# CRYPTO-MAS authentication system with a FortiGate device running firmware version 4.0 MR2 for SSL VPN access



This guide documents how to integrate the CRYPTO-MAS authentication system with a FortiGate device running firmware version 4.0 MR2 for SSL VPN access.

Below is a list of the software and hardware used for this example :

- CRYPTOCard Authentication token (software based)
- FortiGate 60B running version 4.0 MR2

## **Configuring CRYPTO-MAS server**

CRYPTO-MAS authentication uses RADIUS to communicate between "access points" (the FortiGate) and to authenticate users.

For secure connectivity, provide the CRYPTO-MAS server with the IP Address of the FortiGate (where the authentication requests originate from) and the customisable RADIUS Pre Shared Key (used for encryption)

To complete setup, follow the steps below:

With the details provided from CRYPTOCard, login to the portal at https://mas.cryptocard.com

- 1 Select *OPTIONS* from the tabs along the top of the interface
- 2 In the Service Request drop down box select SCR-Access Point
- 3 Verify the information in *Requestor* and *Customer Information* are correct
- 4 Under sub section Access Point Configuration enter details of the FortiGate device.
- 5 Scroll down and submit the form

Soon after completion, an email confirming the request will be sent. This will also provide details of the CRYPTO-MAS server (IP Address etc...) which are used later in this configuration.

🕹 CRYPTO-MAP - Mozilla Firefox	100	1						<b>X</b>
<u>File Edit View History Bookmarks</u>	s <u>T</u> ools <u>H</u> elp							
C X 🏠 Cryptoc	card.com https://r	nas.cryptocard.com/	ccmap/main.jsp		☆ -	🚼 - Google	🔎 😣	• 🔝
👌 СКУРТО-МАР	*							~
r r								
CRYPTOCard						SUPPO	DRT LOGOUT	
	HOME	USER	TOKEN	GROUP	COMPANY	REPORT	OPTIONS	
Reseller End User Organization	SERVICE REQUES	r Point 💌						
t)	CRYPTO-	MAS Service Char	ige Request				-	
	Date/Time:	April 07, 2010 2:08	:42 P.M.					
	Company Name: Auth ID: User Name:	Requester:						
	С	ustomer Informa	tion:					
	Company Name:							
	Auth ID:						E	
	Acc	ess Point Configu	ration					
	Action:	Add 💌						
	Make:	60B						
	Host Name:	example.host						
	LAN IP Address:	<devices internal<="" td=""><td>IP&gt;</td><td></td><td></td><td></td><td></td><td></td></devices>	IP>					
	WAN IP Address:	<ext -="" ip="" of<="" source="" td=""><td>your auth requests&gt;</td><td></td><td></td><td></td><td></td><td></td></ext>	your auth requests>					
	Shared Secret:	examplesecret1234	4					
	Access	Control List Con	figuration					
	Action:	Add 💌						
	Group Name:							-
Done								

**Note:** It is important that the shared secret chosen be strong. Use the table below to keep a note of the shared secret and the CRYPTO-MAS RADIUS Server IP's (once received from CRYPTOCard):

CRYPTO-MAS RADIUS Shared Secret	
Primary CRYPTO-MAS RADIUS Server IP or	
fully qualified hostname	
Secondary CRYPTO-MAS RADIUS Server IP or	
fully qualified hostname (OPTIONAL)	
CRYPTO-MAS RADIUS port number	
(OPTIONAL)	

Additional users can be created and assigned tokens in your CRYPTO-MAS portal under the *Users* section. In the example below "testuser" has been created in the portal then assigned and emailed a software token

🕘 CR	YPTO-MAP - Mozilla Firefox								
<u>F</u> ile	<u>Edit V</u> iew Hi <u>s</u> tory <u>B</u> ookma	irks <u>T</u> ools <u>H</u> elp							
<ul> <li></li> </ul>	🕞 🗸 🔂 🔁 🔁 CTYP	tocard.com https://m	as.cryptocard.com/ccn	nap/main.jsp		☆ -	Soogle ₹	م	🐵 · 🔝
👌 C	RYPTO-MAP	+							
F									
	CRYPTOCard								Т
_		номе	USER	TOKEN	GROUP	COMPANY	REPOR	OPTIONS	
	Se:Reseller	SELECTED GROUP	$\sim$		MANAGE USERS		SEAF	CH USER LIST	
	End User Organization				👃 🛛 Add 📃	dit Delete R	ADIUS User	Login:	
	( III)	User Login	First Name	Last Name	e Stati	ic Admin			
							First	Name:	
		a testuser	Test	User	-	-			
							Last	Name:	
						-			
									_
							AUT	ENTICATION LEGEND	
							Icon	Authentication Type	
								No Token Assigned	
								Static Password	
							<b>T</b>		
Done									<u>A</u>
Done									📕

# **Configuring the FortiGate**

Login to the FortiGate:

- 1 Browse to User-> Remote-> RADIUS
- 2 Click Create New

Minimum settings required for configuring the RADIUS server.

- 1. Name: Enter the name that is used to identify the RADIUS server on the FortiGate unit.
- 2. **Primary Server Name/IP**: Enter the domain name or IP address of the primary RADIUS server.
- 3. **Primary Server Secret:** Enter the RADIUS server secret key for the primary RADIUS server. The primary server secret key should be a maximum of 16 characters in length.
- 4. Authentication Scheme: Leave this in its default setting as shown below
- 5. Click on OK

🅹 FortiGate - FGT60B3907504775 - Mozill	a Firefox		
<u>File Edit View History Bookmarks T</u>	ools <u>H</u> elp		
😋 🔊 🗸 C 🗙 🏠 🗋 http://192	.168.1.1/index	☆ 👻 🚼 ד Google	욙 - 🚱
FortiGate - FGT60B3907504775	+		
FortiGate 60B	2	Image: Constraint of the second sec	FCRTINET
System		Edit RADIUS Server	
Router	Name	CRYPTO-MAS	
Firewall	Primary Server Name/IP		
UTM	Primary Server Secret	•••••	
VPN	Secondary Server Name/IP		
User	Secondary Server Secret	•••••	
🕀 🌇 User	Authentication Scheme	Ose Default Authentication Scheme	
🕀 👸 User Group		Specify Authentication Protocol	
LDAP		MS-CHAP-v2 💌	
RADIUS	NAS IP/Called Station ID		
TACACS+	Include in every User Group	Enable	
Girectory Service      Monitor		OK Cancel	
Endpoint			
Wireless Controller			
Log&Report			
Done	<b>1</b>		

## Create Users and Groups on the FortiGate

Now create a User on the FortiGate. This user needs to have the same *Username* as one that exists on the CRYPTO-MAS Server. For example, the "testuser" created earlier. Configuration settings as follows:

- 1 Go to User-> User-> User
- 2 Click Create New.
  - a. Enter the username (as appears in the CRYPTO-MAS portal i.e. testuser).
  - b. Select Match user on RADIUS server. From the drop down box select CRYPTO-MAS.
  - c. Click OK to complete configuration

🕙 FortiGate - FGT60B3907504775 - Mozill	la Firefox			
<u>File Edit View History Bookmarks T</u>	<u>F</u> ools <u>H</u> elp			
C X 🟠 (L) http://192	2.168.1.1/index		🖾 🔻 🏹 🖌 Googl	e 🖉 🔍 🕷
FortiGate - FGT60B3907504775	*			*
FortiGate 60B	0		Image: Weight of the second	FCRTINET
System		New Us	ser	
Router	User Name	testuser		
Firewall		Disable		
UTM	Password	•••••		
VPN	Match user on LDAP server	[Please Select] 👻		
User	Match user on RADIUS server	CRYPTO-MAS -		
🖻 🌇 User	Match user on TACACS+ server	[Please Select] 👻		
User		ОК	Cancel	
⊕ 🖓 User Group				
⊕ 🧿 Remote				
🗉 🚰 Directory Service				
⊕				
Endpoint				
Wireless Controller				
Log&Report				
Done				

Next add this user (testuser) to a group that will be associated with SSL VPN Access. Either create a new group or use the existing "SSLVPN\_USERS" group. The steps below are based on using the existing.

Configuration settings as follows:

- 1 Go to User-> User Group-> User Group
- 2 Expand the *Firewall* group type by clicking on the blue arrow
- 3 Select SSLVPN\_USERS and then select Edit from the tab above

🔮 FortiGate - FGT60B3907504775 - Mozi	lla Firefox	the second bullet have	A Real And and and	
<u>File Edit View History B</u> ookmarks	<u>T</u> ools <u>H</u> elp			
🔁 🔊 🗸 😋 🗶 🏠 📋 http://19.	2.168.1.1/index		😭 👻 🚼 🗝 Google	Ρ 🕶 🔹 🔝
FortiGate - FGT60B3907504775	+			-
FortiGate 60B			Image: Constraint of the second sec	RTINET
System	Create New Z Edit Delete			
Router		Group Name	Members	
Element I	▼ Firewall			
Firewall		SSLVPN_USERS	CRYPTO-MAS	
UTM	birectory service			
VPN				
User				
🕀 🖪 User				
Ser Group				
User Group				
🗉 💱 Directory Service				
🗈 🗐 Monitor				
Endpoint				
Wireless Controller				
Log&Report				
Done				

In the *Edit User Group* menu:

- 4 From Available Users/Groups section select user i.e. testuser in our case.
- 5 Click the arrow pointing to the right to move user to the *Members* section
- 6 Click OK

🍪 FortiGate - FGT60B3907504775 - Mozil	la Firefox	
<u>File Edit View History B</u> ookmarks	<u>I</u> ools <u>H</u> elp	
😋 🔊 🗸 C 🗙 🏠 🕒 http://192	2.168.1.1/index	😭 🚽 🚰 🛛 Google 🛛 🔎 🐵 🔹 🔝
FortiGate - FGT60B3907504775	*	· · · · · · · · · · · · · · · · · · ·
FortiGate 60B		
System	Edit User G	Group
Router	Name SSLVPN_USERS	
Firewall	Type 🛛 🖲 Firewall 🔘 Directory Service	
UTM	Allow SSL-VPN Access full-access 🔹	
VPN	Available Users/Groups Members	
User User Group User Group	Local Users -     Users on RADIUS/LDAP/TACACS+ servers -     CRYPTO-MAS  Match one of these group names  Add  Remote Server  Group Name  OK	ers - I RADIUS/LDAP/TACACS+ servers - Delete Cancel
Endpoint		
Wireless Controller		
Log&Report		
Done		

#### ALTERNATIVE METHOD

All users created on the CRYPTO-MAS server can be given access to SSL VPN at once without creating users on the FortiGate individually. This does not provide granular control of users who have access to SSL VPN, but does make it easier to configure if there are many users on the CRYPTO-MAS server.

Configuration settings as follows:

- 1 Go to User-> User Group-> User Group
- 2 Select SSLVPN\_USERS and then select Edit from the tab above
- 3 Add the **RADIUS Server** created earlier (CRYPTO-MAS) into the *Members* section (instead of a user)

# **Enable and Configure SSL VPN**

Configuration settings as follows:

- 1 Browse to VPN-> SSL-> Config
- 2 Tick Enable SSL VPN
  - a. Edit any additional parameters of the SSL VPN configuration as required or leave default settings
- 3 Click Apply

🕹 FortiGate - FGT60B3907504775 - Mozil	la Firefox	and the second second	-	August .	
<u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks	<u>T</u> ools <u>H</u> elp				
🕒 🗸 C 🗙 🏠 🗋 http://192	2.168.1.1/index		☆ ·	- 🔧 - Goo	ogle 👂 💀 🔹 🔝
FortiGate - FGT60B3907504775	*				
FortiGate 60B			(2) Help	Logout	F
System		SSL-VPN S	Settings		
Router	Enable SSL-VPN				
Firewall	IP Pools	[Edit]			
UTM VPN SSL - Config - Portal - Virtual Desktop Applicati - Host Check - Monitor	Server Certificate Require Client Certificate Encryption Key Algorithm Idle Timeout Advanced (DNS and W	Self-Signed   High - AES(128/256 bits)  Default - RC4(128 bits) au Low - RC4(64 bits), DES a 300 (seco INS Servers)	and 3DES nd higher and higher onds)		
User Endpoint Wireless Controller					
Done					

# Configuring Firewall Policy to Allow SSL Access

- 1 Go to Firewall-> Policy-> Policy
- 2 Click Create New

🕹 FortiGate - FGT60B3907504775 - Mozill	a Firefox	the summer Audited Audited. And	and summer of	
<u>File Edit View History B</u> ookmarks I	ools <u>H</u> elp			
🗲 🕞 🗸 C 🗙 🏠 🕒 http://192	.168.1.1/index		🟠 👻 🚼 🕶 Google	P 🚇 - 🔒
FortiGate - FGT60B3907504775	+			
FortiGate 60B			Image: Weight of the second	F
System		New Policy		
Router	Source Interface/Zone	wan1(External)	•	
Firewall	Source Address	all	🗕 🗉 Multiple	
Policy	Destination Interface/Zone	internal	•	
Policy	Destination Address	all	▼ ■ Multiple	
Central NAT Table	Action	SSL-VPN	-	
- DoS Policy - Sniffer Policy - Protocol Options	SSL Client Certificate Res	Any -		
⊕ G Service ⊕ G Schedule ⊕ ∰ Traffic Shaper ⊕ ∰ Virtual IP ⊕ ⊕ Load Balance	Configure SSL-VPN Users Display Implicit Policie	s Add		
	Comments (maximum 63 cha	aracters)		
UTM		,		
VPN				
User				
Endpoint				
Wireless Controller				
Log&Report				
Done				ai

3 Enter the below policy options:

Source Interface/Zone	WAN1 (or another external interface where external users will
	be accessing from)
Source Address	All
Destination Interface/Zone	Internal (or the interface(s) behind which required network
	resources reside)
Destination Address	All
Action	SSL-VPN

Under "Configure SSL-VPN Users":

🕙 FortiGate - FGT60B3907504775 - Mozill	a Firefox	And And And And And And	And and and and	
<u>File Edit View History Bookmarks T</u>	ools <u>H</u> elp			
🗲 🕑 🗸 🔁 🗋 http://192	.168.1.1/index		🟠 👻 🚼 🗝 Google	P 💀 - 🔝
FortiGate - FGT60B3907504775	+			<b>•</b>
FortiGate 60B	5		Image: Point of the second s	
System		Edit Policy		
Router	Source Interface/Zone	wan1(External)	~	
Firewall	Source Address	all	▼ I Multiple	
B-III Policy	Destination Interface/Zone	internal	<b>.</b>	
Policy	Destination Address	all	✓ I Multiple	
···· • Central NAT Table	Action	SSL-VPN	•	
Dos Policy     Siffer Policy     Protocol Options     Address     Service     Schedule     Traffic Shaper     Morrison IP     Load Balance	SSL Client Certificate Res Cipher Strength Configure SSL-VPN Users Display Implicit Policie Rule ID User Group Se 1 SSLVPN_USERS A	strictive Any • s s rvice ScheduleUTM_Logging NY always & @ î 2 2		
VPN	Comments (maximum 63 cha	iracters)		
User				
Endpoint				
Wireless Controller				
Log&Report		OK Ca	incel	
Done	L			

- 4 Click *add* (the window below appears)
  - a. Move the SSLVPN\_USERS group into Selected User Groups.
  - b. Choose which firewall ports the group can pass traffic over (in the example below *ANY* traffic is allowed
  - c. Scroll down and Click OK
  - d. Click OK again

FortiGate - FGT60B3907504775 - Mozil	la Firefox			
File Edit View History Bookmarks	Tools Help			
C × 🟠 🗋 http://192	2.168.1.1/index		😭 🖣 🚼 - Google	Ρ 💀 - 🔝
FortiGate - FGT60B3907504775	*			*
FortiGate 60B	9-1		Help Logout	F
System		New Policy	1	
Router	Source Interface/Zone wa	n1(Evternal)		
Firewall	Available User Groups:	Edit Authentication Selected User G	n Rule roups:	
<ul> <li>Policy</li> <li>Policy</li> <li>Central NAT Table</li> <li>DoS Policy</li> <li>Sniffer Policy</li> <li>Protocol Options</li> <li>Address</li> <li>Service</li> <li>Schedule</li> <li>Traffic Shaper</li> <li>Virtual IP</li> <li>Load Balance</li> </ul>	Service Available Services: GOPHER GRE H323 HTTP HTTPS ICMP_ANY IKE IMAP INFO_ADDRESS INFO_REQUEST	Selected Service	s: 	Move Up Move Down
Endpoint		ОК	Cancel	
Wireless Controller				
Log&Report				
Done				4

The configuration will look similar to the one below :

🥹 FortiGate - FGT60B3907504775 - Mozilla	a Firefox						
<u>File Edit View History Bookmarks T</u>	ools <u>H</u> elp						
C X 🟠 🗋 http://192.	168.1.1/index		☆ - Google	₽ 💩 - 🔝			
FortiGate - FGT60B3907504775	+			-			
FortiGate 60B			Image: Weight of the second	BTINET			
System		Edit Policy					
Router	Source Interface/Zone	wan1(External)	Ŧ				
Firewall	Source Address	all	▼ III Multiple				
Policy	Destination Interface/Zone	internal	Ŧ				
Policy	Destination Address	all	▼ I Multiple				
Central NAT Table     DoS Policy	Action	SSL-VPN	•				
Sniffer Policy	SEL Client Catificate Pactrictive						
Protocol Options	Cipher Strength						
Address							
	Configure SSL-VPN Users						
🗉 🗐 Traffic Shaper	Display Implicit Policies						
🗉 🏫 Virtual IP		Add					
⊕ 🌐 Load Balance	Rule ID User Group Service Schedule UTM Logging						
	1 SSLVPN_USERS A	NY always 😣 😢 💼 🌌 🚔					
UTM	Comments (maximum 63 cha	aracters)					
VPN							
User							
Endpoint							
Wireless Controller		ОК	Cancel				
Log&Report							
Done							

The Firewall Policy will be as follows :

🕘 FortiGate - FGT60B3907504775 - Mozil	lla Firefox						
<u>File Edit View History B</u> ookmarks	<u>T</u> ools <u>H</u> elp						
🔄 🕑 📲 😋 🗶 🏠 🗋 http://192	2.168.1.1/index				🟠 🔹 🚼 🛛 Goo	gle	P 🐵 🔹 🔝
FortiGate - FGT60B3907504775	4					-	-
FortiGate 60B	1	-			Image: Weight of the second	FCR	INET
System	🔾 Create New 👻	📝 Edit 👻 📋 D	elete 🛛 🖗 Move To	🖅 Insert	[ Column Setting	s] 🔍 Section View	O Global View
Router	I ID	V Source	T Destination	▼ Schedule	Service	Action	▼ Status
Firewall	wan1(External	) -> internal (1)					
Policy	16	• <u>all</u>	• <u>all</u>	always	ANY	SSL-VPN	
- • Policy	Implicit (1)						
- • Central NAT Table							
- • DoS Policy							
- Sniffer Policy							
- • Protocol Options							
Address							
B G Schodulo							
Traffic Shaper							
Wirtual IP							
B 🚯 Load Balance							
UTM							
VPN							
User							
Endpoint							
Wireless Controller							
Log&Report							

# **Testing with CRYPTO-MAS Server**

Everything is now in place to test. An email should have been received from <u>mas@cryptocard.com</u> with a user's software token. Import this into the software token client (downloaded from <u>http://www.cryptocard.com/support/endusersoftware/</u>) and follow the instructions to generate a One Time Password (OTP).

The quickest way to test authentication is via the FortiGate CLI. There are many ways to access the CLI; the easiest is from the Management GUI:

Login to the FortiGate:

- 5 If not already at the Dashboard, browse to System-> Dashboard
- 6 Scroll down to the CLI Console Window and click on it to connect
- 7 In the CLI type: diag test auth rad <RADIUS Server Name> <auth protocol> <username> <password>

Note: Using the example configuration provided, the command will be :

## diag test auth rad CRYPTO-MAS pap testuser <password>

Authentication successful:

OLI Console (connected) - Mozilla Firefox	- C X
http://192.168.1.1/system/jsconsole	☆
Connected	
FGT60B3907504775 # diag test auth rad CRYPTO-MAS pap testuser authenticate 'testuser' against 'pap succeeded, server=primary assign	ed_rad_ses:
FGT60B3907504775 #	
Customize Attach	4
Done	