Cisco 1841
MyDigitalShield BYOG Integration Guide

CONTENTS

INTRODUCTION

Congratulations on your sale of MyDigitalShield using the BYOG option.

This guide is written specifically for the **Cisco 1841** It can be used as a reference guide to configure the IPSEC tunnel, which will provide the connection to the MDS cloud.

ASSUMPTIONS

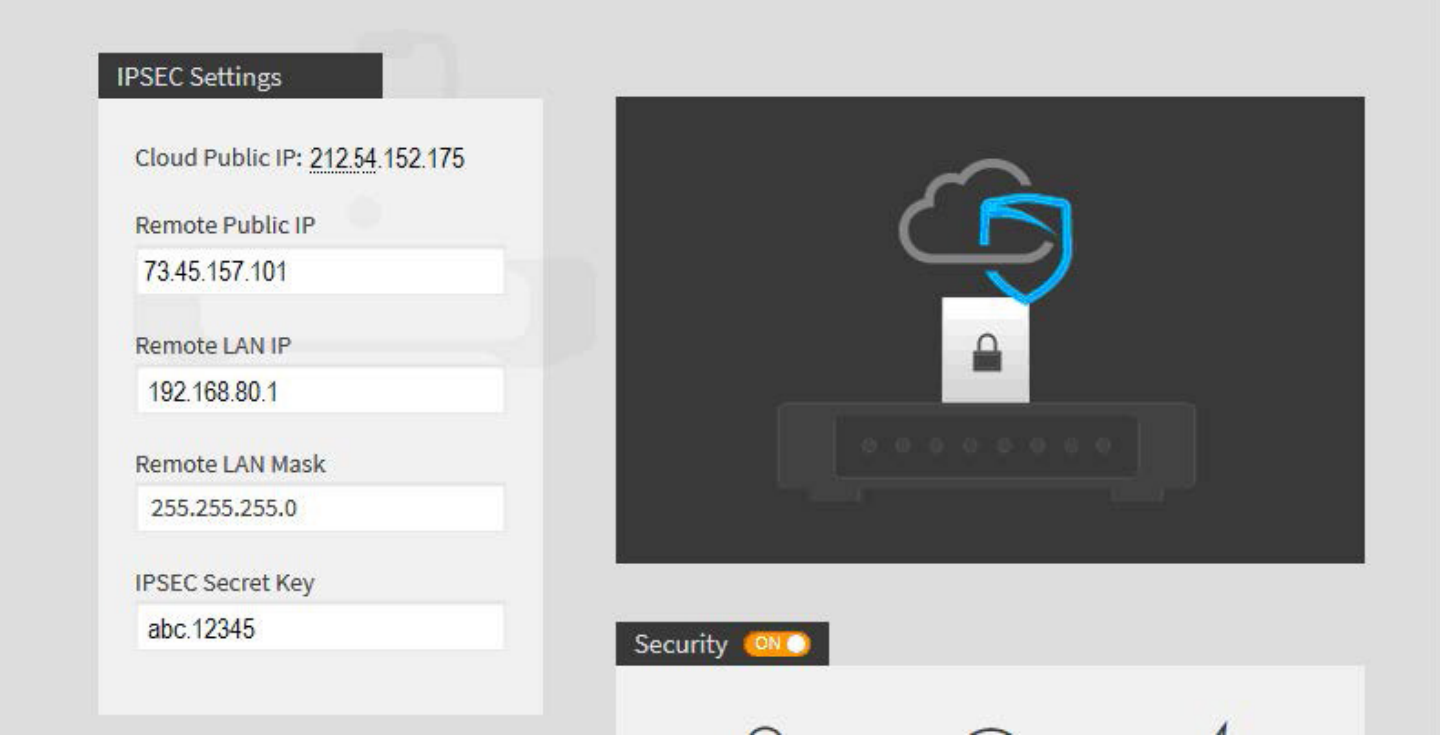
- This guide was developed to provide configuration information of the Cisco 1841 gateway specifically for the setup of the IPSEC tunnel to the MDS Cloud.
- The configuration was tested using the Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(23)
- This guide is NOT intended to be a full configuration guide for the Cisco gateway
- It is assumed that an Internet port and Lan port are configured and operational.
- Responsibility of the management of the Cisco 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)		73.45.157.101/23
Local LAN Network (x.x.x.x/mask)		192.168.80.0/24
Cloud Public IP (x.x.x.x)		212.54.152.175

VERIFY IP ADDRESS

 # show ip interface brief
Sample results:

```
Router#ship interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        73.45.157.101   YES manual up                    up
FastEthernet0/1        192.168.80.1    YES manual up                    up
NVI0                   unassigned      NO unset up                      up
```

This guide is using interface FA0/0 as the WAN and interface FA0/1 as the LAN interface. Follow the examples and adjust the interfaces used here to match the interfaces at the site you are configuring.

CONFIGURE THE IPSEC TUNNEL

While in enable mode, type the following commands. The two highlighted objects are the pre-shared key and the MDS Cloud Public IP. Replace them with the defined information configured in the MDS portal.

```
conf terminal
crypto isakmp policy 1
encr aes
authentication pre-share
group 2
lifetime 28800 crypto isakmp key abc.12345 address 212.54.152.175
crypto ipsec transform-set TS esp-aes esp-sha-hmac
```

Replace the peer IP address with the MDS Cloud Public IP.

```
crypto map CMAP 10 ipsec-isakmp
set peer 212.54.152.175
set transform-set TS
match address VPN-TRAFFIC


interface FastEthernet0/0
  ip address 73.45.157.101 255.255.254.0
  ip nat outside
  ip virtual-reassembly
  duplex auto
  speed auto
  crypto map CMAP
!
interface FastEthernet0/1
  ip address 192.168.80.1 255.255.255.0
  duplex auto
!
```

CONFIGURE ACCESS LIST FOR LOCAL INTERFACE

For VPN traffic to be allowed, an access list is needed. Permit the local LAN subnet.

```
interface FastEthernet0/1
ip access-list extended VPN-TRAFFIC
  permit ip 192.168.80.0 0.0.0.255 any
```

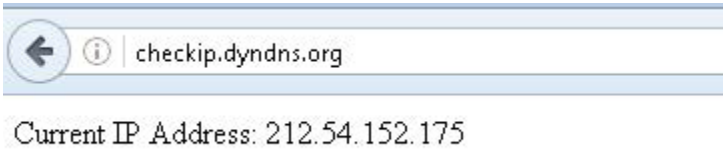
BRING THE TUNNEL UP

The tunnel will come up when a packet is generated from a computer connected to the Local LAN network. In the example used for this guide, traffic coming from 192.168.80.0/24 should pass through the tunnel. To generate traffic, ping 8.8.8.8 from a computer attached to the Local LAN.

If the ping test fails, verify the configuration to make sure all configurations are present and correct.

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 WEB BLOCK TO MDS

Access a gambling site. For example: gamblingsites.org

TROUBLESHOOTING COMMANDS

Below are some commands to verify the ipsec configuration.

Displays ISAKMP policy

```
Router#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:       AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm: Secure      Hash Standard
        authentication method:      Pre-Shared Key
        Diffie-Hellman group:             #2 (1024 bit)
        lifetime:                   28800 seconds, no volume limit
Default protection suite
        encryption algorithm:       DES - Data Encryption Standard (56 bit keys).
        hash algorithm:             Secure Hash Standard
        authentication method:      Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:             #1 (768 bit)
        lifetime:                   86400 seconds, no volume limit
Router#
```

Displays ISAKMP sa

```
Router#show crypto isakmp sa
dst                 src                 state                 conn-id slot status
73.45.157.101  212.54.152.175      QM_IDLE              10       0  ACTIVE
```

Displays ISAKMP key (pre-shared key)

```
Router#sh crypto isakmp sa    key    key
Keyring          Hostname/Address          Preshared Key

default          212.54.152.175            abc.12345
```

Displays IPSEC SA timeouts

Router#show crypto ipsec security-association-lifetime
Security association lifetime: 4608000 kilobytes/3600 seconds

Displays IPSEC SA

Router#show crypto ipsec sa

interface: FastEthernet0/0
Crypto map tag: CMAP, local addr 73.45.157.101

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.80.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 212.54.152.175 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 13560, #pkts encrypt: 13560, #pkts digest: 13560
#pkts decaps: 15940, #pkts decrypt: 15940, #pkts verify: 15940
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 3, #recv errors 0

local crypto endpt.: 73.45.157.101, remote crypto endpt.: 212.54.152.175
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x40FB60DB(1090216155)

inbound esp sas:
spi: 0xB27D84F(187160655)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 3001, flow_id: FPGA:1, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4405020/1358)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE <- Indicates that inbound ESP is ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x40FB60DB(1090216155)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 3002, flow_id: FPGA:2, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4405047/1353)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE <- Indicates that outbound ESP is ACTIVE

outbound ah sas:

outbound pcp sas:

Displays Connections Active Engine

Router#show crypto engine connections active

ID	Interface	IP-Address	State	Algorithm	Encrypt	Decrypt
4	FastEthernet0/0	73.45.157.101	set	HMAC_SHA+AES_CBC	0	0
3001	FastEthernet0/0	73.45.157.101	set	AES+SHA	0	745
3002	FastEthernet0/0	73.45.157.101	set	AES+SHA	599	0

KNOWN ERRORS

During an established IPSEC session with the MDS cloud. An error is generated in the cisco router. This error pertains to an authentication failed error. This is a false negative error and a bug is present with the current version IOS 12.4(23).

Error:

*Apr 2 13:46:53.564: %CRYPTO-4-RECVD_PKT_MAC_ERR: decrypt: mac verify failed for connection id=3004 local=73.45.157.101 remote=212.54.152.175 spi=5745B05F seqno

Reference:

https://quickview.cloudapps.cisco.com/quickview/bug/CSCsx24725https://quickview.cloudapps.cisco.com/quickview/bug/CSCsx24725

https://quickview.cloudapps.cisco.com/quickview/bug/CSCsx24725

https://quickview.cloudapps.cisco.com/quickview/bug/CSCsx24725