debian, kanet, captive, portal, wifi, shibboleth

Kanet is a WIFI captive portal written in Vala by Cyrille Colin in Metz university.
It is a fast application (compiled bytecode) based on reliable Open Source softwares (Apache, IPTables, Radius…).
This article is about the installation under Debian Squeeze.
We will use both an LDAP and Shibboleth authentication.

System

```
debian squeeze AMD64
```

A public interface `eth0` and a private one `eth1`

```
eth0: 140.77.64.3
eth1: 192.168.240.3
```

Install the required packages

```
aptitude install locate unzip libwww-perl libcrypt-ssleay-perl libnet-dns-perl libtemplate-perl
# vala
aptitude install build-essential flex bison pkg-config libglib2.0-dev
# kanet
aptitude install libgee-dev libgee2 sqlite3 libsqlite3-dev libsoup2.4-1 libsoup2.4-1-dev libjson-glib-dev libdaemon-dev libradiusclient-ng-dev libnetfilter-conntrack-dev libnetfilter-queue-dev
# apache
aptitude install apache2 libapache2-mod-shib2 libapache2-mod-php5
# DHCP
aptitude install dhcp3-server
# freeradius
aptitude install freeradius freeradius-ldap
```

VALA installation

You have to compile VALA because Debian packages are too old for Kanet. The minimum required version is `0.11.2`.

```
cd /usr/local/src
wget http://ftp.acc.umu.se/pub/GNOME/sources/vala/0.11/vala-0.11.2.tar.gz
tar jxvf vala-0.11.2.tar.gz
cd vala-0.11.2/
./configure
```

```
make
make install
```

Reconfiguring the library path.

```
ldconfig
```

Updating the `PKG_CONFIG_PATH`.

```
PKG_CONFIG_PATH=/usr/local/src/vala-0.11.2/
export PKG_CONFIG_PATH
```

Kanet installation

```
cd /usr/local/src
wget http://kanet.googlecode.com/files/kanet-0.2.3.tar.bz2
tar jxvf kanet-0.2.3.tar.bz2
cd kanet-0.2.3
./waf configure
./waf
./waf install
```

Creation of the iptables file

copy the `kanet-rules` file in `/etc/init.d/` and:

```
chmod +x /etc/init.d/kanet-rules
```

Apache2 configuration

```
a2enmod rewrite
a2enmod proxy
a2enmod ssl
a2enmod shib2
```

adding the 8080 port in `/etc/apache2/ports.conf`:

```
NameVirtualHost 192.168.240.3:8080
Listen 8080
```

Creation of the Apache2 virtualhost

We use the configuration given in the Kanet Web site.

```
<VirtualHost 192.168.240.3:443>
        #
        # HTTPS stuff...
        #
        ServerName eduspot.ens-lyon.fr
        SSLEngine On
        SSLCertificateFile /etc/ssl/certs/eduspot.ens-lyon.fr.pem
        SSLCertificateKeyFile /etc/ssl/certs/eduspot.ens-lyon.fr.key
        SSLCACertificateFile /etc/ssl/certs/cacru_comodo.crt
        SSLVerifyClient none
        SSLProxyEngine On

        DocumentRoot /var/www
        Alias /www /usr/local/share/kanet/

        ProxyPreserveHost On
        ProxyRequests On
        ProxyPass /Shibboleth.sso  !
        ProxyPass /wayf  !
        ProxyPass /www  !
        ProxyPass  / http://127.0.0.1:8181/ disablereuse=on retry=0
flushpackets=on
        ProxyPassReverse / http://127.0.0.1/
        ProxyTimeout 3

        <location />
        Allow From All
        #
        # Shibboleth authentitcation
        #
        AuthType shibboleth
        Require shibboleth
        ShibUseHeaders On
        ShibRequestSetting exportAssertion true
        </location>
        <location /www>
        Allow From All
        </Location>
        <Location /login_shibboleth>
                Allow from all
                AuthType shibboleth
                ShibRequireSession On
                ShibRequestSetting exportAssertion true
                require valid-user
        </Location>
        ErrorLog /var/log/apache2/error.log
        LogLevel warn
        CustomLog /var/log/apache2/access.log combined

</VirtualHost>
<VirtualHost 192.168.240.3:80>
  ServerName eduspot.ens-lyon.fr
  RewriteEngine On
  RewriteCond %{HTTPS} off
  RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</VirtualHost>
<VirtualHost 192.168.240.3:8080>
        ServerName eduspot.ens-lyon.fr
        RewriteEngine On
        RedirectMatch .* https://eduspot.ens-lyon.fr/www/login_double.php
        ErrorLog /var/log/apache2/error.log
        LogLevel warn
        CustomLog /var/log/apache2/access.log combined
</VirtualHost>
```

```
a2ensite kanet
a2dissite default
```

WAYF (where are you from) installation

```
cd /usr/local/src
https://forge.switch.ch/redmine/attachments/download/337/SWITCHwayf_1.15_20111021.zip
unzip SWITCHwayf_1.15_20111021.zip
mv SWITCHwayf_1.15 /var/www/
cd /var/www
ln -s SWITCHwayf_1.15/ wayf
chown -R www-data:www-data SWITCHwayf_1.15
```

configuring the WAYF: copying the `config.dist.php` in `config.php` and editing it (and chown) configuring the WAYF: copying the `IDProvider.conf.dist.php` in `IDProvider.conf.php` and editing it (and chown) moving the WAYF file in `WAYF.php`

Shibboleth configuration

look at the `/etc/shibboleth/shibboleth2.xml`

```
...
<InProcess logger="native.logger">
    <ISAPI normalizeRequest="true" safeHeaderNames="true">

```

```
        <Site id="1" name="eduspot.ens-lyon.fr"/>
    </ISAPI>
</InProcess>
...
    <RequestMapper type="Native">
        <RequestMap applicationId="default">
            <Host name="eduspot.ens-lyon.fr">
                <Path name="login_shibboleth" authType="shibboleth"
requireSession="true"/>
            </Host>
            <Host name="admin.example.org" applicationId="admin"
authType="shibboleth" requireSession="true"/>
        </RequestMap>
...
   <ApplicationDefaults id="default" policyId="default"
        entityID="https://eduspot.ens-lyon.fr/login_shibboleth"
        REMOTE_USER="eppn"
        signing="false" encryption="false">
        <Sessions lifetime="28800" timeout="3600" checkAddress="false"
            handlerURL="/Shibboleth.sso" handlerSSL="false"
            exportLocation="/Shibboleth.sso/GetAssertion"
exportACL="127.0.0.1"
            idpHistory="false" idpHistoryDays="7">
            <SessionInitiator type="Chaining" Location="/DS" id="DS"
isDefault="true" relayState="cookie">
                <SessionInitiator type="SAML2" acsIndex="1"
template="bindingTemplate.html"/>
                <SessionInitiator type="Shib1" acsIndex="5"/>
                <SessionInitiator type="SAMLDS"
URL="https://eduspot.ens-lyon.fr/wayf/WAYF.php/https://shibboleth.ens-lyon.f
r/idp/shibboleth"/>
            </SessionInitiator>
...
        </Sessions>
        <MetadataProvider type="Chaining">

            <MetadataProvider type="XML"
uri="https://services-federation.renater.fr/metadata/renater-metadata.xml"
                 backingFilePath="renater-metadata.xml"
reloadInterval="7200">
               <MetadataFilter type="Signature" certificate="metadata-
federation-renater.crt"/>
            </MetadataProvider>
            <CredentialResolver type="File" key="/etc/ssl/certs/eduspot.ens-
lyon.fr.key" certificate="/etc/ssl/certs/eduspot.ens-lyon.fr.pem"/>
 </ApplicationDefaults>
```

```
cd /etc/shibboleth
wget
https://services-federation.renater.fr/metadata/metadata-federation-renater.
crt
```

```
/etc/init.d/shibd restart
```

DHCP configuration

configure your `/etc/dhcp/dhcpd.conf`

```
ddns-updates off;
option domain-name-servers 140.77.1.32;

default-lease-time 600;
max-lease-time 7200;
authoritative;

subnet 192.168.240.0 netmask 255.255.0.0 {
  option routers 192.168.240.1;
  option broadcast-address 192.168.240.255;
  range 192.168.240.10 192.168.240.255;
}
```

```
/etc/init.d/isc-dhcp-server restart
```

Kanet configuration

configure your `/usr/local/etc/kanet/kanet.conf` and `/usr/local/share/kanet/login_double.html`

```
cp /usr/local/share/kanet/update.html.sample
/usr/local/share/kanet/update.html
chown -R www-data:www-data /usr/local/share/kanet
```

Freeradius configuration

Important files:
`/etc/freeradius/radiusd.conf`

```
prefix = /usr
exec_prefix = /usr
sysconfdir = /etc
localstatedir = /var
sbindir = ${exec_prefix}/sbin
logdir = /var/log/freeradius
raddbdir = /etc/freeradius
radacctdir = ${logdir}/radacct
```

```
name = freeradius
confdir = ${raddbdir}
run_dir = ${localstatedir}/run/${name}
db_dir = ${raddbdir}
libdir = /usr/lib/freeradius
pidfile = ${run_dir}/${name}.pid
user = freerad
group = freerad
max_request_time = 30
cleanup_delay = 5
max_requests = 1024
listen {
    type = auth
    ipaddr = *
    port = 0
}
listen {
    ipaddr = *
    port = 0
    type = acct
}
hostname_lookups = no
allow_core_dumps = no
regular_expressions = yes
extended_expressions    = yes
log {
    destination = files
    file = ${logdir}/radius.log
    syslog_facility = daemon
    stripped_names = no
    auth = no
    auth_badpass = no
    auth_goodpass = no
}
checkrad = ${sbindir}/checkrad
security {
    max_attributes = 200
    reject_delay = 1
    status_server = yes
}
proxy_requests  = yes
$INCLUDE proxy.conf
$INCLUDE clients.conf
thread pool {
    start_servers = 5
    max_servers = 32
    min_spare_servers = 3
    max_spare_servers = 10
    max_requests_per_server = 0
}
modules {
    $INCLUDE ${confdir}/modules/
}
instantiate {
    exec
    expr
    expiration
    logintime
}
$INCLUDE policy.conf
$INCLUDE sites-enabled/
```

/etc/freeradius/clients.conf

```
client 127.0.0.1 {
    secret = a_secure_password
    require_message_authenticator = no
}
```

/etc/freeradius/modules/ldap

```
ldap {
    server = "ldap-server.ens-lyon.fr"
    basedn = "ou=people,dc=ens-lyon,dc=fr"
    filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
    ldap_connections_number = 5
    timeout = 4
    timelimit = 3
    net_timeout = 1
    tls {
        start_tls = no
        cacertfile    = /etc/certs/cacru.crt
        require_cert    = "demand"
    }
    dictionary_mapping = ${confdir}/ldap.attrmap
    edir_account_policy_check = no
}
```

/etc/freeradius/sites-enabled/default

```
authorize {
    preprocess
    chap
    mschap
    digest
    suffix
    files
        ldap
    expiration
    logintime
    pap
}
```

```
authenticate {
    Auth-Type PAP {
        pap
    }
    Auth-Type CHAP {
        chap
    }
    Auth-Type MS-CHAP {
        mschap
    }
    digest
    unix
    Auth-Type LDAP {
        ldap
    }
}
preacct {
    preprocess
    acct_unique
    suffix
    files
}
accounting {
    detail
    unix
    radutmp
    exec
    attr_filter.accounting_response
}
session {
    radutmp
}
post-auth {
    exec
    Post-Auth-Type REJECT {
        attr_filter.access_reject
    }
}
pre-proxy {
}
post-proxy {
}
```

/etc/radiusclient-ng/servers

```
127.0.0.1 my_secure_password
```

```
unlink /etc/freeradius/sites-enabled/inner-tunnel
```

logs configuration

`/etc/rsyslog.d/kanet.conf`

```
#kanet syslog rules
:msg,contains,"[KANET]" /var/log/kanet/kanet.log
:msg,contains,"[KANET-ERROR]" /var/log/kanet/error.log
:msg,contains,"[KANET-ACCESS]" /var/log/kanet/access.log
```

Comment the line `*.emerg  *` in the `/etc/rsyslog.conf` file to avoid logs in the console.

Kanet init script

create a `/etc/init.d/kanet` file

```
#!/bin/sh
# Start/stop the Kanet daemon.

### BEGIN INIT INFO
# Provides:          kanet
# Required-Start:    $all
# Required-Stop:     $all
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Start kanet at boot time
# Description:       Enable service provided by daemon.
### END INIT INFO
KANET="/usr/local/bin/kanet"
PIDFILE="/var/run/kanet.pid"

case "$1" in
  start)
    echo "Starting kanet"
    start-stop-daemon --start --quiet --background --make-pidfile --pidfile
$PIDFILE --exec $KANET
    ;;
  stop)
    echo "Stopping kanet"
    start-stop-daemon --stop --quiet --pidfile $PIDFILE --exec $KANET
    ;;
  restart)
    echo "Restarting kanet"
    /etc/init.d/kanet stop
    /etc/init.d/kanet start
    ;;
  *)
```

```
    echo "Usage: /etc/init.d/kanet {start|stop|restart}"
    exit 1
    ;;
esac

exit 0
```

```
chmod +x /etc/init.d/kanet
```

Kanet rc.d scripts

```
update-rc.d kanet-rules defaults start
update-rc.d kanet defaults start
```

Update of the kanet open ACL for the identity providers of the Renater federation

We must let an open access to the identity providers of the Renater federation to allow their members to authenticate. We need to put in the KANET_ACL_TYPE_OPEN section of the `kanet.conf` file the IP's of these IdPs.

The CRU has written a Perl script to generate such a section.

```
cd /root/adm
perl ./CreerListeBlanche.pl --template=kanet.tt2 --output=kanet.acl
```

Copy the content of the `kanet.acl` file in the KANET_ACL_TYPE_OPEN section. It is strongly recommanded to do the job every day/week in a cron (I can send mine if requested).

From:
http://thomasbellembois.ddns.net/ - **Thomas Bellembois**

Permanent link:
http://thomasbellembois.ddns.net/doku.php?id=kanet_install

Last update: **2015/05/28 23:03**