nurit

For 3-step authentication to strengthen the security of information assets

BaroPAM Solution Installation Summary (FreeRADIUS)

Jan, 2024

Ⅱ. Install BaroPAM FreeRADIUS

1. Install FreeRADIUS

1) First, BaroPAM must be installed.

See BaroPAM Installation Guide (Linux)

2) Install FeeRADIUS(Written based on the Redhat family)

```
[root]# dnf -y install freeradius freeradius-utils
```

When trying to uninstall FreeRADIUS installed → dnf -y erase freeradius freeradius-utils

3) Generate a certificate for EAP

```
[root]# cd /etc/raddb/certs
[root]# ./bootstrap
```

If you do not generate a certificate for EAP, you will receive the following error:

```
Failed reading private key file /etc/raddb/certs/server.pem
:error:06065064:digital envelope routines:EVP_DecryptFinal_ex:bad decrypt
rlm_eap_tls: Failed initializing SSL context
rlm_eap (EAP): Failed to initialise rlm_eap_tls
/etc/raddb/mods-enabled/eap[17]: Instantiation failed for module "eap"
```

Ⅱ. Install BaroPAM FreeRADIUS

2. FreeRADIUS settings

```
1) User and group updates
[root]# vi /etc/raddb/radiusd.conf
#user = radiusd
#group = radiusd
user = root
group = root

2) Enable logging for troubleshooting
[root]# [root]# vi /etc/raddb/radiusd.conf
auth = yes
auth_badpass = yes
auth_goodpass = yes

3) PAM settings
[root]# vi /etc/raddb/sites-enabled/default

#Pluggable Authentication Modules.
pam

4) Enable auth and reply logs
[root]# vi /etc/raddb/sites-enabled/default
 #       auth_log
        auth_log

#       reply_log
        reply_log

5) Enable PAM module
[root]# ln -s /etc/raddb/mods-available/pam /etc/raddb/mods-enabled/
```

Ⅱ. Install BaroPAM FreeRADIUS

2. FreeRADIUS settings

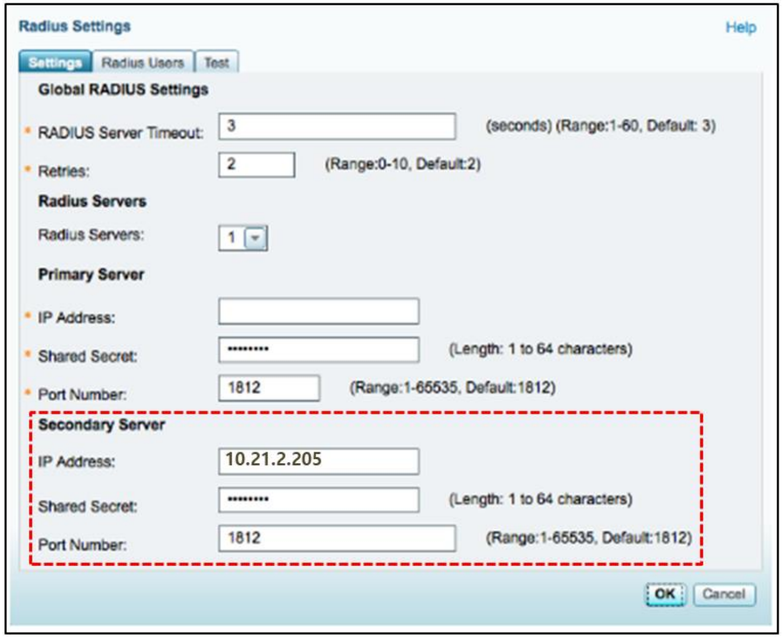
6) Client connection information settings

```
[root]# vi /etc/raddb/clients.conf

client 10.21.2.205 {
     ipaddr = 10.21.2.205     ipv4addr = *     # any. 10.21.2.205 == localhost
     secret = baropam
     require_message_authenticator = no
     nas_type = other
}
```

Basic setting

```
client localhost {
     ipaddr = 127.0.0.1     ipv4addr = *     # any. 127.0.0.1 == localhost
     secret = baropam
     require_message_authenticator = no
     nas_type = other
}
```



Radius Settings

Global RADIUS Settings

* RADIUS Server Timeout:	3	(seconds) (Range:1-60, Default: 3)
* Retries:	2	(Range:0-10, Default:2)

Radius Servers

Radius Servers: 1

Primary Server

* IP Address:		
* Shared Secret:	••••••••	(Length: 1 to 64 characters)
* Port Number:	1812	(Range:1-65535, Default:1812)

Secondary Server

IP Address:	10.21.2.205	
Shared Secret:	••••••••	(Length: 1 to 64 characters)
Port Number:	1812	(Range:1-65535, Default:1812)

7) Set authentication type

```
[root]# vi /etc/raddb/users

DEFAULT Group == "disabled", Auth-Type := Reject
Reply-Message = "Your account has been disabled."
DEFAULT Auth-Type := PAM
```

3. FreeRADIUS basic tests

```
1) Run in debug mode
[root]# radiusd -X
..
[ lines of configuration details]
}
Listening on auth address * port 1812 bound to server default
Listening on acct address * port 1813 bound to server default
Listening on auth address :: port 1812 bound to server default
Listening on acct address :: port 1813 bound to server default
Listening on auth address 127.0.0.1 port 18120 bound to server inner-tunnel
Listening on proxy address * port 45094
Listening on proxy address :: port 35184
Ready to process requests

2) Register users to test
[root]# $ useradd baropam
[root]# $ passwd baropam
Changing password for user baropam.
New password: nurit
Retype new password: nurit
passwd: all authentication tokens updated successfully.

3) Test with default settings → radtest <username> <pasword> <IP Addr> 0 <secret>
[root]# radtest baropam nurit localhost 0 baropam
Sent Access-Request Id 220 from 0.0.0.0:33872 to 127.0.0.1:1812 length 77
        User-Name = "baropam"
        User-Password = "nurit"
        NAS-IP-Address = 192.168.21.1
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "nurit"
Received Access-Accept Id 220 from 127.0.0.1:1812 to 0.0.0.0:0 length 20
```

Ⅱ. Install BaroPAM FreeRADIUS

4. Firewall settings

```
1) Install firewalld
[root]# dnf -y install firewalld

2) Enable firewalld
[root]# systemctl enable firewalld
[root]# systemctl start  firewalld

3) Allow port
[root]# firewall-cmd --permanent --zone=public --add-port=1812/udp
success
[root]# firewall-cmd --permanent --zone=public --add-port=1813/udp
success

4) Reload firewall
[root]# firewall-cmd --reload
success

5) Check if it works
[root]# systemctl status firewalld
* firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-01-09 20:35:10 KST; 14h ago
     Docs: man:firewalld(1)
 Main PID: 1009 (firewalld)
    Tasks: 2 (limit: 102061)
   Memory: 42.5M
   CGroup: /system.slice/firewalld.service
           `-1009 /usr/libexec/platform-python -s /usr/sbin/firewalld --nofork --nopid

Jan 09 20:35:09 vpntest systemd[1]: Starting firewalld - dynamic firewall daemon...
Jan 09 20:35:10 vpntest systemd[1]: Started firewalld - dynamic firewall daemon.
```

5. Preferences

1) BaroPAM settings

```
[root]# vi /etc/pam.d/radiusd
#%PAM-1.0
auth required /usr/baropam/pam_baro_auth.so forward_pass secret=/usr/baropam/radius/.${USER}_auth encrypt=no
```

2) Create directory to create BaroPAM configuration file

```
[root]# mkdir /usr/baropam/radius
[root]# cd /usr/baropam/radius
```

3) Copy BaroPAM configuration file (default)

```
[root]# cp ../.baro_auth .
```

Among the contents, the SECURE_KEY value "jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/" must be changed to "01012341234".

4) User(Login-ID) creation shell script(setuser.sh)

```
#!/bin/sh

export LANG=C
ENV_HOME=/usr/baropam/radius;
ACC_HOME=/home/$1

userdel -rf $1
₩rm ${ENV_HOME}/.$1_auth

useradd -d ${ACC_HOME} -m -s /bin/bash $1
echo $2 | passwd -stdin $1

₩cp ${ENV_HOME}/.baro_auth ${ENV_HOME}/.$1_auth

sed -i "s/01012341234/$3/g" ${ENV_HOME}/.$1_auth
```

Parameters when running the shell script that creates a user(Login-ID)
$1 : Login-ID to create
$2 : Login-ID's password
$3 : Login-ID phone number

```
[root]# sh setuser.sh baropam nurit 01027714076
```

Ⅱ. Install BaroPAM FreeRADIUS

5. Preferences

5) Shell script(setpasswd.sh) to change the password of a user(Login-ID)

```
#!/bin/sh

export LANG=C
echo $2 | passwd -stdin $1
```

Parameter when executing a shell script that changes the password of a user(Login-ID)
$1 : Login-ID
$2 : Change password

```
[root]# sh setpasswd.sh baropam !@Baropam#
```

6) Shell script(setphone.sh) that changes the phone number of a user(Login-ID)

```
#!/bin/sh

export LANG=C
ENV_HOME=/usr/baropam/radius;

sed -i "s/$2/$3/g" ${ENV_HOME}/.$1_auth
```

Parameter when executing a shell script that changes the phone number of the user(Login-ID)
$1 : Login-ID
$2 : Phone number before change
$3 : Phone number after change

```
[root]# sh setphone.sh baropam 01027714076 01012341234
```

7) Shell script(chgpasswd.sh) that changes the password and phone number of the user(Login-ID)

```
#!/bin/sh

export LANG=C

echo $2 | passwd -stdin $1
sed -i "s/$3/$4/g" ${ENV_HOME}/.$1_auth
```

Parameters when executing a shell script that changes the password/phone number of the user(Login-ID)
$1 : Login-ID
$2 : Change password
$3 : Phone number before change
$4 : Phone number after change

```
[root]# sh chgpasswd.sh baropam !@Baropam# 01027714076 01012341234
```

8) Shell script(deluser.sh) to delete a user(Login-ID)

```
#!/bin/sh
export LANG=C
ENV_HOME=/usr/baropam/radius;
ACC_HOME=/home/$1

userdel -rf $1
₩rm ${ENV_HOME}/.$1_auth
```

Parameters when executing a shell script to delete a user(Login-ID).
$1 : Login-ID to delete

```
[root]# sh deluser.sh baropam
```

6. Run FreeRADIUS

```
1) Create a RADIUS service for automatic startup
[root]# systemctl enable radiusd.service
Created symlink /etc/systemd/system/multi-user.target.wants/radiusd.service -> /usr/lib/systemd/system/radiusd.service.

2) Running the FreeRADIUS daemon
[root]# systemctl restart radius → Restart the daemon
[root]# systemctl start   radius → Start the daemon
[root]# systemctl stop    radius → Stop the daemon
[root]# systemctl status  radius → Status the daemon

3) Run the FreeRADIUS daemon, radiusd, in the background
[root]# radiusd -s &
[1] 1961

4) Check 1812, the UDP port used by radiusd, the FreeRADIUS daemon
[root]# netstat -an | grep 1812
udp        0      0 127.0.0.1:18120         0.0.0.0:*
udp        0      0 0.0.0.0:1812            0.0.0.0:*
udp6       0      0 :::1812                 :::*

5) Check logs authenticated by BaroPAM by linking FreeRADIUS
[root]# tail -f /var/log/secure
Mar 26 13:54:11 localhost radiusd(pam_baro_auth)[1857]: Try to update RATE_LIMIT line.[3 30 1616734451]
Mar 26 13:56:46 localhost radiusd(pam_baro_auth)[1857]: Try to update RATE_LIMIT line.[3 30 1616734606]
Mar 26 14:00:48 localhost radiusd(pam_baro_auth)[1934]: Try to update RATE_LIMIT line.[3 30 1616734848]
Mar 26 14:00:48 localhost radiusd(pam_baro_auth)[1934]: Invalid verification code
Mar 26 14:00:48 localhost radiusd[1934]: pam_unix(radiusd:auth): authentication failure; logname=root uid=0 euid=0 tty= ruser= rhost=
user=scjoo1
Mar 26 14:01:13 localhost radiusd(pam_baro_auth)[1934]: Try to update RATE_LIMIT line.[3 30 1616734873]
Mar 26 14:01:36 localhost radiusd(pam_baro_auth)[1934]: Try to update RATE_LIMIT line.[3 30 1616734873 1616734896]

Reference) FreeRADIUS related log files : /var/log/radius/radius.log
```

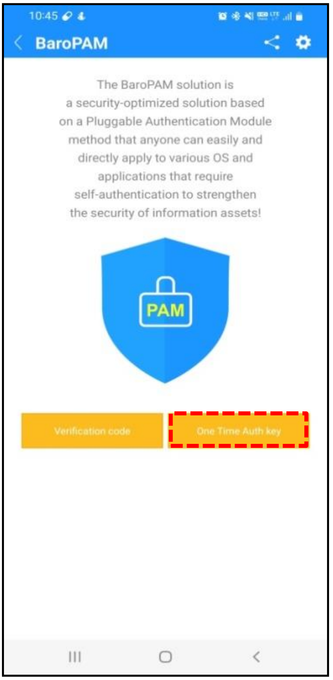
Ⅱ. Install BaroPAM FreeRADIUS

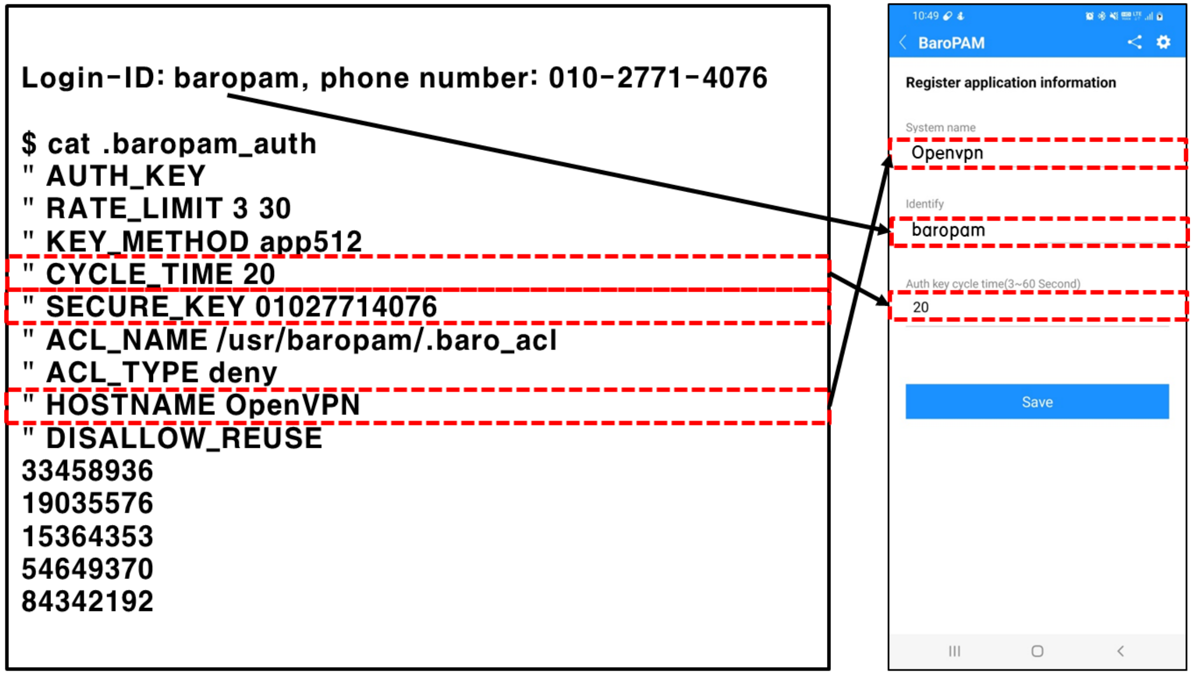
7. Install the BaroPAM app and set up information

BaroPAM App Download

Google Play

App Store


10:45
BaroPAM
The BaroPAM solution is a security-optimized solution based on a Pluggable Authentication Module method that anyone can easily and directly apply to various OS and applications that require self-authentication to strengthen the security of information assets!
PAM
Verification code
One Time Auth key



Login-ID: baropam, phone number: 010-2771-4076

```
$ cat .baropam_auth
" AUTH_KEY
" RATE_LIMIT 3 30
" KEY_METHOD app512
" CYCLE_TIME 20
" SECURE_KEY 01027714076
" ACL_NAME /usr/baropam/.baro_acl
" ACL_TYPE deny
" HOSTNAME OpenVPN
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```

Register application information

System name: Openvpn

Identify: baropam

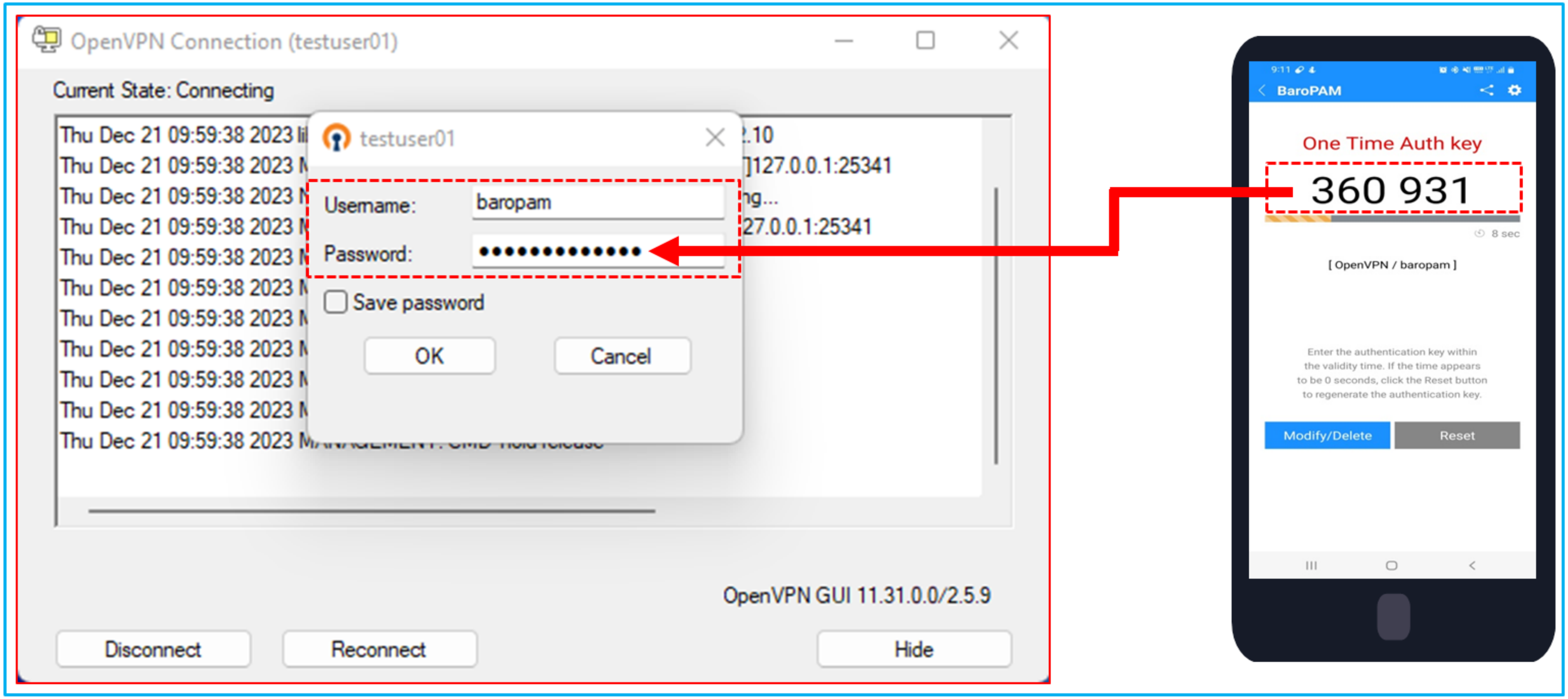
Auth key cycle time(3~60 Second): 20

BaroPAM app can be used on Android 6.0 (Marshmalliw) API 23, iOS 13.0 or higher, and does not support landscape mode. After installing the BaroPAM app, After installing the BaroPAM app, run the BaroPAM app, click the "One Time Auth key" button on the menu selection screen, and enter the "Cycle time, ID, and system name" set in the RADIUS user information in the "Register application information" screen of the BaroPAM app. You must enter the same information. If you set the app code (kr: Korean, en: English, jp: Japanese, cn: Chinese) on the BaroPAM app settings -> change screen settings screen, the BaroPAM app changes accordingly.

Message: The "OTA key" is incorrect because the date and time of the Android phone or iPhone are different from the current time.
Cause: This is caused by not using the time provided by the network for the Android or iPhone's date and time.
Action: For Android phones, go to "Settings" -> "General management" -> "Date and time" -> "Automatic date and time" and "Automatic time zone" -> "Allow" For iPhone, go to "Settings" -> "Date & Time" -> "Set Automatically" -> "Allow"

Message: If you cannot log in because the OTA key does not match.
Cause: BaroPAM is a time synchronization method, so the time of the phone and Server must be the same.
Action: Check if the phone and Servers time are correct.

8. User connection



OpenVPN Connection (testuser01)

Current State: Connecting

```
Thu Dec 21 09:59:38 2023 li                              .10
Thu Dec 21 09:59:38 2023 M                               ]127.0.0.1:25341
Thu Dec 21 09:59:38 2023 M                               ng...
Thu Dec 21 09:59:38 2023 M                               27.0.0.1:25341
Thu Dec 21 09:59:38 2023 M
Thu Dec 21 09:59:38 2023 M
Thu Dec 21 09:59:38 2023 M
Thu Dec 21 09:59:38 2023 M
Thu Dec 21 09:59:38 2023 M
Thu Dec 21 09:59:38 2023 M
Thu Dec 21 09:59:38 2023 MANAGEMENT: CMD 'hold release'
```

testuser01

Username: baropam

Password: ••••••••••••••

□ Save password

OpenVPN GUI 11.31.0.0/2.5.9

9:11

BaroPAM

One Time Auth key

360 931

8 sec

[OpenVPN / baropam]

Enter the authentication key within the validity time. If the time appears to be 0 seconds, click the Reset button to regenerate the authentication key.

Enter the RADIUS user account(Username), the password is "baropam", and the password created in the BaroPAM app on your smartphone.
If the One-Time Authentication key is "360931", enter "baropam360931" in the "Password:" field and click the "OK" button to use BaroPAM.
If authentication is successful by requesting authentication from the module, the connection is established.

nurit

Password you don't need to remember!
BaroPAM will be with you.

Thank You!

www.nurit.co.kr
mc529@nurit.co.kr