Apache v2.x and SafeNet PSG

Integration Guide

Preface

Part Number: 007-011146-001 (Rev A, 06/2010)

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.
SafeNet, Inc.

4690 Millennium Drive
Belcamp, Maryland 21017
USA

Limitations

This document does not include the detailed steps to set up the third-party software. The steps given in this document must be modified accordingly. Refer to **PSG** documentation for general 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

This document is intended to guide security administrators to install, configure and integrate Safenet protect server gold Hardware Security Module (HSM) with Apache Web Server.

Network Security Services (NSS) is a set of libraries designed to support cross-platform development of communications applications that support SSL, S/MIME, and other Internet security standards. NSS makes use of Netscape Portable Runtime (NSPR), a platform-neutral open-source API for system functions designed to facilitate cross-platform development.
This module was created so that the Apache web server can use the same security libraries as the former Netscape server products got acquired by Red Hat, notably the Fedora Directory Server (now called 389 Directory Server).
mod_nss was created to satisfy our needs for NSS support within Apache

SafeNet Protect Server Gold is a PCI-X compliant expansion card, which offers different performance levels to meet varied system requirements.

Protect Server Gold offers 4MB secure storage which offer a wide range of cryptographic services, including

- Encryption
- User and data authentication
- Message integrity
- Secure key storage and key management for eCommerce
- PKI
- Document managment
- Electronic Bill Presentation and Payment
- Database encryption
- Financial EFT transactions and more.

Audience

This document provides low-level details of how the Hardware Security Modules (HSM) (e.g. SafeNet PSG) can be made to work with Apache Web Server. You must have basic knowledge of using Apache server and PSG concepts to make full use of the recommendations in this document. This document is intended for:

- Developers and enterprise IT professionals who are planning or implementing a HSM deployment. This includes IT security administrators and IT personnel.

Scope

3rd Party Application Details

- Apache v2.x
- nss-3.12.4-with-nspr-4.8
- mod_nss-1.0.8

Supported Platforms

The following platforms are supported for PSG

- RHELv5.4
- Solaris 10 SPARC

HSMs and Firmware Version

- Fw 2.07
- PSG-220

Distributions

- ProtectToolkit C Release 3.33.00

Prerequisites

PSG Setup

Please refer to the **SafeNet PSG** documentation for installation steps and details regarding configuring and setting up the box on Linux systems in whatever mode (PCI or Network Mode) you want to use.
Brief installation summary is provided here:

- Check the items received to ensure none are missing. A separate page that lists the items included is provided for this purpose.
- Check the battery isolation link is placed for normal operation.
- If an external tamper detector is to be used, modify the printed circuit board accordingly.
- Install the Protect Server Gold in the host computer system.
- Install the PCI HSM Access Provider package that includes the device driver and confirm the correct operation of the adapter and driver installation.
- Run hsmstate command to ensure driver is running correctly or not.
- Install the SafeNet application programming interface (API) or net server software supplied with the product.
- Test HSM driver and library installed; token configured, key pair and certificate generated.

Apache web Server

Webserver package and webserver developer tools (httpd-devel) should be installed properly on Test machines (RHEL/Solaris).

Chapter 2
Integrating Apache2 and PSG using NSS

Installation of NSS, NSPR and mod_nss packages

1. Download and extract nss-3.12.4-with-nspr-4.8 (ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_12_4_RTM/src/nss-3.12.4-with-nspr-4.8.tar.gz), mod_nss-1.0.8 (http://directory.fedoraproject.org/wiki/Mod_nss) source trees.

2. Installation of NSS, NSPR and mod_nss packages.

   #cd /usr/src

   #mkdir nss

   #cd nss

   Extract nss-3.12.4-with-nspr-4.8.tar.gz

   # tar -zxf nss-3.12.4-with-nspr-4.8.tar.gz

   #cd nss-3.12.4-with-nspr-4.8/mozilla/security/nss

   # make nss_build_all

   #cd /usr/src

   Extract mod_nss-1.0.8.tar.gz

   #cd mod_nss-1.0.8

   RHEL5 x86
   # ./configure --with-nspr=/usr/src/nss/nss-3.12.4-with-nspr-4.8/mozilla/dist/Linux2.6_x86_glibc_PTH_DBG.OBJ/ --with-nss-lib=/usr/src/nss/nss-3.12.4-with-nspr-4.8/mozilla/dist/Linux2.6_x86_glibc_PTH_DBG.OBJ/lib/ --with-nss-inc=/usr/src/nss/nss-3.12.4-with-nspr-4.8/mozilla/dist/public/nss/ --with-apr-config

   Solaris10 SPARC
   ./configure --with-nspr=/usr/src/nss/nss-3.12.4-with-nspr-4.8/mozilla/dist/SunOS5.10_gcc_DBG.OBJ/ --with-nss-lib=/usr/src/nss/nss-3.12.4-with-nspr-4.8/mozilla/dist/SunOS5.10_gcc_DBG.OBJ/lib/ --with-nss-inc=/usr/src/nss/nss-3.12.4-with-nspr-4.8/mozilla/dist/public/nss/ --with-apr-config
   # make
   # make install

3. Set environment variable

   # export LD_LIBRARY_PATH=/opt/PTK/lib:$LD_LIBRARY_PATH
   RHEL 5.0 x86
   # export PATH=/opt/PTK/bin:/usr/src/nss/nss-3.12.4-with-nspr-4.8/mozilla/dist/Linux2.6_x86_glibc_PTH_DBG.OBJ/bin:$PATH

Solaris10 SPARC
export PATH=/opt/PTK/bin:/usr/src/nss/nss-3.12.4-with-nspr-4.8/mozilla/dist/SunOS5.10_gcc_DBG.OBJ /bin:$PATH

Certificate Generation

4. Certificate generation

   Certutil tool is included to automatically generate a self-signed CA plus one server certificate. This is fine for testing purposes but it is strongly recommended that a valid server certificate be obtained from a trusted CA before moving a mod_nss server into production.

   # certutil -N -d /etc/httpd/alias

   You should now have the following files:

   ```
   /etc/httpd/alias/cert8.db
   /etc/httpd/alias/key3db
   /etc/httpd/alias/secmod.db
   ```

   These 3 files make up an NSS certificate database.

Configuring the Safenet Hardware (PSG) for testing

5. Install the Safenet Protect Server Gold adapter board and software development kit.

   Initialize the adapter, user token and generate a self sign certificate using following commands

   eg.

   # ctconf –x # tamper the adapter (optional)

   Note: For testing PIN's are parsed to the commands, however all PIN's are 0000 (four times zero).you can take any value for PIN password.

   # ctconf -v -o0000 -u0000

   #ctconf -fdc -u0000 # set Netscape Compliant Mode flags on PSG

   #ctkmu t -s0 -l test -o0000 -u0000 # initialise slot 0

   Create a file "cert.cnf" with the following contents

   ```
   issuer
   {
      CN=test SSL cert
      OU=CA
      O=test
      C=US
   }
   subject
   {
      CN=test SSL
      OU=CA
      O=test
      C=US
   }
   serialnumber
   {
   ```

2009091101
}

Run the following command to generate a new keypair and a selfsigned certificate

#ctcert c -l ssl_self_signed -k -z 2048 -x cert.cnf -u 0000

6. Add the HSM to the NSS database

   # modutil -add PSG -libfile /opt/PTK/lib/libcryptoki.so -dbdir /etc/httpd/alias

7. Verify and list that the certificate is available:

   #certutil -L -d /etc/httpd/alias -h test

   #certutil -L -d /etc/httpd/alias -n test:ssl_self_signed

8. Show the information about the installed PKCS #11 modules installed as well as information on the corresponding tokens using the modutil tool.

   # modutil -dbdir /etc/httpd/alias/ -list

   Listing of PKCS #11 Modules
   ---
   1. NSS Internal PKCS #11 Module
      slots: 2 slots attached
      status: loaded

      slot: NSS Internal Cryptographic Services
      token: NSS Generic Crypto Services

      slot: NSS User Private Key and Certificate Services
      token: NSS Certificate DB

   2. PSG
      library name: /opt/PTK/lib/libcryptoki.so
      slots: 3 slots attached
      status: loaded

      slot: ProtectServer Gold:99644
      token: test

      slot: ProtectServer Gold
      token: AdminToken (401047)

Configuring the Apache HTTP Server to use the Safenet module

9. Modify /etc/httpd/conf.d/nss.conf to include:

   NSSNickname $SLOTNAME:$KEYNAME

   [Specify the nickname to be used for this the server certificate. Certificates stored in an NSS database are referred to using nicknames which makes accessing a specific certificate much easier. It is also possible to specify the certificate DN but it is easier to use a nickname. If the nickname includes spaces then the value needs to be enclosed in double quotes]

   NSSEnforceValidCerts off

   NSSCertificateDatabase //path of NSS certificate database//

[Specifies the location of the NSS certificate database to be used. An NSS certificate database consists of 3 files: cert8.db, key3.db and secmod.db. cert8.db stores certificates and Certificate Revocation Lists (CRLs), key3.db stores keys and secmod.db stores information about available pkcs#11 modules.]

e.g.

NSSNickname cisco_test:ssl_self_signed
NSSEnforceValidCerts off
NSSCertificateDatabase /usr/apache2/alias

Server Startup

10. Restart the apache web server
/etc/init.d/httpd restart

```
Please enter password for "internal" token:
```
After this you will be prompted for each token password of PSG HSM.

After that a connection to your webserver on port 443 shall present you a certificate.

References:

1. **http://directory.fedoraproject.org/wiki/Mod_nss**
2. **http://directory.fedoraproject.org/docs/mod_nss.html**
3. **https://developer.mozilla.org/en/NSS_reference/Building_and_installing_NSS/Build_instructions**