



**Sonicwall TZ300
MDS BYOG Integration Guide**

CONTENTS

Introduction	3
Assumptions	3
What You Will Need	4
IPSEC Configuration	5
Configure Routing	9
Verify MDS Connectivity	12

INTRODUCTION

Congratulations on your sale of MyDigitalShield using the BYOG option.

This guide is written specifically for the **Sonicwall TZ300**. It can be used as a reference guide to configure the IPSEC tunnel, which will provide the connection to the MDS cloud.

ASSUMPTIONS

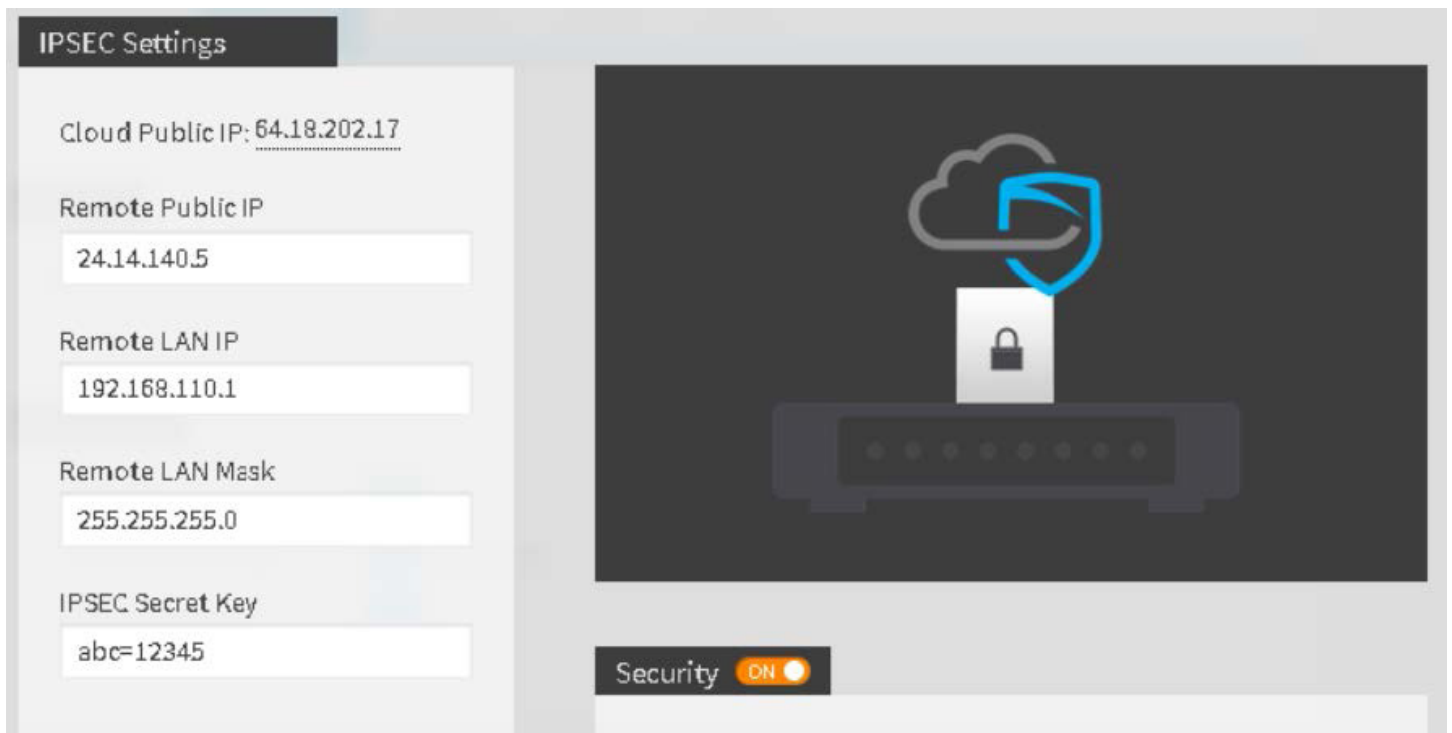
- This guide was developed to provide configuration information of the Sonicwall TZ300 gateway specifically for the setup of the IPSEC tunnel to the MDS Cloud.
- The configuration was tested using the SonicOS Enhanced 6.2.5.1-26n firmware
- This guide is NOT intended to be a full configuration guide for the Sonicwall gateway
- It is assumed that an Internet port and LAN port are configured and operational.
- Responsibility of the management of the Sonicwall 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.
 - The local public IP GW address (your customer's default gateway address).
 - Local LAN network/subnet.
 - The MDS Cloud IP address assigned to you.

Please reference the sample configuration from the MDS portal

MDS Portal Configuration



The screenshot displays the 'IPSEC Settings' configuration page in the MDS portal. The page is divided into two main sections: a configuration panel on the left and a visual representation of the device on the right.

IPSEC Settings

- Cloud Public IP: 64.18.202.17
- Remote Public IP: 24.14.140.5
- Remote LAN IP: 192.168.110.1
- Remote LAN Mask: 255.255.255.0
- IPSEC Secret Key: abc=12345

The right section features a dark background with a central graphic of a cloud connected to a server rack icon. A blue shield with a checkmark is overlaid on the cloud, and a padlock icon is on the server rack, symbolizing security. At the bottom of this section, there is a 'Security' toggle switch that is currently turned 'ON'.

IPSEC CONFIGURATION

Goto **VPN > Settings** then click **Add**.



SonicWALL | Network Security Appliance

VPN / **Settings**

Accept Cancel

VPN Global Settings

Enable VPN
Unique Firewall Identifier:

VPN Policies Refresh Interval (secs) Items p

<input type="checkbox"/>	#	Name	Gateway	Destinations	Crypto Suite
<input type="checkbox"/>	1	WAN GroupVPN			ESP: 3DES/HMAC
<input type="checkbox"/>	2	WLAN GroupVPN			ESP: 3DES/HMAC
<input type="checkbox"/>	3	MDS	64.18.202.17		ESP: NULL/HMAC

Add... Delete

Under the **General** tab, Inside the Security Policy, select **Tunnel Interface** from the Policy Type drop down menu. Fill in the Name and Gateway Address (**MDS Cloud Public IP**). In the IKE Authentication section fills in the Preshared key that was defined in the MDS portal.

General

Proposals

Advanced

Security Policy

Policy Type:

Tunnel Interface

Authentication Method:

IKE using Preshared Secret

Name:

MDS

IPsec Primary Gateway Name or Address:

64.18.202.17

IKE Authentication

Shared Secret:

●●●●●●●●●●

Confirm Shared Secret:

●●●●●●●●●●

Mask Shared Secret

Local IKE ID:

IPv1 Address

Peer IKE ID:

IPv4 Address

Ready

OK

Cancel

Help

Select the **Proposals** tab then fill in the appropriate fields as it is depicted in the screenshot.

General	Proposals	Advanced
IKE (Phase 1) Proposal		
Exchange:	Main Mode	▼
DH Group:	Group 2	▼
Encryption:	AES-128	▼
Authentication:	SHA1	▼
Life Time (seconds):	28800	
Ipssec (Phase 2) Proposal		
Protocol:	ESP	▼
Encryption:	AES-128	▼
Authentication:	SHA1	▼
<input type="checkbox"/> Enable Perfect Forward Secrecy		
Life Time (seconds):	28800	

Select the **Advanced** tab. Click the checkbox to enable keep alive. Click OK when finished.

Advanced

Advanced Settings

- Enable Keep Alive
- Disable IPsec Anti-Replay
- Enable Transport Mode
- Enable Windows Networking (NetBIOS) Broadcast
- Enable Multicast
- Permit Acceleration
- Display Suite B Compliant Algorithms Only
- Allow SonicPointN Layer 3 Management

Management via this SA: HTTPS SSH SNMP

User login via this SA: HTTP HTTPS

VPN Policy bound to:

Ready

OK Cancel Help

CONFIGURE ROUTING

Go to **Network > Routing** then click **Add**.

Mode: Configuration

- Dashboard
- System
- Network
 - Interfaces
 - PortShield Groups
 - Fallover & LB
 - Zones
 - DNS
 - Address Objects
 - Services
 - Routing**
 - NAT Policies
 - ARP
 - Neighbor Discovery
 - MAC-IP Anti-spoof
 - DHCP Server
 - IP Helper
 - Web Proxy
 - Dynamic DNS

X1 (WAN) RIP Disabled OSPF Disabled

X2 (N/A) RIP Disabled OSPF Disabled

X0 (WAN) RIP Disabled OSPF Disabled

Apply the following metric to default routes received from Advanced Routing protocols:

Route Policies Items 1 to 7 (of 7)

View Style: All Policies Custom Policies Default Policies View IP Version: IPv4 Only IPv6 Only IPv4 and IPv6

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
<input type="checkbox"/> 1	Any	255.255.255.255/32	Any	0.0.0.0	X0	20	2			<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/> 2	Any	X1 Default Gateway	Any	0.0.0.0	X1	20	3			<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/> 3	Any	X0 Subnet	Any	0.0.0.0	X0	20	4			<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/> 4	Any	X1 Subnet	Any	0.0.0.0	X1	20	5			<input type="button" value="Edit"/> <input type="button" value="Delete"/>
<input type="checkbox"/> 5	X1 IP	Any	Any	X1 Default Gateway	X1	20	6			<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Select the name created in IPSEC configuration for the **Interface** selection. In this example, it is called **MDS**. Select **OK** when done.



SonicWALL | Network Security Appliance

General

Route Policy Settings

Source: Any

Destination: Any

Service: Any

Gateway: 0.0.0.0

Interface: MDS

Metric: 1

Comment:

Disable route when the interface is disconnected

Permit Acceleration

Auto-add Access Rules

Probe: None

Disable route when probe succeeds

Probe default state is UP

Ready

OK

Cancel

Help

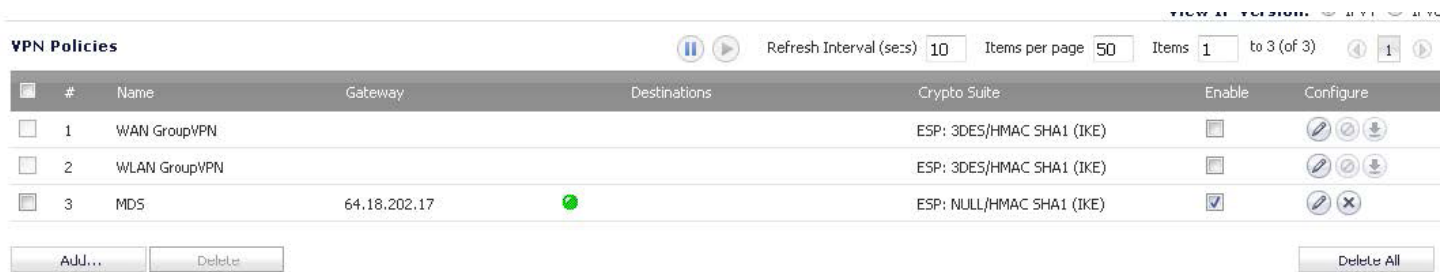
Go back to the VPN configuration to enable the tunnel. Click the checkbox to enable the tunnel.












The screenshot shows the 'VPN Policies' configuration page. On the left, there is a sidebar with 'VPN' selected and sub-items: Settings, Advanced, DHCP over VPN, L2TP Server, and SSL VPN. The main area displays a table of policies. The third policy, 'MDS', has its 'Enable' checkbox checked and highlighted with a red box. The 'Configure' column for this policy shows a red 'X' icon, indicating it is disabled.

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	  
2	WLAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	  
3	MDS	64.18.202.17		ESP: NULL/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	 

A tunnel status icon will turn green when the tunnel is up in the row. The IPSEC tunnel (MDS) is also listed under the “Currently Active VPN Tunnels.”



The screenshot shows the 'VPN Policies' configuration page after the MDS policy has been enabled. The 'Enable' checkbox for the 'MDS' policy is now checked, and a green status icon is visible in the 'Destinations' column. The 'Configure' column for this policy now shows a blue 'X' icon, indicating it is active.

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	  
2	WLAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	  
3	MDS	64.18.202.17		ESP: NULL/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	 

Site To Site Policies: 1 Policies Defined, 1 Policies Enabled, 10 Maximum Policies Allowed
GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 25 Maximum Policies Allowed



The screenshot shows the 'Currently Active VPN Tunnels' page. It displays a single active tunnel for the 'MDS' policy. The 'Local' and 'Remote' IP ranges are both 0.0.0.0 - 255.255.255.255, and the 'Gateway' is 64.18.202.17. A 'Renegotiate' button and a refresh icon are visible in the 'Gateway' column.

#	Created	Name	Local	Remote	Gateway	
1	04/24/2016 22:04:20	MDS	0.0.0.0 - 255.255.255.255	0.0.0.0 - 255.255.255.255	64.18.202.17	<input type="button" value="Renegotiate"/> 

VERIFY MDS CONNECTIVITY

Open up a browser on a computer attached to the local LAN network. Attempt to browse www.eicar.org/download/eicar.com.txt. You should see a block message.



High Security Alert!!

You are not permitted to download the file "eicar.com.bt" because it is infected with the virus "EICAR_TEST_FILE".

URL = <http://www.eicar.org/download/eicar.com.bt>
File quarantined as: .

http://www.fortinet.com/ve?vn=EICAR_TEST_FILE
Client IP: 192.168.110.100
Server IP: 188.40.238.250
User name:
Group name:

Using the same computer, attempt to browse www.gamblingsites.org.



Web Page Blocked!

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

URL: www.gamblingsites.org/
Category: Gambling

Proceed

Go Back