Implementation Guide for protecting

Fortinet Fortigate 60B

with

BlackShield ID

Copyright

Trademarks

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: http://www.cryptocard.com.

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

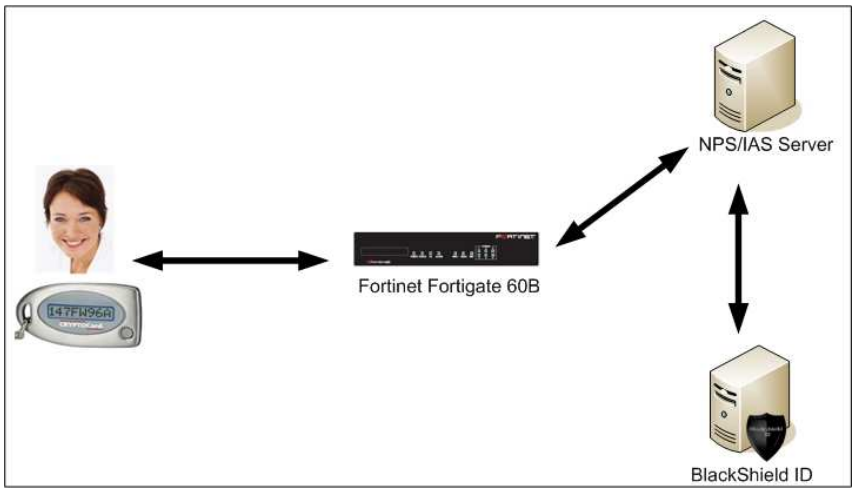
Testing RADIUS Authentication **7**
- Using the Command Line Interface (CLI) 7
- Testing RADIUS Authentication via SSL 8

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+ 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.

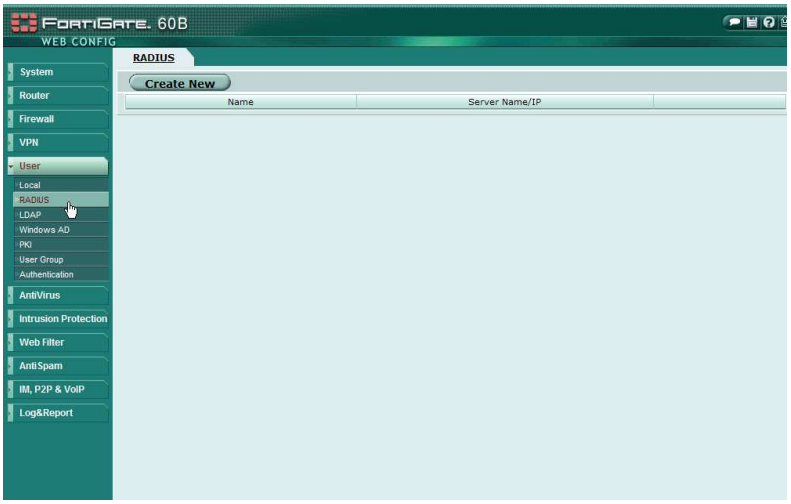
Preparation and Prerequisites

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.

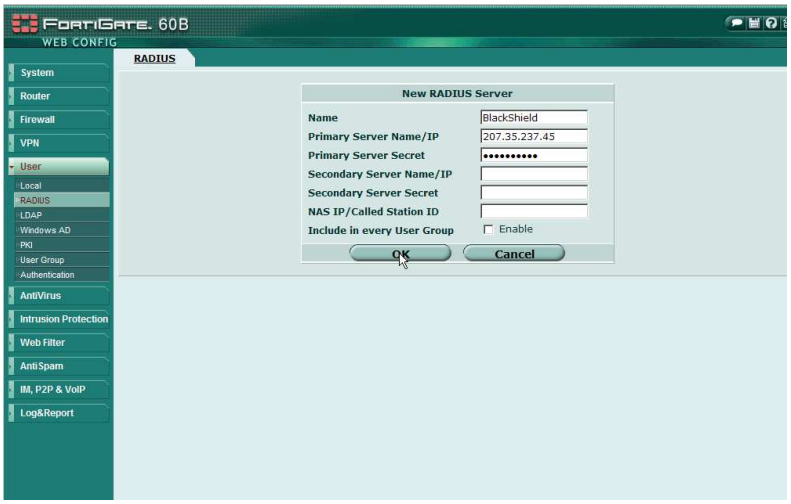
Configuration

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



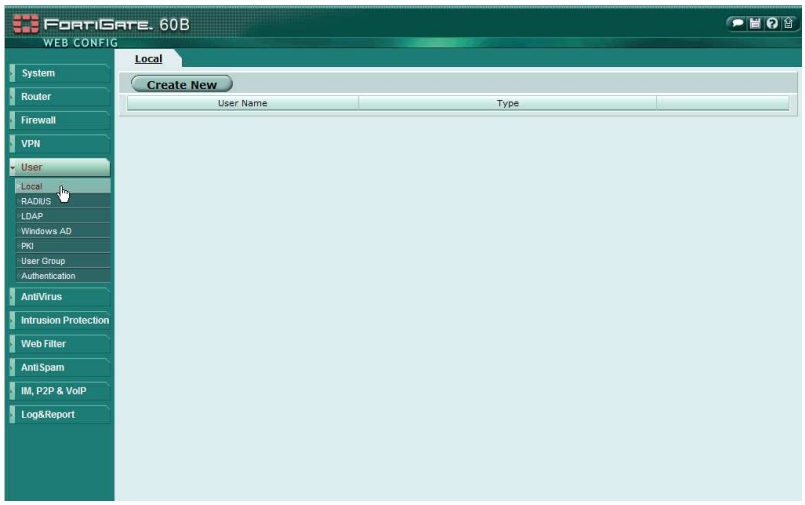
- Give the new RADIUS Server a "Name"
- Enter in the "Primary Server Hostname/IP"
- Enter in the "Primary Server Secret"
- If there is a Secondary RADIUS Server in the environment, please configure the "Secondary Server Name/IP" and the "Secondary Server Secret". If not, skip this section and click "OK"



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

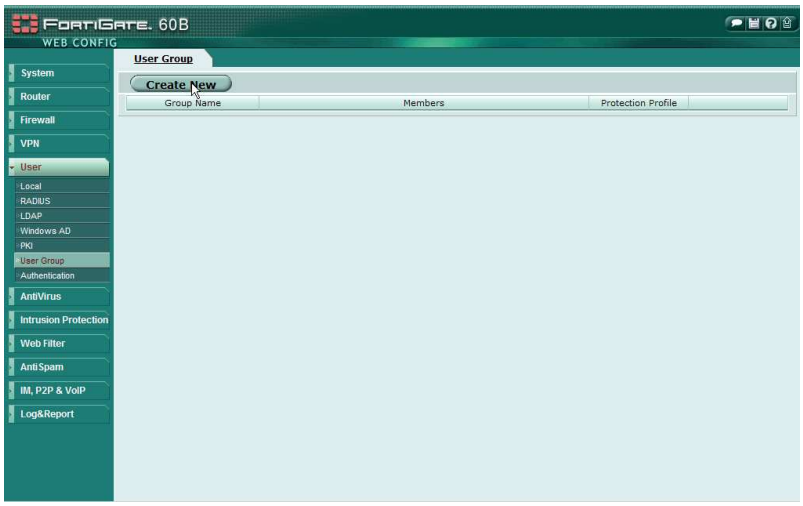
(Note: Ensure that the username entered here match's the username within the BlackShield ID Server)

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

Creating a Group

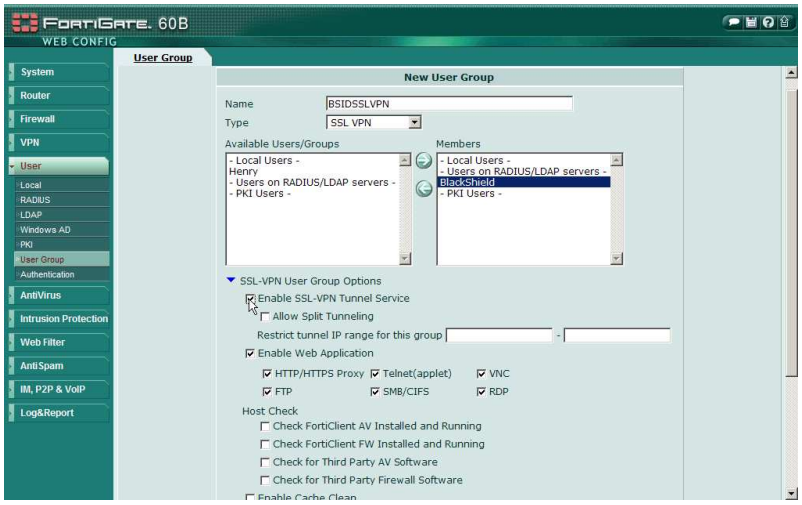
A Group will now need to be created.

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



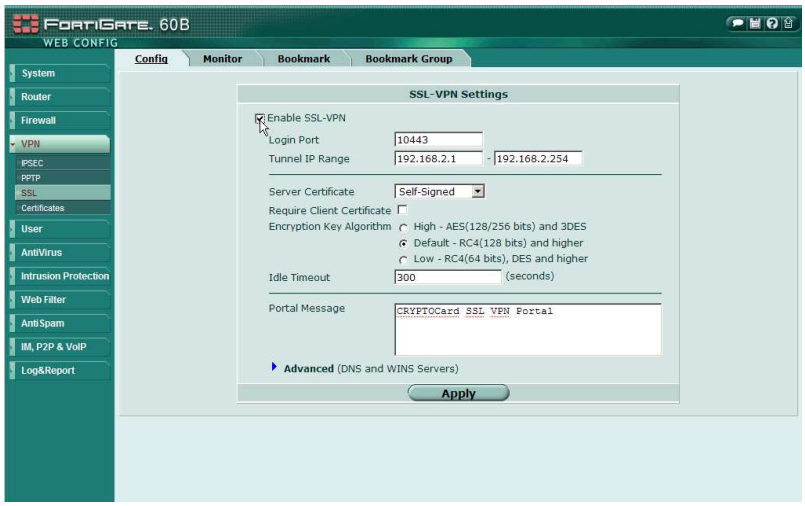
s

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

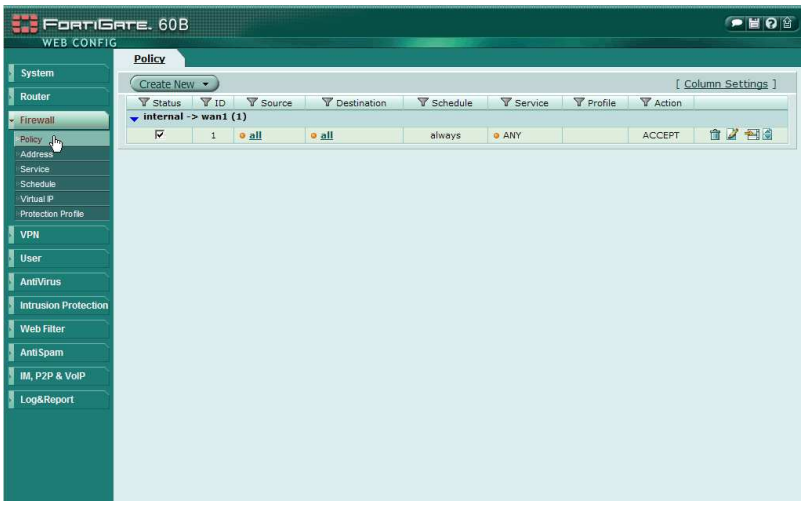
- Next will be to enable the SSL VPN.
- To do this, click on VPN on the left hand side.
- Then click on SSL.
- Enable "Enable SSL-VPN"
- Click Apply all relevant information has been entered.



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

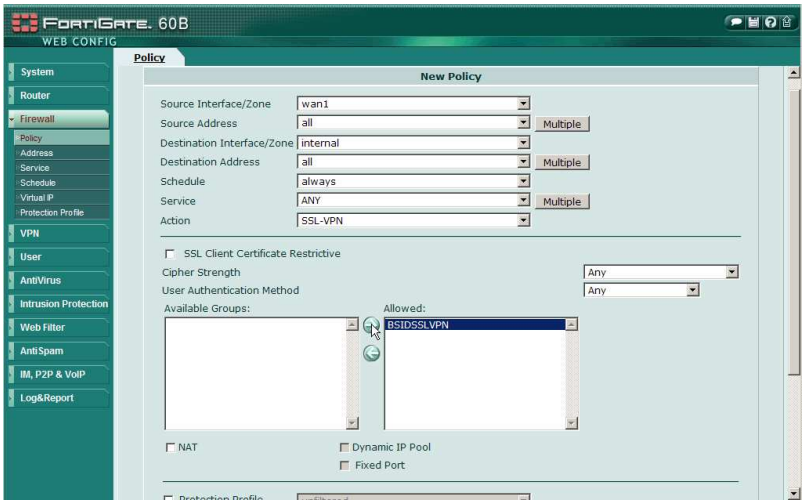
Creating a Firewall Policy

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



Testing RADIUS Authentication

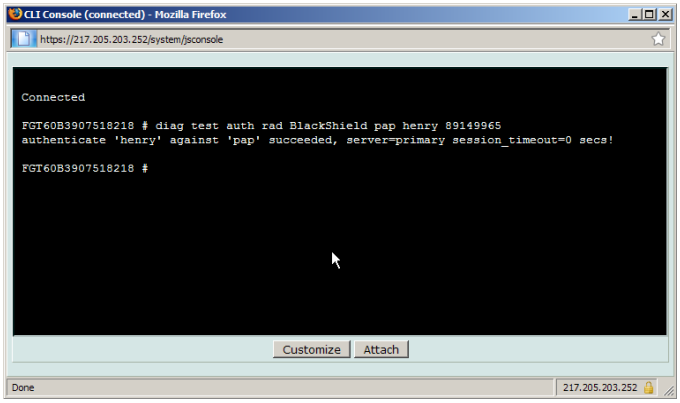
- Change it from "dmz" to "wan1" under "Source Interface/Zone"
- Under the "Action", change it from "ACCEPT" to "SSL VPN"
- Select the user group that was created and move it from "Available Groups" to "Allowed"
- Click "OK" when finished



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>



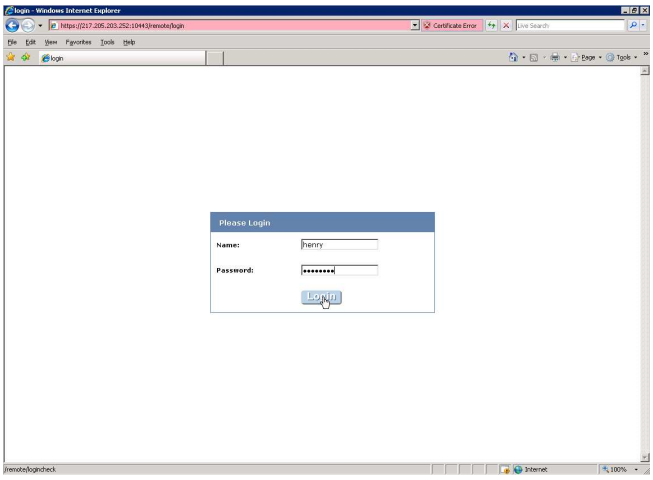
- RADIUS Server Name: Name of RADIUS Server configured
- Username: User that was created in the Fortigate.
- OTP: Code that is generated from the CRYPTOCard token assigned to the user.

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

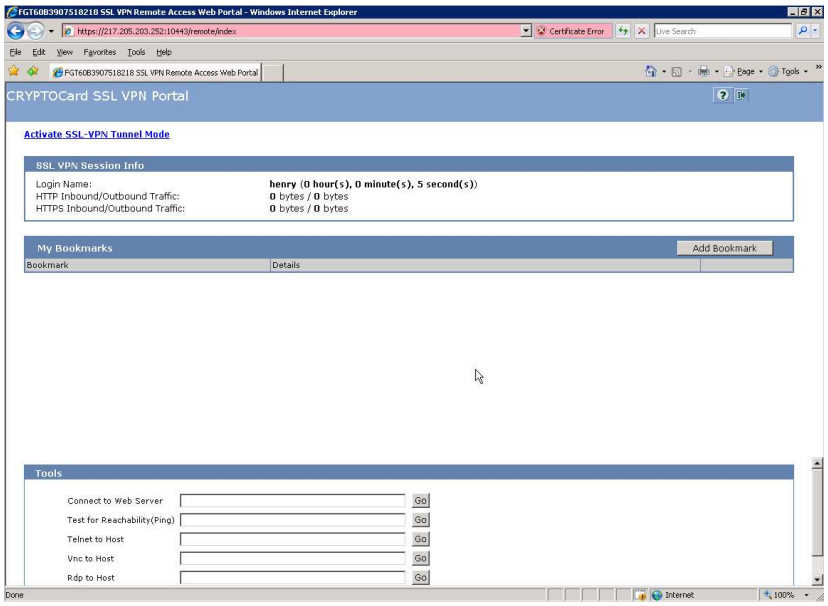


A page will come up with a Name and Password field.

- 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.

Troubleshooting

Failed Logons

Error messages are from the BlackShield ID Server Snapshot tab.

Symptom:	Login Failed
Indication:	11/19/2008 12:36:49 PM Henry Authentication Failure 312191514 192.168.21.120 Invalid 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 12:47:24 PM Henry Authentication Failure 312191514 192.168.21.120 Invalid 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 12:36:49 PM Henry Authentication Failure 312191514 192.168.21.120 Invalid 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