



**Sistemisti
indipendenti**

Zeroshell autenticatore RADIUS per reti Wireless

Introduzione

Come scritto nei precedenti HOWTO, Zeroshell è una distribuzione Linux derivata, orientata alla gestione di numerosi servizi di rete. Offre diverse funzioni tra cui quella di router, firewall, shaper e in particolare di Captive Portal per la gestione degli accessi ad internet tramite autenticazione mediante pagina web.

La gestione ed il controllo degli accessi ad internet è la parte secondo me più interessante e semplice da attivare grazie alle funzioni di Captive Portal e Transparent Proxy. Normalmente chi opta per una rete Wireless con ZS alle spalle come Captive Portal, configura gli Access Point senza autenticazione (WEP o WPA), lasciando proprio al Captive Portal il compito di gestire e registrare l'accesso degli utenti. In questo modo fino al CP l'accesso è libero e vengono superati tutti quei problemi di autenticazione dei dispositivi wireless, alcuni infatti non supportano i metodi più recenti come WPA/WAP2 Enterprise.

Questo metodo se da un lato risolve questo problema costringe i client (Notebook, Palmari, Tablet, Smartphone) ad avere a bordo un browser che supporti le finestre pop-up, per la gestione ed il mantenimento dell'autenticazione con il Captive Portal. E' proprio tramite questa finestra popup, che deve rimanere sempre aperta, che client e CP rinegoziano la chiave condivisa che permette di mantenere la sessione di navigazione attiva.

Questo sistema però non è supportato da molti dispositivi mobili, che hanno browser non in grado di superare questa fase e supportare questo metodo. Un'alternativa consiste nel mappare il MAC Address del dispositivo nel Captive Portal oppure scegliere un'altra strada. In questo caso ZS permette di essere utilizzato come **RADIUS Authenticator**, impostando gli Access Point perche utilizzino come metodo di autenticazione i metodi WPA-Enterprise oppure WEP-802.1x. In particolare la modalità Enterprise, dedicata alle realtà di reti estese, toglie la necessità di avere chiavi condivise uguali per tutti e autentica gli utenti attraverso un server RADIUS compatibile con lo standard 802.1x.

In questo caso però è il dispositivo wireless che deve essere in grado di autenticarsi per accedere successivamente al servizio. In questo caso però si può evitare la parte di autenticazione CP avere dopo l'autenticazione Wifi il libero accesso ad Internet.

Zeroshell Radius Service

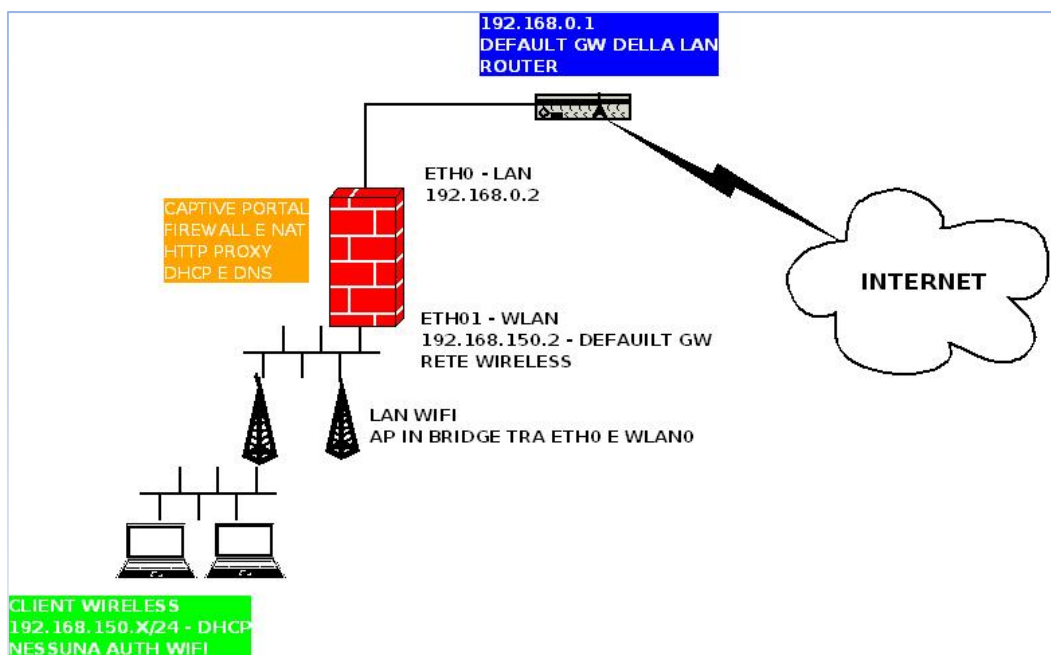
Zeroshell utilizza FreeRADIUS, per l'autenticazione dei client wireless, attraverso username e password (EAP-TTLS e PEAP) oppure tramite certificati digitali X.509 (EAP-TLS). L'utilizzo di WPA2 con un server RADIUS 802.1x offre le massime garanzie di sicurezza, ma obbliga l'utente alla configurazione del dispositivo Wireless. Questa operazione può creare qualche problema, specie per dispositivi wifi obsoleti ed è per questo motivo che in grandi realtà ed ambienti estesi si è preferito optare per la soluzione Hot Spot e



Captive Portal che consente l'accesso libero alla rete Wifi, senza autenticazione, per poi passare dalla pagina di web login per l'accesso ad internet.

Nel caso in cui non si voglia comunque lasciare l'accesso Wifi open e si voglia utilizzare un metodo di autenticazione degli utenti distribuito, ZS permette di gestire gli utenti attraverso il servizio RADIUS, sia tramite l'autenticazione con le credenziali (user e password) che con i certificati X509.

Prima di affrontare la parte di configurazione dei servizi necessari sul nostro sistema ZS, vediamo un semplice schema della nostra struttura di rete.



Il nostro sistema ZS rappresenta il nodo della rete posto tra la rete Wifi, con gli access point alle sue spalle e il gateway che permette l'accesso libero ad internet. In ogni caso ZS funge da strumento di controllo e autenticazione del traffico verso internet della rete Wifi.

Se vogliamo configurare Zs per autenticare tramite RADIUS il traffico proveniente dagli Access Point per prima cosa dobbiamo abilitare il servizio:

User>Radius>Enabled



Dopo aver cliccato su "Enabled", premere il bottone "Save". In questo modo il servizio Radius, si attiva. La gestione degli utenti e dei loro certificati viene fatta normalmente accedendo al menu USER.

A questo punto dobbiamo procedere con la mappatura degli access point che saranno abilitati all'uso del servizio Radius di ZS. Per fare questo servono l'indirizzo IP e la "Shared Secret". Questi due elementi permettono all'AP di associarsi e far passare il traffico crittografato.

Vediamo come aggiungere un AP alla lista, con una banale password di esempio 1234 (voi usatela robusta).

Radius>Access points >Add

Access Point Name	IP or Subnet	Shared Secret
TPALL	192.168.150.100/32	1234

Se il sistema non restituisce errori vuol dire che il nostro AP è associato.

Per visualizzare le connessioni degli utenti esiste un apposito bottone "Show Request" che mostra l'utente che si è connesso con il relativo MAC ADDRESS del suo dispositivo wireless.

Radius>Show Request



Screenshot of a Mozilla Firefox browser window displaying the 'Log Viewer' interface. The address bar shows 'https://192.168.17.235/'. The page title is 'Log Viewer - Mozilla Firefox'. The interface includes a sidebar with navigation options like 'SYSTEM', 'USERS', and 'NETWORK'. The main content area shows a list of system logs with timestamps and descriptions, such as '15:49:13 Loaded virtual server' and '17:02:36 Login OK: [paolo] (from client TPALL port 0)'.

A questo punto occorre solo creare gli utenti con relativi certificati e distribuirli.

USERS>Add

USERS List View Add Edit Delete X509 Kerberos 5

(New User) [Submit] [Reset]

Account Information

Username UID Primary Group GID

Home Directory Default Shell bash sh tcsh other /bin/sh

User Information

Firstname Lastname Organization

Description E-Mail Phone

RADIUS Accounting

Expiration (mm/dd/yyyy) / /

Accounting Class

Limits - MB - Hours - Mb/s Costs

User Password

Password

Confirm

Authentication Protocol

Kerberos 5

RADIUS (VLAN)

Da notare in particolare le voci in basso a destra Kerberos e RADIUS che devono essere abilitate (spuntate), di default lo sono.

Authentication Protocol

Kerberos 5	<input checked="" type="checkbox"/>
RADIUS (VLAN <input type="text"/>)	<input checked="" type="checkbox"/>

Tramite queste checkbox si può abilitare o disabilitare l'accesso dell'utente al servizio di Autenticazione Kerberos e Radius.



L'operazione di distribuzione invece può essere semplificata indicando l'accesso all'host ZS da cui poter scaricare i certificati



[X.509 certificates](#)
[CA](#) [Users](#) [Hosts](#) [CRL](#)

Username
Password

Nella parte destra della pagina di accesso al sistema ZS, si ha la possibilità di scaricare il certificato della CA e i certificato utente.

Il certificato della CA va salvato/esportato in formato DER, questo permette di essere installato sul nostro sistema semplicemente cliccandoci sopra e seguendo le fasi per caricare la CA sul nostro sistema (vedi Howto precedente su ZS).

X.509 Certificate View

CA: Status: OK

Certificato CA – FORMATO .DER

Certificate:

```
Data:
  Version: 3 (0x2)
  Serial Number:
    c4:f5:af:27:75:21:8c:2a
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=IT, ST=Piemonte, L=Grugliasco, O=TPALL Universita, OU=TPALL CED, CN=TPALL CA/emailAd
  Validity
    Not Before: May 24 10:03:11 2011 GMT
    Not After : May 21 10:03:11 2021 GMT
  Subject: C=IT, ST=Piemonte, L=Grugliasco, O=TPALL Universita, OU=TPALL CED, CN=TPALL CA/emailAd
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:c9:31:57:fe:c3:1d:00:1a:81:19:35:2a:9d:eb:
        97:58:86:02:61:68:97:7c:7d:20:6a:02:fa:14:a6:
        28:41:cl:6d:f5:d5:31:18:3d:e2:22:23:bf:b8:12:
        cc:df:fc:10:34:ea:f2:f2:3d:ab:dc:d3:15:43:ad:
        71:c6:8b:22:ed:0d:8f:10:1a:f7:a7:ed:02:f1:72:
        78:57:6e:c6:48:b1:aa:e5:e0:7e:30:22:26:5a:f1:
        72:f5:e2:21:ba:1f:08:90:d4:d5:d8:e8:22:b3:4b:
        42:81:e4:3f:0c:1e:78:6e:f0:62:0d:3b:cc:ba:d5:
        bf:e4:0c:83:a3:f0:bc:d8:e3
      Exponent: 65537 (0x10001)
```

Il certificato utente va invece salvato/esportato in formato PKCS#12(PFX), questo permette di essere installato sul nostro sistema semplicemente cliccandoci sopra e seguendo le fasi per caricare il nostro certificato personale sul nostro sistema.



X.509 Certificate View
user: paolo Status: OK

Export PKCS#12 (PFX)

Certificato Utente – FORMATO .PKCS#12

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 5 (0x5)
  Signature Algorithm: md5WithRSAEncryption
  Issuer: C=IT, ST=Piemonte, L=Grugliasco, O=TPALL Universita, OU=TPALL CED, CN=TPALL CA/emailAdd
  Validity
    Not Before: May 27 11:50:54 2011 GMT
    Not After : May 26 11:50:54 2012 GMT
  Subject: OU=Users, CN=paolo/emailAddress=paolopav@gmail.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:c6:43:69:60:ba:29:57:23:71:a8:42:4d:e7:de:
        dc:b7:5f:13:79:ea:6d:67:12:6b:72:f2:30:16:03:
        a3:fd:05:b7:eb:54:78:74:da:db:c0:f0:4f:2d:65:
        02:48:19:7e:4c:82:dc:cc:da:99:29:26:eb:8f:de:
        f8:be:85:68:e4:4f:9c:fa:46:b6:f6:09:8c:e4:b5:
        a5:a0:23:ba:35:57:71:21:44:b5:57:01:4e:ba:06:
        51:f0:0b:48:c3:ae:ac:8a:0e:90:17:a3:b1:1a:fb:
        8b:95:7b:6a:51:49:c0:dd:7c:cc:ca:c9:e7:25:2e:
        24:7f:1c:14:cf:48:02:4d:47
      Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Key Usage:
```

Attenzione!! E' buona norma fornire comunque ad ogni utente il suo account (user e password), corredato di certificato (CA e Utente)

Configurazione Access Point

Ovviamente gli AP utilizzati per questo tipo di installazione devono supportare metodi di autenticazione per cui poter specificare un server Radius Remoto (nel nostro caso ZS). I metodi supportati sono:

WPA/WAP2-Enterprise

WEP-802.1x

Nel nostro schema di configurazione oltre all'Access Point, al Radius Authenticator (ZS) avremo il supplicant, ovvero il client che richiede di essere autenticato ed ammesso all'accesso alla rete. Come detto il server RADIUS di Zeroshell supporta i metodi di autenticazione EAP e PEAP che sono tra quelli che danno maggiore garanzia di sicurezza e sono supportati da buona parte dei supplicant:

- **EAP-TLS** che usa TLS per la mutua autenticazione tra supplicant e Access Point, tanto il server RADIUS quanto il supplicant devono disporre di una chiave privata e del relativo certificato X.509. Per questo motivo ad ogni utente/client occorre fornire il proprio certificato, cosa che lo rende il metodo di autenticazione più sicuro e comodo poiché non viene richiesto l'inserimento di una password da parte dell'utente
- **PEAP (Protected EAP)** utilizza TLS per autenticare l'Access Point e stabilire un tunnel crittografato in cui utilizzare il protocollo MS-CHAPv2 per autenticare il supplicant tramite l'inserimento di username e password. Questo metodo è più semplice infatti solo il server RADIUS deve disporre di un certificato server e della chiave privata mentre l'utente usa le stesse credenziali (user e password) utilizzate per autenticarsi con Kerberos 5.

Dallo schema di funzionamento sembrerebbe che sia con EAP-TLS che con PEAP gli Access Point non siano in grado di certificare loro identità nei confronti dei supplicant poiché non sono dotati di un certificato e di una chiave privata. In verità non è così poiché gli Access Point condividono con RADIUS una "Shared Secret"



che li rende fidati nei confronti di quest'ultimo. Tale fiducia permette a un supplicante che si fida di RADIUS (grazie al TLS) di fidarsi anche degli Access Point.

Vediamo ad esempio come configurare un AP tipo Cyber Guard SG5560 perché supporti il metodo di autenticazione WPA-Enterprise. Sotto la voce Network Setup selezioniamo:

Network Setup> Wireless>Edit> Security Method> WPA-Enterprise/ WPA Encryption TKIP

SECURE COMPUTING

Network Setup

Connections | Failover & H/A | Routes | System | DNS | IPv6

Wireless Configuration

Access Point | ACL | WDS | Advanced

Access Point Configuration

MAC Address: 00:14:A5:06:BF:75

ESSID: TPALL

Broadcast ESSID:

Channel/Frequency: 1 / 2412 MHz

Bridge Between Clients:

Security Method: WPA-Enterprise

WPA Encryption: TKIP

Update | Cancel

Poi vediamo come configurare e testare la connessione al Radius Server (ZS). Accediamo al menu

SYSTEM>Users>RADIUS

SECURE COMPUTING

RADIUS Configuration

Administrative Users | Local Users | RADIUS | TACACS+

RADIUS | Test RADIUS

RADIUS Server

RADIUS Server: 192.168.150.2

RADIUS Server Port: 1812

RADIUS Secret: ●●●●

Confirm RADIUS Secret: ●●●●

Submit

Inseriamo i parametri necessari:

- 192.168.150.2 → è l'IP dell'Interfaccia di ZS verso la LAN WIFI.
- 1812 è la porta del Radius server



- Radius Secret: è la password associata all'AP, caricato (mappato) precedentemente in ZS

Radius Secret -> quello impostato in ZS per l'access Point

Effettuare il test per provare l'utente.

Test RADIUS Configuration

Administrative Users Local Users **RADIUS** TACACS+

RADIUS Test RADIUS

Action Successful

Access Granted for user: **paolo**

Test RADIUS Configuration

Username

Password

Submit

A questo punto i nostri client (supplicant) dovrebbero poter accedere alla rete in quanto autenticati dal RADIUS Server tramite user password del servizio Kerberos oppure tramite i certificati del servizio CA X509.

Configurazione dei Client Wireless (supplicant)

Per accedere alla rete Wireless attraverso il nostro client, è necessario che il supplicant supporti il metodo di autenticazione scelto, in questo caso WPA/WPA2-Enterprise oppure WPA-802.1x

Per poter accedere occorre installare il certificato della CA in formato DER, e fornire user e password come per un normale login. Solo che in questo caso l'AP passerà nel tunnel crittografato i dati al Radius Server (ZS) che provvederà all'autenticazione dell'utente.

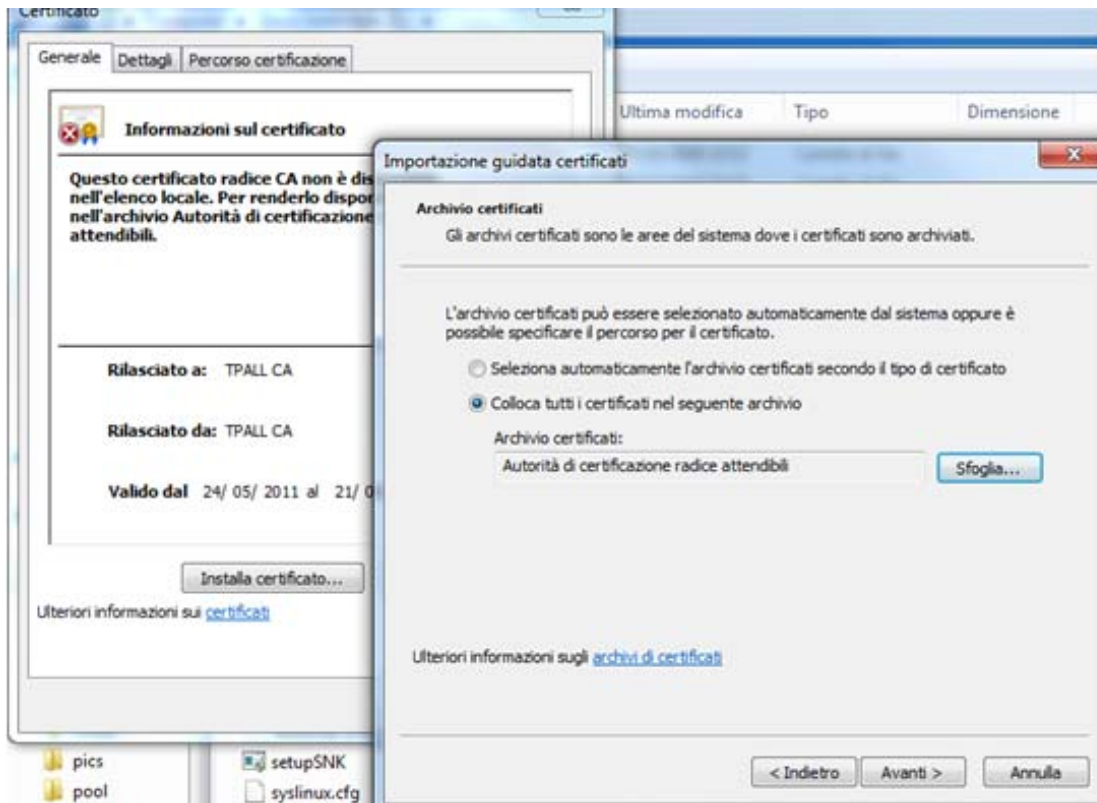
Se volessimo riepilogare in modo generico i dati necessari all'autenticazione:

- Sicurezza Senza Fili: WPA/WPA2
- Autenticazione: TLS via Tunnel
- Certificato CA: CA.DER
- Autenticazione interna: MSCHAPv2
- Nome utente: utente assegnato
- Password: password assegnata

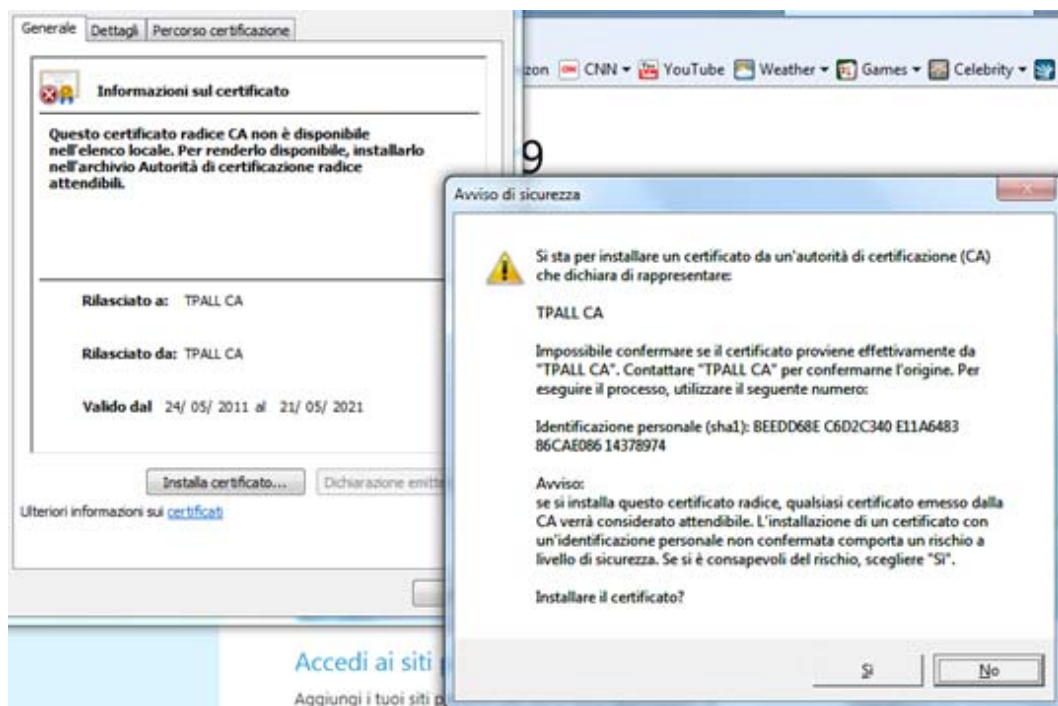
Sotto Windows prima di connetterci alla rete Wireless carichiamo il certificato della CA (formato DER), o da un supporto rimovibile o scaricandolo dalla home di Zeroshell, sezione CA.

Basta un doppio clic sul file certificato CA.DER.

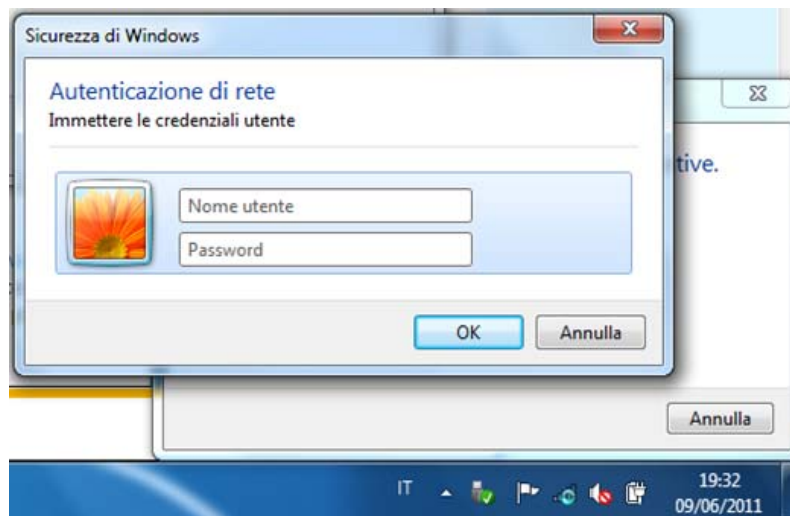
Il certificato va messo nella Sezione "Autorità di certificazione radice attendibili"



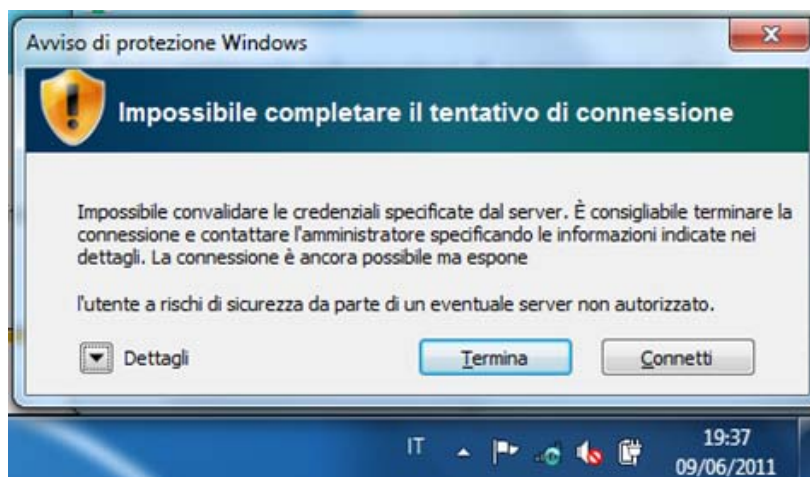
Si può procedere fino al termine dell'importazione che restituisce un Avviso sull'avvenuta importazione del certificato della CA della nostra WLAN.



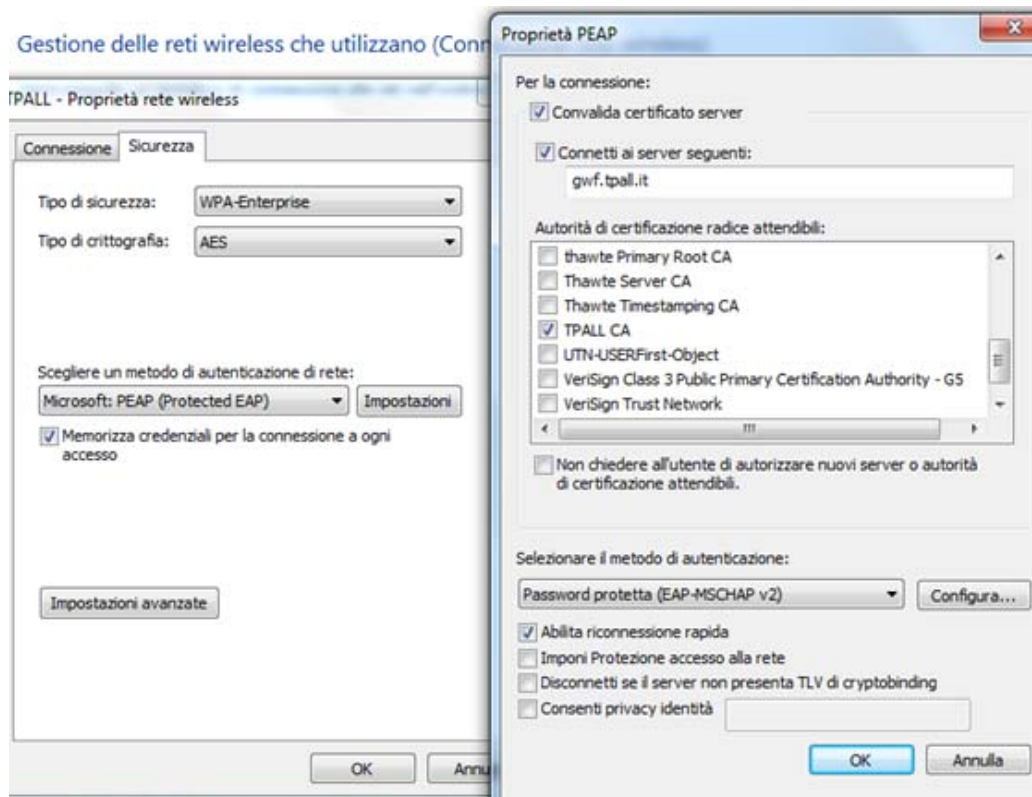
A questo punto si può procedere alla connessione alla rete Wireless:



Nel caso in cui il client mostri un messaggio di server non autenticato, dipende dal fatto che la CA non è riconosciuta dal Browser. Si può tranquillamente accettare e continuare la connessione.



La procedura di autenticazione prevede il salvataggio delle credenziali assieme al certificato della CA, senza il quale sarebbe impossibile accedere. In questo modo le successive riconessioni avvengono automaticamente, senza ulteriori richieste di credenziali.



Come si può vedere il nostro dispositivo wireless (supplicant) identifica la rete WPA-Enterprise e una volta caricato il certificato CA, richiede la validazione delle credenziali fornite al server Radius.

La voce "Abilita connessione rapida" permette appunto la riconnessione con le credenziali salvate.

La connessione da un desktop Linux è ancora più semplice e non presenta difficoltà:





Sistemisti indipendenti

La maschera permette di specificare tutti parametri necessari, in realtà è sufficiente indicare user/password oltre al certificato della CA. Questo permette di connettersi senza ulteriori messaggi o avvisi.

Controllo LOG sotto Zeroshell

Una delle funzioni più interessanti del Captive Portal è quella di poter tracciare l'accesso e l'attività dell'utente. Nel caso in cui si opti per l'autenticazione tramite Radius e si disabiliti il servizio di Captive Portal, si può comunque effettuare una traccia completa dell'accesso (utente) incrociando le informazioni di diversi file di log. I file di log da analizzare sono radiusd, Contrack e proxy.

```
root@gwf gwf> tail -f radiusd
Jun  8 18:55:56 gwf radiusd[2831]: Login incorrect: [paolo] (from client TPALL port 0)
Jun  8 18:56:13 gwf radiusd[2831]: Login incorrect: [paolo] (from client TPALL port 0)
Jun  8 18:56:35 gwf radiusd[2831]: Login OK: [paolo] (from client TPALL port 0)
Jun  8 18:56:53 gwf radiusd[2831]: Login OK: [paolo] (from client TPALL port 0 via TLS tunnel)
Jun  8 18:56:53 gwf radiusd[2831]: Login OK: [paolo] (from client TPALL port 0 cli 00-21-5D-D3-7C-90)
    → utente con associato MAC ADDRESS
```

Dal MAC Address possiamo ottenere l'indirizzo IP fornito dal nostro DHCP nella sessione.

```
root@gwf gwf> arp -a |grep 00:21:5D:D3:7C:90
? (192.168.150.102) at 00:21:5D:D3:7C:90 [ether] on ETH01
    → Indirizzo IP associato al MAC ADDRESS
```

Nei LOG di Contrack e proxy (se attivo) si possono tracciare le connessioni effettuate dall'utente

```
root@gwf gwf> tail -f ConnTrack |grep 192.168.150.102
Jun  8 18:59:31 gwf ConnTrack: [DESTROY] udp    17 src=192.168.150.102 dst=192.168.150.2 sport=51802
dport=53 packets=1 bytes=73 src=192.168.150.2 dst=192.168.150.102 sport=53 dport=51802 packets=1
bytes=329
Jun  8 18:59:31 gwf ConnTrack: [DESTROY] udp    17 src=192.168.150.102 dst=192.168.150.2 sport=55190
dport=53 packets=1 bytes=62 src=192.168.150.2 dst=192.168.150.102 sport=53 dport=55190 packets=1
bytes=268
Jun  8 18:59:49 gwf ConnTrack: [DESTROY] udp    17 src=192.168.150.102 dst=192.168.150.255 sport=138
dport=138 packets=1 bytes=237 src=192.168.150.255 dst=192.168.150.102 sport=138 dport=138
packets=0 bytes=0
```

Se impostato anche il proxy trasparente sarà possibile anche risalire ai siti consultati.

```
root@gwf gwf> tail -f proxy |grep 192.168.150.102
Jun  8 18:45:11 gwf proxy[28324]: 192.168.150.102 GET 200 http://secure-it.imrworldwide.com/cgi-bin/m?
305+44 OK
Jun      8      18:45:12      gwf      proxy[28352]:      192.168.150.102      GET      200
http://www.repubblica.it/images/2011/06/08/090122871-b2db75f7-1c33-400d-9e86-9a084d828cb8.jpg
385+73821 OK
Jun  8 18:45:13 gwf proxy[383]: 192.168.150.102 GET 200 http://secure-it.imrworldwide.com/cgi-bin/m?
305+44 OK
```



Sistemisti indipendenti

Jun 8 18:45:14 gwf proxy[32204]: 192.168.150.102 GET 200
http://www.repubblica.it/images/2011/06/08/090122887-c2aa04f1-b1f4-4c1f-9e55-a5f782497657.jpg
385+97754 OK

Considerazioni finali

Come si può notare anche optando per questa soluzione, disabilitando il Captive Portal, si può comunque mantenere traccia degli accessi e delle consultazioni effettuate dagli utenti. La differenza sostanziale è che la rete Wireless non è open, ma bensì protetta da un robusto metodo di autenticazione e che la centralizzazione ed il controllo degli utenti avviene sempre attraverso il nostro sistema Zeroshell attraverso cui gli utenti sono costretti a passare.

Mettere in piedi una soluzione di questo tipo è semplice quanto efficace e consente di realizzare una struttura di autenticazione valida e robusta per la nostra rete Wifi. E' consigliabile in quelle situazioni in cui non si vuole realizzare una Wifi area di tipo Open e si preferisce gestire la fase di autenticazione direttamente dal dispositivo Wireless.

Risorse

- <http://www.zeroshell.net/radiusdetails/>
- <http://www.zeroshell.net/fag/wifi/>
- <http://bryanpopham.com/tutorials/ZeroShell-WPA-Enterprise.pdf>
- <http://www.linuxplanet.com/linuxplanet/tutorials/6737/1>

Doc: zeroshell-radius1.pdf

Dott. Paolo PAVAN [Netlink Sas]– admin@sistemistiindipendenti.org

Data: Giugno 2011

Note finali

- Il presente documento è a semplice scopo divulgativo
- L'autore non si assume la responsabilità di eventuali danni diretti o indiretti derivanti dall'uso dei programmi, o dall'applicazione delle configurazioni menzionate nel seguente articolo
- I marchi citati sono di proprietà dei rispettivi proprietari e sono stati utilizzati solo a scopo didattico o divulgativo.
- Il documento viene rilasciato sotto Licenza Creative Commons.
- Sono possibili errori o imprecisioni, segnalatemele a admin@sistemistiindipendenti.org
- Chi volesse integrare il presente documento, può scrivere a admin@sistemistiindipendenti.org
- Questo documento è stato pubblicato su <http://www.sistemistiindipendenti.org>