Eduroam presso IISS “Euclide” - Bari

Vito A. Smaldino
vitoantonio.smaldino@istruzione.it

Agenda

- Contesto e vincoli
- Una soluzione pronta per l'uso?
- Lo strumento scelto (Zeroshell + Ubuntu/FreeRadius)
- L'architettura della soluzione
- La configurazione di FreeRadius
- La configurazione di Zeroshell
- Strumenti di test
- Suggerimenti per iOS
- L'implementazione delle VMs

NB: Questa presentazione ha come prerequisito la conoscenza degli elementi di base del protocollo Radius

Contesto e vincoli

- Budget & Tempo
- Facile gestione delle utenze
  - Creazione, disabilitazione, scadenze, lotti, …….
- Infrastruttura wireless unica
  - Unico SSID: *eduroam*
- Utenze ad uso Globale + Utenze ad uso Locale
  - Utenze che pur utilizzando l'SSID *eduroam*, siano attive solo nell'Istituto (es. ospiti di convegni, studenti immaturi, ….)
- Quick & Dirty

Una soluzione pronta per l'uso?

Radius: Protocollo estremamente complesso, in particolare l'integrazione con il repository delle utenze (es. LDAP, Windows A.D., SQL, ….)
Scartata l'opzione di realizzarlo da zero

Sistemi già pronti valutati da me:

- Daloradius (www.daloradius.com)
  progetto fermo (2012), la VM non sono riuscito a farla funzionare completamente
- RADIUS Desk (www.radiusdesk.com)
  interessante ma piuttosto complesso e non sono riuscito a farlo funzionare completamente
- ZeroShell (www.zeroshell.net)

ZEROSHELL

Eccezionale pezzo di software - Fulvio Ricciardi INFN Lecce

Router, Firewall, DNS, Load Balancer, LDAP, Radius, Captive Portal, …….

Pelo nell'uovo: interfaccia Web spartana

Limiti:

- non semplice da patchare (almeno per me)
- unico livello di privilegi per la sua gestione/configurazione

Vantaggi:

- Ben noto perchè già in uso (o usato) con funzioni di Load Balancer/Failover e Captive Portal
- Disponibilità di Zerotruth
- FreeRadius e LDAP già integrati

ZEROSHELL & ZEROTRUTH

Zerotruth: Plugin di ZS per la gestione delle utenze del Captive Portal

Vantaggi:

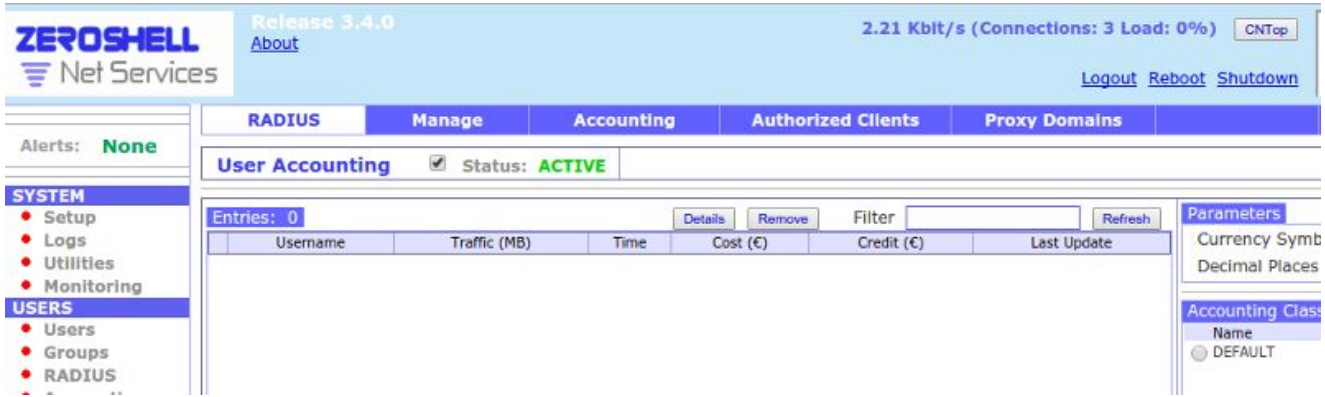
- Introduce un portale dedicato alla gestione delle utenze
- Prevede livelli di privilegi differenti per l'accesso al portale

Le utenze vengono memorizzate in LDAP pertanto sono utilizzabili da qualunque servizio, tra cui FreeRADIUS

Suggerimento: Per installare ZT occorre abilitare il Captive Portal in ZS, farlo su una interfaccia di rete non utilizzata (es. VPN99)

ARCHITETTURA DELLA SOLUZIONE

Il Radius di ZS supporta i protocolli EAP-TLS, EAP-TTLS e PEAP e dispone di una interfaccia web che consente di configurarlo in modo facile e veloce.



ma ….

ARCHITETTURA DELLA SOLUZIONE

…. gli attribute files non sono conformi a quanto richiesto dalla Federazione Eduroam

- mods-config/attr_filter/pre-proxy o raddb/attrs.pre_proxy

```
DEFAULT
        User-Name =* ANY,
        EAP-Message =* ANY,
        Message-Authenticator =* ANY,
        State =* ANY,
        Proxy-State =* ANY,
        Operator-Name =* ANY,
        Class =* ANY,
        Calling-Station-Id =* ANY,
        Chargeable-User-Identity =* ANY,
        CHAP-Password =* ANY,
        CHAP-Challenge =* ANY,
        MS-CHAP-Challenge =* ANY,
        MS-CHAP-Response =* ANY,
        NAS-IP-Address =* ANY,
        NAS-Identifier =* ANY,
        NAS-Port-Type =* ANY,
```

- mods-config/attr_filter/post-proxy o raddb/attrs(.post_proxy)

```
DEFAULT
        Reply-Message =* ANY,
          Proxy-State =* ANY,
          EAP-Message =* ANY,
          Message-Authenticator =* ANY,
          MS-MPPE-Recv-Key =* ANY,
          MS-MPPE-Send-Key =* ANY,
          State =* ANY,
          Calling-Station-Id =* ANY,
          Operator-Name =* ANY,
          User-Name =* ANY,
          Class =* ANY,
          Chargeable-User-Identity =* ANY
```

Si potrebbe patchare ZS!

Optato per un'altra soluzione

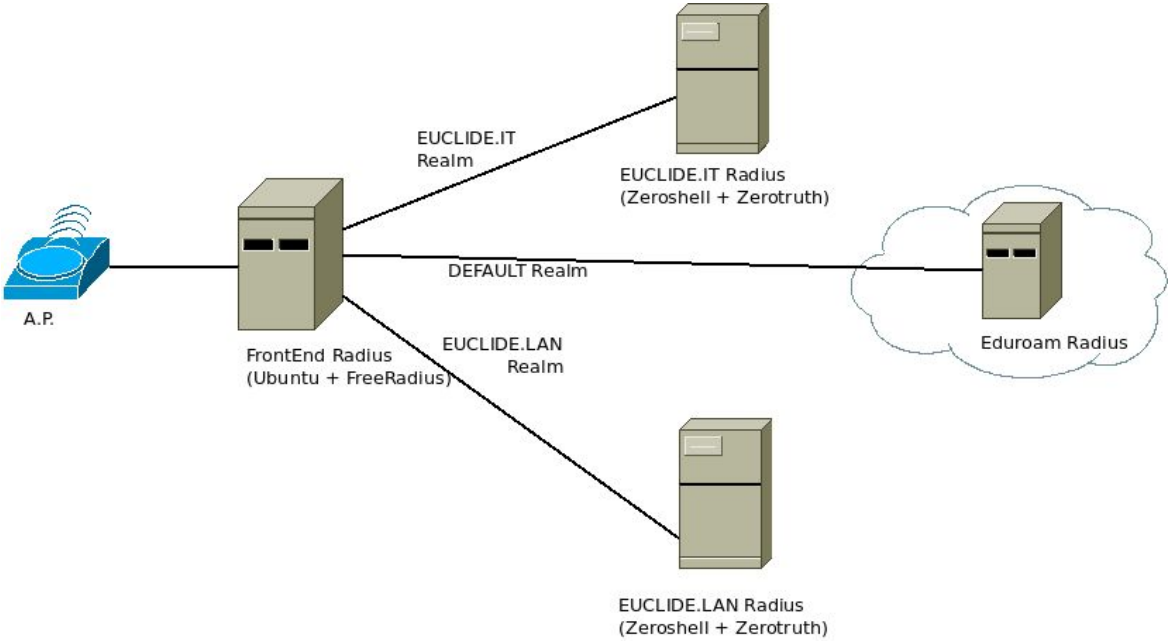
……

ARCHITETTURA DELLA SOLUZIONE

FrontEnd Radius: Inoltra le richieste provenienti dagli A.P.

EUCLIDEBARI.IT Radius: Responsabile autenticazione del Realm euclidebari.it

EUCLIDEBARI.LAN Radius: Responsabile autenticazione del Realm euclidebari.lan (utenti abilitati solo alla connessione locale)



INSTALLAZIONE DEL FRONTEND RADIUS

FreeRadius è stato installato su una installazione di Ubuntu, prendendolo dal repository ufficiale:

```
# apt-get update; apt-get install freeradius freeradius-utils
```

Suggerimenti per Ubuntu:

- Usare sempre versioni LTS - Long Term Support (14.04 o 16.04 quando sarà disponibile)
- Installare Ubuntu Server o se si desidera l'interfaccia grafica, Xubuntu

CONFIGURAZIONE DI FREERADIUS

root@edurub1404-2: /etc/freeradius

```
home_server_pool EDUROAM-FTLR {
        type    = fail-over
        home_server     = radius.garr.net
        home_server     = radius2.garr.net
}
home_server_pool EUCLIDEBARI-IT-FTLR {
        type    = fail-over
        home_server     = zs1.euclidebari.it
}
home_server_pool EUCLIDEBARI-LAN-FTLR {
        type    = fail-over
        home_server     = zs1.euclidebari.lan
}
realm DEFAULT {
        pool    = EDUROAM-FTLR
        nostrip
}
realm EUCLIDEBARI.IT {
        pool    = EUCLIDEBARI-IT-FTLR
        nostrip
}
realm EUCLIDEBARI.LAN {
        pool    = EUCLIDEBARI-LAN-FTLR
        nostrip
}
realm LOCAL {
}
realm NULL {
}
(END)
```

proxy.conf

root@edurub1404-2: /etc/freeradius

```
home_server radius.garr.net {
        type    = auth+acct
        ipaddr  = 192.84.145.15
        port    = 1812
        secret  = [redacted]
        status_check    = status-server
}
home_server radius2.garr.net {
        type    = auth+acct
        ipaddr  = 193.206.158.71
        port    = 1812
        secret  = [redacted]
        status_check    = status-server
}
home_server zs1.euclidebari.it {
        type    = auth+acct
        ipaddr  = 192.168.[redacted].11
        port    = 1812
        secret  = [redacted]
        status_check    = status-server
}
home_server zs1.euclidebari.lan {
        type    = auth+acct
        ipaddr  = 192.168.[redacted].14
        port    = 1812
        secret  = [redacted]
        status_check    = status-server
}
```

CONFIGURAZIONE DI FREERADIUS

```
client ReteGARREuclide {
        ipaddr          = [redacted]
        netmask         = [redacted]
        secret          = [redacted]
        shortname       = ReteGARREuclide
}
client radius.garr.net {
        ipaddr = 192.84.145.15
        netmask = 32
        secret = [redacted]
        shortname = radius.garr.net
}
client radius2.garr.net {
        ipaddr = 193.206.158.71
        netmask = 32
        secret = [redacted]
        shortname = radius2.garr.net
}
(END)
```

client.conf

```
server eduroam-inner-tunnel             {
      authorize      {
            auth_log
            eap
            files
            mschap
            pap   }

      authenticate  {
            Auth-Type PAP {
                  pap   }
            Auth-Type MS-CHAP {
                  mschap    }
            eap          }


      post-auth                        {
            reply_log
            Post-Auth-Type REJECT {
                  reply_log     }} }
```

sites-enabled/eduroam-inner-tunnel

CONFIGURAZIONE DI FREERADIUS

```
server eduroam
{
      authorize
{
            update request                              {
                  Operator-name := euclidebari.it }
            auth_log
            suffix
            eap                                       }
      authenticate
{
            eap
}
      preacct
{
            suffix
}
```

```
accounting { }
      post-auth                          {
            reply_log
            Post-Auth-Type REJECT {
                  reply_log     } }
      pre-proxy
{
            pre_proxy_log
            if("%{Packet-Type}" != "Accounting-
Request") {
                  attr_filter.pre-proxy
} }
      post-proxy                         {
            post_proxy_log
            attr_filter.post-proxy }
}
```

sites-enabled/eduroam

CONFIGURAZIONE DI FREERADIUS

```
DEFAULT
      User-Name =* ANY,
      EAP-Message =* ANY,
      Message-Authenticator =* ANY,
      State =* ANY,
      Proxy-State =* ANY,
      Operator-Name =* ANY,
      Class =* ANY,
      Calling-Station-Id =* ANY,
      Chargeable-User-Identity =* ANY,
      CHAP-Password =* ANY,
      CHAP-Challenge =* ANY,
      MS-CHAP-Challenge =* ANY,
      MS-CHAP-Response =* ANY,
      NAS-IP-Address =* ANY,
      NAS-Identifier =* ANY,
      NAS-Port-Type =* ANY
```

attrs.pre-proxy

```
DEFAULT
      Reply-Message =* ANY,
      Proxy-State =* ANY,
      EAP-Message =* ANY,
      Message-Authenticator =* ANY,
      MS-MPPE-Recv-Key =* ANY,
      MS-MPPE-Send-Key =* ANY,
      State =* ANY,
      Calling-Station-Id =* ANY,
      Operator-Name =* ANY,
      User-Name =* ANY,
      Class =* ANY,
      Chargeable-User-Identity =* ANY
```

attrs.post-proxy

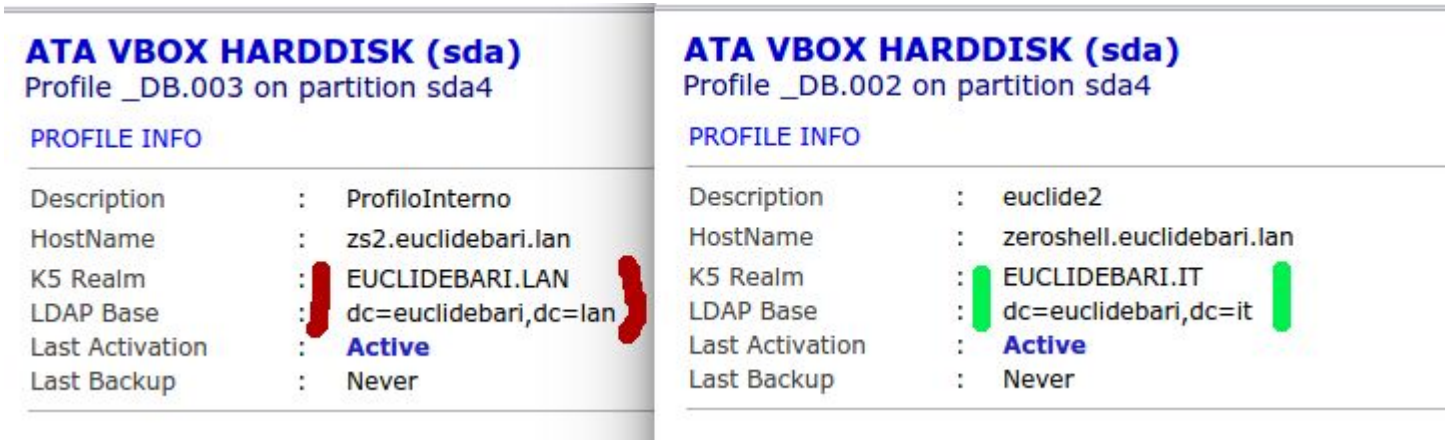
CONFIGURAZIONE DI ZEROSHELL

In rete ci sono tanti tutorial che spiegano come fare l'installazione, pertanto solo alcuni consigli:

- Fare una installazione basata sull'uso del LiveCD. Questo semplifica gli aggiornamenti (basta sostituire il CD), se si usa una VM ed un'immagine ISO, è praticamente la stessa cosa che installare su HD
- Fare un'installazione standard (come da guide) e solo successivamente creare ed attivare un apposito profilo

CONFIGURAZIONE DI ZEROSHELL

Dati di configurazione dei profili (.LAN e .IT)



ATA VBOX HARDDISK (sda)
Profile _DB.003 on partition sda4

PROFILE INFO

Description	:	ProfiloInterno
HostName	:	zs2.euclidebari.lan
K5 Realm	:	EUCLIDEBARI.LAN
LDAP Base	:	dc=euclidebari,dc=lan
Last Activation	:	**Active**
Last Backup	:	Never

ATA VBOX HARDDISK (sda)
Profile _DB.002 on partition sda4

PROFILE INFO

Description	:	euclide2
HostName	:	zeroshell.euclidebari.lan
K5 Realm	:	EUCLIDEBARI.IT
LDAP Base	:	dc=euclidebari,dc=it
Last Activation	:	**Active**
Last Backup	:	Never

Sono richiesti durante la creazione del profilo.
N.B. quello che conta sono il K5 Realm e LDAP Base, che devono essere coerenti, l' hostname è indipendente e poco importante.

CONFIGURAZIONE DI ZEROSHELL

Chi può utilizzare il Radius (equivale al client.conf). Occorre inserire il server FrontEnd Radius.

ZEROSHELL & ZEROTRUTH

Perchè ZeroTruth?

ZeroTruth mette a disposizione un'interfaccia dedicata alla sola gestione delle utenze.

E' possibile definire apposite utenze di gestione di ZeroTruth con livelli di privilegi differenziati.

Da http://www.zerotruth.net/

... il "limite" [di Zeroshell], … , era poi dare in mano la gestione ad una persona con poche competenze che, dall'interfaccia di zeroshell, potesse aver accesso a tutte le funzioni.

INSTALLAZIONE DI ZEROTRUTH

Da http://www.zerotruth.net/ è possibile scaricare il software http://www.zerotruth.net/download.php ed è disponibile la **guida all'installazione**, peraltro molto semplice (può durare diversi minuti!)

Ricordarsi di attivare da ZS il Captive Portal prima di procedere con l'installazione di ZT (farlo su un NIC inutilizzato, come VPN99)

Del manuale http://www.zerotruth.net/controldl.php?file=ZEROTRUTH.pdf consultare i capitoli 3, 4.1, 4.2, 4.3, 4.4 e 5

ZEROTRUTH


22:12:05 Martedi, 12 Aprile
ZeroTruth
Interface For Zeroshell Captive Portal
ZEROSHELL
Net Services
ZeroTruth
interface for Zeroshell Captive Portal
Lista Utenti
Aggiungi Utente
Profili
Config
Esci
Utenti Registrati
L
Aggiorna
Disconnetti Tutti
Blocca Tutti
Sblocca Tutti
Cancella Scaduti
Connessi
Cerca
N. S. Username Nome Cognome Email Telefono Scadenza S. I. Azioni
1 0 leonardo. Leonardo @gmail.com Illimitato
2 0 liborio. Liborio liborio@tiscali.it Illimitato
3 0 lucia. Lucia @gmail.com Illimitato
4 0 luciano. Luciano luciano. @gmail.com 31/08/2016

STRUMENTI DI TEST

http://deployingradius.com si trovano ottime indicazioni scritte da Alan DeKok, uno degli sviluppatori di FreeRadius

http://deployingradius.com/scripts/eapol_test/ è possibile scaricare i **sorgenti** di **EAPOL_TEST** che esegue tutte le funzioni di un wpa_supplicant (anche di più)

- PEAPv0
  - EAP-GTC
  - **EAP-MSCHAPv2**
- EAP-TTLS
  - **PAP**
  - **CHAP**
  - **MS-CHAP**
  - **EAP-MD5**
  - **EAP-MSCHAPv2**

Scaricando i file di configurazione di eapol_test (ci sono i link) e inserendo le giuste credenziali, è possibile **testare i protocolli indicati in celeste**
N.B. Taluni protocolli potrebbero non essere supportati

La compilazione sotto Linux-Ubuntu, oltre agli strumenti di sviluppo standard (make, gcc, …), potrebbe richiedere **l'installazione di librerie aggiuntive** la cui mancanza verrà indicata durante la fase di compilazione.
N.B. Le librerie che servono in fase di compilazione hanno il suffisso "-dev"

SUGGERIMENTI PER IL TEST

- Iniziare testando direttamente le installazioni di Zeroshell
  - Assicurarsi di aver abilitato l'IP dell'host da cui si lancia eapol_test
- Solo dopo aver superato il test dei ZS, passare a testare FreeRadius
  - Assicurarsi di aver abilitato l'IP dell'host da cui si lancia eapol_test
- Controllare sempre il log di FreeRadius per vedere cosa accade
  - In ZS aprire la finestra del log e selezionare la sezione `radiusd`
  - In FreeRadius il log si trova in /var/log/freeradius

N.B. *Nei file di test occorre commentare la riga* `anonymous_identity` *in quanto il valore assegnato non contiene il REALM*

Con iOS

Con iOS (solo) la prima connessione può andare in timeout:

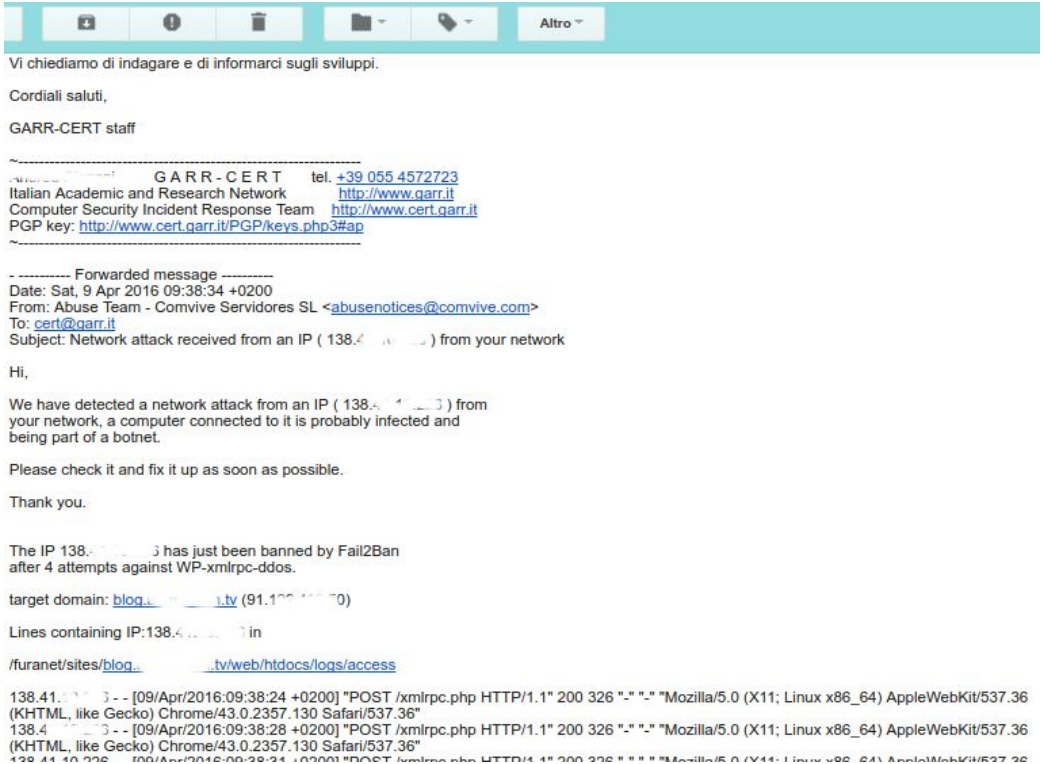
- è lunga di suo (non ho capito perchè)
- se il certificato proviene da una CA non riconosciuta, chiede la sua esplicita approvazione (timeout certo!)

Se è configurata un'altra rete WiFi presente nel range, questa viene subito attivata impedendo così il completamento dell'operazione.

Consiglio: rimuovere temporaneamente da iOS le reti WiFi presenti nel range per forzare iOS a completare la prima autenticazione.

Dopo la prima volta non c'è nessun problema.

E in caso di incidenti?



Altro

Vi chiediamo di indagare e di informarci sugli sviluppi.

Cordiali saluti,

GARR-CERT staff

~----------

GARR-CERT tel. +39 055 4572723
Italian Academic and Research Network http://www.garr.it
Computer Security Incident Response Team http://www.cert.garr.it
PGP key: http://www.cert.garr.it/PGP/keys.php3#ap
~----------

- ---------- Forwarded message ----------
Date: Sat, 9 Apr 2016 09:38:34 +0200
From: Abuse Team - Comvive Servidores SL <abusenotices@comvive.com>
To: cert@garr.it
Subject: Network attack received from an IP (138.) from your network

Hi,

We have detected a network attack from an IP (138.) from
your network, a computer connected to it is probably infected and
being part of a botnet.

Please check it and fix it up as soon as possible.

Thank you.

The IP 138. has just been banned by Fail2Ban
after 4 attempts against WP-xmlrpc-ddos.

target domain: blog. .tv (91.1 0)

Lines containing IP:138. in

/furanet/sites/blog. .tv/web/htdocs/logs/access

138.41. - - [09/Apr/2016:09:38:24 +0200] "POST /xmlrpc.php HTTP/1.1" 200 326 "-" "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.130 Safari/537.36"
138.4 - - [09/Apr/2016:09:38:28 +0200] "POST /xmlrpc.php HTTP/1.1" 200 326 "-" "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/43.0.2357.130 Safari/537.36"

SQUID+SQUIDGuard

- Filtro navigazione con blacklist
- Logging del traffico http e hhtps
- ……..

La presenza di un Proxy è ammessa.

Modalità di funzionamento di Squid:

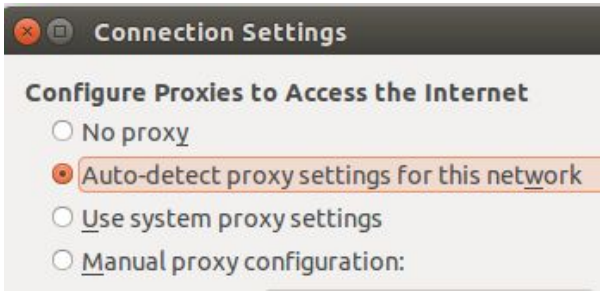
1. **Trasparente** - nessuna configurazione del client
2. **Explicita** - richiesta la configurazione del client

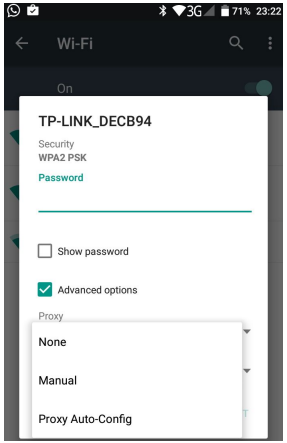
SQUID in Eduroam

- **Modalità Trasparente**. Con HTTPS è necessario che SQUID effettui l'SSL Bump, ma i browser rileverebbero un attacco MITM e comunque sarebbe "poco corretto" violare una connessione HTTPS
- **Modalità Esplicita**. Le connessioni HTTPS vengono gestite tramite l'apertura di un tunnel tra browser e server web; nessuna violazione della connessione SSL.
  E' necessario impostare sul client l'IP/hostname del proxy e la porta, ma questo potrebbe mettere in *difficoltà gli utenti "non tecnici"*

SOLUZIONE: Protocollo **WPAD/PAC** - Web Proxy Auto Discovery Protocol / Proxy Auto Config
Richiede: DHCP, DNS, Web Server locale

Il client richiede una configurazione semplice, di solito presente di default e compatibile con reti sprovviste di proxy.
NON Funziona con Android < 5





IMPLEMENTAZIONE DELLA PIATTAFORMA

+

La soluzione proposta prevede la presenza di 3 macchine.
Sono state implementate come VM con VirtualBox su Ubuntu.

Vantaggi di Ubuntu come Host di VirtualBox

1. La virtualizzazione delle reti funziona perfettamente senza alcun limite, in particolare le reti virtuali “interne” (usata per collegare fra loro le 3 macchine) e le VLAN 802.1Q
2. E’ possibile l’avvio automatico in background delle VMs http://yakupkorkmaz.info/?p=191