

Cisco ASA 5505 MDS BYOG Integration Guide

CONTENTS

Introduction	3
Assumptions	3
What You Will Need	4
IPSEC Configuration	6
Validate Traffic to MDS	13
Validate MDS Web Block	13

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.

PSEC Settings	
Cloud Public IP: 66.163.23.209 Remote Public IP	
73.74.101.150	
Remote LAN IP	
192.168.101.0	
Remote LAN Mask	0 0 8 0 0 0 0 0
255.255.255.0	
IPSEC Secret Key	
welcome_me	Security ONO

- **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

liew T	Tools Wizards Window Help				Туре	topic to search	Go	11.
me o	Conf Startup Wizard	Back C Forward 9 Help					CIS	co
	VPN Wizards	Site-to-site VPN Wizard						_
Device	High Availability and Scalability Wizard Device I Unified Communication Wizard Infor Packet Capture Wizard	AnyConnect VPN Wizard Clientless SSL VPN Wizard IPsec (IKEv1) Remote Access	; VPN Wizard					
Genera	ral License		Interface	IP Address/Mask	Line	Link	Kbps	1
			inside	192.168.101.1/24	🕒 up	🕤 up	12	
ASA V ASDM Firew	Civane: Ciscoasa Version: 9.0(1) Device Uptime: 3d M Version: 7.1(1)52 Device Type: AS wall Mode: Routed Context Mode: Si Glabe: 128 MB Total Mode: Si	d 3h 42m 8s 5A 5505 ngle 12 MB	outside	73.74.101.150/23	3 up	🕤 ир	2	
TOTAL	Total Memory: 51		Select an interface	to view input and output Kbps				
VPN See	essions		Traffic Status					
IPsec:	1 Clientless SSL VPN: 0 AnyConnect Cl	lient: 0 Details	- Connections Per 9	Second Lisage				
<mark>yste</mark> m PU Usaç	m Resources Status age (percent)						/	
System PU Usag 8%	m Resources Status age (percent)		0	31 17:32 ■ TCP: 1 ■ Total: 1	17:33	17:34	17:35	F
System CPU Usaç 8% 17:35:27	m Resources Status age (percent)		0 UDP: 0	31 17:32 ■ TCP: 1 ■ Total: 1 : Traffic Usage (Kbps)	17:33	17:34	17:35	
System PU Usag 8% 17:35:27 4emory U 253MB	m Resources Status age (percent)		UDP: 0	31 17:32 ■ TCP: 1 ■ Total: 1 • Traffic Usage (Kbps)	17:33	17:34	17:35	
System CPU Usag 8% 17:35:27 4emory L 253MB test AS	m Resources Status age (percent) 100 50 Usage (MB) 400 200 SDM Syskog Messages		Currectory of a	31 17:32 ■ TCP: 1 ■ Total: 1 : Traffic Usage (Kbps)	17:33	17:34	17:35	<u></u>
System CPU Usag 8% 17:35:27 Memory U 253MB test AS e 15:25 15:25 15:25	Implement Sources Status age (percent) 100 100 50 50 100 7 400 100 200 100 100 50H Syslog Messages 100 100 Syslog ID Source IP Source Destination IP Destination IP 302016 8.8.8.8 53 192.168.101.7 6311 302016 8.8.8.8 53 192.168.101.7 6181	stha Description L27 Teardown UDP connection 113222 for 31 Teardown UDP connection 113221 for 120 Teardown UDP connection 113221 for 121 Teardown UDP connection 113221 for 122 Teardown UDP connection 113221 for	r outside:8.8.8.9/53 to in r outside:8.8.8.9/53 to in r outside:8.8.8.9/53 to in r outside:8.8.8.9/53 to in	31 17:32 ■ TCP: 1 ■ Total: 1 ■ Traffic Usage (Kbps) side: 192. 168. 101.7/63127 duration side: 192. 168. 101.7/59340 duration side: 192. 168. 101.7/59340 duration	17:33 10:02:01 bytes 112 10:02:01 bytes 112 10:02:01 bytes 112 10:02:01 bytes 118	17:34	17:35	р × • •

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

Site-to-site VPN Connection S	Setup Wizard	×
Site-to-site VPN Connection S	Setup Wizard Introduction Use this wizard to setup new site-to-site VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A site-to-site VPN tunnel protects the data using the IPsec protocol. Site-to-Site VPN Local Content Conte	
į (< Back Next > Cancel Help	,

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

🚰 Site-to-site VPN Connectio	Setup Wizard	
Steps	Peer Device Identification	
 Introduction Peer Device Identification IKE Version IKE Version Traffic to protect Authentication Methods Encryption Algorithms Miscellaneous Summary 	This step lets you identify the peer VPN device by its IP address and the interface used to access the peer. Peer IP Address: 66.163.23.209 VPN Access Interface: outside	
	< <u>Back</u> <u>Next</u> Cancel Help	

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

Steps	IKE Version
 Introduction Peer Device Identification IKE Version Traffic to protect Authentication Methods Encryption Algorithms Miscellaneous Summary 	ASA supports both version 1 and version 2 of the IKE (Internet Key Exchange) protocol. This step lets you decide which version or versions to support in this connection profile.
	< <u>Back</u> <u>Next</u> Cancel Help

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.

🚰 Site-to-site VPN Connection	Setup Wizard
Steps	Traffic to protect
 Introduction Peer Device Identification IKE Version Traffic to protect Authentication Methods Encryption Algorithms Miscellaneous Summary 	This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption. Local Network: 192.168.101.0/24 Remote Network: any
	< Back Next > Cancel Help

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.

Site-to-site VPN Connection	Setup Wizard	×
Site-to-site VPN Connection Steps I. Introduction 2. Peer Device Identification 3. IKE Version 4. Traffic to protect 5. Authentication Methods 6. Encryption Algorithms 7. Miscellaneous	Setup Wizard Authentication Methods This step lets you configure the methods to authenticate with the peer device. IKE version 1 Pre-shared Key: Device Certificate: None Manage	
8. Summary		
	< Back Next > Cancel H	Help

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

Steps	Encryption Algorithms	
 Introduction Peer Device Identification IKE Version Traffic to protect Authentication Methods Encryption Algorithms Miscellaneous Summary 	This step lets you select the types of encryption algorithms used to protect the data. IKE version 1 IKE Policy: pre-share-aes-256-sha IPsec Proposal: ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-] Select.	
	< Back Next > Cancel Hel	n

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.

IKE policy is global. It is shared by all IPsec connection profiles.
ОК

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

ADD M	Edit 🔟 Delete	Eind:	6	O Match Case	e
riority #	Encryption	Hash	D-H Group	Authentication	Lifetime (seconds)
	120 aes-255	sha		5 pre-share	864

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.

Priority:	120	
Authentication:	pre-share	•
Encryption:	aes-256	•
D-H Group:	5	+
Hash:	sha	•
Lifetime:	Unlimited 86400	seconds 🗸

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.

Site-to-site VPN Connection	n Setup Wizard
Steps	Miscellaneous
 Introduction Peer Device Identification IKE Version Traffic to protect Authentication Methods Encryption Algorithms Miscellaneous Summary 	This step lets you configure some other important parameters.
	< <u>Back</u> <u>Next</u> Cancel Help

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.

'PN Wizard	Summary	
Branch	Here is the summary of the configuration.	
EST T	Name	Value
T = ISP	🗆 Summary	
	Peer Device IP Address	66.163.23.208
Home	VPN Access Interface	outside
(Corporate)	Protected Traffic	Local Network: 192.168.101.0/24 Remote Network: any
Network	IKE Version Allowed	IKE version 1 only
r . At	📃 🖂 Authentication Method	
THE SHA	IKE v1	Use pre-shared key
and the second	Encryption Policy	
19.9 <u>+</u>	Perfect Forward Secrecy (PFS)	Enabled using Diffie-Hellman Group: group2
	🖃 IKE v1	
	IKE Policy	pre-share-aes-256-sha
TT	IPsec Proposal	ESP-AES-128-SHA, ESP-AES-128-MD5, ESP-AES-192-SHA, ESP-AES-192-MD5, ESP-AES-256-SHA, ESP-AES-256-MD5, ESP-3DES-SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5
a la	Bypass Interface Access List	Yes
	Network Address Translation	The protected traffic is subjected to network address translation
	<u> </u>	Cancel Help

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.

	v (*	Q Search	\$	é l	1 🔿	Ø	B	=
) (i) checkip.dyndns.org		Q Search	돠		• 🏠	9	6	=

VALIDATE MDS WEB BLOCK

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







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