SafeNet Authentication Service

Integration Guide

Protecting WatchGuard Firebox with SAS

Document Information

Document Part Number	007-012629-001, Rev A
Release Date	July 2009

Trademarks

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as WatchGuard Firebox.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Overview

By default, WatchGuard Firebox requires that a user provide a correct user name and password to successfully log on. This document describes the steps necessary to augment this logon mechanism with strong authentication by adding a requirement to provide a one-time password (OTP) generated by a SafeNet token using the instructions in this guide.

SAS works in conjunction with 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 tunnel to gain access to protected resources:

- Using the Firebox MUVPN Client, the user establishes a connection using his/her logon name and SafeNet token-generated one-time password.
- WatchGuard Firebox passes the authentication information via RADIUS to the SAS Internet Authentication Service (IAS) or Network Policy Server (NPS) agent configured to communicate to the SAS server.
- The SAS server verifies the username and password, and an “Access-Accept” message, is returned to WatchGuard Firebox, allowing the user to access the network.

Applicability

This guide is applicable to the following:

Security Partner Information	
Security Partner	WatchGuard
Product Name and Version	WatchGuard Firebox
Protection Category	Remote Access

SAS Server	
Authentication Server	SafeNet Authentication Service Cloud SafeNet Authentication Service PCE/SPE

Prerequisites

The following must be installed and operational prior to configuring WatchGuard Firebox to use SafeNet Authentication Service:

- SafeNet Authentication Service has been installed and configured, and a “Test” user account has been created.
- Ensure users can authenticate through WatchGuard Firebox with a static password before configuring the WatchGuard Firebox to use RADIUS authentication.
- The SAS server is installed and a user account is assigned a SafeNet token.
- The SAS Agent for Internet Authentication Service (IAS) or Network Policy Server (NPS) is installed.

Operation

SafeNet Authentication Service works in conjunction with 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 tunnel to gain access to protected resources:

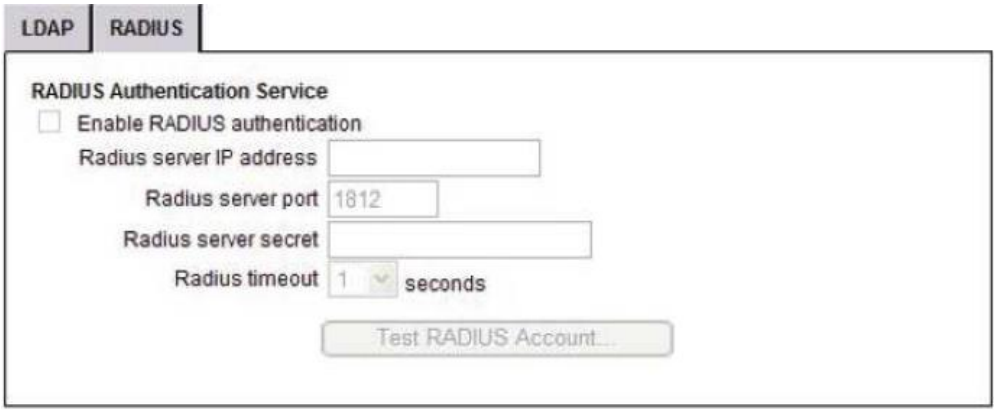
1. Using the Firebox MUVPN Client, the user establishes a connection using his/her logon name and SafeNet token-generated one-time password.
2. The WatchGuard Firebox passes the authentication information via RADIUS to the SAS Internet Authentication Service (IAS) or Network Policy Server (NPS) agent configured to communicate to the SAS server.
3. The SAS server verifies the username and password and an “Access- Accept” message is returned to the WatchGuard Firebox, allowing the user to access the network.

Configuring WatchGuard Firebox

Step 1: Enable RADIUS Authentication

1. Connect to the Firebox **System Status** page by entering **https://** in a web browser followed by the IP address of the Firebox trusted interface.
2. Click **Firebox Users > Settings**.
3. Click the **RADIUS** tab. Complete the following fields:

Security Partner Information	
Enable RADIUS Authentication	Select this option.
RADIUS server IP address	Enter the IP address of the RADIUS server.
RADIUS server port	Enter **1812**.
RADIUS server secret	Enter the shared secret between Firebox and the RADIUS server. The shared secret between Firebox and the RADIUS server is case sensitive.
RADIUS timeout	Select **10** seconds.



Step 2: Add a Firebox group for Mobile VPN Users (IPsec or SSL)

Once RADIUS authentication has been enabled, a Firebox group must be added to the WatchGuard Firebox setup so users can properly authenticate using a SafeNet token.

1. Connect to the Firebox System Status page by entering **https://** in a web browser followed by the IP address of the Firebox trusted interface.
2. Click **Firebox Users > New Group**.
3. On the **Settings** tab, enter the **Account Name** for the group.
4. Click the **MUVPN** tab, do the following:
   - Select **Enable Mobile VPN with IPsec** or **Enable Mobile VPN with SSL**.
   - In the **Shared key** field, enter a shared key. The Shared key is used to encrypt the **.wgx** file for the MUVPN clients. It is not the Shared Secret used between Firebox and RADIUS server.
   - If necessary, select **All traffic uses tunnel** if the remote client sends all traffic through the VPN tunnel.
   - In the **Virtual IP address range** field, enter a starting and ending IP Address.
5. Click **Submit**.

Step 3: Add a RADIUS Filter-Id to the RADIUS Server

A **Filter-Id** in must be added to the RADIUS server configuration so users can properly authenticate using a SafeNet token.

Internet Authentication Service (IAS) with SAS Agent Enabled

1. Under **Administrative Tools**, launch Internet Authentication Service.
2. Expand **Connection Request Processing** and then click **Connection Request Policies**.
3. Right-click on the SAS entry (by default **Allow all users to authenticate with SAS**) and select **Properties**.
4. Click **Edit Profile** and then select the **Advanced** tab.
5. Click **Add**. In the **Add Attribute** window, highlight **Filter-Id** and then select **Add**.
6. In the **Attribute Values** section, select **Add**.

7. In the **Enter the attribute value in** field, select **String**.
8. In the text box, enter the WatchGuard Firebox MUVPN group name.
9. Click **OK** to apply the settings.

Network Policy Server (NPS) with SAS Agent Enabled

1. Under **Administrative Tools**, launch **Network Policy Server**.
2. Expand **Policies** and then highlight **Connection Request Policies**.
3. Right-click on the SAS entry (by default **Allow all users to authenticate with SAS**) and select **Properties**.
4. Select the **Settings** tab, highlight **RADIUS Attributes Standard** and then select **Add**.
5. Under **Access type**, select **All**. In the **Attributes** section, highlight **Filter-Id** and then click **Add**.
6. On the **Attribute Information** window, select **Add**.
7. Below **Enter the attribute value in**, select **String**.
8. In the text box, enter the WatchGuard Firebox MUVPN group name.
9. Click **OK** to apply the settings.

Troubleshooting

When troubleshooting issues for setting up RADIUS authentication on WatchGuard Firebox, it may be helpful to refer to the Firebox logs or the WatchGuard Log Server. Refer to the Firebox documentation for details.

All logging information for Internet Authentication Service (IAS) or Network Policy Server (NPS) can be found in the Event Viewer.

All logging information for the SAS IAS\NPS agent can be found in the following directory:

\Program Files\CRYPTOCard\BlackShield ID\IAS Agent\log

Failed Logons

The following is an explanation of the logging messages that may appear in the Event Viewer for the Internet Authentication Service (IAS) or Network Policy Server (NPS) RADIUS Server.

Error Message	Solution
Packet DROPPED: A RADIUS message was received from an invalid RADIUS client.	Verify a RADIUS client entry exists on the RADIUS server.
Authentication Rejected: Unspecified	This will occur when one or more of the following conditions occur: • The username does not correspond to a user on the SAS server. • The SafeNet password does not match any tokens for that user. • The shared secret entered in WatchGuard Firebox does not match the shared secret on the RADIUS server

Authentication Rejected: The request was rejected by a third-party extension DLL file.	This will occur under one or more of the following conditions: • The SAS Agent for IAS/NPS cannot contact the SAS server. • The Pre-Authentication Rules on the SAS server do not allow incoming requests from the SAS Agent for IAS/NPS. • The SAS Agent for IAS/NPS Key file does not match the key file stored on the SAS server. • The username does not correspond to a user on the SAS server • The SafeNet password does not match any tokens for that user.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when phone support is available to you.

Table 1: Support Contacts

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	