BaroPAM 가이드(FreeBSD)

목차

목차 0

1. BaroPAM 설치 1
   - 1.1 BaroPAM 설치 전 준비사항 1
   - 1.2 BaroPAM 설치 모듈 다운로드 1
   - 1.3 BaroPAM 환경 설정 파일 생성 2
   - 1.4 BaroPAM 환경 설정 6

2. BaroPAM 적용 12
   - 2.1 BaroPAM 적용 프로세스 12
   - 2.2 BaroPAM 적용 화면 12
   - 2.3 FreeBSD 로그인 방법 13
   - 2.4 ssh/sftp 접속 툴 14

3. BaroPAM 제거 20
   - 3.1 BaroPAM 환경 제거 20

4. BaroPAM FAQ 21

5. About BaroPAM 24

1. BaroPAM 설치

1.1 BaroPAM 설치 전 준비사항

PAM 모듈을 사용하기 위해서는 기본적으로 PAM 패키지가 반드시 설치되어 있어야 한다. 설치 확인은 다음의 명령어를 실행하여 확인한다.

```
[root] /root > ls /usr/lib/pam*
/usr/lib/pam_chroot.so          /usr/lib/pam_ksu.so             /usr/lib/pam_radius.so
/usr/lib/pam_chroot.so.6        /usr/lib/pam_ksu.so.6           /usr/lib/pam_radius.so.6
/usr/lib/pam_deny.so            /usr/lib/pam_lastlog.so         /usr/lib/pam_rhosts.so
/usr/lib/pam_deny.so.6          /usr/lib/pam_lastlog.so.6       /usr/lib/pam_rhosts.so.6
/usr/lib/pam_echo.so            /usr/lib/pam_login_access.so    /usr/lib/pam_rootok.so
/usr/lib/pam_echo.so.6          /usr/lib/pam_login_access.so.6  /usr/lib/pam_rootok.so.6
/usr/lib/pam_exec.so            /usr/lib/pam_nologin.so         /usr/lib/pam_securetty.so
/usr/lib/pam_exec.so.6          /usr/lib/pam_nologin.so.6       /usr/lib/pam_securetty.so.6
/usr/lib/pam_ftpusers.so        /usr/lib/pam_opie.so            /usr/lib/pam_self.so
/usr/lib/pam_ftpusers.so.6      /usr/lib/pam_opie.so.6          /usr/lib/pam_self.so.6
/usr/lib/pam_group.so           /usr/lib/pam_opieaccess.so      /usr/lib/pam_ssh.so
/usr/lib/pam_group.so.6         /usr/lib/pam_opieaccess.so.6    /usr/lib/pam_ssh.so.6
/usr/lib/pam_guest.so           /usr/lib/pam_passwdqc.so        /usr/lib/pam_tacplus.so
/usr/lib/pam_guest.so.6         /usr/lib/pam_passwdqc.so.6      /usr/lib/pam_tacplus.so.6
/usr/lib/pam_krb5.so            /usr/lib/pam_permit.so          /usr/lib/pam_unix.so
/usr/lib/pam_krb5.so.6          /usr/lib/pam_permit.so.6        /usr/lib/pam_unix.so.6
```

정보자산에 접속하여 PAM 모듈을 사용하기 위해서는 신뢰성 있고 안전한 ssh, sftp 서비스를 제공하기 위하여 OpenSSH(Open Secure Shell) 패키지가 반드시 설치되어 있어야 한다. 설치 확인은 다음의 명령어를 실행하여 확인한다. 만약, 설치되어 있지 않으면 "pkg install ssh" 명령어로 설치하면 된다.

```
[root] /root > ssh -V
OpenSSH_7.2p2, OpenSSL 1.0.2k-freebsd  26 Jan 2017
```

BaroPAM 인증 모듈을 다운로드 및 설치하기 위해서 root 계정으로 접속한 후 모듈을 다운로드 및 설치하기 위한 디렉토리(/usr/baropam)를 다음과 같이 생성한다.

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

BaroPAM 모듈을 다운로드 및 설치하기 위한 디렉토리의 권한(읽기, 쓰기, 실행)을 다음과 같이 부여한다.

```
[root]# chmod -R 777 /usr/baropam
```

1.2 BaroPAM 설치 모듈 다운로드

설치하고 하는 FreeBSD 시스템의 운영체제에 대한 이름 또는 시스템 정보, 커널 정보를 확인하기 위하여 root 계정으로 접속한 후 다음과 같은 명령어를 실행한다.

```
[root] /usr/baropam > uname -a
```

```
FreeBSD baropam 11.1-RELEASE-p15 FreeBSD 11.1-RELEASE-p15 #0: Thu Sep 27 06:05:25 UTC 2018
root@amd64-builder.daemonology.net:/usr/obj/usr/src/sys/GENERIC amd64
```

BaroPAM 인증 모듈은 root 계정으로 접속한 후 모듈을 다운로드 및 설치하기 위한 디렉토리(/usr/baropam)로 이동하여 모듈을 다운로드 하는 방법은 다음과 같다.

```
[root] /usr/baropam > wget http://nuriapp.com/download/libpam_baro_auth-x.x.tar
```

BaroPAM 인증 모듈의 다운로드가 완료되면 tar 파일의 압축을 해제하는 방법은 다음과 같다.

```
[root] /usr/baropam > tar -xvf libpam_baro_auth-x.x.tar
```

BaroPAM 인증 모듈의 압축을 해제하면 baropam 디렉토리에 다음과 같은 BaroPAM 관련 모듈이 생성된다.

```
[root] /usr/baropam > ls -al
합계 180
drwxrwxrwx  7 root   root   4096  8월 23 09:59 .
drwxr-xr-x 17 root   root   4096  2월 10  2017 ..
-r--r--r--  1 root   root      8  3월 24  2021 .baro_acl
-r--r--r--  1 root   root    305  7월  2 14:41 .baro_auth
-r--r--r--  1 root   root    290  6월 30 12:55 .baro_curl
-rwxr-xr-x  1 root   root  69149  4월  6 19:12 baro_auth
-rwxr-xr-x  1 root   root  65072  6월 29 16:36 baro_curl
drwxr-xr-x  2 root   root   4096  7월 20  2021 jilee
-rwxr-xr-x  1 root   root 152649  6월  9 08:19 pam_baro_auth.so
-rwxr-xr-x  1 root   root 116158  6월 30 12:54 pam_baro_curl.so
-rw-r--r--  1 root   root    221  6월 27 15:59 setauth.sh
-rw-r--r--  1 root   root    150  6월 29 16:29 setcurl.sh
```

생성한 BaroPAM 인증 모듈이 시스템에 맞는 모듈인지 다음과 같은 명령어를 실행하여 확인한다.

```
[root] /usr/baropam > file pam_baro_auth.so
pam_baro_auth.so: ELF 64-bit LSB shared object, x86-64, version 1 (FreeBSD), dynamically linked,
not stripped

[root] /usr/baropam > ldd pam_baro_auth.so
pam_baro_auth.so:
        libssl.so.7 => /usr/lib/libssl.so.7 (0x801607000)
        libcrypto.so.7 => /lib/libcrypto.so.7 (0x801873000)
        libpam.so.5 => /usr/lib/libpam.so.5 (0x801c68000)
        libz.so.6 => /lib/libz.so.6 (0x801e74000)
        libc.so.7 => /lib/libc.so.7 (0x80081f000)
```

1.3 BaroPAM 환경 설정 파일 생성

1) PAM 인증(.baro_auth)

PAM(Pluggable Authentication Module, 플러그 가능한 인증 모듈)은 Linux/Unix 시스템에서 서비스를 재컴파일하지 않고, 다양한 인증 기술을 시스템 항목 서비스에 접목할 수 있도록 해주는 프레임워크으로 중앙 집중적인 인증 매커니즘을 지원하는 것이다. 게다가 시스템의 기본적인 인증 기법을 제공하여 이것을

사용하면 응용 프로그램 개발자 뿐만 아니라 시스템 관리자들이 인증을 유연성 있게 관리할 수 있도록 도와 준다.

전통적으로 시스템 자원에 대한 접근을 관리하는 프로그램들은 내장된 메커니즘에 의해 사용자 인증 과정을 수행한다. 이러한 방식은 오랫동안 이루어졌지만 이러한 접근 방식은 확장성이 부족하고 매우 복잡하다.

BaroPAM 환경 설정 파일은 baro_auth 프로그램을 실행하여 반드시 생성하는데, BaroPAM 인증 모듈의 디렉토리인 /usr/baropam 밑에 위치하도록 한다.

형식)

```
baro_auth -r rate_limit -R rate_time -t cycle_time -k key_method -e encrypt_flag -H hostname -A
acl_type -a acl_filename -S secure_key -s filename
```

BaroPAM 환경설정 파일의 설정 옵션에 대한 내용은 다음과 같다.

옵션	설명	설정값	비고
-r	일회용 인증키의 제한횟수(1~10)	3	
-R	일회용 인증키의 제한시간(초, 15~600초)	30	
-t	일회용 인증키의 인증주기(초, 3~60초)	30	
-k	일회용 인증키의 인증방식(app1, app256, app384, app512: 앱).	app512	
-e	환경설정 파일의 암호화 여부(yes or no)	no	
-H	서버의 호스트명(uname -n)	nurit.co.kr	
-A	2차 인증에서 허용(allow) 또는 제외(deny)할지 선택	deny	
-a	2차 인증에서 허용(allow) 또는 제외(deny)할 계정에 대한 ACL 파일명(**파일 접근권한은 444**)	/usr/baropam/.baro_acl	
-S	반드시 벤더에서 제공하는 Secure key(라이선스 키)	jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/	
-s	BaroPAM 환경설정 파일을 생성할 디렉토리를 포함한 파일명	/usr/baropam/.baro_auth	

주의) -s 옵션의 filename는 BaroPAM 환경설정 파일을 생성할 디렉토리를 포함한 파일명(**파일 접근권한은 444**)이며, 설정한 서버의 호스트명(hostname)이 맞지 않는 경우 BaroPAM이 정상적으로 작동되지 않을 수 있으니, 호스트명(hostname)가 변경되는 경우 반드시 환경 설정의 해당 항목에 반영해야 한다.

사용 예)

```
[root] /usr/baropam > ./baro_auth -r 3 -R 30 -t 30 -k app512 -e no -H nurit.co.kr -A deny -a
/usr/baropam/.baro_acl -S jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/ -s /usr/baropam/.baro_auth
```

만약, 계정마다 BaroPAM 환경 설정파일을 각각 설정하는 경우 해당 계정으로 접속하여 작업을 진행한다. (Not root)

```
[root] /usr/baropam > ./baro_auth -r 3 -R 30 -t 30 -k app512 -e no -H nurit.co.kr -A deny -a
~/.baro_acl -S jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/ -s ~/.baro_auth
```

1) Your emergency one-time authentication keys are :
 응급 일회용 인증키는 일회용 인증키 생성기인 BaroPAM 앱을 사용할 수 없을 때 분실한 경우를 대비하여 SSH 서버에 다시 액세스하는데 사용할 수 있는 접속이 가능한 Super 인증키 이므로 어딘가에 적어 두는 것이 좋다.

2) 다음에 나오는 물음에 대해서는 모두 "y"를 입력한다.
 중간자(man-in-the-middle) 공격을 예방할 것인가? y
 같은 일회용 인증키는 하나의 계정 외에 다른 계정에도 로그인이 가능하게 할 것인가? y

일회용 인증키의 제한 시간을 30초로 지정할 것인가? y

BaroPAM 환경 설정 파일인 .baro_auth에 설정한 내용은 다음과 같다.

```
[root] /usr/baropam > cat .baro_auth
" AUTH_KEY
" RATE_LIMIT 3 30
" KEY_METHOD app512
" CYCLE_TIME 30
" SECURE_KEY jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/
" ACL_NAME /usr/baropam/.baro_acl
" ACL_TYPE deny
" HOSTNAME nurit.co.kr
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```

BaroPAM 환경설정 파일인 .baro_auth의 설정 항목에 대한 내용은 다음과 같다.

항목	설명	설정값	비고
AUTH_KEY	인증 구분자(고정)		
RATE_LIMIT	일회용 인증키의 제한횟수(1~10), 제한시간(초, 15~600초)	3 30	
KEY_METHOD	일회용 인증키의 인증방식(app1, app256, app384, app512: 앱)	app512	
CYCLE_TIME	일회용 인증키의 인증주기(초, 3~60초)	30	
SECURE_KEY	반드시 벤더에서 제공하는 Secure key(라이선스 키)	jlqlcHbVqdpj7b4PzBpM2DileBvmHFV/	
HOSTNAME	서버의 호스트명(uname -n)	nurit.co.kr	
ACL_TYPE	2차 인증에서 허용(allow) 또는 제외(deny) 구분	deny	
ACL_NAME	2차 인증에서 허용 또는 제외할 계정에 대한 ACL Filename(파일 접근권한은 444)	/usr/baropam/.baro_acl	
DISALLOW_REUSE or ALLOW_REUSE	중간자(man-in-the-middle) 공격을 예방할 경우는 "DISALLOW_REUSE"을 설정한 경우 일회용 인증키의 인증주기 동안은 다른 사용자가 로그인 할 수 없으며, 만약 허용할 경우는 "ALLOW_REUSE"을 설정한다.	DISALLOW_REUSE	

2) cURL 인증(.baro_curl)

curl의 명칭은 "client URL"을 대표하는 것으로 1997년에 처음 출시되었다. 즉 클라이언트가 스크립트로써 서버에 데이터를 요청하는 것으로 BaroPAM은 curl로 http/https 되어 있는 인증 사이트를 호출하여 인증을 요청한다.

BaroPAM 환경 설정 파일은 baro_curl 프로그램을 실행하여 반드시 생성하는데, BaroPAM 인증 모듈의 디렉토리인 /usr/baropam 밑에 위치하도록 한다.

형식)

```
baro_curl -r rate_limit -R rate_time -t cycle_time -k key_method -e encrypt_flag -H hostname -u
auth_url -s filename
```

BaroPAM 환경설정 파일의 설정 옵션에 대한 내용은 다음과 같다.

옵션	설명	설정값	비고
-r	일회용 인증키의 제한횟수(1~10)	3	
-R	일회용 인증키의 제한시간(초, 15~600초)	30	
-t	일회용 인증키의 인증주기(초, 3~60초)	30	
-k	일회용 인증키의 인증방식(app1, app256, app384, app512: 앱).	app512	
-e	환경설정 파일의 암호화 여부(yes or no)	no	
-H	서버의 호스트명(uname -n)	nurit.co.kr	
-u	호출할 URL로 호스트명(hostname), 사용자 계정(username), 인증주기(cycle_time), 일회용 인증키(auth_key) 등의 파라미터가 포함되어 호출	http://1.23.456.789/baropam/web/result_curl.jsp	
-s	BaroPAM 환경설정 파일을 생성할 디렉토리를 포함한 파일명	/usr/baropam/.baro_curl	

주의) -s 옵션의 filename는 BaroPAM 환경설정 파일을 생성할 디렉토리를 포함한 파일명(**파일 접근권한은 444**)이며, 설정한 서버의 호스트명(hostname)이 맞지 않는 경우 BaroPAM이 정상적으로 작동되지 않을 수 있으니, 호스트명(hostname)가 변경되는 경우 반드시 환경 설정의 해당 항목에 반영해야 한다.

사용 예)

```
[root] /usr/baropam > ./baro_curl -r 3 -R 30 -t 30 -k app512 -e no -H nurit.co.kr -u
http://1.23.456.789/baropam/web/result_curl.jsp -s /usr/baropam/.baro_curl
```

1) 다음에 나오는 물음에 대해서는 모두 "y"를 입력한다.
   중간자(man-in-the-middle) 공격을 예방할 것인가? y
   같은 일회용 인증키는 하나의 계정 외에 다른 계정에도 로그인이 가능하게 할 것인가? y
   일회용 인증키의 제한 시간을 30초로 지정할 것인가? y

BaroPAM 환경 설정 파일인 .baro_curl에 설정한 내용은 다음과 같다.

```
[root] /usr/baropam > cat .baro_curl
" AUTH_KEY
" RATE_LIMIT 3 30
" AUTH_URL http://1.23.456.789/baropam/web/result_curl.jsp
" KEY_METHOD app512
" CYCLE_TIME 30
" HOSTNAME baropam
" DISALLOW_REUSE
```

BaroPAM 환경설정 파일인 .baro_curl의 설정 항목에 대한 내용은 다음과 같다.

항목	설명	설정값	비고
AUTH_KEY	인증 구분자(고정)		
RATE_LIMIT	일회용 인증키의 제한횟수(1~10), 제한시간(초, 15~600초)	3 30	
AUTH_URL	호출할 URL로 호스트명(hostname), 사용자 계정(username), 인증주기(cycle_time), 일회용 인증키(auth_key) 등의 파라미터가 포함되어 호출	http://1.23.456.789/baropam/web/result_curl.jsp	
KEY_METHOD	일회용 인증키의 인증방식(app1, app256, app384, app512: 앱)	app512	

CYCLE_TIME	일회용 인증키의 인증주기(초, 3~60초)	30	
HOSTNAME	서버의 호스트명(uname -n)	nurit.co.kr	
DISALLOW_REUSE or ALLOW_REUSE	중간자(man-in-the-middle) 공격을 예방할 경우는 "DISALLOW_REUSE"을 설정한 경우 일회용 인증키의 인증주기 동안은 다른 사용자가 로그인 할 수 없으며, 만약 허용할 경우는 "ALLOW_REUSE"을 설정한다.	DISALLOW_REUSE	

1.4 BaroPAM 환경 설정

1) PAM 인증

PAM(Pluggable Authentication Module, 플러그 가능한 인증 모듈)은 Linux/Unix 시스템에서 서비스를 재컴파일하지 않고, 다양한 인증 기술을 시스템 항목 서비스에 접목할 수 있도록 해주는 프레임워크으로 중앙 집중적인 인증 매커니즘을 지원하는 것이다. 게다가 시스템의 기본적인 인증 기법을 제공하여 이것을 사용하면 응용 프로그램 개발자 뿐만 아니라 시스템 관리자들이 인증을 유연성 있게 관리할 수 있도록 도와 준다.

전통적으로 시스템 자원에 대한 접근을 관리하는 프로그램들은 내장된 메커니즘에 의해 사용자 인증 과정을 수행한다. 이러한 방식은 오랫동안 이루어졌지만 이러한 접근 방식은 확장성이 부족하고 매우 복잡하다.

① 추가 인증(로그인-ID, 비밀번호 이외의 추가 인증으로 일회용 인증키 적용)

BaroPAM 모듈을 설정하기 위해서 sshd, su 파일에 설정하는 방법은 다음과 같이 최 상단에 입력해 준다.

```
[root] /usr/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth       required      /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth
encrypt=no
```

참고로 secret 파라미터는 BaroPAM 환경설정 파일명, encrypt 파라미터는 BaroPAM 환경설정 파일의 암호화 플래그(yes or no)를 설정한다.

만약, 계정마다 BaroPAM 환경 설정파일을 각각 설정하는 경우 BaroPAM 모듈을 설정하기 위해서 sshd 파일에 설정하는 방법은 다음과 같이 최 상단에 입력해 준다.

```
[root] /usr/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth       required      /usr/baropam/pam_baro_auth.so nullok secret=${HOME}/.baro_auth encrypt=no
```

계정마다 BaroPAM 환경 설정파일을 각각 설정하지 않고 특정 디렉토리에 계정별로 BaroPAM 환경 설정파일을 다르게 설정하고자 하는 경우 BaroPAM 모듈을 설정하기 위해서 sshd 파일에 설정하는 방법은 다음과 같이 최 상단에 입력해 준다.

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

* "nullok"는 호출된 PAM 모듈이 null 값의 암호를 입력하는 것을 허용한다는 의미다.

```
[root] /usr/baropam > vi /etc/pam.d/su
#%PAM-1.0
auth          required        /usr/baropam/pam_baro_auth.so  nullok  secret=/usr/baropam/.baro_auth
encrypt=no
```

/etc/pam.d/su 파일에 BaroPAM 모듈을 최 상단에 추가하면 "su" 명령어로 일반계정이 "root"로 권한 상승을 시도하는 경우에도 2차 인증(추가 인증)을 적용할 수 있어서 보안이 한층 더 향상된다.

```
$ su - root
Verification code:
```

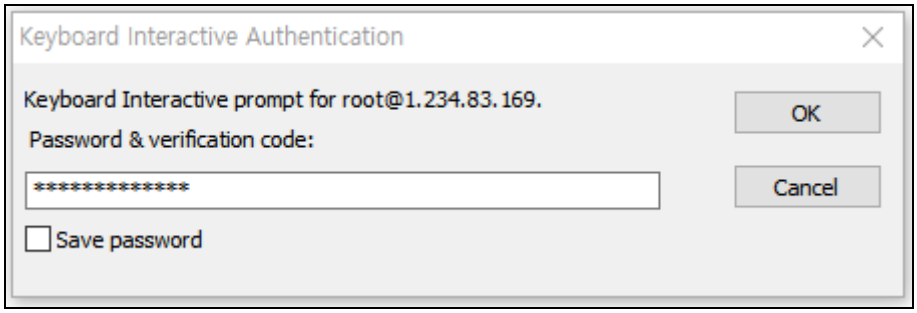
참고) 개방형OS 같은 Desktop Linux인 경우는 "passwd -p *username*" 명령어로 비밀번호를 제거하면 "Verification code"의 입력하는 화면에 일회용 인증키만 입력하면 비밀번호는 묻지 않는다.

② 비밀번호 대체(비밀번호를 대신 일회용 인증키로 대체)

filezilla처럼 "Interactive process"가 불가능한 프로그램들을 위해서는 PAM에서 forward_pass 옵션을 사용하여 암호 입력 시에 일회용 인증키를 입력하도록 하는 수밖에 없다. 이 경우, openssh client나 Windows의 RDP(Remote Desktop Protocol), Radius, filezilla 등 모두 이렇게 입력을 하는 수밖에 없다.

```
[root] /usr/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth       required      /usr/baropam/pam_baro_auth.so forward_pass secret=/usr/baropam/.baro_auth
encrypt=no
```

forward_pass를 이용하여 암호 입력창(Password & verification code:)에 일회용 인증키를 입력하면 된다. 예를 들어, 일회용 인증키가 "123456" 이라면 "123456"만 입력하면 된다.



참고) 비밀번호를 일회용 인증키로 대체하는 경우 해당 계정의 비밀번호는 "passwd *username*" 명령어로 미리 로그인-ID와 동일하게 설정해야 한다.

개방형OS 같은 Desktop Linux인 경우는 "passwd -p *username*" 명령어로 비밀번호를 제거하면 "Password & Verification code"의 입력하는 화면에 일회용 인증키만 입력하면 비밀번호는 묻지 않는다.

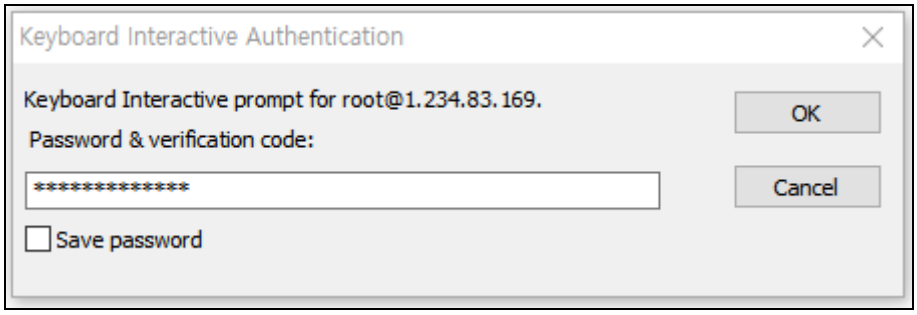
③ 새로운 비밀번호(비밀번호와 일회용 인증키 결합하여 비밀번호를 일회용 인증키 생성주기별로 새로운 일회용 비밀번호를 생성하여 적용)

filezilla처럼 "Interactive process"가 불가능한 프로그램들을 위해서는 PAM에서 forward_pass 옵션을 사용하여 암호 입력 시에 암호와 일회용 인증키를 같이 입력하도록 하는 수밖에 없다. 이 경우, openssh client나 Windows의 RDP(Remote Desktop Protocol), VMWare Horizon, filezilla 등 모두 이렇게 입력을

하는 수밖에 없다.

```
[root] /usr/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth       required     /usr/baropam/pam_baro_auth.so forward_pass secret=/usr/baropam/.baro_auth
encrypt=no
```

forward_pass를 이용하여 암호 입력창(Password & verification code:)에 암호와 같이 일회용 인증키를 입력할 경우, 암호를 먼저 입력하고 공백 없이 이어서 일회용 인증키를 입력하면 된다. 예를 들어 암호가 "baropam" 이고 일회용 인증키가 "123456" 이라면 "baropam123456"으로 입력하면 된다.



forward_pass를 이용하면 인증을 필요로 하는 대부분의 서비스에 2-factor 인증을 가능하게 할 수 있다.

2) cURL 인증

BaroPAM 모듈을 설정하기 위해서 sshd, su, sudo 파일 등에 설정하는 방법은 다음과 같이 최 상단에 입력해 준다.

```
[root] /usr/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth       required     /usr/baropam/pam_baro_curl.so nullok secret=/usr/baropam/.baro_curl
encrypt=no
```

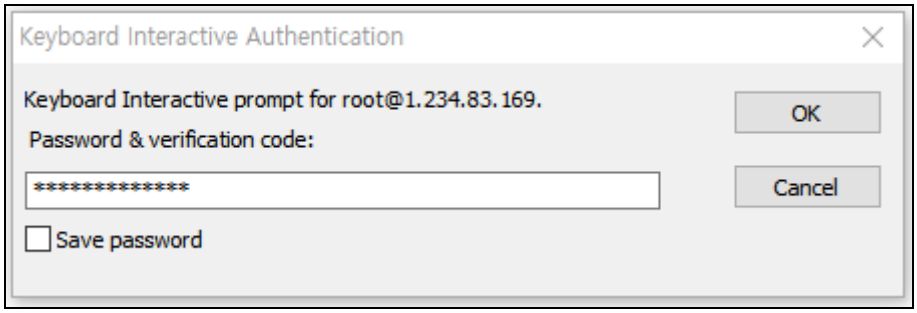
참고로 secret 파라미터는 BaroPAM 환경설정 파일명, encrypt 파라미터는 BaroPAM 환경설정 파일을 암복호 플래그(yes or no) 설정한다.

* "nullok"는 호출된 PAM 모듈이 null 값의 암호를 입력하는 것을 허용한다는 의미다.

filezilla처럼 "Interactive process"가 불가능한 프로그램들을 위해서는 PAM에서 forward_pass 옵션을 사용하여 암호 입력 시에 암호와 일회용 인증키를 같이 입력하도록 하는 수밖에 없다. 이 경우, openssh client나 Windows의 RDP(Remote Desktop Protocol), Radius, filezilla 등 모두 이렇게 입력을 하는 수밖에 없다.

```
[root] /usr/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
auth       required     /usr/baropam/pam_baro_curl.so forward_pass secret=/usr/baropam/.baro_curl
encrypt=no
```

forward_pass를 이용하여 암호 입력창(Password & verification code:)에 암호와 같이 일회용 인증키를 입력할 경우, 암호를 먼저 입력하고 공백 없이 이어서 일회용 인증키를 입력하면 된다. 예를 들어 암호가 "baropam" 이고 일회용 인증키가 "123456" 이라면 "baropam123456"으로 입력하면 된다.



forward_pass를 이용하면 인증을 필요로 하는 대부분의 서비스에 2-factor 인증을 가능하게 할 수 있다.

```
[root] /usr/baropam > vi /etc/pam.d/su
#%PAM-1.0
auth        required      /usr/baropam/pam_baro_curl.so forward_pass secret=/usr/baropam/.baro_curl
encrypt=no
```

/etc/pam.d/su 파일에 BaroPAM 모듈을 최 상단에 추가하면 "su" 명령어로 일반계정이 "root"로 권한 상승을 시도하는 경우에도 2차 인증(추가 인증) 입력을 적용할 수 있어서 보안이 한층 더 향상된다.

```
$ su - root
Password & verification code:
```

Desktop Linux 인 경우 GUI 로그인 화면에서 BaroPAM을 사용하고자 하는 경우 설정하는 방법은 다음과 같이 최 상당에 입력해 준다.

3) sshd 데몬의 환경 설정

sshd 데몬 설정을 위한 설정 파일인 "/etc/ssh/sshd_config" 파일의 내용 중 다음과 같은 인자는 변경이 필요하다.

인자	기존	변경	비고
PasswordAuthentication	yes	no	
ChallengeResponseAuthentication	no	yes	
UsePAM	no	yes	

sshd 설정이 끝나면 반드시 PAM 모듈이 제대로 추가되었는지 확인한 후 SSH Server의 Restart 작업이 반드시 필요하다.

```
[root] /usr/baropam > /etc/rc.d/sshd restart
erforming sanity check on sshd configuration.
Stopping sshd.
Performing sanity check on sshd configuration.
Starting sshd.
```

sshd 설정이 끝나면 반드시 PAM 모듈이 제대로 추가되었는지 확인한 후 ssh 데몬을 재부팅해야 한다.

4) ACL(Access Control list) 설정

BaroPAM 모듈 사용 시 2차 인증에서 제외할 계정에 대한 ACL에 제외해야 하는 경우 BaroPAM 환경 설정 시 설정한 디렉토리에 ACL 파일을 생성한 후 제외할 계정을 다음과 같이 입력한다. (.baro_acl에 대한 파일

접근권한을 444로 설정해야 한다.)

```
[root] /usr/baropam > vi .baro_acl
barokey
baropam
```

5) NTP(Network Time Protocol) 설정

정보자산의 시간이 현재 시간과 다를 경우 일회용 인증키와 매칭이 되지 않아 일회용 인증키가 맞질 않으므로 시간을 같게 초기화 하는 방법은 crontab에 다음과 같이 설정한 후 crontab을 restart하면 된다.

```
#Time setting
11 4 * * * /usr/bin/rdate -s time.simplexi.com; /sbin/hwclock —systohc
or
11 4 * * * /usr/bin/rdate -s time.bora.net;
```

정보자산의 시간이 현재 시간과 다를 경우 일회용 인증키와 매칭이 되지 않아 일회용 인증키가 맞질 않으므로 정보자산을 설치할 때 시간대(타임존;Timezone)를 맞추지 않으면, 컴퓨터 시계가 미국 태평양 시간인 PST로 나온다. (서머타임 기간에는 PDT.) 즉 캘리포니아 시간으로 나온다. 이것을 한국 표준시인 KST로 다음과 같이 변경해야 한다.

```
> ln -sf /usr/share/zoneinfo/Asia/Seoul /etc/localtime
> date 1804191024.00
```

최근에는 정보자산에 대한 시간 동기화(타임서버 시간 동기화)하는 방법으로 NTP(Network Time Protocol)을 이용하여 root 계정에서 시스템의 시각을 현재 시각으로 설정할 수 있다.

NTP를 사용하기 위해서는 기본적으로 NTP 패키지가 반드시 설치되어 있어야 한다. 설치 확인은 다음의 명령어를 실행하여 확인한다. 만약, 설치되어 있지 않으면 "pkg install ntp" 명령어로 설치하면 된다.

```
[root]# pkg install ntp
```

ntpd 서비스를 활성화 하기 위해서는 다음 같은 명령어를 사용하여 "/etc/rc.conf"에 등록 해야 한다.

```
[root]# /etc/rc.d/ntpd enabled
```

우리나라에서 운영되고 있는 NTP 서버는 다음과 같다.

```
server kr.pool.ntp.org
server time.bora.net
```

우리나라에서 운영되고 있는 NTP 서버를 ntpd 데몬 설정을 위한 설정 파일인 "/etc/ntp.conf"에 다음과 같이 설정한다.

```
[root]# vi /etc/ntp.conf
#
# NTP
#
server kr.pool.ntp.org iburst
server time.bora.net   iburst
```

iburst 옵션은 일종의 옵션 설정으로써 동기화 하는데 걸리는 시간을 짧게 줄여주는 옵션임.

ntpd 데몬 설정을 위한 설정이 끝나면 반드시 NTP 설정이 제대로 추가되었는지 확인한 후 NTP 데몬의 Restart 작업이 반드시 필요하다.

```
[root]# /etc/rc.d/ntpd restart
ntpd not running? (check /var/run/ntpd.pid).
Starting ntpd.
```

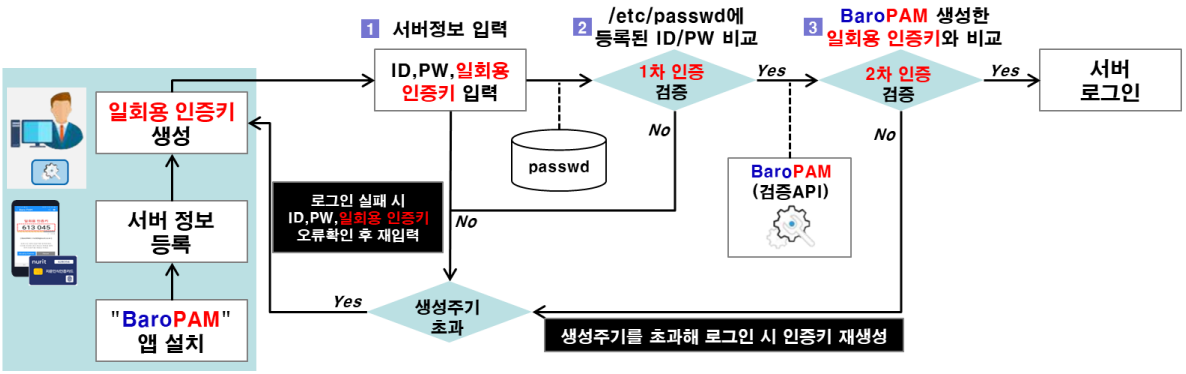
ntpd 시간 확인은 다음과 같은 명령어로 확인할 수 있다.

```
[root]# ntpq -p
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 0.freebsd.pool. .POOL.          16 p    -   64    0    0.000    0.000   0.000
 106.247.248.106 141.223.182.106  2 u    7   64    1    4.412    0.544   0.000
 time.bora.net   204.123.2.5      2 u    7   64    1    5.206    7.741   0.000
*send.mx.cdnetwo 204.123.2.5      2 u    1   64    1    3.968    3.807   0.446
 211.52.209.148  216.239.35.12    2 u    1   64    1   11.862    2.838   0.259
 dadns.cdnetwork 204.123.2.5      2 u    2   64    1    4.833    0.005   0.408
 92.223.73.5 (st 106.247.248.106  3 u    -   64    1    5.015    1.397   0.482
```

* 표시된 ip가 현재 시간을 가져오고 있는 ntp 서버임

2. BaroPAM 적용

2.1 BaroPAM 적용 프로세스

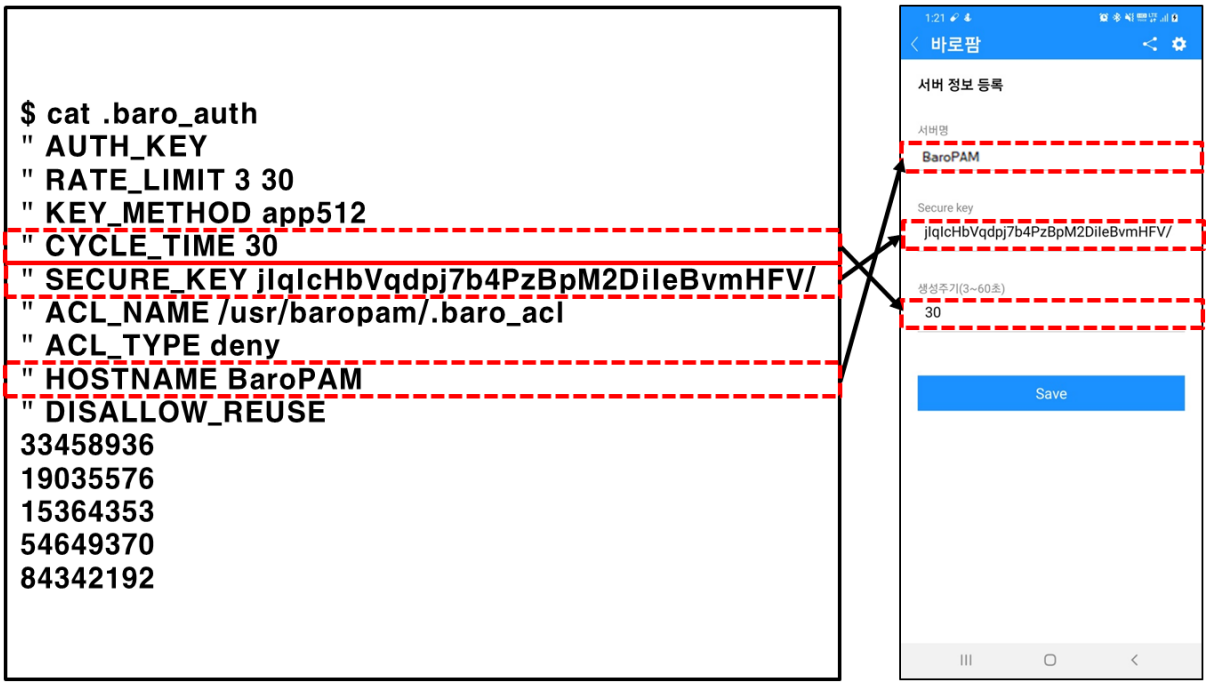


No	구분	내용	설명
1	2차 인증 앱 (BaroPAM)	BaroPAM 앱 다운로드 및 설치	-안드로이드폰: 구글 플레이스토어 접속 및 "바로팜" 앱 다운로드 -아이폰: 애플 앱스토어 접속 및 "BaroPAMs" 앱 다운로드
2		BaroPAM 앱 실행	
3		"인증 코드" 버튼 선택	-실행된 앱 하단 왼쪽 버튼 선택
4		서버 정보 등록	-시스템명: 서버 명칭(임의 등록 가능) -Secure key: 서버에 부여된 Secure key(벤더발급) -생성주기: 3~60초 사이 입력
5		저장 후 목록 조회 시 나오는 항목 클릭, 일회용 인증키 생성	
6		서버에 접속해 ID, PW, 일회용 인증키를 입력해 로그인	-Secure key, 생성주기, 일회용 인증키를 이용해 2차 인증 검증

2.2 BaroPAM 적용 화면

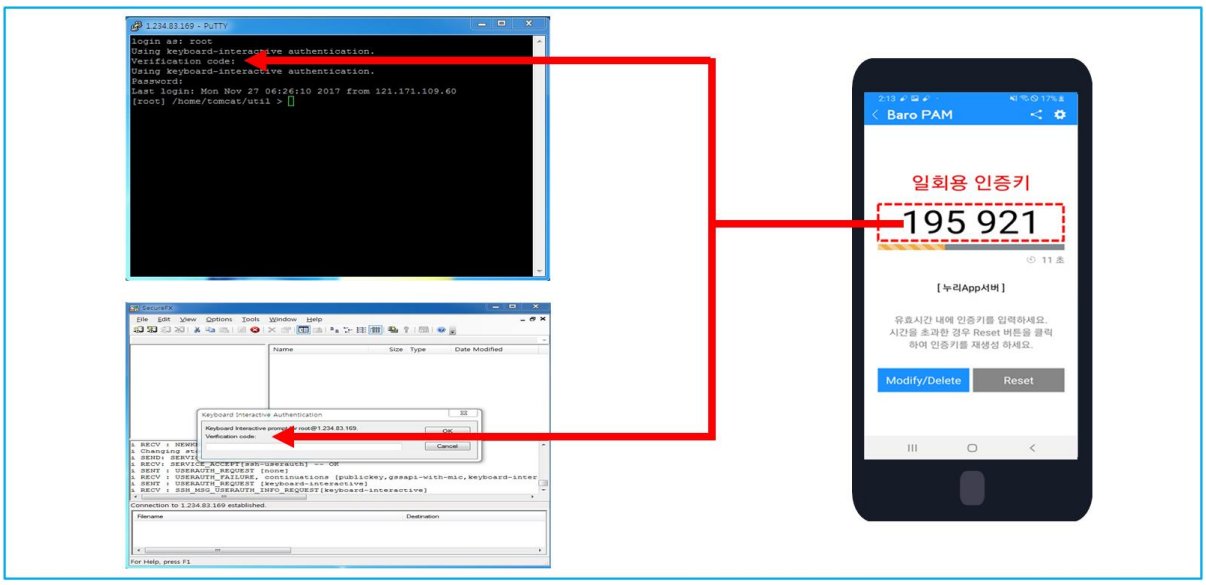
2.3 FreeBSD 로그인 방법

먼저, "BaroPAM Setup" 화면에서 입력한 "**인증주기, Secure key, 서버명**"을 "BaroPAM" 앱의 "**서버 정보 등록**" 화면에서 동일하게 입력해야 한다.



FreeBSD 환경에 로그인 시 사용자 계정(Username)을 입력하고, 스마트 폰의 "BaroPAM" 앱에서 **일회용 인증**

키를 생성한 후 "Verification code"에 생성한 일회용 인증키와 "Password"를 입력한 후 "Enter" 버튼을 클릭하면 BaroPAM 모듈에 인증을 요청하여 검증이 성공하면 FreeBSD의 로그인 인증 정책이 적용된다.



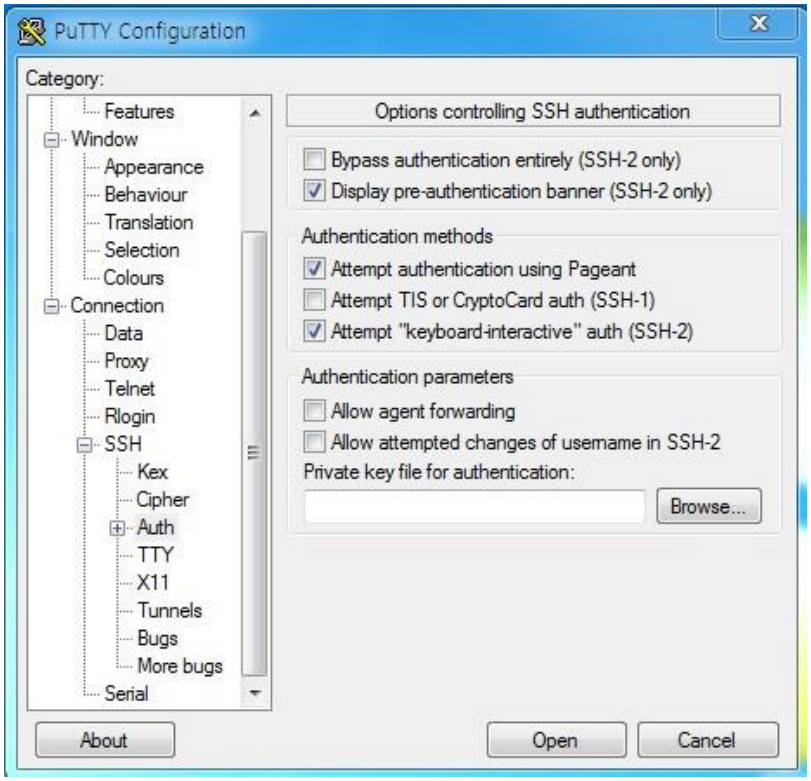
FreeBSD의 로그인 화면에서 입력한 일회용 인증키를 BaroPAM 검증모듈에서 인증에 실패하면 "Access denied." 메시지가 로그인 화면에 나타난다. BaroPAM의 인증과 관련한 각종 메시지는 syslog에 남긴다.

```
Mar 25 11:10:42 qsh-0415 sshd[27482]: pam_unix(sshd:session): session closed for user root
Mar 25 13:52:25 qsh-0415 sshd(pam_baro_auth)[2052]: Try to update RATE_LIMIT line.[3 30 1648183945]
Mar 25 13:52:45 qsh-0415 sshd[2050]: Accepted keyboard-interactive/pam for root from 222.108.117.41 port 49835 ssh2
Mar 25 13:52:45 qsh-0415 sshd[2050]: pam_unix(sshd:session): session opened for user root by (uid=0)
Mar 25 15:25:47 qsh-0415 sshd(pam_baro_auth)[14119]: Try to update RATE_LIMIT line.[3 30 1648189547]
Mar 25 15:25:49 qsh-0415 sshd(pam_baro_auth)[14119]: Verification code generation failed.[Success]
Mar 25 15:25:49 qsh-0415 sshd(pam_baro_auth)[14119]: Invalid verification code
Mar 25 15:25:51 qsh-0415 sshd[14118]: Received disconnect from 222.108.117.41: 13: The user canceled au
```

2.4 ssh/sftp 접속 툴

putty인 경우)

Putty로 접속할 때 보통 접속 과정과 동일하게 해주시면 되는데, 하나 설정해 주어야 할 것이 있다. 환경 설정에서 "connection -> SSH -> auth"에서 attempt "Keyboard-Interactive" auth(SSH-2)를 선택한 후 SSH 접속을 하면 된다.

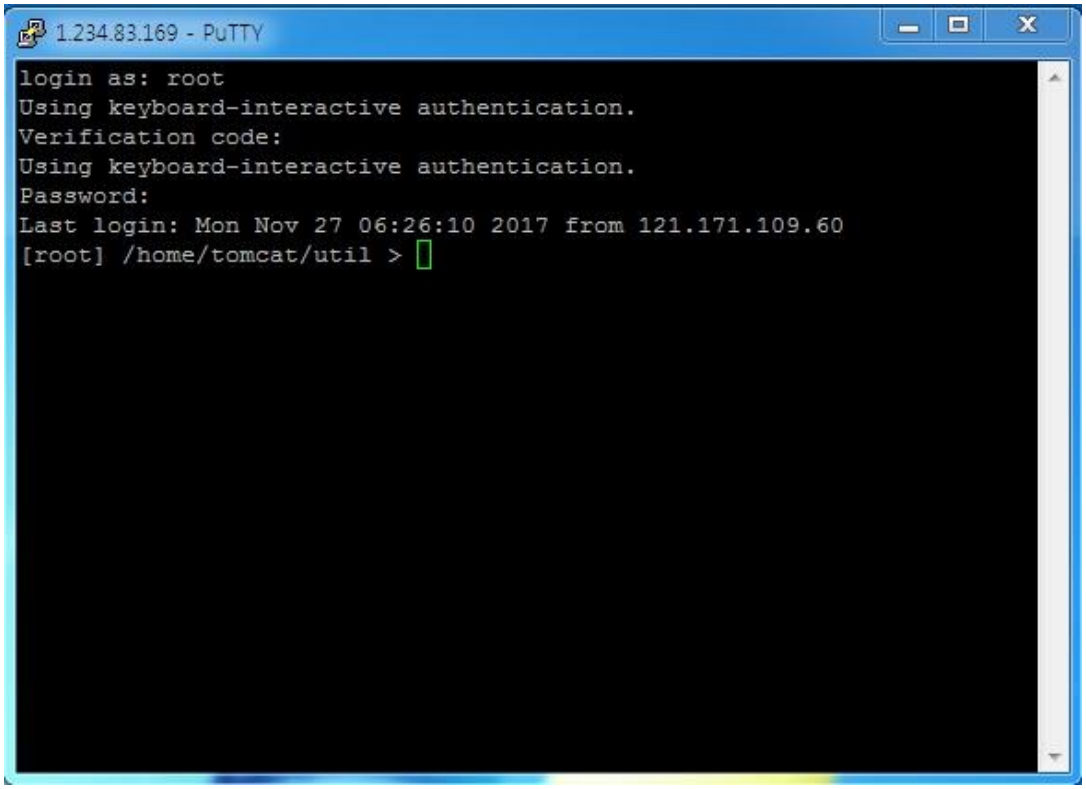


Putty Download 및 Documentation 관련 자료는 다음 URL에서 찾을 수 있다.

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

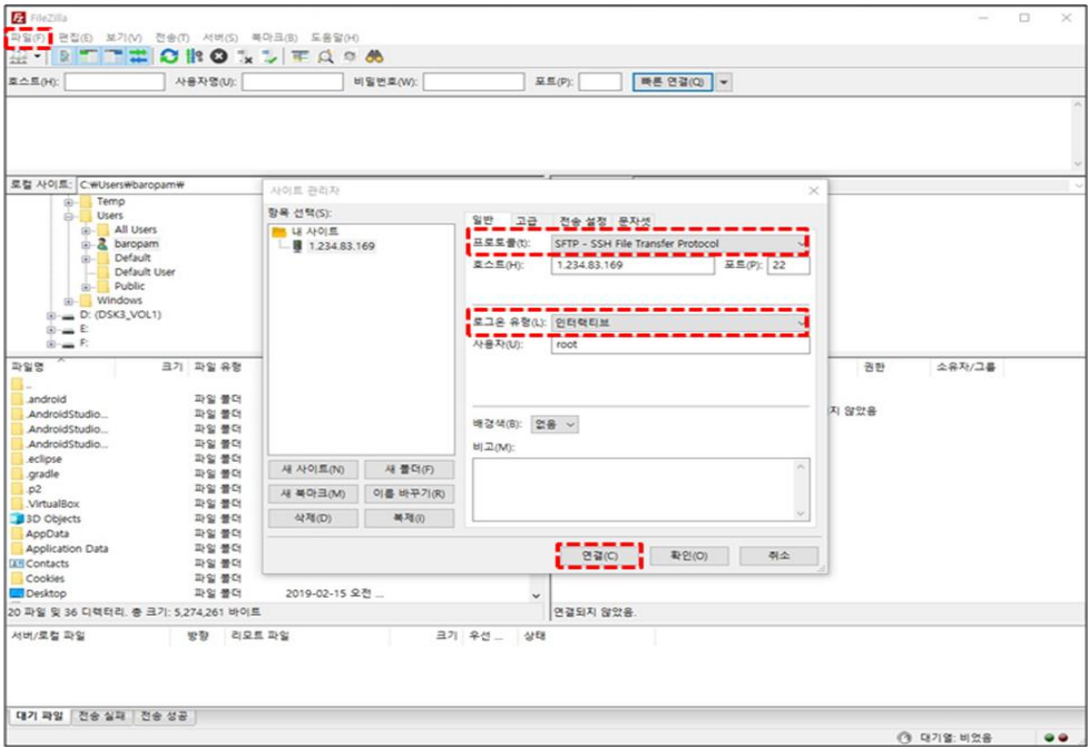
"Verification code"를 입력하라는 메시지가 표시되면 BaroPAM 앱에서 생성한 일회용 인증키를 입력한다.

인증에 성공하면 다음과 같이 SSH 로그인 비밀번호를 입력할 수 있다.

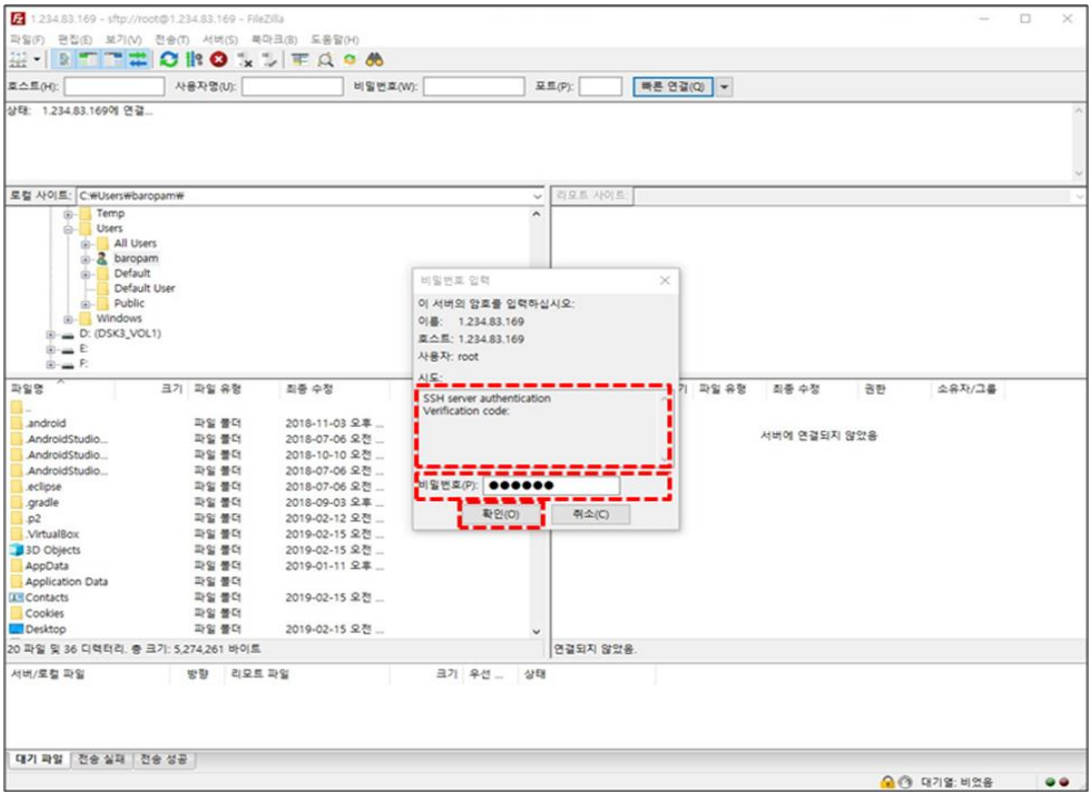


FileZilla인 경우)

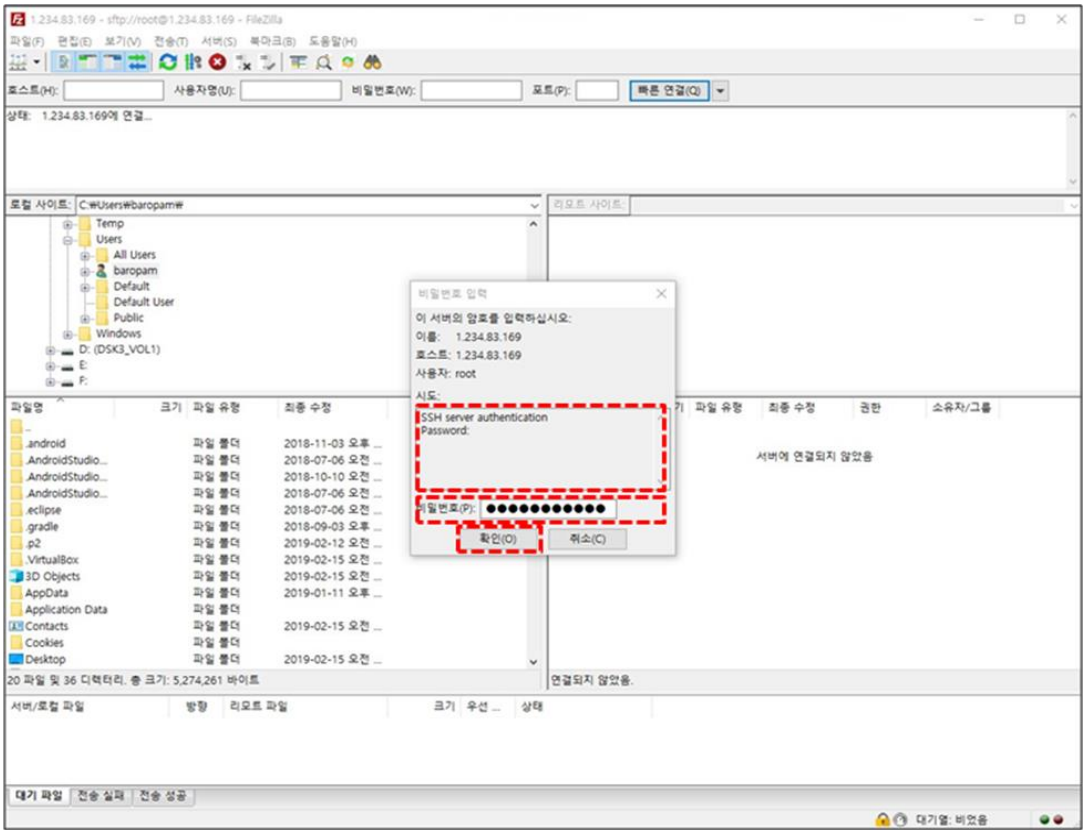
FileZilla로 접속할 때 보통 접속 과정과 다른데, 상단 왼쪽 메뉴에서 "**파일(F) -> 사이트 관리자(S)**"를 선택하여 일반 탭 화면에서 "**프로토콜(t):**" 항목에서 "**SFTP - SSH File Transfer Protocol**"과 "**로그온 유형(L):** " 항목에서 "**인터랙티브**"를 선택한 후 다음과 같이 "**연결(C)**" 버튼을 클릭한다.



그러면 다음과 같이 비밀번호 입력 화면이 나타난다. 비밀번호 입력 화면에서 "**시도:**" 내용을 확인하고, 스마트 폰에서 생성한 **일회용 인증키**를 "**비밀번호(P):**" 입력 항목에 입력한 후 "**확인(O)**" 버튼을 클릭한다.



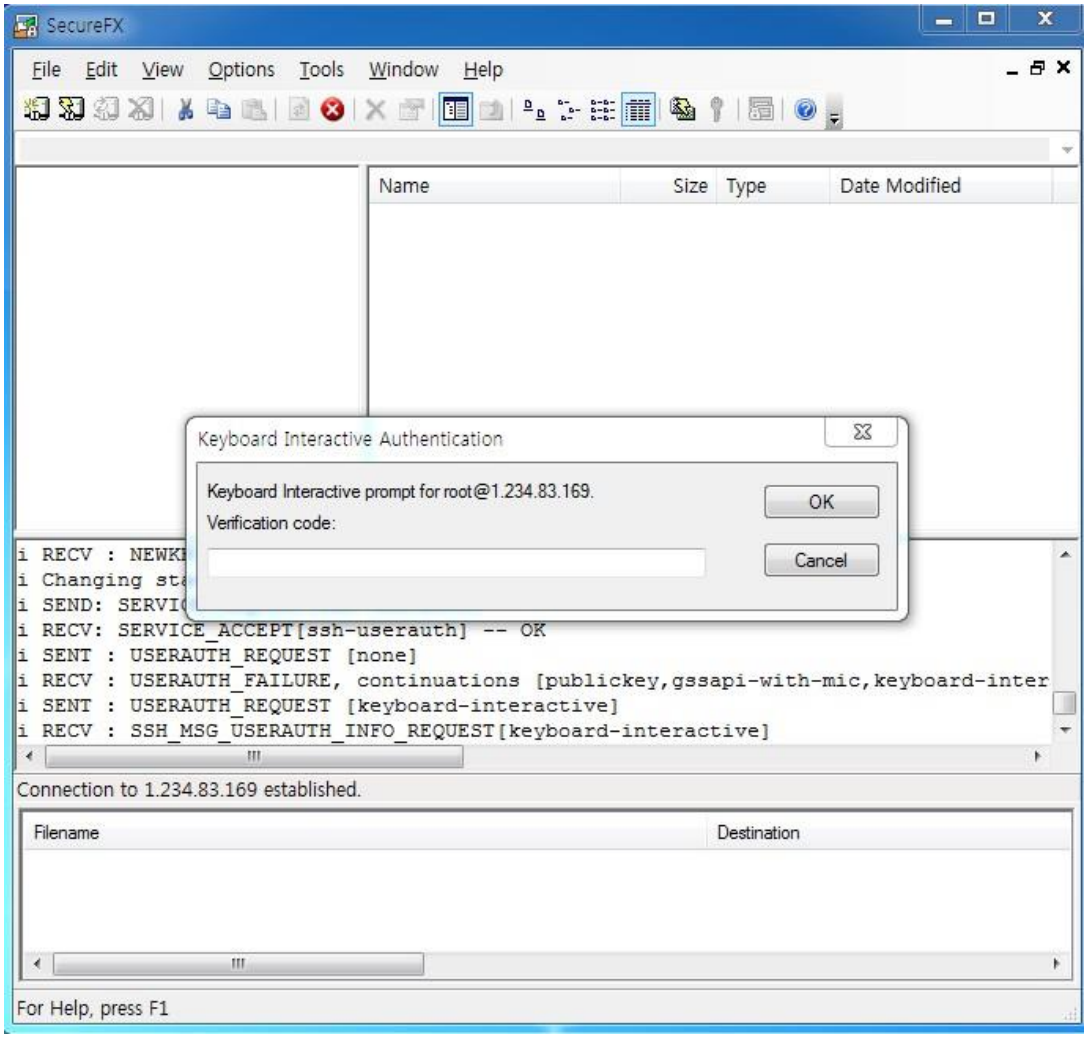
그러면 다음과 같이 비밀번호 입력 화면이 나타난다. 비밀번호 입력 화면에서 "**시도:**" 내용을 확인하고, 로그인 계정에 대한 비밀번호를 "**비밀번호(P):**" 입력 항목에 입력한 후 "**확인(O)**" 버튼을 클릭하여 서버에 접속한다.



SFTP인 경우)

"Verification code"를 입력하라는 메시지가 표시되면 BaroPAM 앱에서 생성한 일회용 인증키를 입력한다.

인증에 성공하면 다음과 같이 SFTP 로그인 비밀번호를 입력할 수 있다.



SecureFX Download 및 Documentation 관련 자료는 다음 URL에서 찾을 수 있다.

https://www.vandyke.com/

결론적으로, 2차 인증은 추가 보호 계층을 추가하여 암호 인증을 보호하는 효과적인 수단이 될 수 있으며, 사용 여부와 상관없이 사용자의 선택에 달려 있지만 2차 인증의 채택은 산업의 동향이다.

3. BaroPAM 제거

3.1 BaroPAM 환경 제거

BaroPAM 이 설치된 상태에서 BaroPAM 모듈을 사용하지 않을 경우 sshd 파일에 설정한 내용을 제거하는 방법은 다음과 같이 주석(#) 처리나 삭제하면 된다.

```
[root] /usr/baropam > vi /etc/pam.d/sshd
#%PAM-1.0
#auth       required     /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth
```

sshd 데몬에 설정한 "/etc/ssh/sshd_config" 파일의 내용 중 다음과 같은 인자를 변경해야 한다.

인자	기존	변경	비고
PasswordAuthentication	no	yes	
ChallengeResponseAuthentication	yes	no	
UsePAM	yes	no	

sshd 설정이 끝나면 반드시 PAM 모듈이 제대로 제거되었는지 확인한 후 SSH Server의 Restart 작업이 반드시 필요하다.

```
[root] /usr/baropam > /etc/rc.d/sshd restart
```

sshd 설정이 끝나면 반드시 PAM 모듈이 제대로 제거되었는지 확인한 후 ssh 데몬을 재부팅해야 한다.

4. BaroPAM FAQ

현상 : 일회용 인증키가 맞지 않아서 로그인을 하지 못하는 경우
원인 : BaroPAM은 시간 동기화 방식으로 폰과 Windows나 Server의 시간이 동일해야 함,
조치 : 폰과 Windows나 Server의 시간이 맞는지 확인.

현상 : Feb 7 07:59:09 eactive sshd(pam_baro_auth)[29657]: ACL file ".baro_acl" must only be accessible by user id root
원인 : .baro_acl 파일의 Permission이 다름.
조치 : .baro_acl 파일의 Permission를 444로 설정.

현상 : Feb 7 08:02:15 eactive sshd(pam_baro_auth)[29739]: Failed to acl file read ".baro_acl"
원인 : .baro_acl 파일이 존재하지 않는 경우에 발생.
조치 : baropam 홈 디렉토리에 .baro_acl 파일을 생성. (Permission를 444로 설정)

현상 : Cannot look up user id xxxxx
원인 : 사용자 ID xxxxx를 조회 할 수 없는 경우 발생.
조치 : /etc/passwd 파일에 user id xxxxx를 등록.

현상 : Failed to secret file read .baro_auth
원인 : 사용자 ID xxxxx를 조회 할 수 없는 경우 발생.
조치 : /etc/passwd 파일에 user id xxxxx를 등록.

현상 : Failed to secret file read
원인 : Secret file이 존재하지 않은 경우에 발생.
조치 : Secret file의 존재여부를 확인.

현상 : Secret file .baro_auth must only be accessible by root
원인 : .baro_auth 파일의 Permission이 다른 경우에 발생.
조치 : .baro_auth 파일의 Permission를 444로 설정.

현상 : Invalid file size for .baro_auth
원인 : .baro_auth 파일의 크기가 1 < size < 64K 가 아닌 경우 발생.
조치 : .baro_auth 파일의 크기를 확인.

현상 : Could not read .baro_auth
원인 : .baro_auth 파일이 존재하지 않거나 파일의 Permission이 444가 아닌 경우 발생.
조치 : .baro_auth 파일의 존재여부 및 파일의 Permission를 확인.

현상 : Invalid file contents in .baro_auth
원인 : .baro_auth 파일의 내용(규칙)이 잘못된 경우에 발생.
조치 : .baro_auth 파일의 내용을 확인.

현상 : Failed to create tmp secret file[*error message*]
원인 : 임시 secret file을 생성하지 못한 경우에 발생.
조치 : 임시 secret file을 생성하지 못한 이유는 error message를 확인.

현상 : Failed to open tmp secret file .baro_auth~[*error message*]
원인 : 임시 secret file인 .baro_auth~을 오픈하지 못한 경우에 발생.
조치 : 임시 secret file인 .baro_auth~을 오픈하지 못한 이유는 error message를 확인.

현상 : Secret file .baro_auth changed while trying to use one-time authentication key
원인 : 일회용 인증키를 사용하는 동안 비밀 파일 .baro_auth가 변경된 경우 발생.

조치 : 다시 로그인을 시도.

현상 : Failed to update secret file .baro_auth[*error message*]
원인 : secret file을 변경하지 못한 경우에 발생.
조치 : secret file을 변경하지 못한 이유는 error message를 확인.

현상 : Invalid RATE_LIMIT option. Check .baro_auth
원인 : Secret file인 .baro_auth 파일의 내용 중 RATE_LIMIT 설정값이 잘못 설정되어 있는 경우 발생.
조치 : 제한 횟수(1 < RATE_LIMIT < 100), 제한 시간(1 < interval < 3600)의 설정 값을 확인.

현상 : Invalid list of timestamps in RATE_LIMIT. Check .baro_auth
원인 : Secret file인 .baro_auth 파일의 내용 중 RATE_LIMIT 옵션에 Update된 timestamps가 잘못된 경우 발생.
조치 : Secret file인 .baro_auth 파일의 RATE_LIMIT 옵션에 Update된 timestamps를 확인.

현상 : Try to update RATE_LIMIT line.
원인 : 정상적으로 로그인 한 경우 출력되는 메시지.
조치 : No action

현상 : Too many concurrent login attempts. Please try again.
원인 : Secret file인 .baro_auth 파일의 DISALLOW_REUSE 옵션(일회용 인증키 생성 주기 내에는 하나의 로그인만 가능)이 설정된 경우
로그인 성공 후 일회용 인증키 생성 주기 내에 로그인을 재 시도한 경우 발생.
조치 : 일회용 인증키 생성 주기 후에 로그인 재 시도.

현상 : Trying to reuse a previously used time-based code.
Retry again in 30 seconds.
Warning! This might mean, you are currently subject to a man-in-the-middle attack.
원인 : Secret file인 .baro_auth 파일의 DISALLOW_REUSE 옵션은 중간자 공격(man-in-the-middle)을 대비한 옵션.
중간자 공격(man-in-the-middle)은 권한이 없는 개체가 두 통신 시스템 사이에서 스스로를 배치하고 현재 진행 중인 정보의 전달을 가로채면서 발생.
간단히 말해서, 현대판 도청 시스템이라고 할 수 있는 것
조치 : No action

현상 : Failed to allocate memory when updating .baro_auth
원인 : Secret file인 .baro_auth를 업데이트 할 때 메모리 할당에 실패한 경우 발생.
조치 : Technical support

현상 : Can't find SECURE_KEY[*error message*]
원인 : Secret file인 .baro_auth 파일의 SECURE_KEY 옵션이나 설정값이 없는 경우에 발생.
조치 : Secret file인 .baro_auth 파일의 SECURE_KEY 옵션이나 설정값 확인.

현상 : Verification code generation failed.[*error message*]
원인 : 일회용 인증키 검증에 실패한 경우 발생.
조치 : 로그인 재 시도.

현상 : Invalid verification code
원인 : 일회용 인증키 검증에 실패한 경우 발생.
조치 : 로그인 재 시도.

현상 : Invalid verification code
Can not make/remove entry for session.

원인 : 서버의 시스템 시간이 맞지 않아서 발생.
조치 : date 명령어로 서버의 시스템 시간이 맞는지 확인하여 틀리면 시간을 맞춰져야 함.
1. date 명령어 서버의 시스템 시간을 변경(임시 방편)
2. ntp가 설정되어 있는지 확인하여 설정되어 잇으면 ntp 시간을 설정하는 주기를 줄여 주여야 하며, 설정되어 있지 않으면 ntp를 설정해야 함.

현상 : Mar 12 15:37:01 baropam gdm(pam_baro_auth)[1215]: [ID 128276 auth.error] No user name available when checking verification code
원인 : 인증 코드를 검증할 때 사용 가능한 사용자가 아닌 경우(등록된 사용자가 아닌 경우 발생).
조치 : 시스템 관리자에게 로그인-ID가 등록되어 있는지 확인.

현상 : Apr 3 13:06:13 kdn sshd[3577]: PAM unable to dlopen(/usr/baropam/pam_baro_auth.so): /usr/baropam/pam_baro_auth.so: cannot open shared object file: No such file or directory
Apr 3 13:06:13 kdn sshd[3577]: PAM adding faulty module: /usr/baropam/pam_baro_auth.so
원인 : /usr/baropam/pam_baro_auth.so 파일이 존재하지 않아서 발생.
조치 : BaroPAM 모듈 파일(pam_baro_auth.so)의 존재하는지 확인하여 없으면 BaroPAM의 설치 파일에서 복사한다.

현상 : May 19 12:37:37 baropam sshd(pam_baro_auth)[1416]: Failed to acl file read "(null)"
원인 : acl file 존재여부 및 파일 permission 문제로 발생
조치 :

현상 : Failed to compute location of secret file
원인 : pam에 설정된 secret file이 해당 디렉토리에 존재하지 않은 경우 발생.
조치 : pam에 설정된 secret file이 해당 디렉토리에 존재하지 않으면 secret file을 해당 디렉토리에 생성해 줘야 함.
ex) auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no

현상 : Failed to compute location of encrypt flag
원인 : pam에 암호화 플래그가 존재하지 않은 경우 발생.
조치 : pam에 암호화 플래그(yes, no)을 설정해 줘야 함.
ex) auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no

현상 : Did not receive verification code from user
error: ssh_msg_send: write: Broken pipe
원인 : Secure key가 잘못 설정된 경우에 발생
조치 : 설정된 Secure key를 확인.
벤더에서 제공된 Secure key인지 확인.

현상 : PAM: authentication thread exited unexpectedly.
***** glibc detected *** su: free(): invalid pointer: 0x00002aede020c9e2 *****
원인 : BaroPAM 환경 설정 파일(.baro_nurit)이 존재하지 않는 경우에 발생.
조치 : BaroPAM 환경 설정 파일(.baro_nurit)의 존재하는지 확인하여 없으면 BaroPAM의 설치 파일에서 복사한다.

5. About BaroPAM

Version 1.0 - Official Release - 2016.12.1
Copyright ⓒ Nurit corp. All rights reserved.
http://www.nurit.co.kr

제 조 사 : 주식회사 누리아이티
등록번호 : 258-87-00901
대표이사 : 이종일
대표전화 : 02-2665-0119(영업문의/기술지원)
이 메 일 : mc529@nurit.co.kr
주　　소 : 서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)