

A dark blue rectangular box containing the text "CRYPTO-Server™" in white, with "6.x" below it. To the right of the box is a white vertical bar with the text "3rd Party Integration" written vertically in dark blue.

WatchGuard Firebox Implementation Guide

Copyright

Copyright © 2006, CRYPTOCARD Corp. 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 Corp.

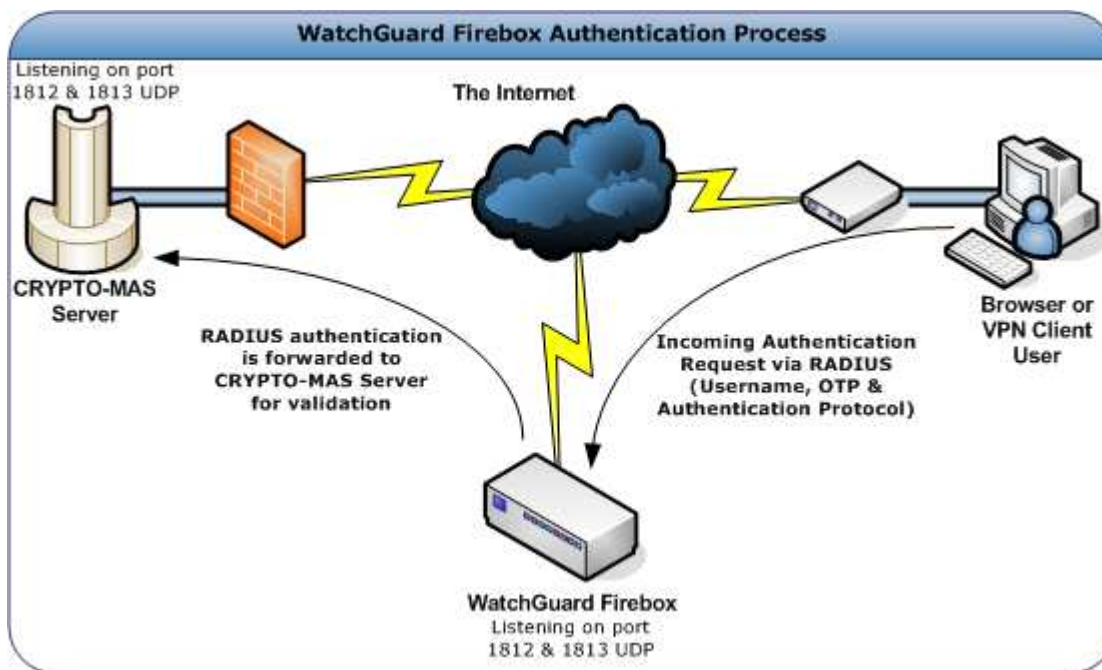
WatchGuard Firebox Overview

This document presents an overview and necessary steps in configuring a WatchGuard Firebox for use with CRYPTO-MAS and CRYPTOCARD tokens.

WatchGuard Firebox is used to create an encrypted tunnel between hosts. CRYPTO-MAS works in conjunction with the WatchGuard Firebox to replace static passwords with strong two-factor authentication that prevents the use of lost, stolen, shared, or easily guessed passwords when establishing a VPN/Browser connection to gain access to protected resources.

With CRYPTO-MAS acting as the authentication server for a VPN/Browser enabled resource, an authenticated connection sequence would be as follows:

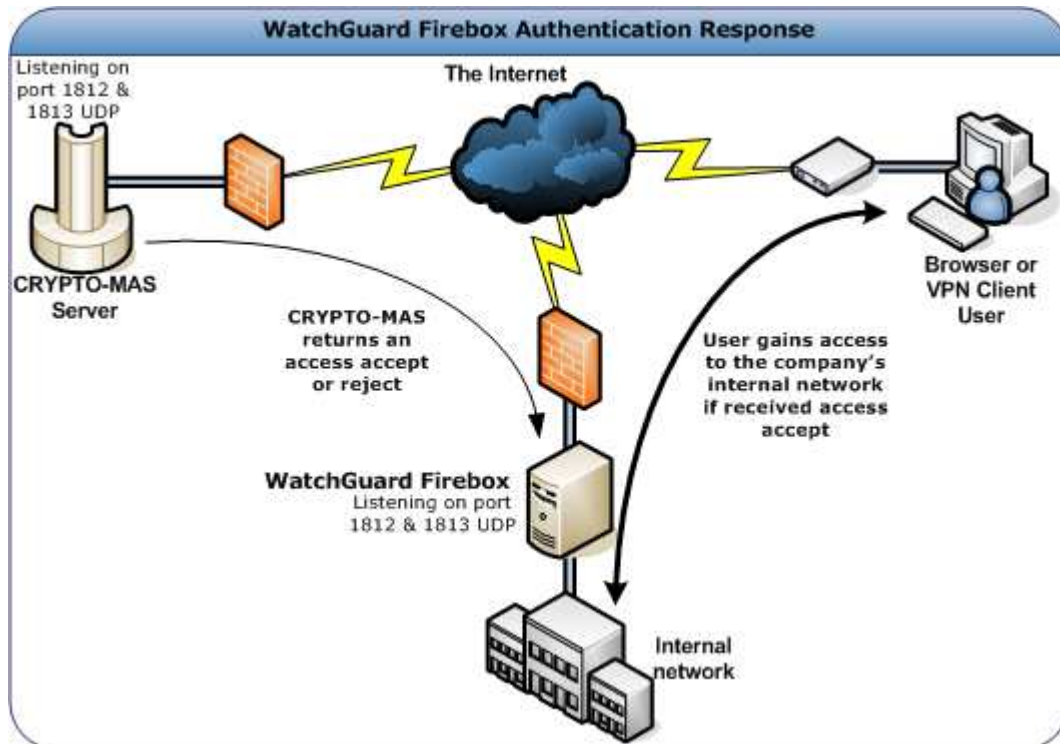
1. The administrator configures the WatchGuard Firebox to use RADIUS Authentication.
2. The incoming RADIUS authentication request is relayed over to the CRYPTO-MAS Server that is shown below.



3. The CRYPTO-MAS Server examines the incoming packet. It checks for the user in the correct VAR or company.
4. If the user exists, it then checks the token associated with the user for the expected OTP.

- Once the OTP is verified against the user's token and it is valid, it will then send an access accepted. This is illustrated in the diagram below.

If the user does not exist, or the OTP is incorrect, it will send an access reject.



Prerequisites

The following systems must be installed and operational prior to configuring WatchGuard to use CRYPTOCARD authentication:

- Ensure that end users can authenticate through WatchGuard with a static password before configuring WatchGuard to use CRYPTOCARD authentication.
- An initialized CRYPTOCARD token assigned to a valid CRYPTOCARD user.

The following CRYPTO-MAS server information is also required:

Primary CRYPTO-MAS RADIUS Server Fully Qualified Hostname or IP Address:	
Secondary CRYPTO-MAS RADIUS Server Fully Qualified Hostname or IP Address (OPTIONAL):	
CRYPTO-MAS RADIUS Authentication port number:	
CRYPTO-MAS RADIUS Accounting port number (OPTIONAL):	
CRYPTO-MAS RADIUS Shared Secret:	
Name of WatchGuard group configured to perform CRYPTOCARD authentication.	

WatchGuard Firebox Configuration

In order for the WatchGuard Firebox to authenticate CRYPTOCARD token users, RADIUS authentication must be configured on the WatchGuard Firewall and a group must be created for CRYPTOCARD token users. Alternatively this can also be applied to a single user. Configuring the WatchGuard Firebox consists of 3 steps:

- Step 1: Defining the CRYPTOCARD RADIUS Server
- Step 2: Assigning CRYPTOCARD Authentication to a WatchGuard MUVPN Connection.
- Step 3: Assigning CRYPTOCARD Authentication to a Service.

Step 1- Defining a CRYPTOCARD RADIUS Server

From the Firebox Policy Manager, select Setup | Authentication Servers

Select the **RADIUS Server** tab

Fill in the information for the CRYPTO-MAS RADIUS server obtained from the prerequisites section.

Click **OK**.

Step 2 – Assigning CRYPTOCARD Authentication to a WatchGuard MUVPN Connection

WatchGuard MUVPN (Mobile User Virtual Private Networking) clients are able to use CRYPTOCARD tokens to authenticate their VPN connection. The WatchGuard Firebox allows MUVPN clients to authenticate to a RADIUS server.

Follow the WatchGuard instructions for setting up MUVPN as usual, but choose the CRYPTOCARD RADIUS server, configured in Step 1, as the authentication server.

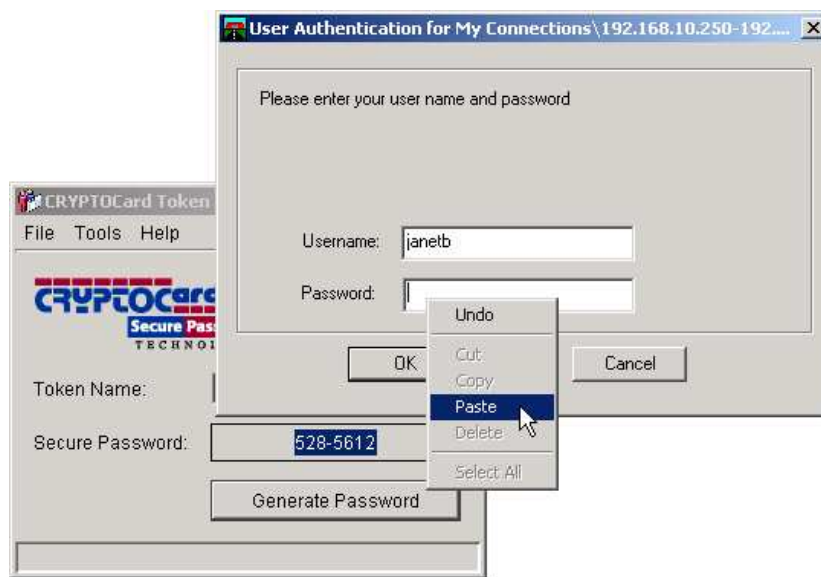
Note: If CRYPTOCARD RADIUS authentication is being assigned to a WatchGuard MUVPN group, CRYPTOCARD must be notified of the group name in order to create a matching RADIUS Filter-Id within the CRYPTO-MAS Server.

Performing a MUVPN Connection

Once the CRYPTOCARD enabled MUVPN profile has been created, it may be distributed to the client systems to allow clients to form a VPN connection to the Firebox.

If using CRYPTOCARD software based tokens: When the MUVPN client prompts for a username and password, launch the CRYPTOCARD Authenticator, click on Generate Password, enter the token PIN, and enter the CRYPTOCARD username and one-time password into the MUVPN prompt.

If using CRYPTOCARD hardware tokens (RB or KT): When the MUVPN prompts the end-user for a username and password, enter the CRYPTOCARD username and one-time password¹ into the MUVPN prompt.



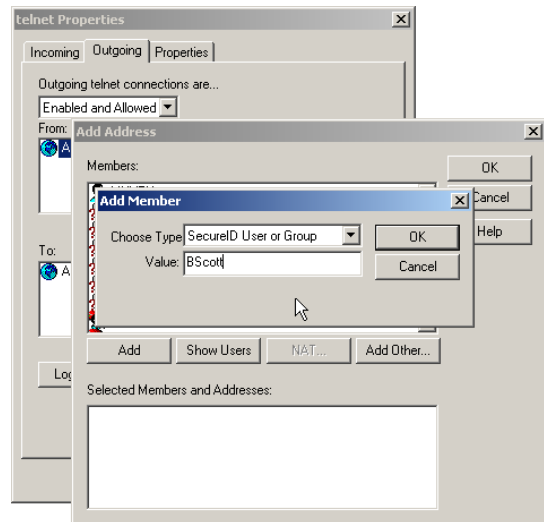
¹ In some cases this may include a PIN and the Response from the users token.

Step 3- Assigning CRYPTOCARD Authentication to a Service

To protect a service/port with CRYPTOCARD authentication, select the rule for that service/port and choose the incoming our outgoing tab, depending on the rule. Then select Add Other.

From the dropdown menu, choose SecurID User or Group. In the Value field, enter a CRYPTOCARD username or a groupname.

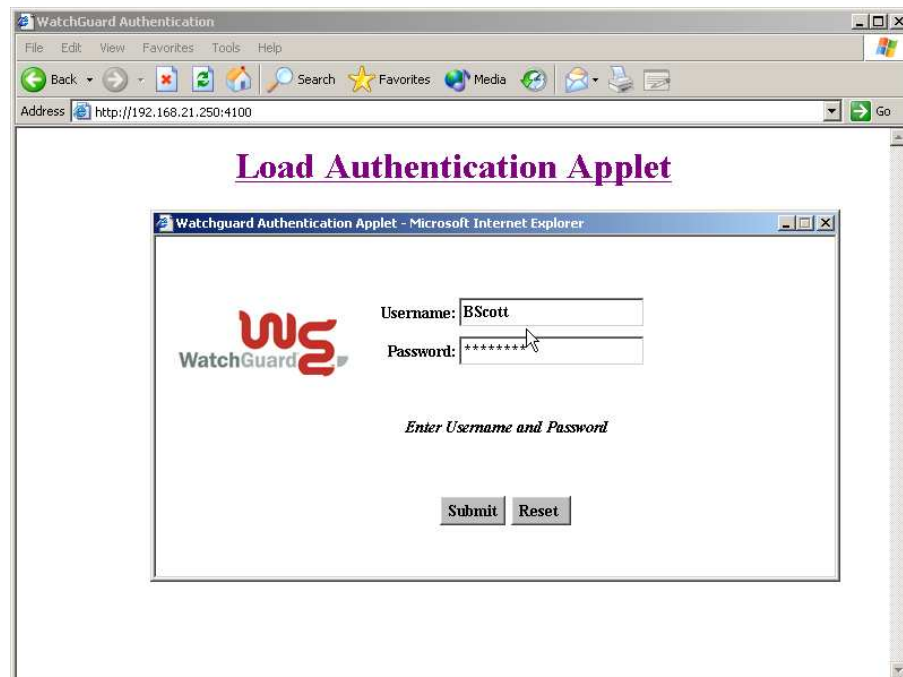
Note: If CRYPTOCARD RADIUS authentication is being assigned to a group, CRYPTOCARD must be notified of the group name in order to create a matching RADIUS Filter-Id within the CRYPTO-MAS Server.



Authenticated Logon

In order to authenticate, users must connect to the Firebox using a Java-enabled Web browser to this URL: `http://[Firebox IP here]:4100`.

This loads a Java applet which prompts for a username and response. The user is then authenticated, and as long as the applet window remains open, the user will be able to access the protected services from that same computer. Please consult extra information below.



Additional Information WatchGuard Logon Applet

When RADIUS authentication is configured, the WatchGuard Java based logon applet performs CHAP-based RADIUS authentication requests. The CRYPTOCARD RADIUS server supports PAP and MSCHAPv2 authentication requests. The SecurID Authentication server must be selected to enforce the PAP based Java logon applet for RADIUS authentication requests. From the Firebox Policy Manager, select Setup | Authentication Servers. Select the **SecurID Server** tab. Fill in the information for the CRYPTO-MAS RADIUS server obtained from the prerequisites section then select OK.

Solution Overview

Summary	
Product Name(s)	WatchGuard Firebox
Vendor Site(s)	http://www.watchguard.com
Supported VPN/Browser Client Software	IE 6 Mozilla Firefox 1.5+ WatchGuard Windows VPN Client
Authentication Method	RADIUS Authentication
Supported RADIUS Functionality for WatchGuard Firebox	
Packet Encryption Type	PAP MSCHAPv2
Authentication Method	One-time password Challenge-response Static password
New PIN Mode	User-changeable Alphanumeric 4-8 digit PIN User-changeable Numeric 4-8 digit PIN Server-changeable Alphanumeric 4-8 digit PIN Server-changeable Numeric 4-8 digit PIN

Trademarks

CRYPTOCARD, CRYPTO-Server, CRYPTO-Web, CRYPTO-Kit, CRYPTO-Logon, CRYPTO-VPN, CRYPTO-MAS are either registered trademarks or trademarks of CRYPTOCARD Corp.

Microsoft Windows and Windows XP/2000/2003/NT are registered trademarks of Microsoft Corporation. All other trademarks, trade names, service marks, service names, product names, and images mentioned and/or used herein belong to their respective owners.

Publication History

Date	Changes
October 27 th , 2006	Initial Draft
November 13 th , 2006	Global Draft
November 30, 2006	Revision Draft