SafeNet Authentication Service
Integration Guide

Protecting CheckPoint Firewall-1/VPN-1 with SAS
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012633-001, Rev A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>July 2009</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

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.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
Contents

Introduction .......................................................................................................................................................... 4
Third-Party Software Acknowledgement ........................................................................................................... 4
Overview ............................................................................................................................................................ 4
Applicability .......................................................................................................................................................... 4
Prerequisites .......................................................................................................................................................... 4
Operation .............................................................................................................................................................. 4
Configuration ......................................................................................................................................................... 5
Defining the RADIUS Server Object .................................................................................................................. 5
Defining the RADIUS Server .................................................................................................................................. 6
Applying RADIUS Authentication ...................................................................................................................... 7
Configuring the VPN-1 Settings and IKE (Internet Key Exchange) Encryption ...................................................... 8
Creating an Authentication Group (VPN-1) ......................................................................................................... 10
Adding SAS Users in FireWall-1/VPN-1 ............................................................................................................... 11
Configuring a Generic User Entry ..................................................................................................................... 14
Creating a FireWall-1/VPN-1 Rule Set ............................................................................................................... 16
Troubleshooting ................................................................................................................................................... 16
Failed Logons ....................................................................................................................................................... 16
Support Contacts .................................................................................................................................................. 17
Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as CheckPoint Firewall-1/VPN-1.

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, CheckPoint VPN connections 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 SafeNet token using the instructions below.

Applicability

<table>
<thead>
<tr>
<th>Security Partner Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Partner</td>
</tr>
<tr>
<td>Product Name and Version</td>
</tr>
<tr>
<td>Protection Category</td>
</tr>
</tbody>
</table>

Prerequisites

- SafeNet Authentication Service has been installed and configured
- A “Test” user account can be selected in the Assignment tab
- A RADIUS server is installed (for example, Microsoft Internet Authentication Service)
- The appropriate SAS plug-in is installed on the RADIUS server

Operation

The CheckPoint Firewall-1 or VPN-1 server will send all RADIUS authentication requests to the SAS server. The SAS server will then return a message to either allow or reject the connection.
Configuration

Defining the RADIUS Server Object

1. Log in to the CheckPoint management console. (Refer to the CheckPoint documentation for instructions on performing this step.)

2. From the CheckPoint SmartDashboard, select Manage > Network Objects.

3. Click New, select Node, and then click Host.

4. Under General Properties, enter the Host Node Properties:
   - Name
   - IP Address – Enter the address of the Microsoft IAS Server.
   - Comment
   - Color

5. Click OK > Close.
Defining the RADIUS Server

Once the actual network object has been created, the server needs to be configured so that it is aware of a server object.

1. From the CheckPoint SmartDashboard, select Manage > Servers.
2. Click New > RADIUS.

3. Define the RADIUS Server Properties:
   - Name
   - Comment
   - Color
   - Host - This should be the Host Node you defined in the previous section.
   - Service – Select NEW-RADIUS.
   - Shared Secret - The shared secret must match the shared secret defined on the RADIUS server.
   - Version - Select RADIUS Version 2.0.
4. Click **OK > Close**.

5. Click the **Policy** menu and then click **Install**.

![Image](image-url)

**Applying RADIUS Authentication**

1. From the Check Point SmartDashboard, click **Manage > Network Objects**.
2. Select the **win2k-8 FireWall-1/VPN-1** object, and then click **Edit**.

![Image](image-url)
3. Under **General Properties**, select **Authentication**, and then verify that the **VPN-1 & FireWall-1 Password** and **RADIUS** options are selected.

### Configuring the VPN-1 Settings and IKE (Internet Key Exchange) Encryption

The following steps allow the SecuRemote users to download the VPN-1 topology from the FireWall and to encrypt connections to the inside network.

1. From the FireWall-1/VPN-1 network object, under **General Properties**, choose **VPN**.
2. Select your VPN Community (RemoteAccess).
3. Click **Traditional mode configuration**. Select **Exportable for SecuRemote/SecureClient** (if the FireWall-1 is already in the Remote Access community, this option is selected by default and cannot be disabled.)

![Configuration Screenshot]
4. In the VPN section, under **General Properties**, verify that a certificate exists in the **Certificate List**.

5. Verify that **Hybrid Mode Authentication** has been enabled. Select **Policy > Global Policy > Remote Access > VPN – Basic**.

6. Under **Support authentication methods**, verify that **Hybrid Mode** has been selected.
Creating an Authentication Group (VPN-1)

1. From the Manage menu, select Users and Administrators and then click New > Group. This group will be used to reference all users being authenticated by SAS.

2. In the Group Properties field, enter the following:
   - Name
   - Comment
   - Color

3. Click OK.
Adding SAS Users in FireWall-1/VPN-1

SafeNet token users can be configured to use RADIUS authentication in two methods on FireWall-1/VPN-1. Each SafeNet token user can be added to the FireWall-1/VPN-1 database individually, or a generic user entry can be configured. Use the method that best meets your network authentication requirements.

1. In the CheckPoint SmartDashboard, select Manage > Users and Administrators.
2. Click New > Template.

3. In the User Template Properties window, under the General tab, enter a Login Name.
4. Click the **Personal** tab to define the **Expiration Date**, **Comment**, and **Color**.

5. Click the **Groups** tab.

6. Select the **SecuRemote** group created previously and then click the **Add** button.

7. Click the **Authentication** tab and define the **Authentication Scheme** as RADIUS.

8. Select the RADIUS server you created in the previous section.
9. Click the **Location** tab and then the **Time** tab to define these settings as per your network security policy.

10. Select the **Encryption** tab and select the **IKE** option.

11. Click the **Edit** button to configure the **IKE Encryption** settings.

12. Select the **Encryption** tab to validate the **Encryption Algorithm**.

13. Click the **Install** button to add the user to the FireWall-1 user database.

14. Close the **Users and Administrators** window.
Configuring a Generic User Entry

1. From the Users and Administrators window, click New > External User Profile and then choose Match all users.

2. In the External User Profile Properties window, select the Groups tab and then add the appropriate group.
3. On the **Authentication** tab, choose **RADIUS** as the **Authentication Scheme** and then select the RADIUS server.

4. Select the **Encryption** tab and then select the **IKE** option.
Creating a FireWall-1/VPN-1 Rule Set

Below is an example of two simple rule sets that will require users to authenticate with SafeNet tokens. Configure the rule sets as per your network requirements.

<table>
<thead>
<tr>
<th>NO.</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>IF-MAP</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External@Any</td>
<td>Any</td>
<td>Any</td>
<td>http:</td>
<td>User Auth</td>
<td>Log</td>
<td>Gateways</td>
</tr>
<tr>
<td>2</td>
<td>SecRemote@Any</td>
<td>Any</td>
<td>Any</td>
<td>Telnet</td>
<td>Client Auth</td>
<td>Log</td>
<td>Gateways</td>
</tr>
</tbody>
</table>

Troubleshooting

Failed Logons

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Authentication using the VPN client is rejected.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Possible Causes</td>
<td></td>
</tr>
<tr>
<td>• Verify that the shared secret is correct on both the RADIUS server, and the Checkpoint Firewall-1 / VPN-1</td>
<td></td>
</tr>
<tr>
<td>• Ensure that the BlackShield IAS NPS Agent has been installed and configured properly.</td>
<td></td>
</tr>
<tr>
<td>• Verify that the token is in sync with SAS.</td>
<td></td>
</tr>
</tbody>
</table>
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

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