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

UNIFIED THREAT MANAGEMENT SOLUTIONS

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

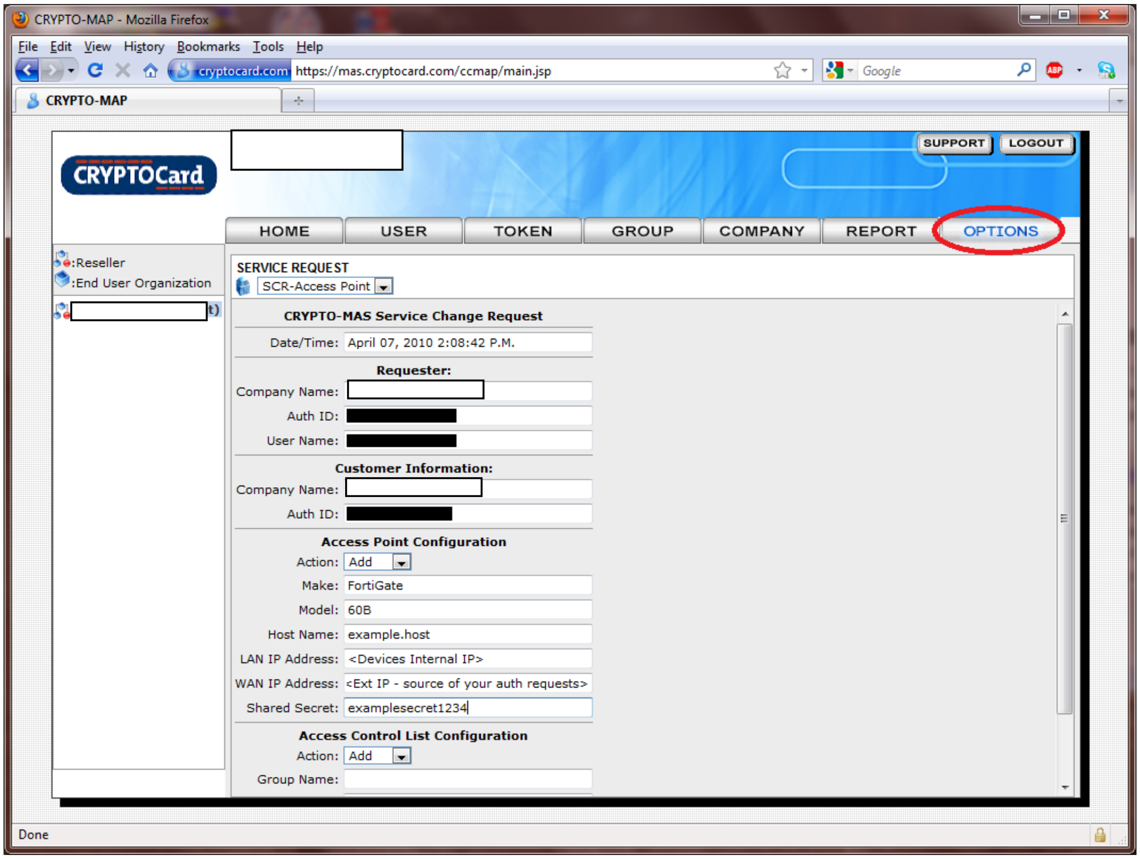
2 In the *Service Request* drop down box select *SCR-Access Point*

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.



SERVICE REQUEST

SCR-Access Point

CRYPTO-MAS Service Change Request

Date/Time: April 07, 2010 2:08:42 P.M.

Requester:

Company Name: [redacted]

Auth ID: [redacted]

User Name: [redacted]

Customer Information:

Company Name: [redacted]

Auth ID: [redacted]

Access Point Configuration

Action: Add

Make: FortiGate

Model: 60B

Host Name: example.host

LAN IP Address: <Devices Internal IP>

WAN IP Address: <Ext IP - source of your auth requests>

Shared Secret: examplesecret1234

Access Control List Configuration

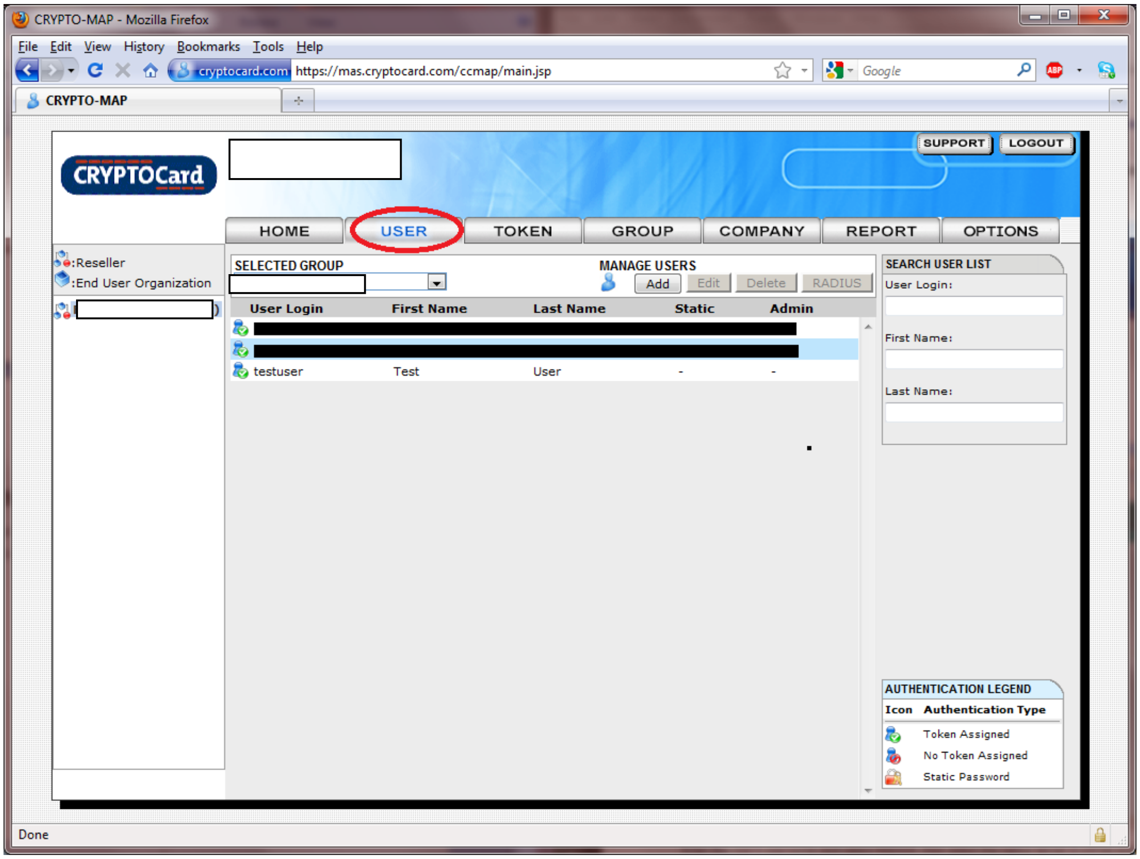
Action: Add

Group Name:

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



https://mas.cryptocard.com/ccmap/main.jsp

User Login	First Name	Last Name	Static	Admin
[redacted]				
[redacted]				
testuser	Test	User	-	-

User Login:

First Name:

Last Name:

AUTHENTICATION LEGEND

Icon	Authentication Type
	Token Assigned
	No Token Assigned
	Static Password

Configuring the FortiGate

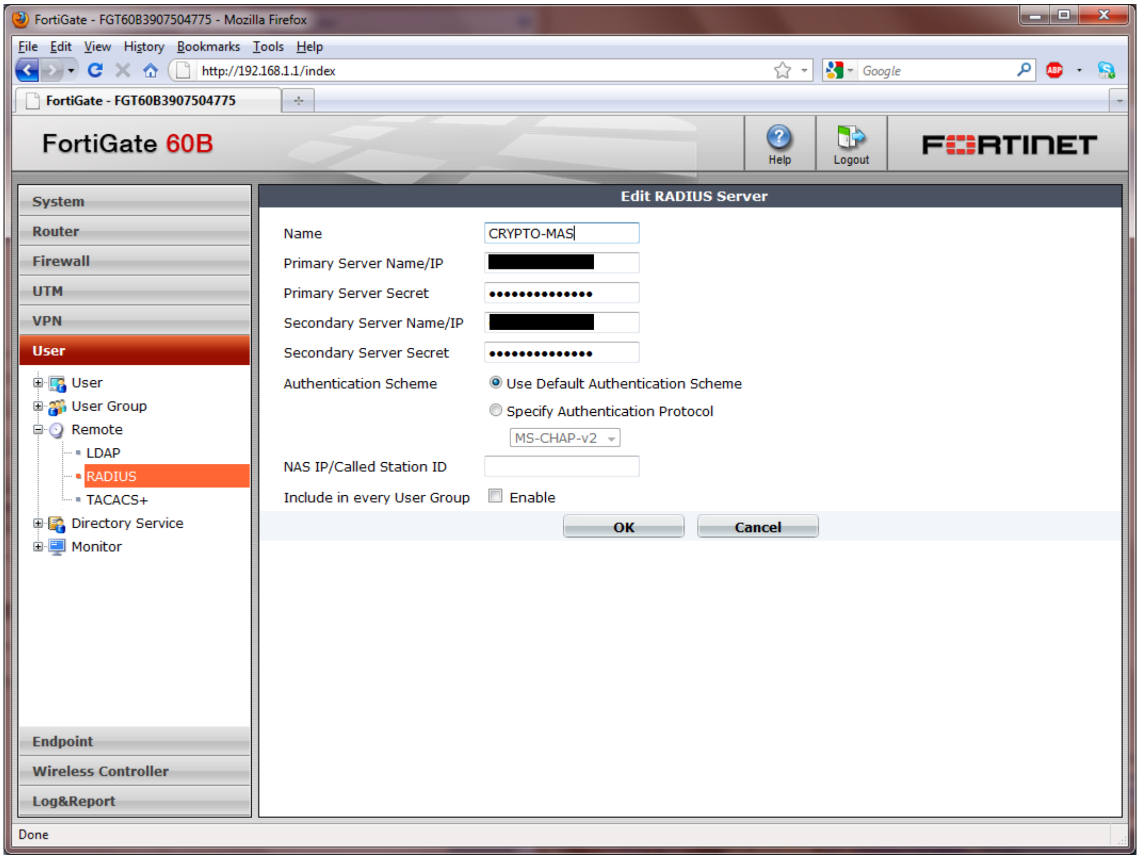
Login to the FortiGate:

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*



Edit RADIUS Server

Name	CRYPTO-MAS
Primary Server Name/IP	[redacted]
Primary Server Secret	••••••••••••••
Secondary Server Name/IP	[redacted]
Secondary Server Secret	••••••••••••••
Authentication Scheme	● Use Default Authentication Scheme ○ Specify Authentication Protocol MS-CHAP-v2
NAS IP/Called Station ID	
Include in every User Group	□ Enable

OK Cancel

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:

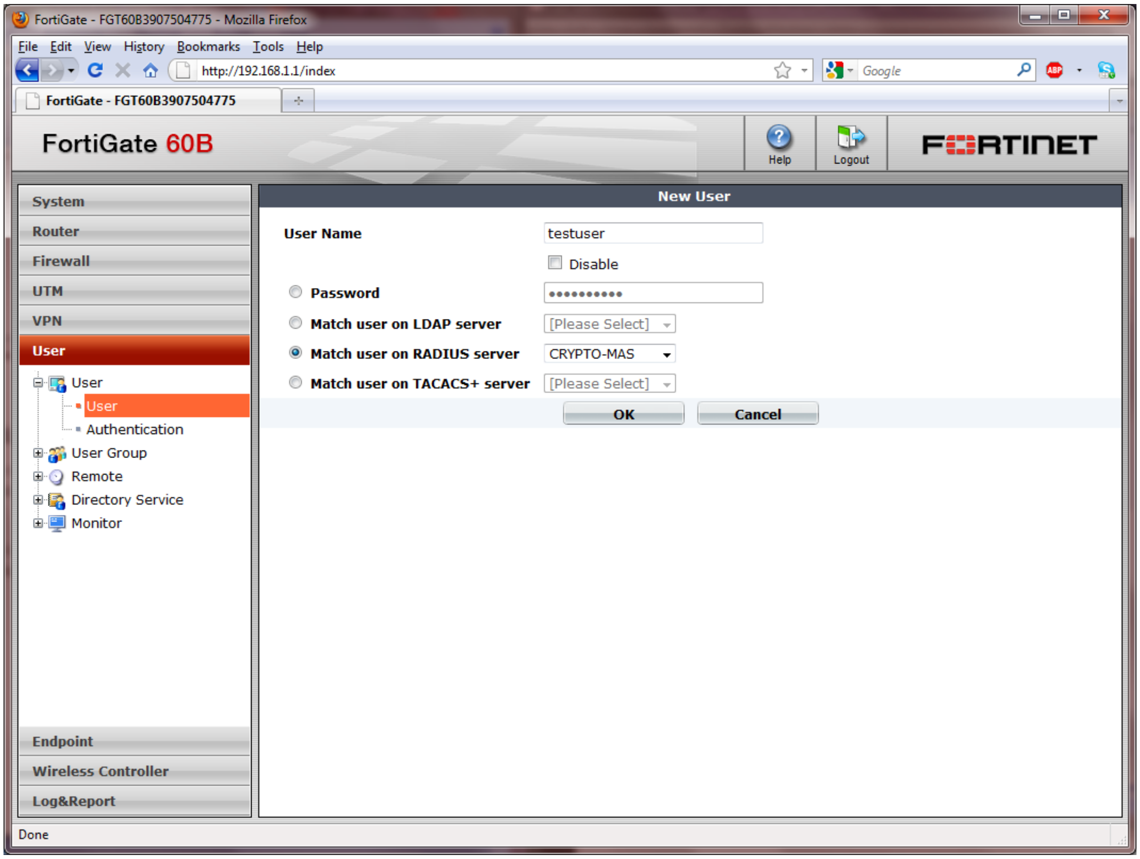
1 Go to *User-> User-> User*

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 - Mozilla Firefox

http://192.168.1.1/index

New User

User Name: testuser

□ Disable

○ Password: ••••••••••

○ Match user on LDAP server: [Please Select]

● Match user on RADIUS server: CRYPTO-MAS

○ Match user on TACACS+ server: [Please Select]

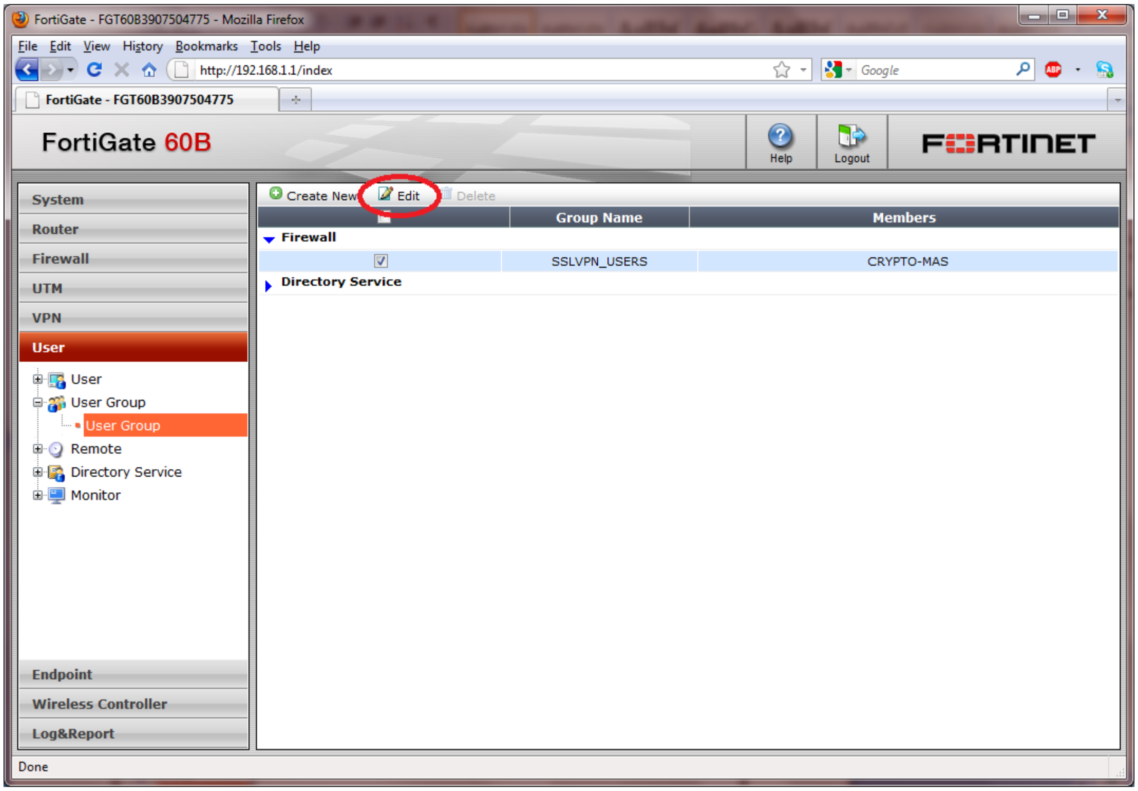
Next add this user (testuser) to a group that will be associated with SSL VPN Access. Either create a new group or use the existing “SSLVPN_USERS” group. The steps below are based on using the existing.

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



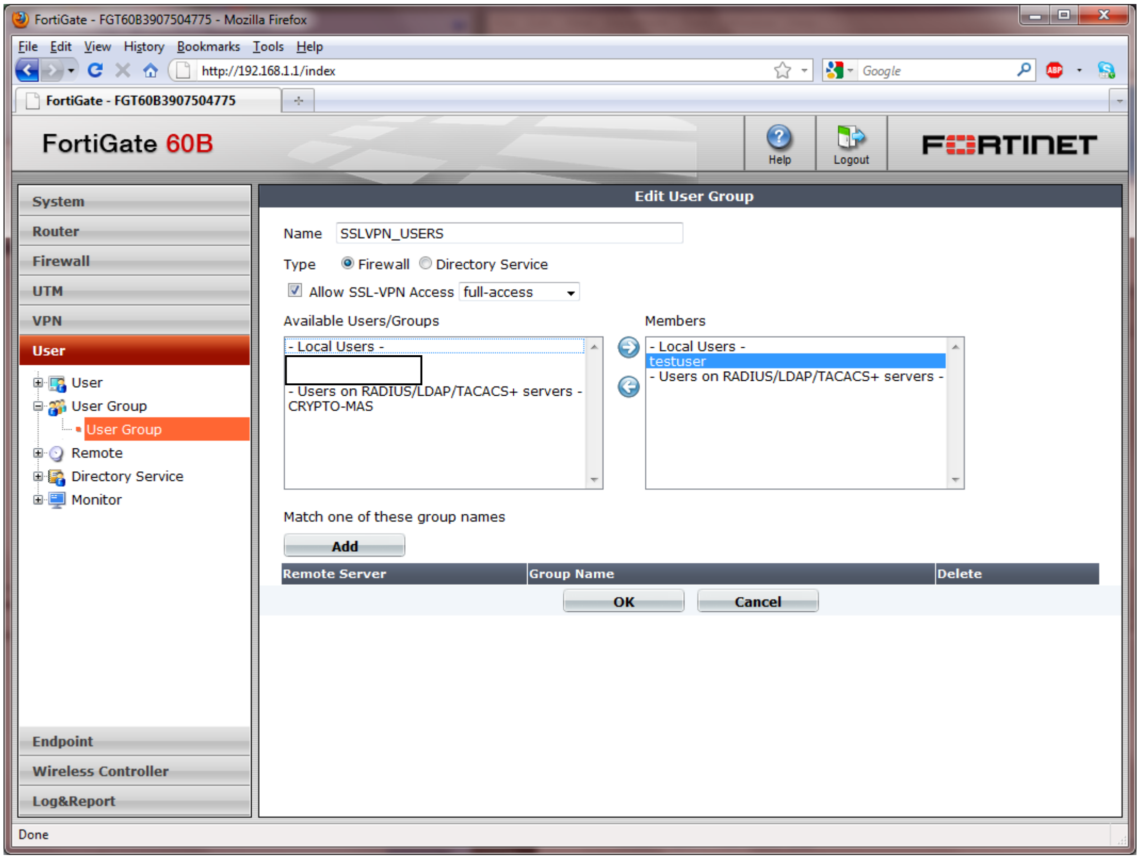
	Group Name	Members
Firewall		
☑	SSLVPN_USERS	CRYPTO-MAS
Directory Service		

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



Edit User Group

Name SSLVPN_USERS

Type ● Firewall ○ Directory Service

☑ Allow SSL-VPN Access full-access

Available Users/Groups
- Local Users -
- Users on RADIUS/LDAP/TACACS+ servers -
CRYPTO-MAS

Members
- Local Users -
testuser
- Users on RADIUS/LDAP/TACACS+ servers -

Match one of these group names

Remote Server	Group Name	Delete

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

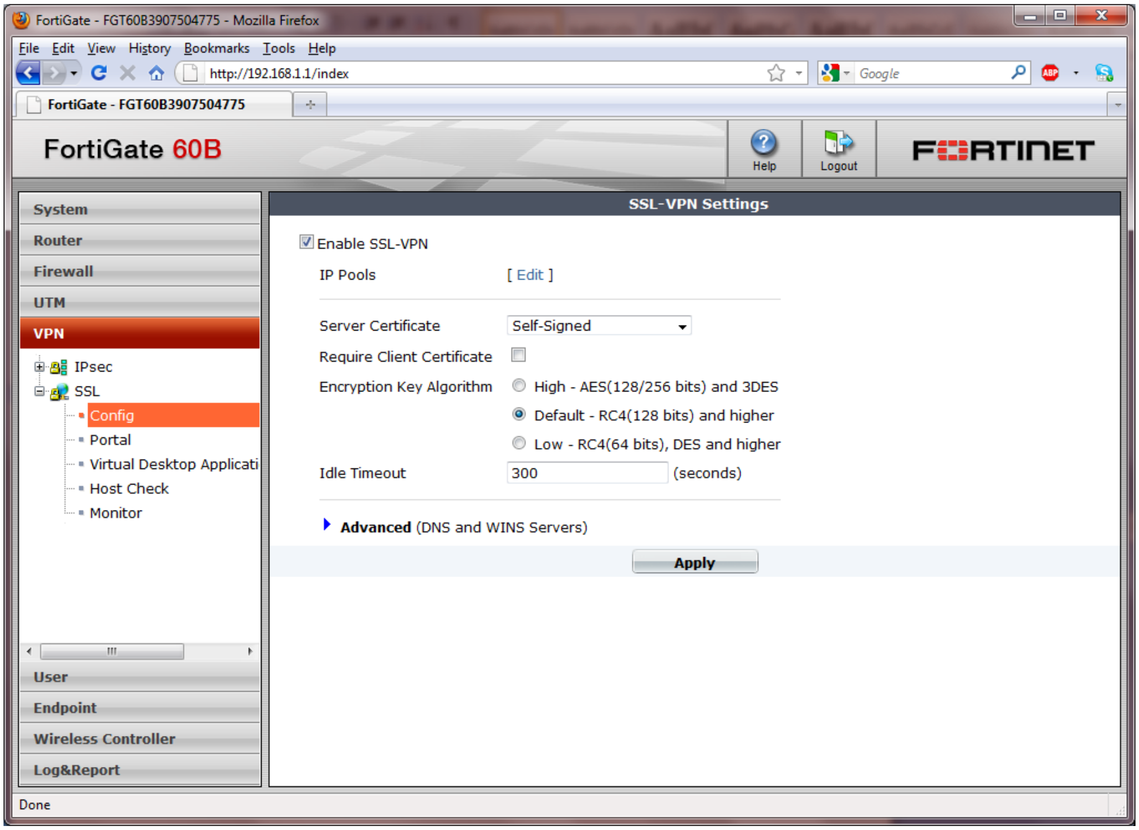
Configuration settings as follows:

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*



SSL-VPN Settings

☑ Enable SSL-VPN

IP Pools [Edit]

Server Certificate: Self-Signed

Require Client Certificate: □

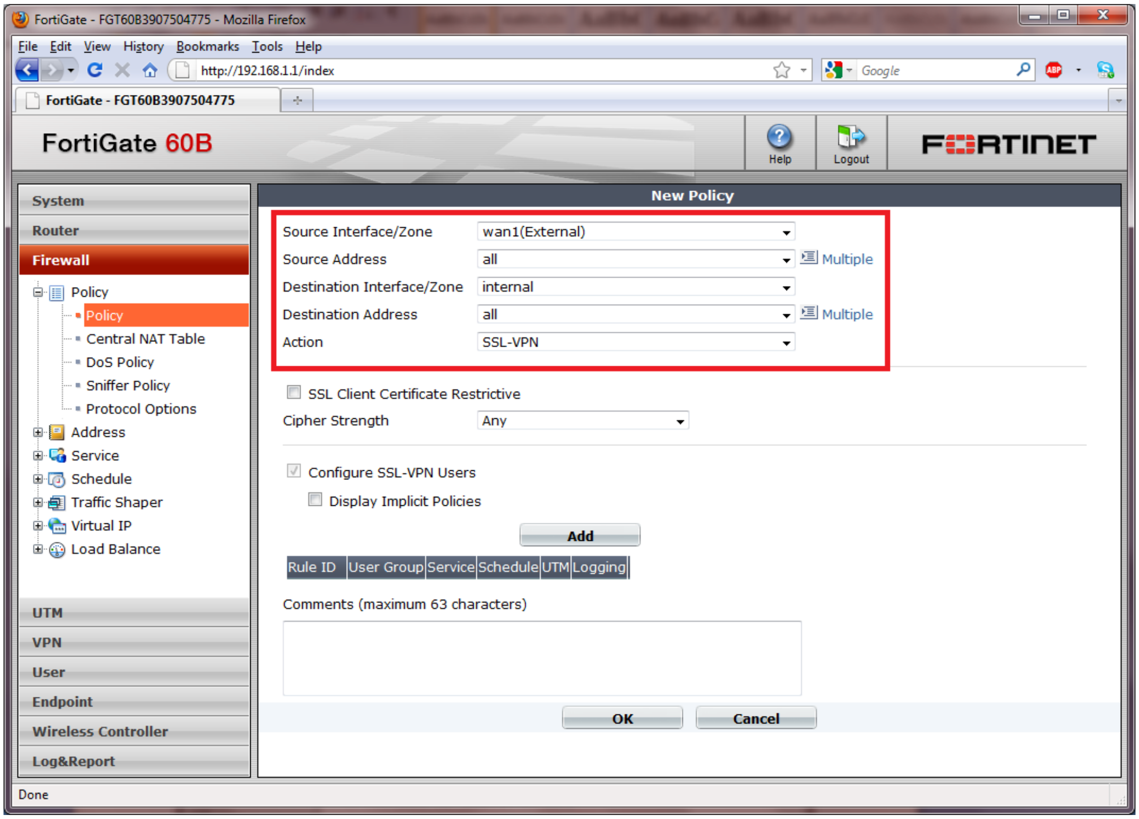
Encryption Key Algorithm:
○ High - AES(128/256 bits) and 3DES
● Default - RC4(128 bits) and higher
○ Low - RC4(64 bits), DES and higher

Idle Timeout: 300 (seconds)

Configuring Firewall Policy to Allow SSL Access

1 Go to *Firewall-> Policy-> Policy*

2 Click *Create New*



New Policy

Source Interface/Zone	wan1(External)
Source Address	all
Destination Interface/Zone	internal
Destination Address	all
Action	SSL-VPN

☐ SSL Client Certificate Restrictive

Cipher Strength: Any

☑ Configure SSL-VPN Users

☐ Display Implicit Policies

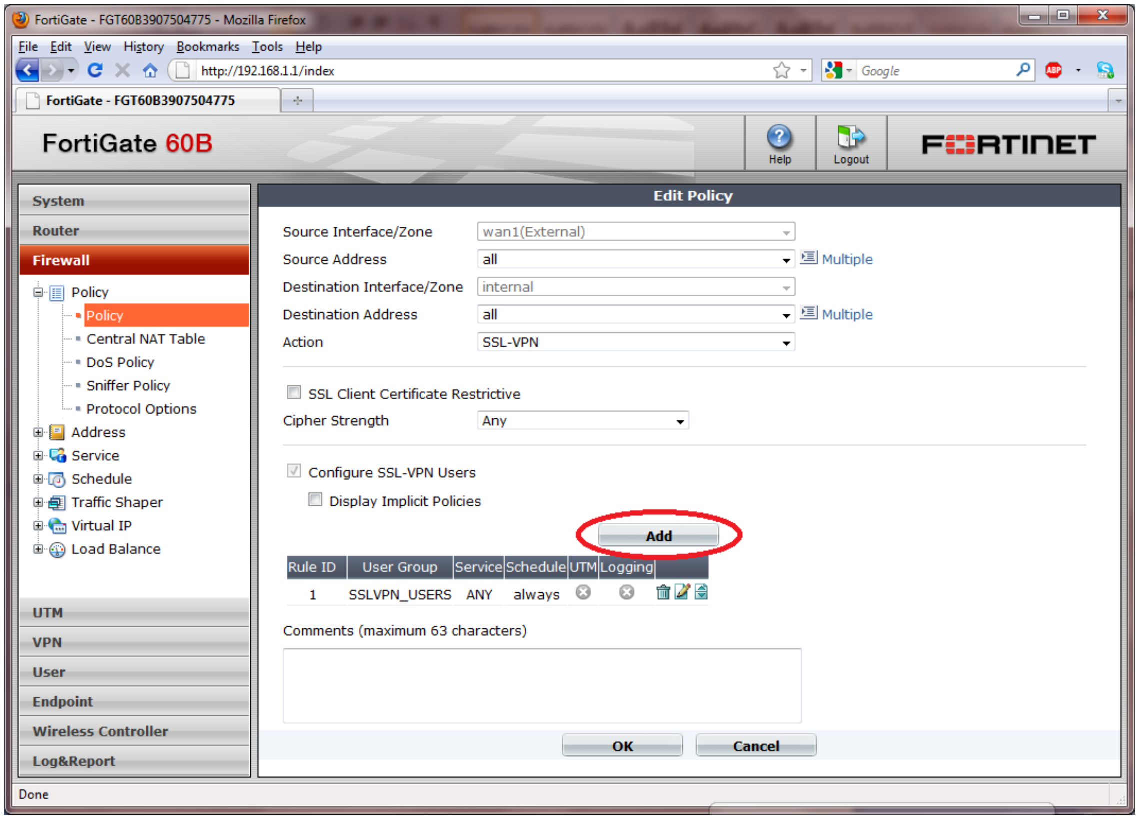
Rule ID	User Group	Service	Schedule	UTM	Logging

Comments (maximum 63 characters)

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”:



Edit Policy

Source Interface/Zone: wan1(External)
Source Address: all
Destination Interface/Zone: internal
Destination Address: all
Action: SSL-VPN

☐ SSL Client Certificate Restrictive
Cipher Strength: Any

☑ Configure SSL-VPN Users
☐ Display Implicit Policies

Rule ID	User Group	Service	Schedule	UTM	Logging
1	SSLVPN_USERS	ANY	always	⊗	⊗

Comments (maximum 63 characters)

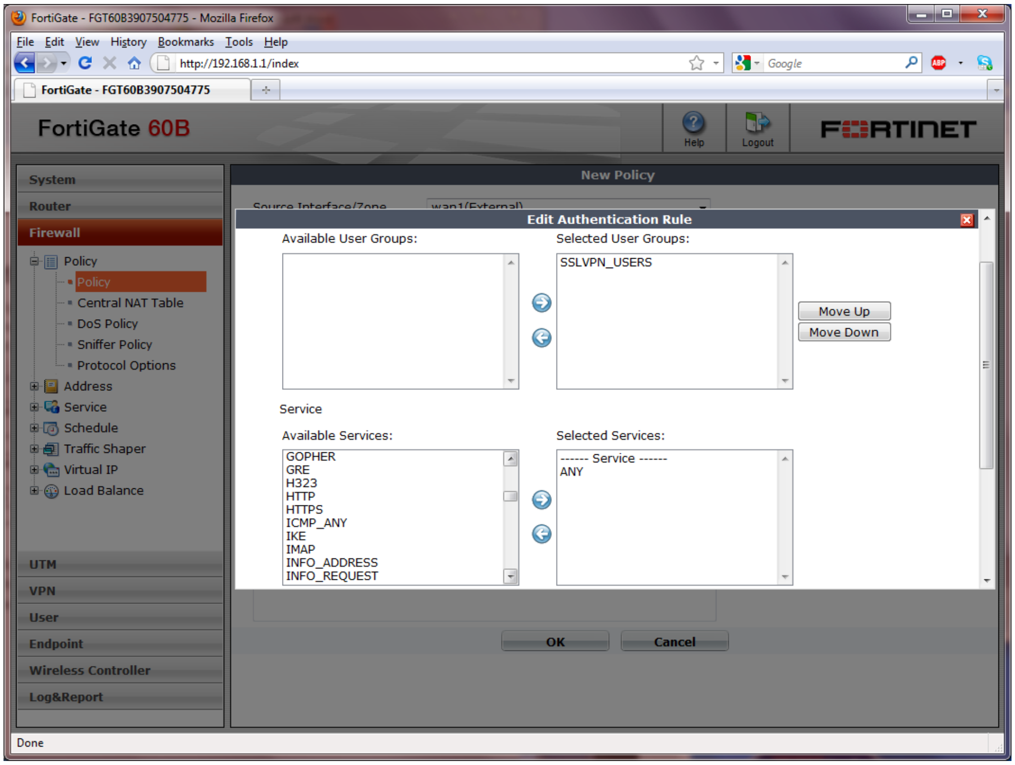
4 Click *add* (the window below appears)

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



Edit Authentication Rule

Available User Groups:

Selected User Groups: SSLVPN_USERS

Service

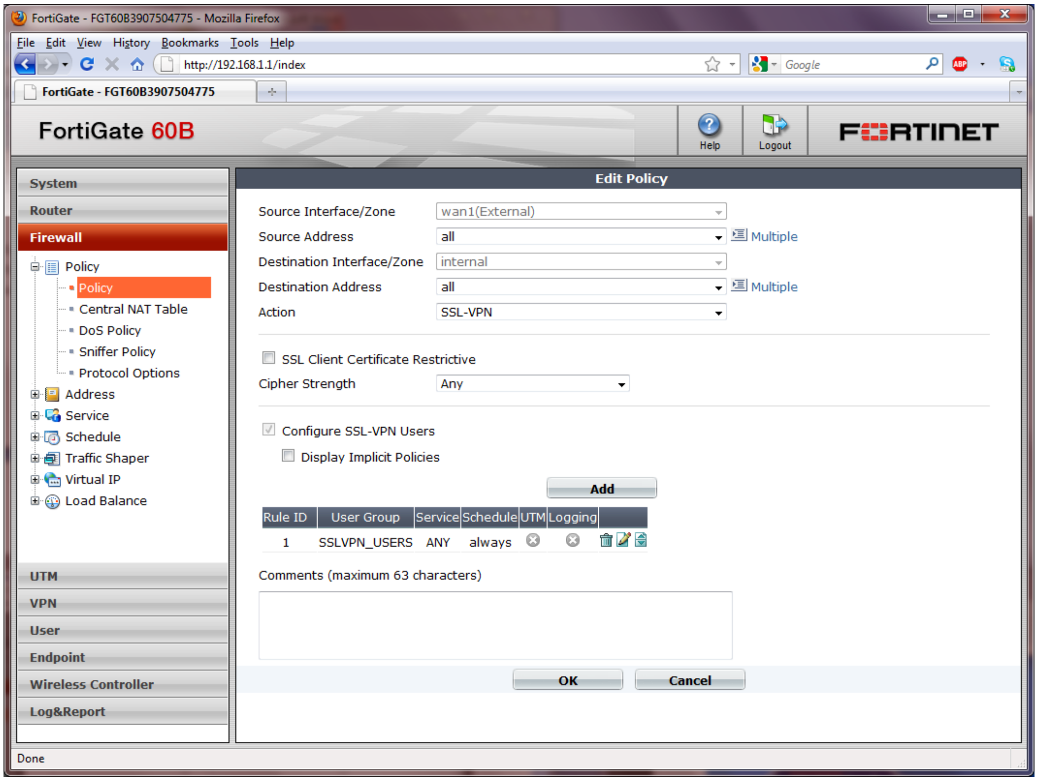
Available Services:

GOPHER
GRE
H323
HTTP
HTTPS
ICMP_ANY
IKE
IMAP
INFO_ADDRESS
INFO_REQUEST

Selected Services:

------ Service ------
ANY

The configuration will look similar to the one below :



Edit Policy

Source Interface/Zone	wan1(External)
Source Address	all
Destination Interface/Zone	internal
Destination Address	all
Action	SSL-VPN

□ SSL Client Certificate Restrictive

Cipher Strength: Any

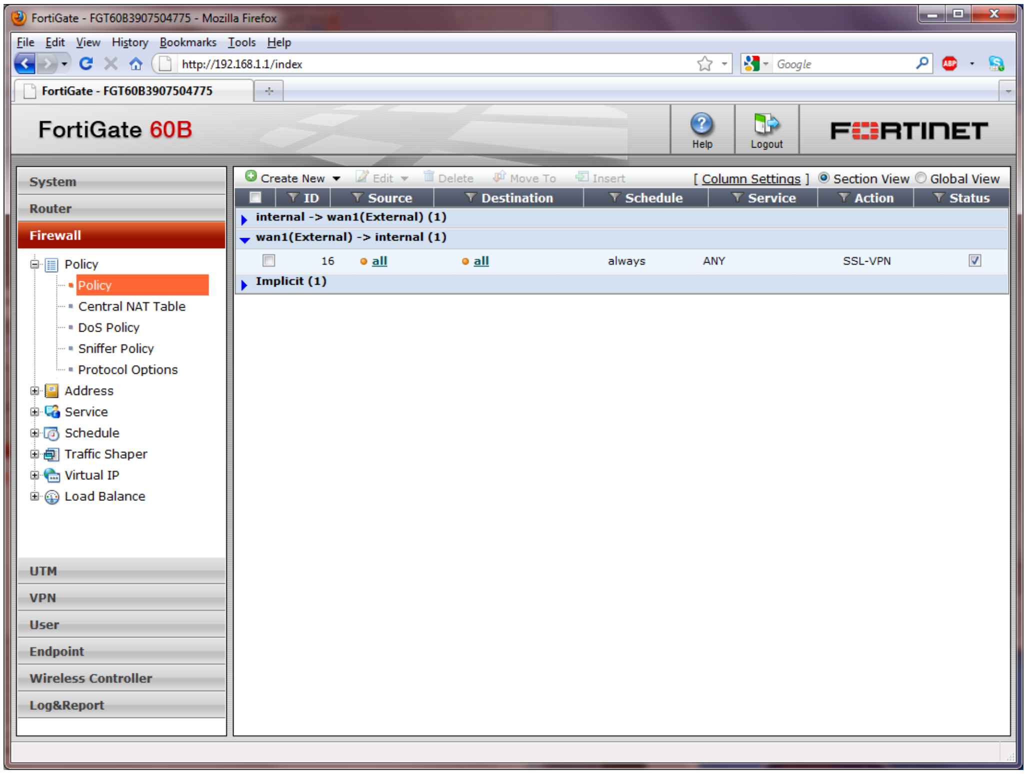
☑ Configure SSL-VPN Users

□ Display Implicit Policies

Rule ID	User Group	Service	Schedule	UTM	Logging	
1	SSLVPN_USERS	ANY	always	☒	☒	

Comments (maximum 63 characters)

The Firewall Policy will be as follows :



□	ID	Source	Destination	Schedule	Service	Action	Status
internal -> wan1(External) (1)							
wan1(External) -> internal (1)							
□	16	all	all	always	ANY	SSL-VPN	☑
Implicit (1)							

Testing with CRYPTO-MAS Server

Everything is now in place to test. An email should have been received from mas@cryptocard.com with a user's software token. Import this into the software token client (downloaded from http://www.cryptocard.com/support/endusersoftware/) 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*

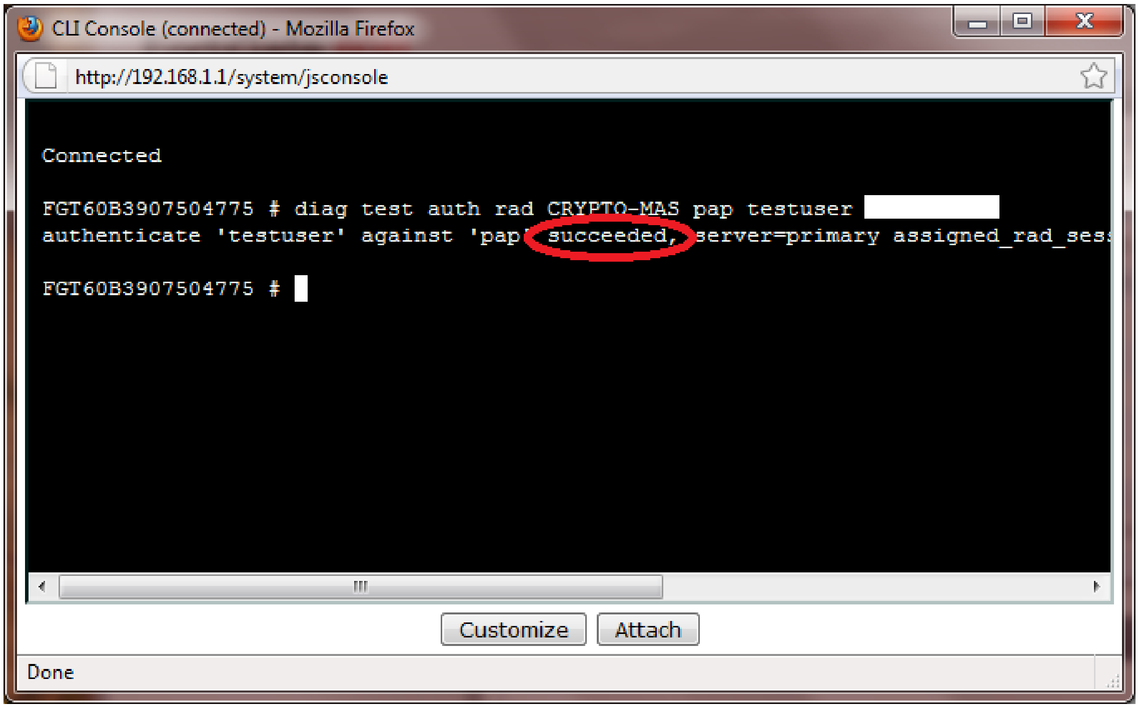
6 Scroll down to the CLI Console Window and click on it to connect

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:


CLI Console (connected) - Mozilla Firefox
http://192.168.1.1/system/jsconsole
Customize
Attach
Done

```
Connected

FGT60B3907504775 # diag test auth rad CRYPTO-MAS pap testuser [redacted]
authenticate 'testuser' against 'pap' succeeded, server=primary assigned_rad_ses

FGT60B3907504775 #
```