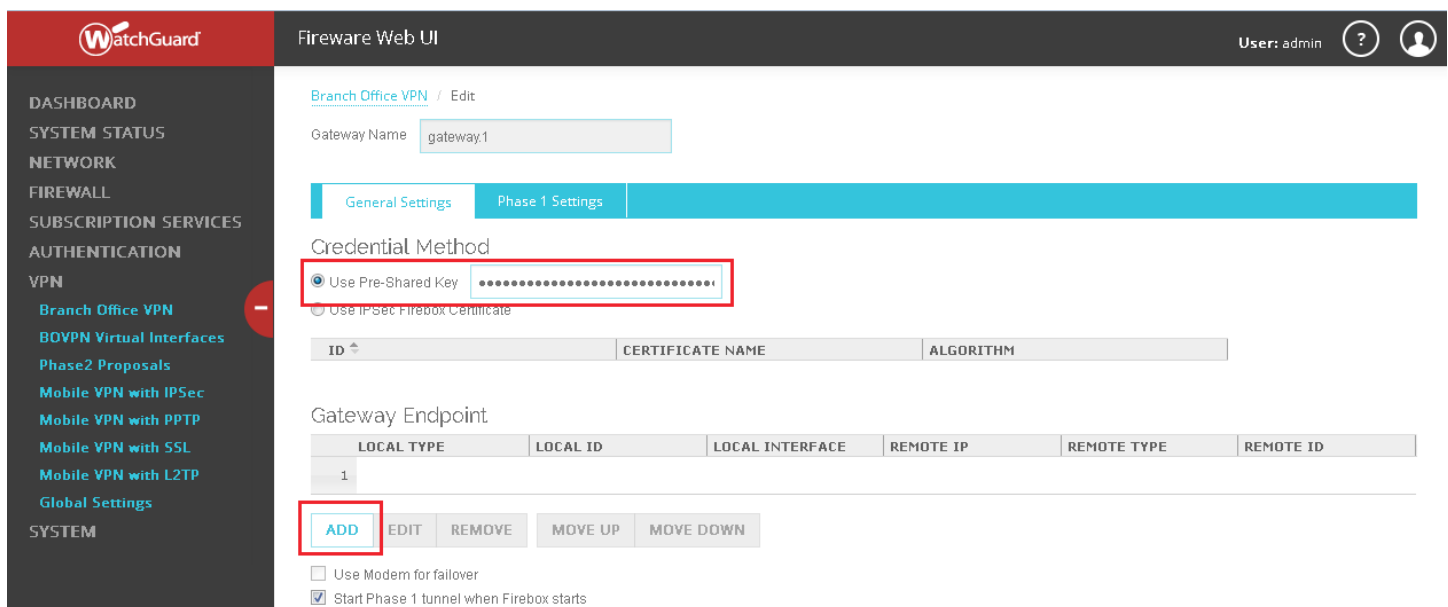
Login to the router using the credentials created during activation.

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**.

Gateway Endpoint Settings ✕

A tunnel needs authentication on each side of the tunnel. Provide the configuration details for the gateway endpoints below.

Local Gateway Remote Gateway

Specify the gateway ID for tunnel authentication.

By IP Address

By Domain Name

By User ID on Domain

By x500 Name

External Interface

OK CANCEL

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

Gateway Endpoint Settings ×

A tunnel needs authentication on each side of the tunnel. Provide the configuration details for the gateway endpoints below.

Local Gateway

Remote Gateway

Specify the remote gateway IP address for a tunnel.

Static IP Address

199.91.85.19

Dynamic IP Address

Specify the remote gateway ID address for tunnel authentication.

By IP Address

199.91.85.19

By Domain Name

By User ID on Domain

By x500 Name

Attempt to resolve domain

OK

CANCEL

Click on **Phase1 Settings**.

General Settings

Phase 1 Settings

Credential Method

Use Pre-Shared Key

.....

Use IPsec Firebox Certificate

ID

CERTIFICATE NAME

ALGORITHM

Gateway Endpoint

	LOCAL TYPE	LOCAL ID	LOCAL INTERFACE	REMOTE IP	REMOTE TYPE	REMOTE ID
1	IP Address	24.14.85.102	External	199.91.85.19	IP Address	199.91.85.19

ADD

EDIT

REMOVE

MOVE UP

MOVE DOWN

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

[Branch Office VPN](#) / Edit

Gateway Name

General Settings

Phase 1 Settings

Mode

NAT Traversal

Keep-alive Interval seconds

IKE Keep-alive

Message Interval seconds

Max failures

Dead Peer Detection (RFC3706)

Traffic idle timeout seconds

Max retries

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

Dead Peer Detection (RFC3706)

Traffic idle timeout seconds

Max retries

Transform Settings

PHASE 1 TRANSFORM

KEY GROUP

ADD

EDIT

REMOVE

MOVE UP

MOVE DOWN

SAVE

CANCEL

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

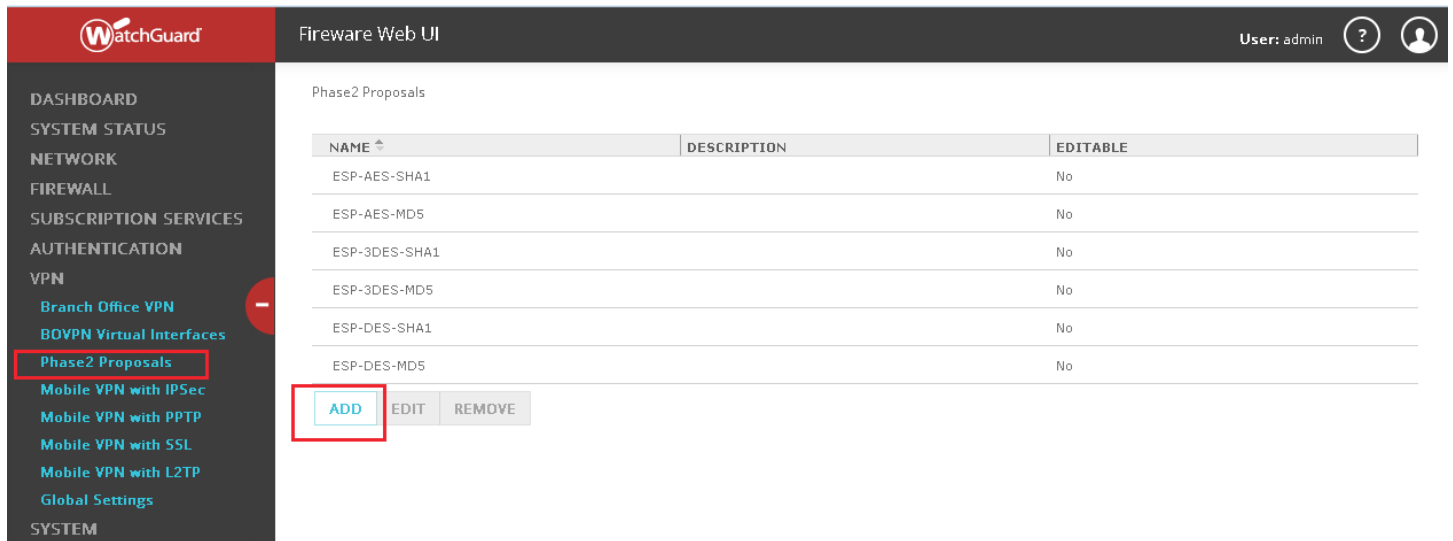
Transform Settings ×

Authentication	SHA1	▼		
Encryption	AES(128-bit)	▼		
SA Life	8	▲▼	hours	▼
Key Group	Diffie-Hellman Group 2	▼		

OK **CANCEL**

PHASE2 PROPOSALS

Click Phase2 Proposals and Click ADD.

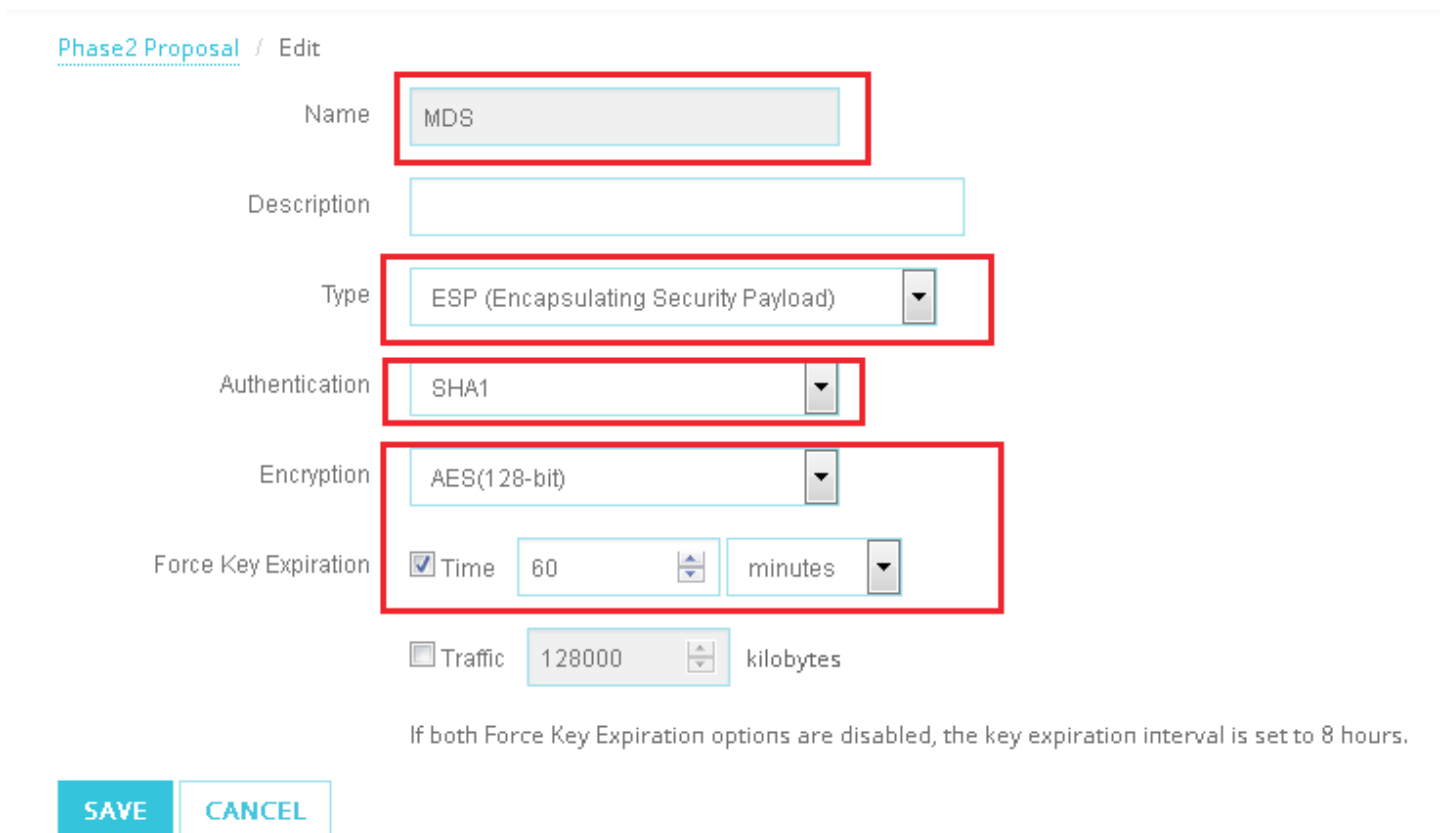


The screenshot shows the WatchGuard Fireware Web UI interface. On the left is a navigation menu with the following items: DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN (with sub-items: Branch Office VPN, BOVPN Virtual Interfaces, Phase2 Proposals, Mobile VPN with IPSec, Mobile VPN with PPTP, Mobile VPN with SSL, Mobile VPN with L2TP, Global Settings), and SYSTEM. The 'Phase2 Proposals' item is highlighted with a red box. The main content area is titled 'Phase2 Proposals' and contains a table with the following data:

NAME	DESCRIPTION	EDITABLE
ESP-AES-SHA1		No
ESP-AES-MD5		No
ESP-3DES-SHA1		No
ESP-3DES-MD5		No
ESP-DES-SHA1		No
ESP-DES-MD5		No

Below the table are three buttons: 'ADD', 'EDIT', and 'REMOVE'. The 'ADD' button is highlighted with a red box.

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



The screenshot shows the 'Phase2 Proposal / Edit' form. The following fields are highlighted with red boxes:

- Name: MDS
- Description: (empty)
- Type: ESP (Encapsulating Security Payload)
- Authentication: SHA1
- Encryption: AES(128-bit)
- Force Key Expiration: Time 60 minutes
- Traffic 128000 kilobytes

At the bottom of the form are two buttons: 'SAVE' and 'CANCEL'.

If both Force Key Expiration options are disabled, the key expiration interval is set to 8 hours.

TUNNEL CONFIGURATION

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

WatchGuard Fireware Web UI

User: admin

Branch Office VPN

Gateways

NAME	EDITABLE
gateway.1	Yes

ADD EDIT REMOVE ENABLE DISABLE REPORT

Tunnels

NAME	EDITABLE
------	----------

ADD CLONE EDIT REMOVE REPORT MOVE UP MOVE DOWN SAVE ORDER

Click **ADD**.

Branch Office VPN / Add

Name: tunnel.1

Gateway: gateway.1

Addresses Phase 2 Settings Multicast Settings

Addresses

Configure tunnel routes for the tunnel

LOCAL	DIRECTION	REMOTE
-------	-----------	--------

ADD EDIT REMOVE

Helper Addresses

Local IP: []

Remote IP: []

Add this tunnel to the BOVPN-Allow policies

SAVE CANCEL

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**.

Tunnel Route Settings ✕

Addresses NAT

Local IP

Choose Type Network IPv4

Network IP 192.168.80.0 / 24

Remote IP

Choose Type Any (0.0.0.0/0)

Direction bi-directional

Enable broadcast routing over the tunnel

OK **CANCEL**

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

DASHBOARD
SYSTEM STATUS
NETWORK
FIREWALL
SUBSCRIPTION SERVICES
AUTHENTICATION
VPN
Branch Office VPN
BOVPN Virtual Interfaces
Phase2 Proposals
Mobile VPN with IPSec
Mobile VPN with PPTP
Mobile VPN with SSL
Mobile VPN with L2TP
Global Settings
SYSTEM

Branch Office VPN / Edit

Name tunnel.1

Gateway gateway.1

Addresses **Phase 2 Settings** Multicast Settings

Perfect Forward Security

Enable Perfect Forward Security Diffie-Hellman Group 2

IPSec Proposals

PHASE 2 PROPOSALS

ESP-AES-SHA1

ESP-AES-SHA1 **ADD** REMOVE MOVE UP MOVE DOWN

SAVE **CANCEL**

Select **MDS**.

The screenshot shows the 'Phase 2 Settings' tab. Under 'Perfect Forward Security', the 'Enable Perfect Forward Security' checkbox is unchecked, and the 'Diffie-Hellman Group 2' dropdown is selected. In the 'IPSec Proposals' section, the 'PHASE 2 PROPOSALS' list is expanded to show 'ESP-AES-SHA1'. Below this, a search box contains 'MDS', and the 'ADD' button is highlighted with a red box. Other buttons like 'REMOVE', 'MOVE UP', and 'MOVE DOWN' are visible but dimmed. At the bottom, 'SAVE' and 'CANCEL' buttons are present, with 'SAVE' highlighted in blue.

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

The screenshot shows the 'Phase 2 Settings' tab. The 'PHASE 2 PROPOSALS' list now shows 'MDS' as the first and only entry, highlighted with a red box. Below the list, the search box contains 'ESP-AES-SHA1', and the 'ADD' button is highlighted in blue. The 'REMOVE', 'MOVE UP', and 'MOVE DOWN' buttons are dimmed. At the bottom, the 'SAVE' button is highlighted in blue and also has a red box around it, while the 'CANCEL' button is dimmed.

VPN STATUS VERIFICATION

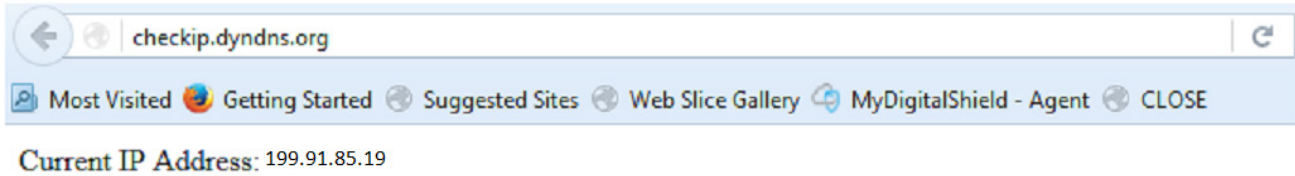
Under the Dashboard Menu, select **VPN Statistics**. Click **Branch Office VPN** tab, then the **Gateway**. Click the tunnel to show the current status of the VPN connection. The **Sent** and **Received** counters should increase. If the **Received** counter is zero, the VPN is not established. Check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

The screenshot displays the VPN Statistics interface. On the left is a sidebar menu with 'VPN Statistics' highlighted. The main content area shows 'VPN Statistics' with a refresh timer at '38 SECONDS'. A tab bar at the top has 'Branch Office VPN' selected with a count of '2'. Below this is a search bar and a 'REKEY ALL TUNNELS' button. A 'Gateway: gateway.1' section is selected with a count of '3', featuring 'EDIT', 'DEBUG', and 'REKEY TUNNELS' buttons. The 'Tunnels' section is expanded to show details for 'Local: 192.168.80.0/24 Remote: 0.0.0.0/04', with 'EDIT' and 'REKEY TUNNEL' buttons. The details are organized into two columns:

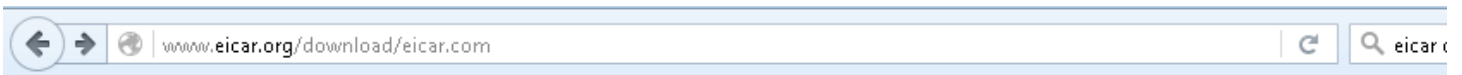
Statistic	Value
Sent	26.39 MB (133,230 packets)
Received	49.75 MB (121,161 packets)
Created	06:33:14 3/9/2016
Expires in	0 days 0 hours 59 minutes
Security	ESP - CBC(AES128) - HMAC(SHA1)
Tunnel Name	tunnel.1
Gateways	24.14.85.102 - 199.91.85.19
Number of Rekeys	249

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.



Web Page Blocked!

You have tried to access a web page which is in violation of your internet usage policy.

URL: www.eicar.org/download/eicar.com

Category: **Malicious Websites**