Configuring FortiGate 200B with RSA SecurID for Two Factor Authentication

Copyright © 2011 – BPS Info Solutions, Inc. Written by Jonathan Tew

Introduction

Our company had an existing RSA installation and wanted to leverage this investment with new FortiGate appliances. The installation was not as easy as we had anticipated even though both vendors hold leadership positions in their respective industries. The available documentation did not cover the actual scenario of true two factor authentication. We were able to determine the proper configuration and it is relatively straight forward. We wanted to document the configuration to improve what is available to the internet community.

Assumptions

This documentation assumes the following components are in place:

- Fortinet 200B Appliance with version 4.0 MR2 Patch 6
- RSA SecurID 130 Appliance

We also assume that you have experience creating your own certificate authority and generating a certificate for the appliance and end users.

Please note that any sensitive information is blurred out. It's a faint blur, so examine the images carefully to note that certain fields are filled in, but blurred.

Configuring the RSA SecurID

First go to the IMS Console for SecurID and login

C	•)•	
	RS	Security Console
[⇒	Log On
		Log on is required. If you have forgotten your logon information, contact your help desk or administrator.
		User ID:
	l	ок >

Next go to RADIUS -> RADIUS Clients -> Manage Existing.

Realm: SystemDomain RADIUS Clients Manage Existing relcome You logged on: Friday, May 6, 2011 9:26 RADIUS Profiles Add New Y Console RADIUS User Attribute Definitions * ADIUS Statistics *	Addrenacadori Access Reporting	RADIUS Servers	
elcome You logged on: Friday, May 6, 2011 9:26 RADIUS Profiles Add New Manage Exi y Console RADIUS User Attribute Definitions * RADIUS Statistics *	Realm: SystemDomain	RADIUS Clients	Manage Existing
y Console RADIUS User Attribute Definitions RADIUS Statistics Image: Console Co	Velcome You logged on: Friday, May 6, 2011 9:2	6 RADIUS Profiles	Add New Manage Exist
RADIUS Statistics	Av Console	RADIUS User Attribute Definitions	;)
My Permissions	,	RADIUS Statistics	•
	My Permissions		

Since I've already configured my FORTIGATE RADIUS client you will see it in the screen shot below. If you are performing a new configuration then click on the "Add New" button.

RSA Security Console Home Identity ▼ Authentication ▼ Access ▼ Reporting ▼ RADIUS ▼ Administration	▼ Setup ▼ Help ▼					
RADIUS Clients Add New >						
RADIUS client passes user entered authentication information to the designated RADIUS server.	RADIUS client passes user entered authentication information to the designated RADIUS server.					
2 found. Showing 1-2.						
Show 25 👻 per page						
Client Name	IP Address					
(†) FORTIGATE 🗸						
Client Name	IP Address					
Show 25 👻 per page						
2 found. Showing 1-2.						
	Copyright @					

The configuration is really simple. Just make sure the IP address matches the internal management IP address of the FortiGate unit.

RSA Security Console						
Home Identity Authentication Access Reporting RADIUS Administration Setup Help Help						
RADIUS Client: FORTIGATE						
Edit						
RADIUS Client RSA Agent						
Edit properties of RADIUS Clients.						
Cancel X Reset 5 Save 5						
* Required field						
RADIUS Client Basics						
Client Name: * FORTIGATE						
Associated RSA Agent: FORTIGATE						
RADIUS Client Settings						
IP Address:						
i Make / Model: * - Standard Radius - ←						
i Shared Secret: * ••••••						
Accounting: Use different shared secret for Accounting						
Client Status: Assume down if no keepalive packets are sent in the specified inactivity time.						
Notes:						
b.						
Cancel 🗙 Reset 5 Save >						

FortiGate Configuration RADIUS Configuration

The next step is configuring the FortiGate RADIUS user. Begin by navigating to User \rightarrow Remote \rightarrow RADIUS. Here you will see I have a Remote user named "RSA" configured.



Notice that the configuration of the RSA user is relatively simple. I have the Primary and Secondary IP address (blurred out) configured for the RSA SecurID 130 appliances.

• • • • • • • • • • • • • • • • • • •		🚖 - 🕑 🚼 - Goog	le 👂 🍙 💽
FortiGate 200B	5	Help Logout	F
System		Edit RADIUS Serve	۲
Router	Name	RSA	
Firewall	Primary Server Name/IP		
UTM	Primary Server Secret	•••••	
VPN	Secondary Server Name/IP		
User	Secondary Server Secret		
User User Authentication	Authentication Scheme	 Use Default Authentia Specify Authentication MS-CHAP-v2 	cation Scheme In Protocol
User Group	NAS IP/Called Station ID		
E- O Remote	Include in every User Group	Enable	
- RADIUS		OK Can	cel
TACACS+			

Next we need to create an actual user under User \rightarrow User \rightarrow User in the left hand navigation. Notice that I've created a single user with the type of RADIUS below.

•		🟫 🛛 😋 🚼 🗸 Google	P 🏦 📴 🐖 •
FortiGate 200B	- A	Help Logout	FCRTINET
System	Create New 🖉 Edit	Delete	
Pouter		User Name	Туре
			RADIUS
Firewall			
UTM			
VPN			
User			
🖶 🛐 User			
• User			
 Authentication 			
🖃 碋 User Group			
User Group			

Notice that the user is simple to configure. I've provided the username (which needs to match the user on the RSA box) and selected Match user on RADIUS server and selected RSA. This means that when the user tries to connect the authentication credentials are sent over to the RSA server for validation.

↔	☆ -	- C 🛃 - Google 👂 🍙 💽 🕐 -
FortiGate 200B	H	
System		Edit User
Router	User Name	
Firewall		Disable
UTM	Password	•••••
VPN	Match user on LDAP server	[Please Select] 👻
User	Match user on RADIUS server	RSA 🔻
🖶 🌇 User	Match user on TACACS+ server	r [Please Select] 👻
• User	ОК	Cancel
Ser Group		

At this point we have a user that is doing OTP authentication with the RSA SecurID appliance. I learned how to test this authentication with the RSA box on the command line from a CryptoCard FortiGate implementation guide. *Thanks CryptoCard for the excellent documentation*! So if we open up the CLI console and type in the following command:

```
diag test auth rad <radius server name><auth protocol><username><One-Time Password>
```

We should see it successfully authenticate.

CLI Console (connected) - Mozilla Firefox
Connected
fg_ha_1
fg_ha_1 #
Customize Attach

At this point though we have only achieved a single factor of authentication (the one time password from the RSA token). We need to have two factors of authentication.

Configuring Certificate Authentication

For this exercise you are going to need the following certificates:

• Your own certificate authority root certificate

- A private key and certificate for the FortiGate appliance that matches the host name that you are going to access the appliance with.
- A client certificate for your windows machine.

The actual generation of these certificates is out of the scope of this documentation. There are tons of great documents about how to accomplish this task with either Windows Server 2008 or OpenSSL.

The first step is to import the certificate authority root into the System -> Certificates -> CA Certificates. Click on the Import button and upload the certificate. After the certificate is imported the screen will look like the picture below:

€ → □			☆ マ C 🎦 Google 👂 🏫 💽 🦗 •
FortiGate 200B	4	54	
System	D D	elete 🖉 Import	🕄 View Certificate Detail 🛛 🚵 Download
		Name	Subject
E- 🕑 Dashboard		CA_Cert_1	C = US,
- • Usage		Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = support, emailAddress = support@fortinet.com
🕀 💭 Network		Fortinet_CA2	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = Fortinet 2nd Root Certificate, emailAddress = support@fortinet.com
DHCP Server			
Config			
🕀 🔛 Admin			
Certificates			
- • Local Certificates			
• Remote			
CA Certificates			
- • CRL			
🗴 🗄 🌼 Maintenance			

Notice the CA_Cert_1 has been added to the list. Next click on System -> Certificates -> Local Certificates -> Import within the FortiGate left navigation. On that screen choose the type "Certificate" from the drop down list. This will allow you to upload both the certificate and private key file into the FortiGate appliance. You'll need the private key password which should be provided to you by whoever within your organization generated the key pair.

				😭 🗝 🥙 🚼 🗝 Google
FortiGate 200B	9			e constante de la constante de
System				Import Certificate
 S Dashboard Dashboard Usage Metwork DHCP Server 	Type Certificate file Key file Password	Certificate	•	Browse
Config Gertificates Certificates Certificates Certificates				OK Cancel

After the certificate is imported it will display in the list underneath all the factory installed FortiGate certificates.

♦ □			습 - C 🚼 - Google	۹ 🝙 💽	
FortiGate 200B			Image: Weight of the second	FCRTINE	ЕТ
System	🗊 Delete 📑 Generat	e 📲 Import 🔍 View Certificate Detail	🛁 🣥 Download 🛛 🖉 Edit Con	nments	
	Name Name	Subject	Comm	ents	Status
Dashboard Dashboard Usage	Fortinet_CA_SSLProxy	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FortiGate CA, emailAddress = support@fortinet.com	This certificate is embedded in on every unit (not unique). Thi the SSL Inspection will use w certific	the firmware and is the same s is the default CA certificate hen generating new server ates.	ок
🖲 📜 Network 🗷 🕶 DHCP Server 🗷 📇 Config	Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FG200B3911600242, emailAddress = support@fortinet.com	This certificate is embedded in and is unique to this unit. It has	the hardware at the factory been signed by a proper CA.	A Control
Admin Gertificates	Fortinet_Factory2	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FG200B3911600242, emailAddress = support@fortinet.com	This certificate is embedded in and is unique to this unit. It has	the hardware at the factory been signed by a proper CA.	ок
- = Remote - = CA Certificates - = CRL	Fortinet_Firmware	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortigate, CN = Fortigate, emailAddress = support@fortinet.com	This certificate is embedded in on every unit (not unique). It CA. It is not recommended functionality since any other certificate to spoof the	the firmware and is the same has been signed by a proper to use it for server type of r unit could use this same identity of this unit.	ок
🕀 😳 Maintenance	FG	And the second second			ок

VPN Configuration

Now that we have the RSA authenticating user configured and the certificates installed on the server we need to configure the VPN. First we need to configure our VPN to use our server certificate and require a client certificate. This is configured under VPN \rightarrow SSL \rightarrow Config. The required Client Certificate is what will provide us the second factory of authentication. The client certificate will have to be signed by our internal certificate authority that we imported in the prior steps of this documentation.

FortiGate 200B	J.			2 Help	Logout
System			SSL-VPN Setti	ngs	
Router	Enable SSL-VPN				
<u>Firewall</u>	IP Pools	ManagementVPN [[Edit]		
UTM VPN	Server Certificate		×		
B BE IPsec	Require Client Certificate				
Auto Key (IKE)	Encryption Key Algorithm	High - AES(128)	/256 bits) and 3DE	ES	
- Manual Key		Default - RC4(1	28 bits) and highe	r	
Concentrator		Low - RC4(64 b	its), DES and high	er	
- Monitor	Idle Timeout	300	(seconds)		
Config	Advanced (DNS and V	/INS Servers)			
 Virtual Desktop Applicati Host Check 	c		Apply		

Next configure the VPN portal under VPN \rightarrow SSL \rightarrow Portal. In this case we configured "portal1"

FortiGate 200B	J.L	Image: Weight of the second
System	🖸 Create New 📝 Edit 📋 Delete	
Router		Name
		full-access
Firewall		portal1
UTM		
VPN		
E BE IPsec		
- Auto Key (IKE)		
Manual Key		
- Concentrator		
Monitor		
SSL		
- Config		
Portal		

Finally we need to configure a user group that includes our user and grants them access to the VPN portal. This configuration is done under User -> User Group -> User Group.

FortiGate 200B	1		Image: Weight Heip Image:
System	Create New 🖉 Edit 📋 De	Group Name	Members
Router	▼ Firewall		
Firewall		group1	
UTM	Directory Service		
VPN			
User			
User User Authentication User Group User Group			

Notice we have a group "group1" configured with our single user over in the members section.

FortiGate 200B	Image: Constraint of the second sec	F
System	Edit User Group	
Router	Name group1	
Firewall	Type	
UTM	✓ Allow SSL-VPN Access portal1	
VPN	Available Users Members	
User User - User - Authentication User Group - User Group - LDAP	- Local Users -	*
RADIUS		
Directory Service Monitor	Remote Server Group Name OK Cancel	Delete

Testing VPN Connection

Before fighting with the FortiClient VPN users you should do the following:

- 1) Make sure your OTP token is working properly by RSA SecurID by testing it through their selfservice console.
- 2) Test the OTP token on the FortiGate CLI using the diag command shown above.
- 3) See if you can properly connect to the web interface of the FortiGate at Error! Hyperlink reference not valid. Please note that your browser should prompt for your client side certificate AND the server should present the CA signed server certificate. Try logging in through the web interface first. It is more tolerant of token syncing, etc.

If we fire up our FortiClient SSL VPN application we can attempt to connect to the FortiGate we should enter our RSA OTP into the password field and select our client certificate. Only client certificates installed into Windows are going to show in the drop down. Make sure you've installed the certificate. Once you connect it should look like this:

FortiClient SSL VPN
Connection Name: fg_ha 📃 💌
Server Address:
Username:
Password:
Client Certificate: [Issued by:
Connection
Status: Connected Bytes Sent: 3,490
Duration: 00:00:04 Bytes Received: 1,077
Settings Connect Disconnect Exit

If something is wrong the FortiClient will stop at a certain percentage and display a negative error code. The error messages provide very little meaningful information. There are some CLI commands that can display meaningful information to help debug what is going on:



It is critical to run the "FortiClient SSL VPN" as administrator to successfully connect. You cannot connect without it running as administrator.

We did not complete a connection via the larger FortiClient software. It spawns a "FortiClient SSL VPN" login window like the standalone client does, but in our trial it did not connect successfully.