



Implementation Guide for protecting

Fortinet Fortigate 60B

with

BlackShield ID



Copyright

Copyright © 2009, CRYPTOCard All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of CRYPTOCard.

Trademarks

BlackShield ID, BlackShield ID SBE and BlackShield ID Pro are either registered trademarks or trademarks of CRYPTOCard Inc. All other trademarks and registered trademarks are the property of their owners.

Additional Information, Assistance, or Comments

CRYPTOCard's technical support specialists can provide assistance when planning and implementing CRYPTOCard in your network. In addition to aiding in the selection of the appropriate authentication products, CRYPTOCard can suggest deployment procedures that provide a smooth, simple transition from existing access control systems and a satisfying experience for network users. We can also help you leverage your existing network equipment and systems to maximize your return on investment.

CRYPTOCard works closely with channel partners to offer worldwide Technical Support services. If you purchased this product through a CRYPTOCard channel partner, please contact your partner directly for support needs.

To contact CRYPTOCard directly:

International Voice: +1-613-599-2441

North America Toll Free: 1-800-307-7042

support@cryptocard.com

For information about obtaining a support contract, see our Support Web page at http://www.cryptocard.com.

Related Documentation

Refer to the Support & Downloads section of the CRYPTOCard website for additional documentation and interoperability guides: <u>http://www.cryptocard.com</u>.

Publication History

Date	Changes	Version
January 26, 2009	Document created	1.0
July 9, 2009	Copyright year updated	1.1



Table of Contents

Overview	1
Applicability	1
Assumptions	2
Operation	2
Preparation and Prerequisites	2
Configuration	3
Adding a RADIUS Server	3
Creating a User	4
Creating a Group	5
Enabling SSL-VPN	6
Creating a Firewall Policy	6
Testing RADIUS Authentication	7
Using the Command Line Interface (CLI)	7
Testing RADIUS Authentication via SSL	8
Troubleshooting	9
Failed Logons	9
Information	9



Overview

By default Fortinet Fortigate VPN logon requests require that a user provide a correct user name and password to successfully logon. This document describes the steps necessary to augment this logon mechanism with strong authentication by adding a requirement to provide a one-time password generated by a CRYPTOCard token using the implementation instructions below.



Applicability

This integration guide is applicable to:

Security Partner Information	
Security Partner	Fortinet
Product Name and Version	Fortigate-60B / 3.00-b5101 (MR5 Patch 2)
Protection Category	SSL Remote Access

CRYPTOCard Server	
Authentication Server	BlackShield ID
Version	Small Business Edition 1.2+
Version	Professional Edition 2.3+



Assumptions

BlackShield ID has been installed and configured and a "Test" user account can be selected in the Assignment Tab.

BlackShield ID NPS IAS Agent has been installed and configured on the NPS IAS Server to accept RADIUS authentication from the Foritnet Fortigate.

Operation

By configuring the Fortinet Fortigate 60B to require two factor authentication, the user will use a one-time password (OTP) in place of their regular static password.

Preparation and Prerequisites

- 1. Verify that a "Test" user account can successfully authenticate via the Fortinet Fortigate
- 2. Ensure that Ports 1812 and 1813 UDP are open to the NPS IAS Server
- 3. The NPS IAS Agent must be configured to use either port 80 or port 443 to send authentication requests to the BlackShield ID server. Ensure that the port to be configured on the Agent is open to the BlackShield ID server.
- 4. Create or define a "Test" account that will be used to verify that the Fortinet Fortigate has been properly installed and configured. Verify that this account can successfully authenticate using a standard password before attempting to apply changes and test authentication using a token. Ensure that the user name for this account exists in BlackShield ID by locating it in the Assignment Tab.



Configuration

Adding a RADIUS Server

- To add a new RADIUS Server, click "User"
- Then click on "RADIUS"
- Then click on "Create New" to add a new RADIUS Server



- Give the new RADIUS Server a "Name"
- Enter in the "Primary Server Hostname/IP"
- Enter in the "Primary Server Secret"
- If there is a Secondary RADIUS Server in the environment, please configure the "Secondary Server Name/IP" and the "Secondary Server Secret". If not, skip this section and click "OK"





Creating a User

Next, a user must be created.

- Under the User section on the left hand side, click "Local"
- Then click "Create New" to create a new user.



 Enter a name for the User

(Note: Ensure that the username entered here match's the username within the BlackShield ID Server)

- Select the "RADIUS" radio button.
- In the dropdown menu, select the RADIUS Server that was just configured.
- Click "OK" when finished

	0B		- 6 6 6
WEB CONFIG			
System	2		
Router		New User	
Firowall	Licer Name	Henry	
ritewaii	User Name	Disable	
VPN	C Password		
✓ User	C LDAR	[Bloase Select]	
Local	G RADIUS	[PlackShield	
RADIUS	(KADIUS	BlackSilleru	
LDAP	o	Cancel	
Windows AD	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		
User Group			
Authentication			
AntiVirus			
Intrusion Protection			
Web Filter			
AntiSpam			
M, P2P & VolP			
Log&Report			



Creating a Group

A Group will now need to be created.

- Under the User section on the left hand side, click
 "User Group"
- Then click "Create New" to create a new group.



- Give a Name for the new Group
- Select SSL VPN in the dropdown menu

s

- Move the RADIUS Server from "Available Users/Groups" to the "Members" Section.
- Expand the "SSL-VPN User Group Options"
- Enable "Enable SSL-VPN Tunnel Service" and "Enable Web Application"
- Also enable the following also:
 - HTTP/HTTPS Proxy
 - Telnet(applet)
 - **VNC**
 - **FTP**
 - SMB/CIFS
 - **RDP**
- Click "OK" when finished





Enabling SSL-VPN

- Next will be to enable the SSL VPN.
- To do this, click on VPN on the left hand side.
- Then click on SSL.
- Enable "Enable SSL-VPN"
- Click Apply all relevant information has been entered.

Rauter SSL-VPN Settings Firewall SE-VPN Settings VPN Enable SSL-VPN Votion Port 10443 rezc Tunnel IP Range 192.168.2.1 removes Server Certificate Self-Signed IM SSL Server Certificate Self-Signed IM Gentratas Require Client Certificate Image: Client Certificate User Encryption Key Algorithm (Pigh) - AES(128/256 bits) and 3DES Group Certificate Image: Client Certificate	Sut-VPN Settings Enable SSL-VPN Login Port Tunnel IP Range Server Certificate Require Client Certificate Encryption Key Algorithm High - AES(128/256 bits) and 3DES C Default - RC4(128 bits) and higher C Low - RC4(64 bits), DES and higher Idia Timopote 200 (Server())	Contraction of the local data		
Firewall Call Fable SSL-VPN VPN Login Port PSC Tunnel IP Range PSTP Server Certificate Server Certificate Self-Signed Centracates Require Client Certificate Ver Encryption Key Algorithm (* High - AES(128/256 bits) and 3DES AntWrigs © Default RC4(128 bits) and higher	Enable SSL-VPN Login Port Tunnel IP Range 192.166.2.1 Server Certificate Server Certificate Server Certificate Encryption Key Algorithm Chigh - AES(128/256 bits) and 3DES Cow - RC4(128 bits) and higher Chow - RC4(64 bits), DES and higher Idea	Router	SSL-VPN Settings	
VPN IO443 resc Tunnel IP Range 192.168.2.1 PPP Server Certificate Self-Signed Seture Certificate Self-Signed Ver High - AES(128/256 bits) and 3DES Genductor © Default RC4(128 bits) and higher	Server Certificate Self-Signed Require Client Certificate Self-Signed Comparison Server Certificate Require Client Certificate Self-Signed Comparison High - AES(128/256 bits) and 30ES Comparison Default - RC4(128 bits) and higher Comparison Comparison	Firewall	Enable SSL-VPN	
PSC PPTP SSL Centrotans Ce	Tunnel IP Range 192.166.2.1 - [192.166.2.254 Server Certificate Self-Signed C Require Client Certificate Encryption Key Algorithm C High - AES(128/256 bits) and 3DES C Default - RC4(128 bits) and higher C Low - RC4(64 bits), DES and higher Idla Timopote (Seconds)	VPN	Login Port 10443	
pppp Server Certificate Self-Signed centrostes Require Client Certificate Image: Certificate Image: Certificate User Encryption Key Algorithm High - AES(128/256 bits) and 3DES AntWrigs C Default - RC4(128 bits) and higher	Server Certificate Self-Signed S Require Client Certificate High - AES(128/256 bits) and 3DES Encryption Key Algorithm (~ High - AES(128/256 bits) and higher (~ Der - RC4(128 bits) and higher (~ Low - RC4(64 bits), DES and higher Idle Timport (Second)	PSEC	Tunnel IP Range 192.168.2.1 - 192.168.2.254	
SSL Server Certificate Self-Signed Centificates Require Client Certificate I User Encryption Key Algorithm (r) High - AES(128/256 bits) and 3DES AntWrigs C Default - RC4(128 bits) and higher	Server Certificate Self-Signed Require Client Certificate Encryption Key Algorithm High - AES(128/256 bits) and 3DES Default - RC4(128 bits) and higher Cuow - RC4(64 bits), DES and higher Idla Timoput Idla Timoput	PPTP		
User Cardodas Require Client Certificate F High - AES(128/256 bits) and 3DES Certificate C Default - RC4(128 bits) and higher C Default - RC4(128 bits) and higher	Require Client Certificate Final Action Certificate Final Action Certificate Final Action Certificate Final Action Certification Certifica	SSL	Server Certificate Self-Signed	
User Encryption Key Algorithm C High - AES(128/256 bits) and SUES C Default - RC4(128 bits) and higher	Encryption Key Algorithm (* Hagn - Abs.) 128/250 bits) and 3055 (* Default: Rec(21(28 bits) and higher (* Low - RC4(64 bits), DES and higher Idle Timeout (seconds)	Certificates	Require Client Certificate	
AntiVirus	Contract Processor and mane Contract Processor and mane Contract Processor Proces	User	Encryption Key Algorithm C High - AES(128/256 bits) and 3DES	
C Low - RC4(64 bits), DES and higher	Idle Timout (seconds)	AntiVirus	C Low - RC4(64 bits), DES and higher	
Intrusion Protection Idle Timeout 300 (seconds)	The fine of 1900 (secondary	Intrusion Protection	Idle Timeout 300 (seconds)	
Web Filter Portal Message CPVPTOCand SST. URL Dovta1	Portal Message	Web Filter	Portal Message [DVPTOCard SST_VPN_Portal	=
AntiSpam		AntiSpam		
IM, P2P & VolP		IM, P2P & VolP		
		Log&Report	Advanced (DNS and WINS Servers)	
Log&Report Advanced (DNs and WINS Servers)	Advanced (DNS and WINS Servers)		Apply	
LopAReport / Advanced (UNS and WINS Servers) Apply	Advanced (DNS and WINS Servers) Apply			
AntiSpam	CKIPTOCAL 332 VPN FOLGE	AntiSpam	CATFIOLATE SSE VER FOLDET	
IM, P2P & VoIP		IM, P2P & VolP		
		Log&Report	Advanced (DNS and WINS Servers)	
Log&Report / Advanced (DNS and WINS Servers)	Advanced (DNS and WINS Servers)		Apply	
Log&Report Advanced (DNS and WINS Servers)	Advanced (DNS and WINS Servers)		Apply	

A firewall policy must now be created to allow RADIUS authentication via SSL VPN

Creating a Firewall Policy

- Under the Firewall section on the left hand side, click "Policy"
- Then click "Create New" to create a new policy.





Testing RADIUS Authentication

- Change it from "dmz" to "wan1" under "Source Interface/Zone"
- Under the "Action", change it from "ACCEPT" to "SSL VPN"
- Select the user group that was created and move it from "Available Groups" to "Allowed"
- Click "OK" when finished

m)		New Poli	cv		
s Sour s Dest le Sche P Servi on Profile	ce Interface/Zone Ce Address Ination Interface/Zone Ination Address dule Ce	wan1 ali nternal ali always ANY	-7	Multiple Multiple Multiple	
rus User	SSL Client Certificate Re STrength Authentication Method	strictive		Any Any	-
In Protection Available	lable Groups:				
teport	AT	Dynamic IP Pool		X	

Using the Command Line Interface (CLI)

- In the Fortigate Web Config, click on "System" then "Status".
- There will be a CLI Console there. Click on the screen to activate a prompt
- Type the following syntax to test authentication:

diag test auth rad <RADIUS Server name> pap <Username> <OTP>

- RADIUS Server Name: Name of RADIUS Server configured
- Username: User that was created in the Fortigate.
- OTP: Code that is generated from the CRYPTOCard token assigned to the user.

Note: Ensure user has a CRYPTOCard token assigned to them in the BlackShield ID Server.





Testing RADIUS Authentication via SSL

To test RADIUS Authentication via SSL, launch a Web browser client and navigate to:

https://Fortinet DNS Name:10443

A page will come up with a Name and Password field.

- Enter in the user that was created in the Fortinet Fortigate.
- Enter in a code that is generated by the CRYPTOCard Token

Note: Ensure user has a CRYPTOCard token assigned to them in the BlackShield ID Server.

If the authentication is successfully, the new page will appear with all the applications and bookmarks the user is allowed access to.

If the authentication fails, please see the **"Troubleshooting"** section.

logn - Windows Internet Explorer	- 19
🚱 🕗 👻 https://217.205.203.252:10443/remote/login	Centificate Error 🤧 🗙 Live Search
file Edit Yerr Pgrontes Iools Help	
🔓 🐼 🍘 login	🚹 • 🗔 × 🖶 • 🖓 Bage • 🕥 Tgols •
Please	pgin
Name:	henry
Parmon	
	Login
ener als e An ata ale a de	C O Married W 1994
enticeptionets	Lo 🗸 JANIK 1, 1000 *





Troubleshooting

Failed Logons

Error messages are from the BlackShield ID Server Snapshot tab.

Symptom:	Login Failed
Indication:	11/19/2008 Henry Authentication Failure 312191514 192.168.21.120 Invalid 12:36:49 PM OTP
Possible Causes:	The One Time Password provided for the user is incorrect.
Solution:	Attempt to re-authenticate against BlackShield again. If it comes up as invalid OTP again, test the token out via the BlackShield ID Manager.

Symptom:	Login Failed
Indication:	11/19/2008 Henry Authentication Failure 312191514 192.168.21.120 Invalid 12:47:24 PM PIN PIN PIN PIN
Possible Causes:	The PIN provided for the user is incorrect.
Solution:	Attempt to re-authenticate against BlackShield again. If it comes up as invalid PIN again, changing the initial PIN back to default and forcing a PIN change would solve the issue, or have the user access the BlackShield Self Service page.

Symptom:	Login Failed
Indication:	11/19/2008 Henry Authentication Failure 312191514 192.168.21.120 Invalid 12:36:49 PM OTP OTP OTP OTP
Possible Causes:	The One Time Password provided for the user is incorrect.
Solution:	Attempt to re-authenticate against BlackShield again. If it comes up as invalid OTP again, test the token out via the BlackShield ID Manager.

Information

For more information, please refer to the BlackShield ID Admin Guide located at: http://www.cryptocard.com