Microsoft Forefront Threat Management Gateway

Integration Guide
Preface

All intellectual property is protected by copyright. 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.

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.

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 below.

4690 Millennium Drive
Belcamp, Maryland 21017, USA

Limitations

This document does not include the steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to Luna SA documentation for general Luna setup procedures.

Disclaimers

The foregoing integration was performed and tested only with the specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

Technical Support

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, please contact your supplier or SafeNet support.

SafeNet 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 telephone support is available to you.

Technical Support Contact Information:

Phone: 800-545-6608, 410-931-7520
Email: support@safenet-inc.com
Table of Contents

Chapter 1 Introduction.......................................................................................................................................................... 5
  Understanding the Forefront Threat Management Gateway ..........................................................................................5
  Scope ....................................................................................................................................................................................5
  Prerequisites .........................................................................................................................................................................6

Chapter 2 Integrating Forefront Threat Management Gateway with Luna SA / Luna PCI ............................ 7
  Setting up Luna SA / Luna PCI for Active Directory Certificate Services .................................................................7
  1. Configuring the CA to issue TMG Server Certificates .............................................................................................7
  Setting up Luna SA / Luna PCI for Forefront Threat Management Gateway (TMG) .................................................8
  1. Generating the SSL Certificate to use with Forefront Threat Management Gateway (TMG) .............................8
  2. Configuring Forefront TMG to use Luna SA / Luna PCI for SSL Communication ..............................................9
Chapter 1
Introduction

This document is intended to guide security administrators through the steps for Microsoft Forefront TMG (Threat Management Gateway) and Luna HSM integration, and also covers the necessary information to install, configure and integrate Microsoft Forefront TMG with SafeNet Luna Hardware Security Modules (HSMs).

The Luna HSMs integrates with the Microsoft Forefront TMG to provide significant performance improvements by off-loading cryptographic operations from the TMG Server to the Luna HSMs. In addition, the Luna HSMs provides extra security by protecting and managing the server’s high value SSL private key within a FIPS 140-2 certified hardware security module.

Understanding the Forefront Threat Management Gateway

Forefront Threat Management Gateway (TMG) is a secure web gateway that provides comprehensive protection against web-based threats by integrating multiple layers of protections into a unified, easy-to-use solution. Forefront TMG allows your employees to safely and productively use the Internet for business without worrying about malware and other threats. Forefront TMG inspects web traffic at the network, application and content layers to help ensure comprehensive protection. It also improves your organization’s firewall performance by offloading processor-intensive functions like inspection for malware.

Forefront TMG can scale performance when administrators cluster multiple gateways or deploy Forefront TMG at individual sites. It can easily be deployed in two modes: as a standalone server to deliver maximum performance, or as a virtualized machine that can be combined with other applications to reduce hardware costs.

Scope

This guide provides instructions for setting up a small test lab with Forefront Threat Management Gateway (TMG) on a server running the Windows Server 2008 R2 operating system and using Luna HSM for securing the SSL certificate private keys. It explains how to install and configure the software that is required for setting up a TMG server while storing certificate keys on Luna HSM.

3rd Party Application Details

- Microsoft Forefront Threat Management Gateway 2010
  
  You can download the TMG 2010 from Microsoft site:  

Supported Platforms

The following platforms are supported for Luna SA v5.1.1

- Windows Server 2008 R2

The following platforms are supported for Luna PCI 5.0

- Windows Server 2008 R2

HSMs and Firmware Support

We did this integration with the following:

- Luna SA v5.1 f/w 6.2.1 with Luna SA Client s/w v5.1.1 (64-bit)
- Luna PCI 5.0 f/w 6.2.1 with Luna PCI Client s/w v5.0 (64-bit)
- 630-010302-001_Alpha1.exe

630-010302-001_Alpha1.exe is a patch released for Safenet CSP and KSP which required for this integration and you can download it from Safenet Customer Support.

Prerequisites

**Luna SA Setup**

Please refer to the Luna SA documentation for installation steps and details regarding configuring and setting up the box on Windows systems. Before you get started ensure the following:

- Luna SA appliance and a secure admin password
- Luna SA, and a hostname, suitable for your network
- Luna SA network parameters are set to work with your network
- Initialized the HSM on the Luna SA appliance.
- Created and exchanged certificates between the Luna SA and your Client system.
- Created a partition on the HSM, remember the partition password that will be later used by Forefront TMG. Register the Client with the partition. And run the "vtl verify" command on the client system to display a partition from Luna SA. The general form of command is C:\Program Files\Luna SA > vtl verify for Windows.
- Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

**Luna PCI Setup**

Please refer to the Luna PCI documentation for installation steps and details regarding configuring and setting up the box on Windows systems. Before you get started ensure the following:

- Initialize the HSM on the Luna PCI appliance.
- Create a partition on the HSM that will be later used by the TMG Server.
- Enable Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna PCI with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

**Microsoft TMG 2010 Setup**

You should familiarize yourself with Microsoft Forefront Threat Management Gateway 2010. Refer to the appropriate help files for more information and pre-installation requirements.


- The setup consists of two systems in a private network as per the table below:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Applications and Services</th>
<th>Description</th>
<th>Computer Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server® 2008 R2 Enterprise</td>
<td>Active Directory, Domain Name System (DNS), Active Directory Certificate Services</td>
<td>Domain Controller, DNS Certificate Authority</td>
<td>TMG-DC</td>
</tr>
<tr>
<td>Windows Server® 2008 R2 Enterprise</td>
<td>Microsoft Forefront Threat Management Gateway 2010</td>
<td>TMG Server</td>
<td>TMG-SRV</td>
</tr>
</tbody>
</table>

- TMG-DC is configured as domain controller with domain LUNATMG.COM and a Certificate Authority with Certification Authority Web Enrollment.
- Join TMG-SRV to the LUNATMG.COM domain.
- Install the TMG 2010 on TMG-SRV. To install the TMG 2010 please refer the Microsoft documentation or the following link: [http://technet.microsoft.com/en-us/library/cc441440.aspx](http://technet.microsoft.com/en-us/library/cc441440.aspx)

**Note:** After installation and initial configuration of TMG 2010, you need to create a new access rule using TMG Management Console to communicate with Luna SA on the port 1792.
Chapter 2
Integrating Forefront Threat Management Gateway with Luna SA / Luna PCI

Setting up Luna SA / Luna PCI for Active Directory Certificate Services

To set up Luna SA / Luna PCI for Active Directory Certificate Services, kindly refer the Microsoft Active Directory Certificate Services Integration Guide.

1. Configuring the CA to issue TMG Server Certificates

Configuring a CA to create a certificate template and issuing properties for TMG server certificate.

1.1 Configuring certificate templates for your test environment

a) Log on to TMG-DC as a domain administrator.
b) From the Start menu, select Run.
c) In the Run dialog, type mmc and click OK.
d) In the mmc console that appears, select File > Add/Remove Snap-in…
e) In the Add or Remove Snap-Ins dialog box, find the Certificate Templates snap-in (under the Available snap-ins section) and select it.
f) Click Add, and then click OK.
g) Under Console Root, expand the Certificate Templates snap-in. Listed in the middle section will be all the available certificate templates that you can make your CA issue.
h) Scroll down the list until you locate the Web Server template, right-click and click Duplicate Template.
i) Select Windows Server 2003 Enterprise and click OK.
j) In the pop-up dialog that appears, click the General tab.
k) Enter the Template Display Name for example TMG here.
l) Click the Request Handling tab.
m) Click on CSPs and select Request can use any CSP available on subject’s computer.
n) Click OK to close the window.
o) Click the Security tab and click Add.
p) Type NETWORK SERVICE and click OK.
q) Click on NETWORK SERVICE in the Group and user names area.
r) In the Permissions area, make sure that the Read and Enroll check boxes are ticked.
s) Add and provide the Read and Enroll permissions to the following:
   - Domain Computers
   - Domain Controllers
   - NETWORK SERVICE
   - IIS_IUSRS
t) For Domain Admins and Enterprise Admins, make sure that Read, Write, and Enroll check boxes are ticked.
u) Click Apply and then OK.

1.2 Configuring the CA to support the TMG certificate template

a) Log on to TMG-DC as a domain administrator.
b) From the Start menu select Control Panel > Administrative Tools > Certification Authority.
c) In the console tree (left-hand section), expand the CA. (It has a computer and a green tick next to it.)
d) In console tree of the Certification Authority snap-in, right-click Certificate Templates, and then click New Certificate Templates to Issue.
e) In Enable Certificates Templates, select the TMG template and any other certificate templates you configured previously, and then click OK.
f) Open Certificate Templates in the Certification Authority and verify that the modified certificate templates appear in the list.

Setting up Luna SA / Luna PCI for Forefront Threat Management Gateway (TMG)

To set up Luna HSM for Forefront Threat Management Gateway, perform the following:

Before you install Forefront Threat Management Gateway 2010

- Log on to TMG-SRV as a domain administrator.
- Run the command, register.exe to register Luna CSP. The general form of command is
  C:\Program Files\LunaSA\CSP>Register.exe
  C:\Program Files\LunaPCI\CSP>Register.exe
- To list the Luna Cryptographic Services for Microsoft Windows. The general form of command is
  C:\Program Files\LunaSA\CSP>Register.exe /l
  C:\Program Files\LunaPCI\CSP>Register.exe /l
- KSP must be installed on the TMG Server (TMG-SRV) in a separate step following completion of the main Luna SA / Luna PCI Client software installation.
- Traverse to C:\Program Files\SafeNet.
- Run the KspConfig.exe (KSP configuration wizard).
- Double click Register Or View Security Library on the left side of the pane.
- Browse the library C:\Program Files\LunaSA\cryptoki.dll for Luna SA and C:\Program Files\LunaPCI\cryptoki.dll for Luna PCI and click Register.
- On successful registration you will receive a message as “Success registering the security library”.
- Double click Register HSM Slots on the left side of the pane.
- Enter the Slot (Partition) password.
- Click on Register Slot to register the slot for Domain\User. On successful registration you will receive the message “The slot was successfully and securely registered”.
- Also register the slot for NT_AUTHORITY\SYSTEM under Domain\User.
- Double click on the 630-010302-001_Alpha1.exe to Run it.
- It will create a zip file, extracts the zip file and replace the LunaCSP.dll and SafenetKSP.dll. Refer the Readme.txt for CSP and KSP installation and registry entries for Luna SA and Luna PCI.
- Restart the server after adding registry entry and replacing dlls to make sure that changes take effect.

1. Generating the SSL Certificate to use with Forefront Threat Management Gateway (TMG)

1.1 Create a SSL Certificate using Luna CSP

a) Log on to TMG-SRV as a domain administrator.
b) From the Start menu, select Run.
c) In the Run dialog, type mmc and click OK.
d) In the mmc console that appears, select File > Add/Remove Snap-in…
e) In the Add or Remove Snap-Ins dialog box, find the Certificates snap-in (under the Available snap-ins section) and select it.
f) Click Add, Select Computer Account and Click Next.
g) Select Local Computer, and click Finish.
h) Click OK and expand the Certificates under Console Root.
i) Right click on the Personal folder and select All Tasks -> Request New Certificate…
j) Click Next, Select Active Directory Enrollment Policy and then click Next. It will show you the certificate template you have configured, i.e. TMG
k) Click on More information is required to enroll for this certificate. Click here for configure settings link.
l) Certificate Properties window will open and select the Subject tab.
m) Select Common Name under Subject Name and provide the fully qualified domain name for the computer on which you are installing the certificate in the Value field and click Add. Repeat the same step for adding more values.
n) Click on General tab and provide the Friendly Name. For example SSL Certificate.
o) Click on Private Key tab, and verify that either Luna Cryptographic Services for Microsoft Windows or Luna enhanced RSA and AES provider for Microsoft Windows must be selected under the Cryptographic Service Provider.
p) Click on Certificate Authority tab, and make sure that Enterprise Root CA is selected.
q) Click Apply and then OK.
r) Select TMG certificate template or the certificate template you have configured, and click Enroll.
s) It will take some time to enroll, when enrollment succeeded, click Finish.

2. Configuring Forefront TMG to use Luna SA / Luna PCI for SSL Communication

2.1 Configure a server authentication certificate in IIS

a) Log on to TMG-SRV as a domain administrator.

b) From the Start menu, select All Programs, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.

c) In the console tree, click the root node that contains the name of the computer, click Default Web Site.

d) In the Actions pane, click Bindings.

e) In the Site Bindings dialog box, click Add.

f) In the Add Site Binding dialog box, select https in the Type drop-down list, select the certificate that you have generated using Luna CSP in the SSL certificate drop-down list, click OK, and then click Close.

g) Close the Internet Information Services (IIS) Manager console.

2.2 Creating a Web Listener for TMG Server

a) Log on to TMG-SRV as a domain administrator.

b) On the Forefront TMG server, click Start, point to All Programs, click Microsoft Forefront TMG, and then click Forefront TMG Management.

c) In the Forefront TMG console tree, expand Forefront TMG (TMG-SRV), and then click Firewall Policy.

d) Click the Toolbox tab, under Network Objects click New, and then click Web Listener.

e) On the Welcome to the New Web Listener Wizard page, in the Web listener name box, type SSL Listener (or any name you want), and then click Next.
f) On the Client Connection Security page, verify Require SSL secured connections with clients is selected, and then click Next.

g) On the Web Listener IP Addresses page, under Listen for incoming Web request on these networks, click Internal, and then click Select IP Addresses.

h) On the Internal Network Listener IP Selection page, click Specified IP addresses on the Forefront TMG computer in the selected network, under Available IP Addresses, click listed IP Address, click Add, and then click OK.

i) On the Web Listener IP Addresses page, click Next.

j) On the Listener SSL Certificates page, click Select Certificate.

k) In the Select Certificate window, click Select.

l) On the Listener SSL Certificates page, click Next.

m) On the Authentication Settings page, in the Select how clients will provide credentials to Forefront TMG drop-down list, click No Authentication, and then click Next.

n) On the Single Sign On Settings page, click Next.

o) On the Completing the New Web Listener Wizard page, confirm that the correct settings are specified, and then click Finish.

p) In the Forefront TMG console, click Apply to save changes and update the configuration.

q) In the Configuration Change Description window, for the Change description, type Create Web Listener for SSL Communication, and then click Apply.

r) In the Save Configuration Changes window, the update progress will be noted.

s) In the Save Configuration Changes window, verify that the configuration updates were saved, and then click OK.

2.3 Creating a Web Publishing Rule for TMG Server

a) On the Forefront TMG console tree, expand Forefront TMG (TMG-SRV), and then click Firewall Policy.

b) Click the Tasks tab, and then under Firewall Policy Tasks, click Publish Web Sites.

c) On the Welcome to the New Web Publishing Rule Wizard page, in the Web publishing rule name box, type Secure Web Site Access (or any name you want), and then click Next.

d) On the Select Rule Action page, select Allow, and then click Next.

e) On the Publishing Type page, verify that Publish a single Web site or load balancer is selected, and then click Next.

f) On the Server Connection Security page, click Use SSL to connect to the published Web server or server farm, and then click Next.

h) On the Internal Publishing Details page, in the Internal site name box, type TMG-SRV.lunatmg.com, select Use a computer name or IP address to connect to the published server, and in the Computer name or IP address box, type TMG-SRV.lunatmg.com, and then click Next.

i) On the Public Name Details page, in the Accept requests for drop-down list, select This domain name (type below), and in the Public name box, type TMG-SRV.lunatmg.com, and then click Next.

j) On the Select Web Listener page, in the Web listener drop-down list, select SSL Listener (or whichever you have configured), and then click Next.

k) On the Authentication Delegation page, in the Select the method used by Forefront TMG to authenticate to the published Web server drop-down list, select No delegation, but client may authenticate directly, and then click Next.

l) On the User Sets page, click Next.

m) On the Completing the New Web Publishing Rule Wizard page, verify the configuration, and then click Finish.

n) In the Forefront TMG console, click Apply to save changes and update the configuration.

o) In the Configuration Change Description window, for the Change description text box, type Create Web publishing rule for TMG Server, and then click Apply.
p) In the Save Configuration Changes window, the update progress will be noted.

q) In the Save Configuration Changes window, verify that the configuration updates were saved, and then click OK.

r) Restart the TMG-SRV to make sure that changes take effect.

2.4 Verifying that web site is opening on HTTPS port

a) Log on to TMG-SRV as a domain administrator.

b) On the Forefront TMG server, click Start, and then click Internet Explorer.

c) In the address bar, type https://<fully qualified domain name>, for example https://TMG-SRV.lunatmg.com

d) On the certificate navigation, click Continue to this website (Not Recommended). It will open the IIS Web Page display.

We have successfully created the Web Publishing Rule with SSL using the certificate whose keys are saved on Luna SA.