Authentication Gateway HOWTO

Zorn Nathan

zornnh (at) musc.edu

도운이

金子 研史

kenji (at) rtlinux.pe.kr

무선 네트워크와 공공장소에서의 접속, 이를 테면 도서관이나 기숙사 같은 곳에서의 보안에 대한 많은 관심이 있었다. 현재까지 구현된 보안방법으로는 이에 대한 관심과 부합되지 않는다. 인증게이트웨이를 사용하는 방법이 제안되곤 했다. 인증게이트웨이는, 사용자가 네트워크를 사용하고자자 할 경우 강제로 인증을 받게 함으로써 보안에 대한 관심을 고조시키고자 하는 것이다.

고친 과정

고침 0.01-kr2001-02-08고친이 kenji

0.03을 기반으로 번역

고침 0.03 2001-12-06고친이 nhz

고침 0.02 2001-09-28고친이 KET

고침 0.01 2001-09-06고친이 nhz

1. 서론

무선 네트워크나 공공장소에서의 네트워크 접속의 경우, 비인가 된 사용자가 매우 쉽게 네트워크에 접속할 수 있으며, 비인가 사용자는 신호를 관찰하고 그 신호로부터 접속정보를 가로 챌 수 있다. 비인가 사용자들은 공용터미널에 자신들의 머신을 연결하고 네트워크 접속을 획득할 수 있다. 보안은 WEP과 같은 곳에 적용이 되었지만, AirSnort 같은 툴로 뚫릴 수 있다. 이러한 문제를 해결하는 방법 중 한가지는 무선 보안장치에 의존하지 말고, 무선 네트워크 또는 공용 접속장소의 선단에 인증게이트웨이를 설치하여 사용자들이 네트워크를 사용하기 전

에 강제적으로 인증을 받도록 하는 것이다. 본 HOWTO에서는 리눅스를 이용하여 이와 같은 인증게이트웨이를 설정하는 방법을 기술하고자 한다.

1.1. 저작권 정보

질문이 있는 분들은 `<zornnh@musc.edu>`로 연락하기 바란다.

1.2. 책임 한계

필자는 이 문서의 내용에 대한 그 어떠한 책임도 받아들일 수 없습니다. 본 문서의 개념, 예제 그리고 기타 내용에 대한 사용은 모두 여러분의 책임입니다. 이 것이 본 문서의 가장 최신판이라도, 오류나 틀린 점이 있을 것이고, 그로 인해 여러분의 시스템이 손상을 받을 수도 있습니다. 앞서의 경고를 명심하고 신중하게 진행하기를 바라며, 그다지 바람직하지 않지만, 필자는 그 결과에 대한 책임을 지지 않습니다.

특별한 명시가 없는 한, 모든 저작권은 각각의 소유자에게 귀속된다. 본 문서에서 사용한 용어는 어떠한 트레이드마크나 서비스마크의 유효성에 영향을 주지 않는다.

특정 제품 또는 상표에 대한 언급은 하지 않았습니다.

일상주기로 전면적인 설치와 백업하기 전에 여러분 시스템의 백업을 받아 놓기를 강력히 권유합니다.

1.3. 신 버전

이 문서는 초기버전이다.

최신 문서는 http://www.itlab.musc.edu/~nathan/authentication_gateway/에 있다. 이와 관련된 HOWTO는 Linux Documentation Project (http://www.linuxdoc.org/) 홈페이지에도 있다.

1.4. Credits

Jamin W. Collins

Kristin E Thomas

1.5. Feedback

이 문서에 있어서 가장 환영받는 부분이 바로 피드백이다. 여러분들의 도움이 없이는 이 문서는 존재하지도 못 할 것이다. 여러분들의 추가내용, 의견 또는 비평을 다음 email로 보내주기 바란다. : <zornnh@musc.edu>.

2. 필요 사항

이 절에서는 인증게이트웨이에 필요한 것을 설명한다.

2.1. Netfilter

인증게이트웨이는 방화벽을 관리하기 위해 Netfilter와 iptables를 사용한다. Netfilter HOWTO (http://netfilter.samba.org/unreliable-guides/packet-filtering-HOWTO/index.html)를 참고하기 바란다.

2.2. PAM for Netfilter rules.

Nathan Zorn이 작성한 PAM(pluggable authentication module)은 http://www.itlab.musc.edu/~nathan/pam_iptables (http://www.itlab.musc.edu/~nathan/pam_iptables/)에서 구할 수 있다.

2.3. DHCP 서버

인증게이트웨이는 공용 네트워크에 대해 DHCP(dynamic host configuration protocol) 서버로 동작을 하게 되며, 필자는 ISC DHCP Server (http://www.isc.org/products/DHCP/)를 사용한다.

2.4. 인증 메커니즘

게이트웨이는 어떠한 방법의 PAM 인증이라도 사용할 수 있다. South Carolina 의과대학교의 인증 메커니즘은 LDAP이다. LDAP를 인증방식으로 사용하였기 때문에, 게이트웨이 박스의 pam 모듈은 LDAP를 사용하도록 설정하였다. 보다 자세한 정보는 http://www.padl.com/pam_ldap.html를 참고하기 바란다. PAM은 다양한 인증방법을 사용할 수 있도록 한다. 사용하고자 하는 PAM 모듈에 대한 문서를 참고하기 바라며, 다른 방법에 대한 정보를 얻고자 하는 분들은 pam modules (http://www.kernel.org/pub/linux/libs/pam/modules.html)를 참고하기 바란다.

2.5. DNS 서버

공용 네트워크에 있어서 게이트웨이 박스는 DNS 서버로도 동작한다. 필자는 Bind (http://www.isc.org/products/BIND/)를 설치했으며, 이를 캐싱 네임서버로 설정하였다. 레드햇 패키지에 달려오는 caching-nameserver RPM 패키지를 사용하였다.

3. 게이트웨이 서비스 설정

이 절은 인증게이트웨이의 각 단계별 설정방법을 기술한다. 사용된 예는 서브넷 10.0.1.0의 비공인 ip를 대상으로 하였으며, eth0는 내부네트워크와 연결된 NIC이고, 공용 네트워크와 연결된 장치는 eth1이다. eth1에 대하여 사용된 IP 주소는 10.0.1.1이지만, 여러분들의 환경에 따라 적절히 설정하기 바란다. 게이트웨이 박스로 레드햇 7.1이 사용했기 때문에, 예제의 상당 부분은 레드햇을 중심으로 설명하였다.

3.1. Netfilter 설치

netfilter를 설치하기 위해서는 커널이 넷필터를 지원하도록 반드시 새로 컴파일해야한다. 커널을 구성하고 새로 컴파일하는 방법은 Kernel-HOWTO (http://www.linuxdoc.org/HOWTO/Kernel-HOWTO.html)를 참고하기 바란다.

다음은 필자의 커널 구성중 일부를 보인 것이다.

```
#
# Networking options
#
CONFIG_PACKET=y
# CONFIG_PACKET_MMAP is not set
# CONFIG_NETLINK is not set
CONFIG_NETFILTER=y
CONFIG_NETFILTER_DEBUG=y
CONFIG_FILTER=y
CONFIG_UNIX=y
CONFIG_INET=y
CONFIG_IP_MULTICAST=y
# CONFIG_IP_ADVANCED_ROUTER is not set
# CONFIG_IP_PNP is not set
# CONFIG_NET_IPIP is not set
# CONFIG_NET_IPGRE is not set
# CONFIG_IP_MROUTE is not set
# CONFIG_INET_ECN is not set
# CONFIG_SYN_COOKIES is not set


#   IP: Netfilter Configuration
#
CONFIG_IP_NF_CONNTRACK=y
CONFIG_IP_NF_FTP=y
```

```
CONFIG_IP_NF_IPTABLES=y
CONFIG_IP_NF_MATCH_LIMIT=y
CONFIG_IP_NF_MATCH_MAC=y
CONFIG_IP_NF_MATCH_MARK=y
CONFIG_IP_NF_MATCH_MULTIPORT=y
CONFIG_IP_NF_MATCH_TOS=y
CONFIG_IP_NF_MATCH_TCPMSS=y
CONFIG_IP_NF_MATCH_STATE=y
CONFIG_IP_NF_MATCH_UNCLEAN=y
CONFIG_IP_NF_MATCH_OWNER=y
CONFIG_IP_NF_FILTER=y
CONFIG_IP_NF_TARGET_REJECT=y
CONFIG_IP_NF_TARGET_MIRROR=y
CONFIG_IP_NF_NAT=y
CONFIG_IP_NF_NAT_NEEDED=y
CONFIG_IP_NF_TARGET_MASQUERADE=y
CONFIG_IP_NF_TARGET_REDIRECT=y
CONFIG_IP_NF_NAT_FTP=y
CONFIG_IP_NF_MANGLE=y
CONFIG_IP_NF_TARGET_TOS=y
CONFIG_IP_NF_TARGET_MARK=y
CONFIG_IP_NF_TARGET_LOG=y
CONFIG_IP_NF_TARGET_TCPMSS=y
```

iptables를 설치해야하며, 배포반의 패키지로 설치하거나 소스로 설치를 해도 무방하다. 일단 위의 옵션으로 새로운 커널을 컴파일하고 iptables를 설치한 후, 필자는 다음을 방화벽 기본룰로 설정하였다.

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A INPUT -i eth0 -m state --state NEW, INVALID -j DROP
iptables -A FORWARD -i eth0 -m state --state NEW, INVALID -j DROP
iptables -I FORWARD -o eth0 -j DROP
iptables -I FORWARD -s 10.0.1.0/24 -d 10.0.1.1 -j ACCEPT
```

서버가 부팅할 때 위의 스크립트가 동작하도록 하려면 init 스크립트에 위의 명령을 포함시켜도 된다. 룰이 추가 되었는지 확인하려면 다음과 같은 명령을 실행시키면 된다:

```
iptables -v -t nat -L
iptables -v -t filter -L
```

이러한 룰을 저장하고자 할 경우, 필자는 레드햇의 init 스크립트를 사용했다.

```
/etc/init.d/iptables save
/etc/init.d/iptables restart
```

룰이 추가되었으면, 다음과 같은 명령을 수행하여 IP forwarding을 가능하게 한다.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

머신이 리부팅할 때 ip forwarding이 가능하도록 하려면, `/etc/sysctl.conf`에 다음 라인을 추가하면 된다.

```
net.ipv4.ip_forward = 1
```

이제 게이트웨이 박스는 NAT를 할 수 있지만, 공용 네트워크 내부와 게이트웨이로 향하여 들어오는 forwarding 패킷을 제외한 모든 forwarding 패킷을 버릴 것이다(DROP).

3.2. PAM iptables Module

방화벽 룰을 추가하는 PAM 세션 모듈로, 인증된 클라이언트에 대하여 forwarding을 허용하기 위해 필요하다. 이를 설정하고자 하는 경우는 단순히 소스 (ftp://ftp.itlab.musc.edu/pub/pam_iptables.tar.gz)를 구하여 다음 명령을 이용하여 컴파일하면 된다.

```
gcc -fPIC -c pam_iptables.c
ld -x --shared -o pam_iptables.so pam_iptables.o
```

이제 `pam_iptables.so`과 `pam_iptables.o`이라고 하는 바이너리 파일이 생겼을 것이다. `pam_iptables.so`을 `/lib/security/pam_iptables.so`으로 복사하기 바란다.

```
cp pam_iptables.so /lib/security/pam_iptables.so
```

게이트웨이에 대하여 인증 클라이언트로 선택된 것은 ssh이고 따라서 필자는 다음 라인을 `/etc/pam.d/sshd`에 추가하였다.

```
session    required     /lib/security/pam_iptables.so
```

이제는, 사용자가 ssh를 이용하여 로그인할 경우, 방화벽 룰이 추가될 것이다.

pam_iptables에 대한 기본 인터페이스는 eth0이지만, 인터페이스 파라미터를 추가하여 기본 설정값을 변경할 수 있다.

```
session required /lib/security/pam_iptables.so interface=eth1
```

이 경우는 외부 네트워크와 연결된 인터페이스 이름이 eth0가 아닌 경우에만 필요하다.

pam_iptables 모듈이 잘 동작하고 있는 지 확인하려면 다음과 같은 단계를 수행하면 된다.

1. ssh를 이용하여 게이트웨이 박스에 로그인 한다.
2. **'iptables -L'**을 이용하여 룰이 추가 되었는지 확인 한다.
3. 룰이 제거되도록 하기위해 게이트웨이 박스로부터 로그아웃 한다.

3.3. DHCP Server 설정

필자는 다음과 같은 `dhcpd.conf` 파일을 이용하여 DHCP를 설정하였다.

```
subnet 10.0.1.0 netmask 255.255.255.0 {
# --- default gateway
     option routers                  10.0.1.1;
     option subnet-mask              255.255.255.0;
     option broadcast-address        10.0.1.255;

     option domain-name-servers       10.0.1.1;
     range   10.0.1.3 10.0.1.254;
     option time-offset              -5;     # Eastern Standard Time

     default-lease-time 21600;
     max-lease-time 43200;

 }
```

서버는 공용 네트워크와 연결된 eth1을 이용하여 동작하였다.

```
/usr/sbin/dhcpd eth1
```

3.4. 인증방법 설정

앞 절에서도 설명하였지만, 필자는 인증으로 LDAP를 사용하도록 게이트웨이를 설정하였다. 하지만, 여러분들은 PAM이 허용하는 어떠한 인증방법을 사용해도 무방하다. 더 많은 정보를 얻으려면 2.4절를 보기 바란다.

PAM LDAP으로 인증을 구현하기 위하여, 필자는 OpenLDAP (http://www.openldap.org)을 설치하고 `/etc/ldap.conf`에 다음과 같은 내용으로 구성하였다.

```
# Your LDAP server. Must be resolvable without using LDAP.
host itc.musc.edu

# The distinguished name of the search base.
base dc=musc,dc=edu
ssl no
```

다음에 보이는 파일은 LDAP 인증을 하도록 PAM을 구성하기 위해 사용하였으며, 이 파일들은 레드햇의 configuration 유틸리티로 생성된 것이다.

`/etc/pam.d/system-auth` 다음과 같이 생성된다.

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      /lib/security/pam_env.so
auth        sufficient    /lib/security/pam_unix.so likeauth nullok
auth        sufficient    /lib/security/pam_ldap.so use_first_pass
auth        required      /lib/security/pam_deny.so

account     required      /lib/security/pam_unix.so
account     [default=ok user_unknown=ignore service_err=ignore sys-
tem_err=ignore] /lib/security/pam_ldap.so

password    required      /lib/security/pam_cracklib.so retry=3
password    sufficient    /lib/security/pam_unix.so nul-
lok use_authtok
password    sufficient    /lib/security/pam_ldap.so use_authtok
password    required      /lib/security/pam_deny.so

session     required      /lib/security/pam_limits.so
session     required      /lib/security/pam_unix.so
session     optional      /lib/security/pam_ldap.so
```

다음과 같은 `/etc/pam.d/sshd` 파일이 생성된다.

```
#%PAM-1.0
auth       required     /lib/security/pam_stack.so service=system-
auth
auth       required     /lib/security/pam_nologin.so
account    required     /lib/security/pam_stack.so service=system-
auth
password   required     /lib/security/pam_stack.so service=system-
auth
session    required     /lib/security/pam_stack.so service=system-
auth
#this line is added for firewall rule insertion upon login
session    required     /lib/security/pam_iptables.so debug
session    optional     /lib/security/pam_console.so
```

3.5. DNS 설정

레드햇 7.1에 포함된 BIND를 설치했고, caching-nameserver RPM을 같이 설치했다. DHCP 서버는 공용 네트워크상의 머쉰들이 게이트웨이 박스를 네임서버로 사용하도록 알리는 역할을 한다.

4. 인증게이트웨이 사용

인증게이트웨이를 사용하기 위해서는, 여러분들의 클라이언트 머쉰이 DHCP를 사용하도록 설정해야한다. 각각의 머쉰에 ssh 클라이언트를 설치하고 게이트웨이로 ssh 접속을 한다. 일단 로그인 되면, 내부 네트워크에 접근할 수 있게 된다. 다음 예는 유닉스 기반의 클라이언트에 대한 세션이다.

```
bash>ssh zornnh@10.0.1.1
zornnh's Password:

gateway>
```

여러분들이 로그인해 있는 한, 접근권한은 계속 유지될 것이다. 만일 로그아웃하면, 접근 권한을 잃게 된다.

5. 결론

- 본 HOWTO에서 소개한 보안방법은 무선네트워크 커뮤니티에서 제공하는 보안방법에 의존하지 않는다. 이는 전체 네트워크가 불안전하고 여러분의 네트워크 외부에 존재한다고 가정한다.
- 게이트웨이는 전송데이터를 암호화하지 않고, 단지 게이트웨이 뒤쪽에 있는 사용자가 네트워크에 접근할 수 있도록 만 한다. 암호화 및 인증이 요구되는 상황이라면 VPN을 사용하는 것이 좋다.

6. 별도의 리소스

- NASA에서 구현한 인증게이트웨이를 설명한 문서 (http://www.nas.nasa.gov/Groups/Networks/Projects/Wireless/index.html).
- University of Alberta에서 인증게이트웨이를 개발한 방법을 기술한 백서 (http://www.ualberta.ca/~beck/authgw.html).

7. 질문과 답변

필자 생각에 다른 사람들이 궁금해 할 만한 가장 평범한 질문을 모아 놓은 것에 불과하다. 필자에게 더 많은 피드백을 주시면, 이 절을 끝내주는 FAQ로 만들어 보겠습니다.