INSTALLAZIONE DI KANET IN IDEM

Guida per l'installazione di un captive portal federato.

Autori:

Antonio Campa
Pierluigi Marra
Giuseppe Marullo
Università del Salento

Data: 26/09/2011

1. CAPTIVE PORTAL FEDERATI

La tecnica di Captive Portal forza un client http connesso ad una rete di telecomunicazioni a visitare una speciale pagina web (usualmente una pagina di autenticazione) prima di poter accedere alla navigazione. Ciò si ottiene intercettando tutti i pacchetti, relativi a indirizzi e porte, fin dal momento in cui l'utente apre il proprio browser e tenta l'accesso a Internet. In quel momento il browser viene rediretto verso una pagina web di login la quale può richiedere l'autenticazione oppure semplicemente l'accettazione delle condizioni d'uso del servizio. È possibile trovare software captive portal in uso presso gli hotspot WiFi. Può essere altresì usato anche per controllare accessi su rete cablata (es: alberghi, hotel, centri commerciali, ecc.).

Limitando l'attenzione ai captive portal specifici per hotspot WiFi si possono avere:

- hardware captive portal, spesso embedded nei controller wireless (CISCO , MeruNetworks ecc.)
- captive portal software
    - open source
    - non open-source

Il servizio di accesso alla rete mediante la tecnica del captive portal, come tutti i servizi che potrebbero richiedere l'autenticazione da parte dell'utente, può ovviamente beneficiare dei vantaggi offerti da sistemi di autenticazione ed autorizzazione (AAI) basati sulla tecnica del Single Sign On (SSO). Tale tecnica dà all'utente la possibilità non solo di utilizzare le stesse credenziali per l'accesso a diversi servizi (Single sign In – SSI), ma di poter effettuare, all'interno di una stessa sessione di lavoro, il login una sola volta, in concomitanza all'accesso al primo servizio utilizzato. Ad esempio un sistema AAI con SSO che venga sfruttato dal servizio di accesso alla rete WiFi in Captive portal e dal servizio di web mail permetterebbe ad un utente di inserire le proprie credenziali solo nel momento dell'accesso alla rete WiFi e di accedere alla propria web mail senza doversi nuovamente autenticare.

La necessità di federare un servizio come quello di accesso alla rete in modalità captive portal nasce nel momento in cui si voglia concedere la possibilità di utilizzare il servizio anche ad utenti esterni alla propria organizzazione ma che facciano comunque parte di una organizzazione afferente ad una federazione comune. Basandosi su degli standard e regole condivise nonché sulla reciproca fiducia, tutte le organizzazioni afferenti ad una federazione come ad esempio la federazione IDEM, permettono ai propri utenti di utilizzare le proprie credenziali per accedere a tutti i servizi federati oltre che a quelli offerti loro dalla propria organizzazione. In tal modo, ad esempio, un docente del Politecnico di Bari in trasferta nell'Università del Salento potrebbe sfruttare le sue credenziali per l'accesso alla rete WiFi di quest'ultimo poiché i due atenei afferiscono ad IDEM.

IDEM è la Federazione Italiana delle Università e degli Enti di Ricerca per l'Autenticazione e l'Autorizzazione. I suoi obiettivi "*sono quelli di creare e supportare un framework, comune agli enti di formazione e di ricerca italiani, per la gestione condivisa degli accessi alle risorse on-line*"(www.idem.garr.it). Il suo sistema federato è basato sul protocollo **Security Assertion Markup Language (SAML)**, uno standard per lo scambio di dati di autenticazione e autorizzazione (asserzioni) tra domini di sicurezza

distinti, tipicamente tra un *identity provider (IdP)* che gestisce le informazioni sull'identità degli utenti e un *service provider (SP)* che fornisce i servizi.

1.1 Federare l'accesso WiFi in Captive Portal : pro e contro

Un'istituzione, anche se già federata ad EDUROAM, potrebbe federare ad IDEM il servizio di accesso WiFi in modalità shibboleth-based captive portal essenzialmente per i seguenti motivi:

- l'accesso alla rete tramite captive portal federato abilita la mobilità degli utenti (studenti, docenti, ..) tra le Università federate ad IDEM (e magari anche tra gli enti appartenenti ad altre federazioni compatibili con l'architettura shibboleth).
- l'accesso alla rete tramite captive portal è più semplice da configurare rispetto all'accesso EDUROAM, e ciò è particolarmente importante nel caso degli studenti.
- l'accesso alla rete tramite captive portal shibboleth abilita anche l'accesso SSO alle risorse web che l'organizzazione intende fornire.
- tramite l'autenticazione shibboleth l'utente fornisce le sue credenziali (username e password) **esclusivamente all'Identity Provider dell'ente di appartenenza** il quale, a sua volta, fornirà in modalità protetta al service provider dell'ente ospitante **solo gli attributi** (es. EduTargedID) necessari all'abilitazione.

I principali ostacoli all'adozione di un captive portal federato shibboleth sono invece:

- problematiche di sicurezza: ciascun servizio abilitato tramite captive portal deve protegge autonomamente le comunicazioni (per esempio tramite https). Inoltre, la maggior parte delle implementazioni richiede agli utenti di superare una pagina SSL di login criptata, dopo la quale i loro indirizzi IP e MAC sono abilitati a passare attraverso il gateway. È stato dimostrato che questo tipo di accesso è facilmente attaccabile tramite un semplice packet sniffer. Una volta ottenuti IP e MAC address di altri computer già autenticati e connessi, chiunque dotato di mezzi e conoscenza tecnica può superare i controlli falsificando le proprie credenziali con quelle degli utenti autorizzati e attraversare indisturbato il gateway. Una soluzione a questo problema consiste nell'utilizzare una finestra di controllo che continuamente rinnova l'autenticazione mandando al gateway un pacchetto criptato. Tale tecnica è implementata per esempio nel captive portal di Zeroshell.
- un captive portal che supporta shibboleth richiede la predisposizione nell'organizzazione di un fornitore di identità (IdP – Identity Provider) generalmente non presente in tutte le organizzazioni.
- tra le soluzioni open source per captive portal solo alcune supportano shibboleth. Si restringe, pertanto, la rosa delle soluzioni di captive portal adottabili da ciascuna organizzazione.

  Tra i captive portal open source che gestiscono l'autenticazione tramite SAML/Shibboleth abbiamo:

  - CoovaChilli http://www.coova.org/
  - Kanet http://code.google.com/p/kanet/

- Hupnet http://hupnet.sourceforge.net/
- NoCatAuth http://nocat.net/
- PepperSpot http://pepperspot.sourceforge.net/
- ZeroShell http://www.zeroshell.net/

In questo documento si riporta la procedura da seguire per l'attivazione del sistema di captive portal open source Kanet e la sua federazione ad IDEM tramite Shibboleth.

2. KANET

2.1 Descrizione di Kanet

Kanet (Kontrol Access to NETwork)[1] è un captive portal open source scritto in un linguaggio di alto livello VALA[2], tradotto in C e compilato per velocizzare l'uso della memoria e per renderlo più veloce. Kanet interagisce con il firewall di linux grazie alle Kernel Netfilter lib ed un meccanismo di gestione delle connessioni attraverso le QUEUE in netfilter. Il suo primo sviluppo è presso l'Università francese di Metz[3]. Kanet gestisce l'autenticazione SAML/Shibboleth in maniera nativa ed è attualmente alla versione 0.2.3.

Documentazione	http://code.google.com/p/kanet/
Libreria SAML utilizzata	Shibboleth SP
Supporto SAML	nativo per Shibboleth
Tipologia del software	open source (CRI - Université de Metz - http://www.univ-metz.fr/)
Metodologia di integrazione alla	modulo Apache (Shibboleth SP) con Apache impostato come proxy
Tipologia di autenticazione	login
Attributi necessari	REMOT_USER
Organizzazioni che utilizzano il captive portal	Université de Metz colin@univ-metz.fr
E-mail Autori	colin@univ-metz.fr
Problematiche	gestisce l'autenticazione con una finestra di popup (notoriamente non gestita dagli smartphone) gestisce solo traffico TCP e non abilita il passaggio di UDP

1 http://code.google.com/p/kanet/
2 http://live.gnome.org/Vala/
3 http://www.univ-metz.fr/

3. INTEGRAZIONE DEL CAPTIVE PORTAL "KANET" CON L'AUTENTICAZIONE FEDERATA IDEM

3.1 Modalità operative di kanet e librerie necessarie

Kanet ha l'autenticazione SAML/Shibboleth nativa ma per sfruttarla esso deve operare nella **modalità proxy** ovvero una modalità che bypassa il captive portal interno e sfrutta Apache per redirigere l'utente ad una pagina di login protetta con Shibboleth e in tale pagina (che viene quindi eseguita una volta che l'utente è autenticato dal proprio IdP) si richiama il codice che avvia l'utility di autorizzazione.

Le componenti utilizzate da Kanet sono:

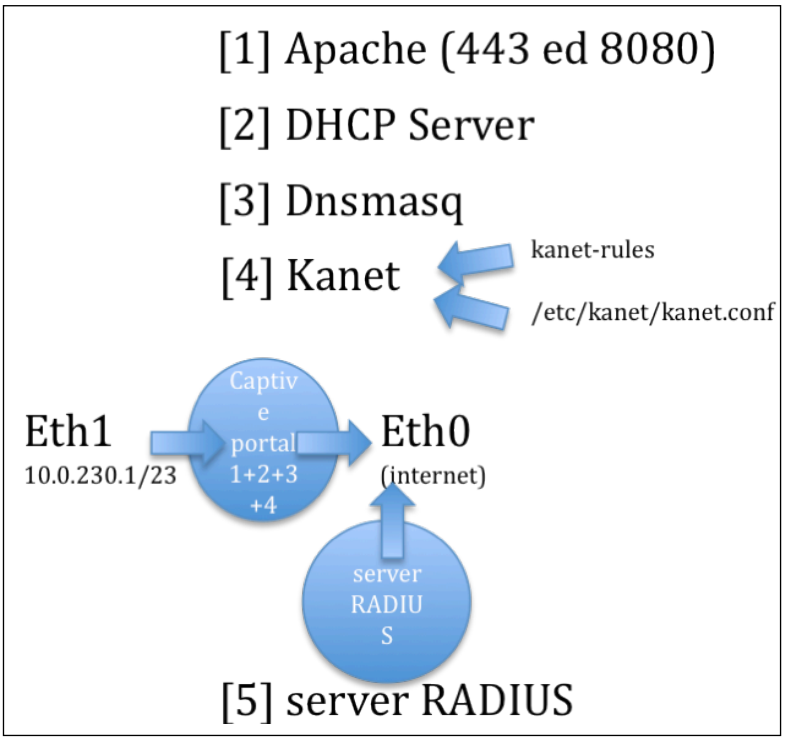
- GLib e simili
- libsoup-2.4 : per attivare i webserver/webservice.
- libdaemon.
- radiusclient-ng
- netfilter_queue, netfilter_conntrack.
- waf.

Questa guida fornisce un aiuto per l'installazione passo passo su una macchina linux Ubuntu 10.0.4.

3.2 Lo scenario

Immaginiamo di avere il seguente scenario:

```
Client --|
Client --|---(wireless or wired) --- eth1 -- (kanet) -- eth0 (internet)
Client --|
```



Supporremo che un utente (client) tenti di collegarsi alla rete e riceva dal server DHCP (implementato sullo stesso server su cui gira il captive portal) un indirizzo della network IP 10.0.230.x o 10.0.231.y e gateway pari all'indirizzo IP del captive portal (10.0.230.1/23).

La prima richiesta http proveniente da un client viene intercettata e diretta verso Kanet e, da quest'ultimo, ruotata su una QUEUE di iptable.

Il demone Kanet controlla i nuovi utenti e tramite apache redirige le url sulla porta 8080 dove è in ascolto apache con una pagina di login.

L'installazione del captive portal Kanet shibboleth-enabled può logicamente essere scomposta nelle seguenti attività:

- installazione e configurazione dello scenario
- installazione e configurazione di Kanet
- installazione e configurazione di Shibboleth Service Provider

3.3 Installazione e configurazione dello scenario (configurazione di rete + dhcp + dns)

3.3.1 Configurazione dell'interfaccia di rete

Aggiungere in /etc/network/interfaces:

```
auto eth1
iface eth1 inet static
        address 10.0.230.1
        netmask 255.255.254.0
        network 10.0.230.0
        broadcast 10.0.231.255
```

Abilitazione dell'interfaccia di rete

Eseguire:

```
/etc/init.d/networking restart
```

3.3.2 Installazione del server DHCP

```
apt-get install dhcp3-server
```

Configurazione DHCP: modificare /etc/dhcp3/dhcpd.conf:

```
ddns-updates off;
option domain-name-servers 10.0.230.1;

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

subnet 10.0.230.0 netmask 255.255.254.0 {
  option routers 10.0.230.1;
  option broadcast-address 10.0.231.255;
  range 10.0.230.10 10.0.231.250;
}
```

Lanciare il demone DHCP:

```
/etc/init.d/dhcp3-server restart
```

3.3.3 Installazione di Dnsmasq per il caching del DNS

```
apt-get install dnsmasq
```

3.3.4 Installazione di Bind e configurazione dei forwarders in /etc/bind/named.conf.options

```
options {
          listen-on {10.13.0.1;};
    forwarders {
```

```
      XX.XX.XX.XX;
    };
    auth-nxdomain no;
  };
```

riavviare bind

```
/etc/init.d/bind9 restart
```

3.4 Installazione e configurazione di Kanet

Installare i seguenti pacchetti:

```
apt-get install libsqlite3-0 [OK]
apt-get install libjson-glib-1.0-0 [OK]
apt-get install libglib2.0-0 [OK]
apt-get install libgee2 [OK]
apt-get install libsoup2.4-1 [OK]
apt-get install libradiusclient-ng2 [OK]
apt-get install libnetfilter-conntrack3 [OK]
apt-get install libnetfilter-queue1 [OK]
apt-get install shared-mime-info [OK]
apt-get install libdaemon0 [OK]
```

Scaricare kanet:

```
wget http://kanet.googlecode.com/files/kanet_0.2-3_i386_lucid.deb
```

Installare Kanet

```
dpkg -i kanet_0.2-3_i386_lucid.deb
```

Editare uno script per la gestione del firewall che interagisce con le iptables:

vi /etc/init.d/kanet-rules

```
#!/bin/sh

IPT="/sbin/iptables"
SLEEP="/bin/sleep"

IP_PRIVATE="10.0.230.1"
NTINT="eth1"
NTOUT="eth0"

test -f $IPT || exit 0

case "$1" in
  start)
     echo -n "Loading kanet firewall's rules: enabling routing"
     echo 1 > /proc/sys/net/ipv4/ip_forward

     # Flush table
     $IPT -t nat -F
     $IPT -t mangle -F
     $IPT -t filter -F

     $IPT -t mangle -A PREROUTING -i $NTINT -j CONNMARK --restore-mark
     $IPT -t mangle -A PREROUTING -p TCP -i $NTINT -d $IP_PRIVATE -j ACCEPT
     $IPT -t mangle -A PREROUTING -p TCP -i $NTINT -m state --state NEW -j QUEUE
     $IPT -t nat -A PREROUTING -p TCP -i $NTINT -j CONNMARK --save-mark

     # MARK 0xFFFFFFFF = Openacls
     $IPT -t nat -A PREROUTING -p TCP -i $NTINT -m mark --mark 0xFFFFFFFF -j ACCEPT

     # MARK 0x0 = unauthenticated - 80 is redirected to authentication page using DNAT translation
     $IPT -t nat -A PREROUTING -p TCP --dport 80 -i $NTINT -m mark --mark 0 -j DNAT --to-
destination $IP_PRIVATE:8080
```

```
    # MARK 0x1 blacklistacls
    $IPT -t filter -A FORWARD -i $NTINT -m mark --mark 0x1 -j REJECT

    $IPT -t filter -A FORWARD -i $NTINT -m mark --mark 0 -j REJECT

    $IPT -t nat -A POSTROUTING -o $NTOUT -m mark ! --mark 0 -j MASQUERADE

    echo "Done."
 ;;
 stop)
    echo -n "Flushing kanet firewall's rules: "
    echo 0  > /proc/sys/net/ipv4/ip_forward

    ############################
    # FLUSH TABLES
    ############################
    $IPT -t filter -F
    $IPT -t nat -F
    $IPT -t mangle -F
    echo "Done."
 ;;

 status)
    # List tables
    echo
    echo "---------- FILTER TABLE ----------"
    echo
    $IPT -t filter -L -v
    echo
    echo "----------   NAT TABLE  ----------"
    echo
    $IPT -t nat -L -v
    echo
    echo "----------   MANGLE TABLE  ----------"
    echo
    $IPT -t mangle -L -v
    echo
 ;;
 restart|force-reload)
    $0 stop
    $SLEEP 3
    $0 start
    echo "Done."
 ;;

 *)
    echo "Usage: /etc/init.d/kanet-rules {start|stop|status|restart}"
    exit 1
 ;;
esac

exit 0
```

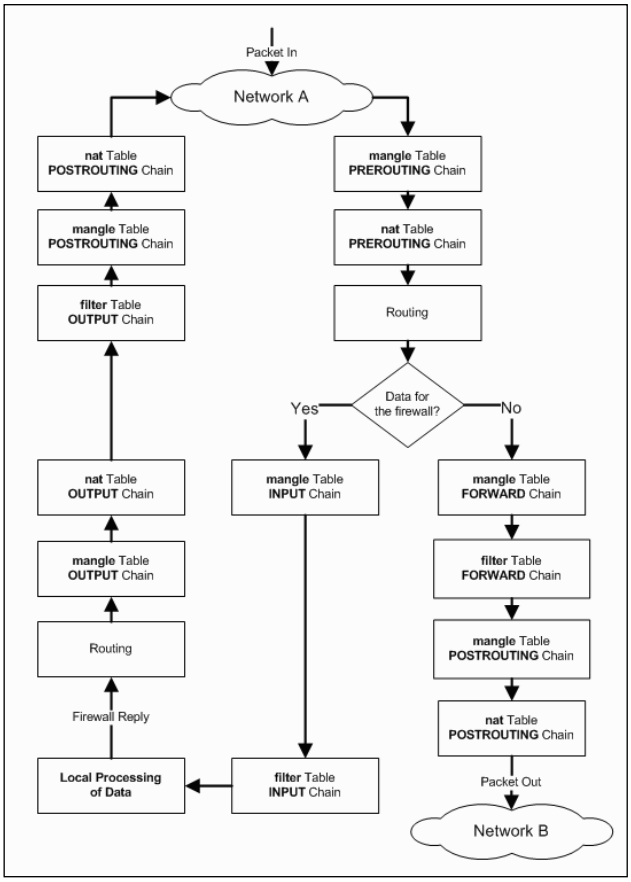
Rendere eseguibile e lanciare:

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

A questo punto sulla rete 10.0.230.0/23 sono attivi:

- dhcp
- dns

- uno script di gestione del firewall per avviare l'inoltro a KANET basato su iptable che agisce:
    - sulla tabella mangle di linux per inoltrare su QUEUE le nuove connessioni
    - sulla tabella nat per marcare a zero il traffico TCP sulla porta 80 non autenticato redirigendolo sulla porta TCP 8080 dello stesso server (PORT FORWARDING).



Attivare il logrotate:

vi /etc/logrotate.d/kanet

```
/var/log/kanet/*.log {
        daily
        missingok
        rotate 52
        compress
        delaycompress
        notifempty
        sharedscripts
        postrotate
                if [ -f /var/run/kanet.pid ]; then
                        /etc/init.d/kanet restart > /dev/null
                fi
        endscript
}
```

attivare anche rsyslog

```
vi /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
```

e riavviare il servizio rsyslog.d:

```
service rsyslog stop
service rsyslog start
```

Verificare se kanet è attivo con il comando:

```
netstat -tuan
```

Riscontrare la riga:

```
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN.
```

Fermare il servizio per procedere alla configurazione:

```
/etc/init.d/kanet stop
```

3.4.1. Configurare Kanet tramite il file di configurazione /etc/kanet/kanet.conf

Creare i certificati necessari per https usando una CA self signed:

```
cd /etc/kanet/
openssl genrsa -out ssl-kanet.key 1024
openssl req -new -key ssl-kanet.key -out ssl-kanet.csr
openssl x509 -req -days 365 -in ssl-kanet.csr -signkey ssl-kanet.key -out ssl-kanet.crt
```

dove ssl-kanet.crt è il certificato self signed

Per il radius, configurare il file:

```
/etc/radiusclient-ng/radiusclient.conf
```

Kanet ha due modalità di autenticazione: CAS ed esterna (RADIUS per il momento). Quella di interesse è RADIUS.

Installare apache:

```
apt-get install apache2
a2enmod rewrite
a2enmod proxy
a2enmod proxy_http
a2enmod ssl
```

Modificare il file di configurazione /etc/kanet/kanet.conf come segue:

```
/*
    Configuration file for kanet
*/

{
    /*
            Server configuration
            SERVER_MODE="STANDALONE" (default) or "PROXY"
    */
    "SERVER_MODE" : "PROXY",
    "SERVER_URL" : "https://10.0.230.1",
    "SERVER_PORT" : "8181",
    "SERVER_IP" : "",
    "REDIRECT_SERVER_PORT" : "8080",
    "QUEUE_NUM" : "0",
    "SSL_CERT_FILE" : "/etc/kanet/ssl-kanet.crt",
    "SSL_KEY_FILE" : "/etc/kanet/ssl-kanet.key",
    "DEBUG" : "1",
    /*
            Persistent data,
            only sqlite is available.
    */
    "database" : "sqlite",
    "sqlite_connection_string" : "/var/lib/kanet/kanet.sqlite",
    "mysql_connection_string" : "Server=xxx; Port=3306; Database=xxx; uid=xxx; pwd=xxx;",
    /*
            Server behavior
    */
    "login_page" : "https://10.0.230.1/www/login.html",
    "captive_portal_page" : "https://10.0.230.1/www/update.html",
    "cas_url" : "https://auth.univ-metz.fr/",
    "www_path" : "/usr/share/kanet/",
    "module_path" : "/usr/lib",
    "auth_module_name" : "kanet-radiusclient",


    /*
            blacklist acls
            always rejected.
    */
    "KANET_ACL_TYPE_BLACKLIST": [
```

```
        { "address" : "127.0.0.1", "port" : 9090 },
        { "address" : "www.denied.com" },
        { "port" : 8089 }
    ],
    /*
            open acls
            always open
    */
    "KANET_ACL_TYPE_OPEN": [
        { "address" : "127.0.0.1" },
        { "address" : "auth.univ-metz.fr" },
        { "address" : "www.unisalento.it" },
        { "address" : "www.umail.univ-metz.fr", "port" : 443 },
        { "address" : "www.crium.univ-metz.fr" },
        { "port" : 60 }
    ],
    /*
            default acls
            open to authenticated users.
    */
    "KANET_ACL_TYPE_DEFAULT": [
            { "port" : 8089 },
            { "port" : 443 },
            { "port" : 53 },
            { "port" : 80 }
    ],

    /* Admins : comma separated login list */
    "admins": "colin,colin@upvm",
    /*
            blacklist_part
    */
    "blacklist_users" : [
            { "login" : "colin", "message" : "hi foo ! you're login have been locked .." },
            { "login" : "johndoe", "message" : "hi john doe ! this account is locked .." }
    ],
    "default_blacklist_message" : "Your account have been locked",

    /*
            auto_blacklist_acl
            used to inform user they are probably infected, if a user try to join
            one of this address, the user is automatically blacklisted and the message
            display on is login window
    */
    "auto_blacklist_acls": [
            { "address" : "192.168.1.45", "message" : "You're account have been temporarily locked
<br/> because you're probably infected by a virus" },
            { "port" : 45678, "message" : "You're account have been temporarily locked <br/>
because you're probably infected by a virus" }
    ],
    /*
            quota, in bytes or seconds. 0 is unlimited.
    */
    "bytes_quota" : "1000",
    "time_quota" : "10",
    /*
            message variables : $upbytes $downbytes $duration
    */
    "update_msg" : "Informazioni sulla navigazione",
    "over_quota_msg" : "Sorry you exceed your quota",
    "blacklist_msg" : "Sorry, you're account have been locked",
    "update_error_msg" : "An error occured during authentication process, please restart your
browser",

}
```

Dove:

```
...
        "KANET_ACL_TYPE_BLACKLIST": [
                { "address" : "forbidden.com", "port" : 9090 },
        ],
        "KANET_ACL_TYPE_OPEN": [
                { "address" : "auth.univ-metz.fr" },
                { "address" : "www.umail.univ-metz.fr", "port" : 443 },
                { "port" : 60 }
        ],
        "KANET_ACL_TYPE_DEFAULT": [
                { "port" : 443 },
                { "port" : 80 }
        ],
  ...
```

rappresentano:

- blacklist : tutti i pacchetti sono filtrati
- openacls : White list – tutti i pacchetti sono consentiti anche se l'utente non è connesso
- defaultacls : tutti i pacchetti sono accettati se e solo se l'utente si è autenticato positivamente. In tal caso le cossessioni sono tracciate in un file di log e gli stream di traffico bidirezionale sono consentiti da e verso l'utente.

Per disabilitare il sito di default effettuare le seguenti operazioni per Apache:

```
a2dissite default
```

Editare il file /etc/apache2/ports.conf:

```
NameVirtualHost 10.0.230.1:443
Listen 443
NameVirtualHost 10.0.230.1:8080
Listen 8080
```

Creare il file di configurazione per il sito /etc/apache2/sites-available/kanet:

```
<VirtualHost 10.0.230.1:443>
        SSLEngine On

        SSLCertificateFile /etc/apache2/server.crt
        SSLCertificateKeyFile /etc/apache2/server.key

        SSLVerifyClient none
        SSLProxyEngine On

        Alias /www /usr/share/kanet/

        ProxyPreserveHost On
        ProxyRequests On
        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
        </location>


        ErrorLog /var/log/apache2/error.log
```

```
        LogLevel warn
        CustomLog /var/log/apache2/access.log combined

</VirtualHost>

<VirtualHost 10.0.230.1:8080>
        RewriteEngine On
        RedirectMatch .* https://10.0.230.1

        ErrorLog /var/log/apache2/error.log
        LogLevel warn
        CustomLog /var/log/apache2/access.log combined

</VirtualHost>
```

Abilitare il sito:

```
a2ensite kanet
```

Per attivare il dominio locale aggiungere al file /etc/hosts la seguente riga:

```
10.0.230.1 portal.unisalento.it    portal
```

Copiare e rinominare i certificati:

```
cp /etc/kanet/ssl-kanet.* /etc/apache2/
cd /etc/apache2/
mv ssl-kanet.crt server.crt
mv ssl-kanet.key server.key
```

Far partire i servizi:

```
/etc/init.d/apache2 stop
/etc/init.d/apache2 start
/etc/init.d/kanet stop
/etc/init.d/kanet start
```

3.5 Installazione e configurazione di Shibboleth Service Provider

Assicurarsi che Kanet operi in PROXY mode ed installare Shibboleth SP[1].

Attivare dunque il server web di kanet in ascolto unicamente su 127.0.0.1 porta http.

Cambiare il file di configurazione per il sito /etc/apache2/sites-available/kanet per gestire due virtualhost: il primo, che dialoga con kanet, redirige le richieste ed il secondo veicola le redirezioni verso la pagina di login.

```
<VirtualHost 10.0.230.1:443>
        SSLEngine On

        SSLCertificateFile /etc/apache2/server.crt
        SSLCertificateKeyFile /etc/apache2/server.key

        SSLVerifyClient none
        SSLProxyEngine On

        Alias /www /usr/share/kanet/

        ProxyPreserveHost On
        ProxyRequests On
        ProxyPass /www  !
        ProxyPass  / http://127.0.0.1:8181/ disablereuse=on retry=0 flushpackets=on
```

```
        ProxyPassReverse / http://127.0.0.1/
        ProxyTimeout 3

        <Location />
                AuthType shibboleth
                Require shibboleth
                ShibUseHeaders On
        </Location>

        <Location /login_shibboleth>
                Allow from all
                AuthType shibboleth
                ShibRequireSession On
                require valid-user
        </Location>

        ErrorLog /var/log/apache2/error.log
        LogLevel warn
        CustomLog /var/log/apache2/access.log combined

</VirtualHost>

<VirtualHost 10.0.230.1:8080>
        RewriteEngine On
        RedirectMatch .* https://10.0.230.1/www/login.html

        ErrorLog /var/log/apache2/error.log
        LogLevel warn
        CustomLog /var/log/apache2/access.log combined

</VirtualHost>
```

INDICE

RIFERIMENTI

http://code.google.com/p/kanet/

https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPLinuxInstall

https://federation.renater.fr/docs/fiches/wifi