Zeroshell come CAPTIVE PORTAL

Introduzione

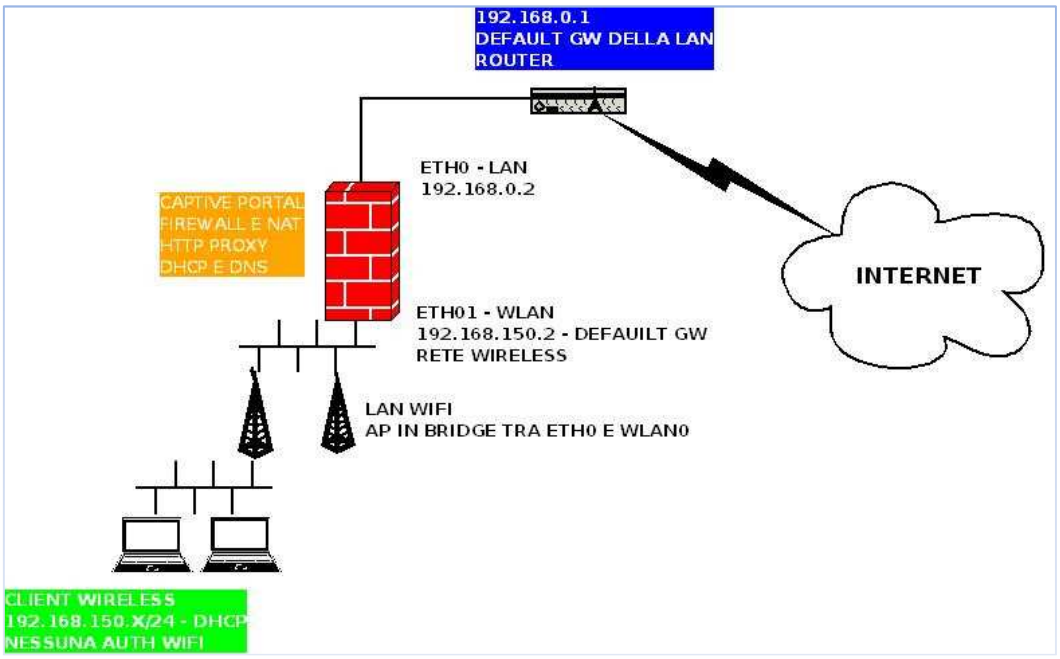
Il Captive Portal

Nel caso in cui si voglia fornire un accesso ad Internet attraverso un accesso autenticato, si può usare un dispositivo noto come *Captive Portal*, che permette di 'autenticare gli utenti mediante credenziali come user e password oppure certificati digitali (X509).
Questo dispositivo in pratica diventa il gateway per una rete, ossia funge da default router per la zona da proteggere, nel mio caso una LAN Wifi posta alle spalle e configurata in bridge su una delle interfacce del Captive Portal.
In questo modo il CP blocca il traffico IP diretto verso l'esterno, mentre "cattura" qualsiasi richiesta HTTPS o HTTPS diretta alle porte TCP 80 e 443 e la redirige verso un web server per l'autenticazione, a cui fornire credenziali. Se l'utente dispone delle credenziali corrette, l'Autentication Server comunica al gateway che l'host è autorizzato e gli viene permesso l'accesso ad Internet..

L'obiettivo è quello di realizzare un captive portal per una struttura ad accesso controllato su rete Wireless. Si dispone di:

- uno o più Access Point ad accesso Libero senza schema di autenticazione per facilitare la connessione di qualsiasi dispositivo,
- un piccolo PC da utilizzare come Captive Portal per autorizzare e registrare le connessione degli utenti autorizzati
- Un accesso ADLS attraverso la LAN (Default GW)

Vediamo lo schema:



Descriviamo brevemente la struttura:

- Rete Wireless con uno o più Access Point, con un bridge realizzato tra eth0 e wifi0
  - br0 192.168.150.100
- Zeroshell con due schede: una connessa allo switch della WIFI (AP) e una allo switch della LAN
  - ETH01 192.168.150.2
  - ETH00 192.168.0.2
  - SU ZS abilitare http Proxy, Captive portal e NAT
  - Abilitare il DNS e impostare un forwarder verso il DNS della tua rete.
- Assegnare come default GW quello della LAN
  - 192.168.0.1

Attenzione!! Gli indirizzi IP e le classi utilizzate sono puramente indicative e possono essere sostituite della propria struttura.

Note di Lettura

Alcune sigle utilizzate:

- ZS: Zeroshell
- CP: Captive Portal
- LAN: Local Ara Network
- GW: Default Gateway
- AP: Access point
- QoS: Quality of Service
- VPN: Virtual Private Network
- DHCP: Dynamic Host Configuration Protocol
- CA: Certification Authority

Zeroshell: La Scelta

Lo strumento che ho scelto come cardine di questo lavoro è **Zeroshell** (versione b14), di cui mi hanno interessato da subito le funzioni come Captive Portal, le atre funzioni in parte utilizzate mi sono servite solo a livello accessorio e non le ho approfondite.

Zeroshell è una distribuzione Linux per server e dispositivi embedded il cui scopo è fornire i principali servizi di rete, tra cui Firewall, NAT, VPN e Captive Portal. Una delle sue qualità migliori e la semplificazione dell'amministrazione che avviene tramite interfaccia web, ma che permette comunque anche il controllo via console della maggior parte delle funzioni.
E' stato sviluppato da *Fulvio Ricciardi*, che ha "donato" alla comunità uno strumento integrato davvero valido e ricco di funzionalità.

La home del progetto si trova

- http://www.zeroshell.net/

Per una descrizione dettagliata delle funzioni e per trovare maggiori informazioni, vi consiglio di visitarlo attentamente e di leggere prima bene la documentazione contenuta..

Le domande ed il supporto lo potete chiedere al forum ufficiale. Anche in questo casa essendo uno strumento ricco di funzioni, anche complesse, richiede in molti ambiti di applicazione una certa conoscenza dei sistemi e delle reti, per cui è bene prima di tutto fare una serie di prove e applicarsi per la risoluzione del problema, ricercando sul forum o su google eventuali documenti che possano aiutarci ad andare oltre. In caso contrario è bene chiedere alla comunità, fatelo qui:

- http://www.zeroshell.net/forum/

Vediamo adesso come ho strutturato la mia installazione partendo dal punto di accesso dei Client ovvero l'Access Point.

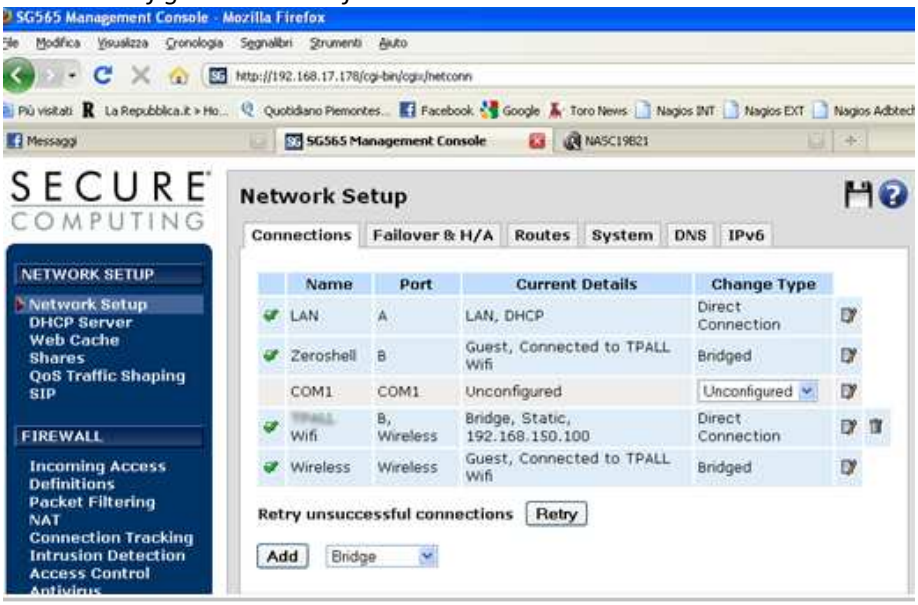
Access Point e rete Wifi

L'accesso ad internet avviene tramite uno o più AP, che per motivi di semplificazione delle procedure di autenticazione, dei vari dispositivi wireless, viene configurato senza lacuna forma di autenticazione nel modo più piatto ed usufruibile possibile.
Dal punto di vista della configurazione, viene realizzato un bridge tra la scheda ethernet connessa al Captive Portal alle spalle della LAN e la scheda wifi, vediamo come sulla base delle mie configurazioni :

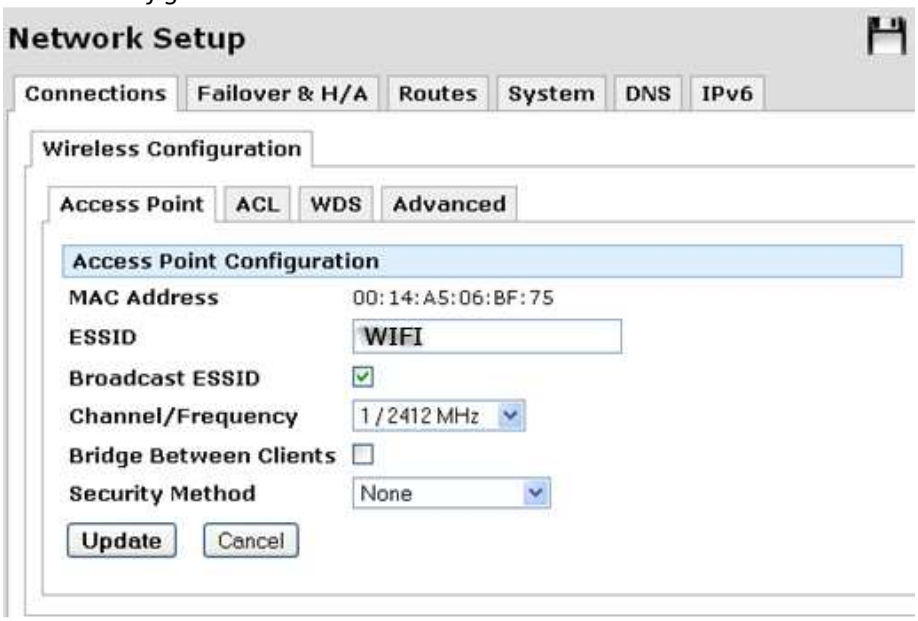
eth+wifi=br0 192.168.150.100 -→ 192.168.150.2 (ETH01 ZS)

Come autenticazione viene impostato NONE, nessuna sicurezza in questo modo la parte di autenticazione viene demandata e centralizzata sul Captive Portal (Zeroshell). Anche il DHCP per i client wifi che si connettono sarà gestito da ZS, in modo da centralizzare la gestione e rendere più semplice possibile.
Vediamo qualche schermata relativa al dispositivo wireless da me utilizzato come PA, ovvero un Cyberguard SG:

SG505 – Configurazione interfacce

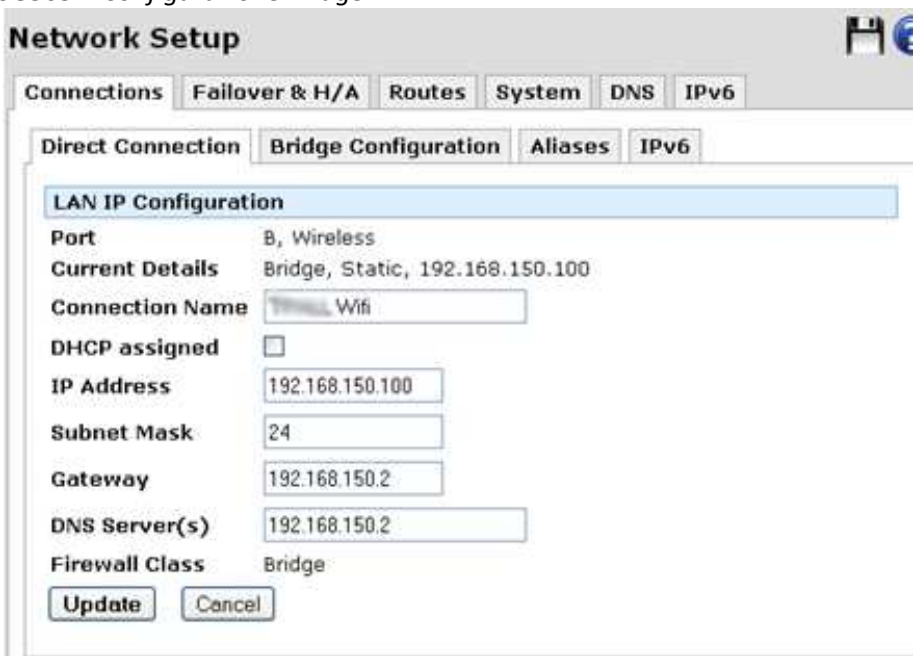


SG565 – Configurazione Wireless



Il bridge è dato dall'unione della scheda Wifi e della scheda LAN connessa al nostro CP. Ogni AP gestisce in modo diverso questa operazioni, per alcuni è addirittura automatica, di tipo autosensing.

SG565 – Configurazione Bridge



Come si può notare l'indirizzo IP di Gateway e DNS è impostato a 192.168.150.2, che è l'indirizzo IP associato all'ETH01 della box Zeroshell.

Attenzione! Nel caso in cui si volesse aumentare la sicurezza si può impostare una protezione WEP o WPA/PSK necessaria per la connessione del dispositivo Wireless a cui seguirà comunque l'autenticazione del Captive Portal, per un meccanismo più sicuro ma con una doppia fase di autenticazione.

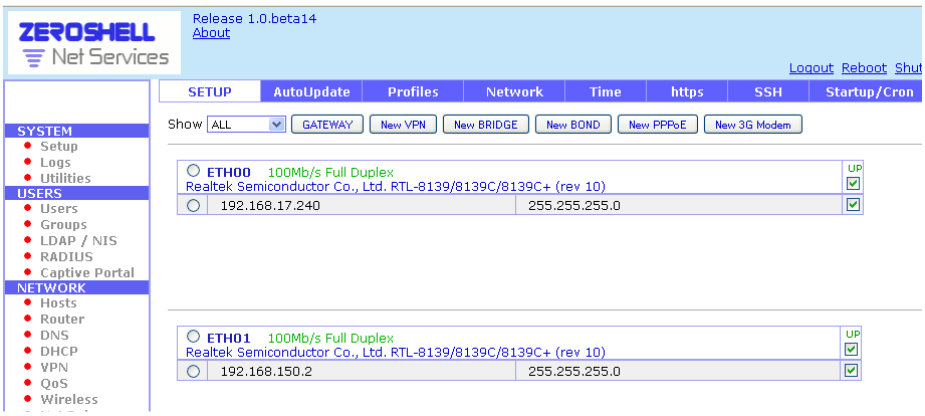
Il Captive Portal

Il nostro Captive Portal è rappresentato da una box con Zeroshell installato. Rappresenta il sistema centrale della nostra installazione, va installato su HD o su Pendrive, configurato con due schede di rete almeno, una sulla LAN in cui è presente il default GW della rete e una connessa ad una LAN dedicata su cui sono collegati gli AP, in caso di un singolo AP si può collegarlo direttamente a ZS con un cavo cross.
In questo documento non trattiamo l'installazione di ZS nello specifico, per quello rimandiamo alla documentazione ufficiale:

- http://www.zeroshell.net/documentation/

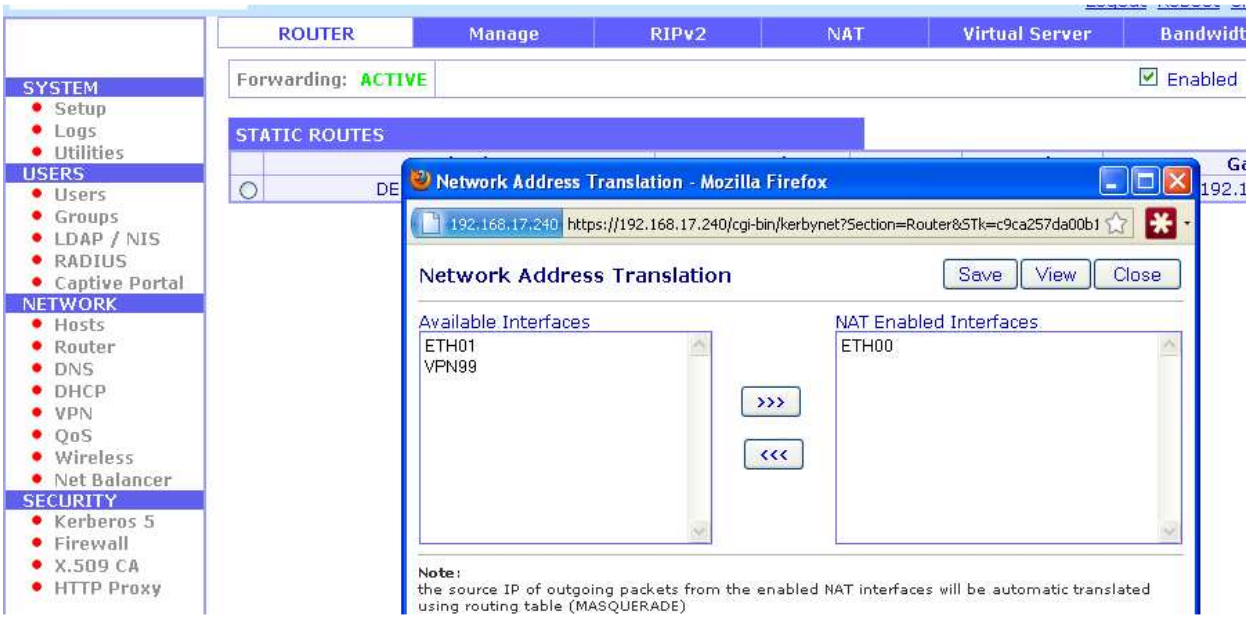
Vediamo comunque i passaggi essenziali per configurare la nostra box ZS come Captive Portal per la rete Wifi. Per prima cosa configuriamo la rete e poi i servizi:

SYSTEM>Setup>Network



Dopo aver configurato le interfacce sui due segmenti di rete attiviamo il NAT sull'interfaccia in uscita:

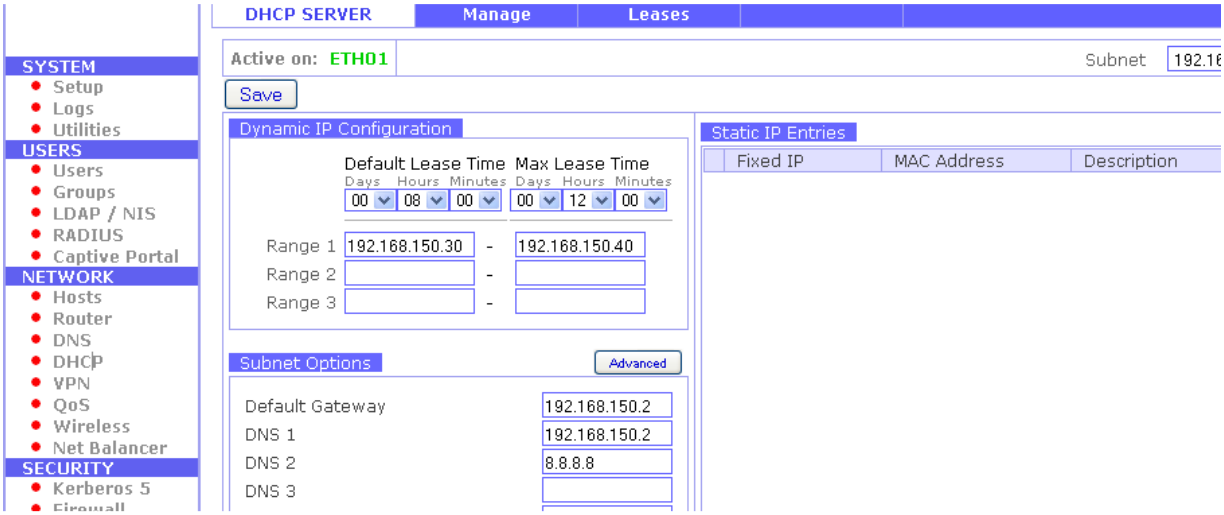
NETWORK>Router>NAT



- ETH00 → 192.168.0.2 è la LAN
- ETH01→ 192.168.150.2 è la rete connessa agli AP

Adesso abilitiamo il DHCP server che servirà la rete a cui sono connessi gli Access Point

NETWORK>DHCP



Impostiamo il segmento di rete che vogliamo mettere in DHCP, nel mio caso uso un range di 10 IP, meglio non mettere più di quelli necessari:

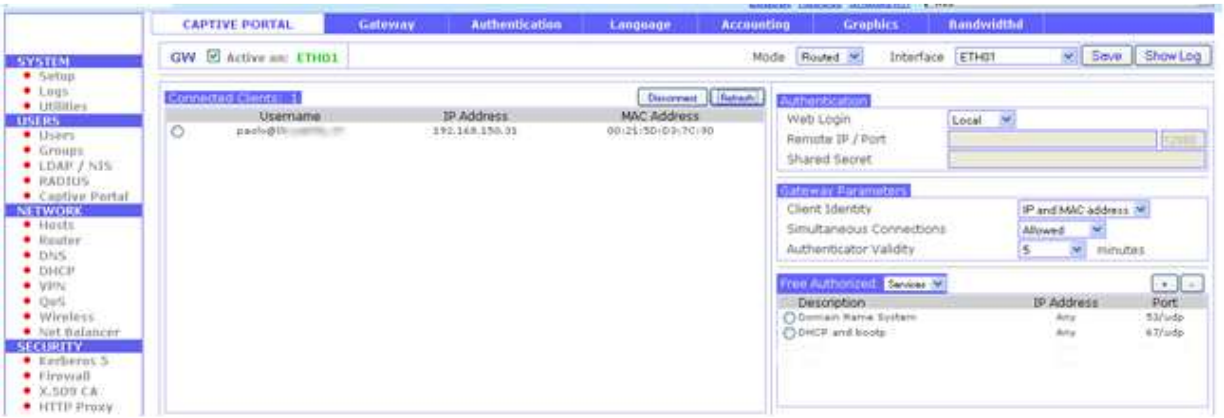
192.168.150.30-192.168.150.40

Per quel che riguarda il DNS conviene abilitarlo in modo che funga da cache resolver per cui sotto:

NETWORK>DNS

Adesso il sistema è pronto per configurare i servizi veri e propri, partiamo dal Captive Portal, sotto la sezione:

USERS >Captive Portal



Se si utilizza l'autenticazione Locale, non modificare la sezione "Authentication" impostare le opzioni:

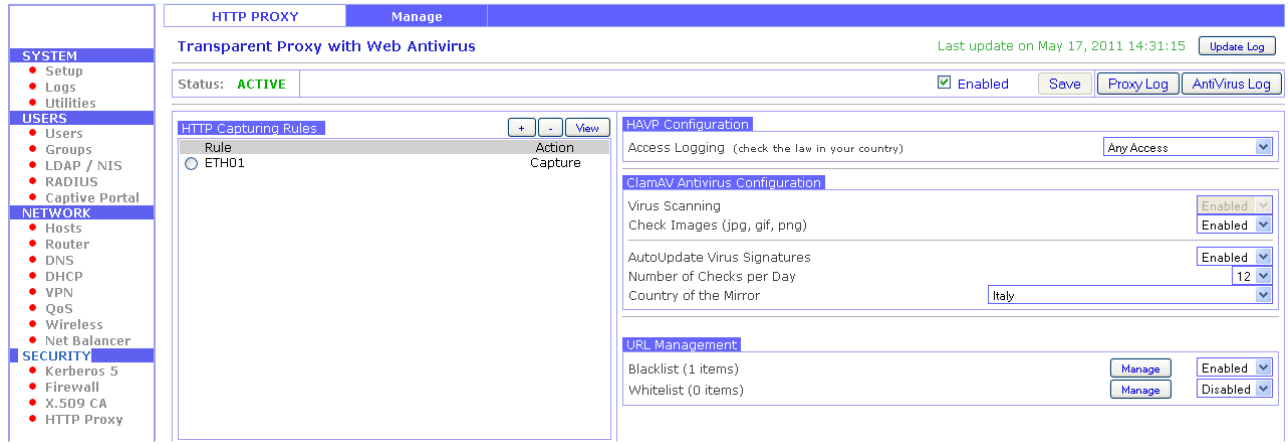
- Client Identity: come identificare il client se tramite IP o anche MAC Address
- Simultaneous Connections: se si accettano connessioni simultanee
- Authenticator Validity: tempo di durata della sessione in caso di inattività

Il modo utilizzato è nel mio caso "Routed" e l'interfaccia è ETH01, quella connessa all'AP oppure ad uno switch a cui sono connessi più AP.

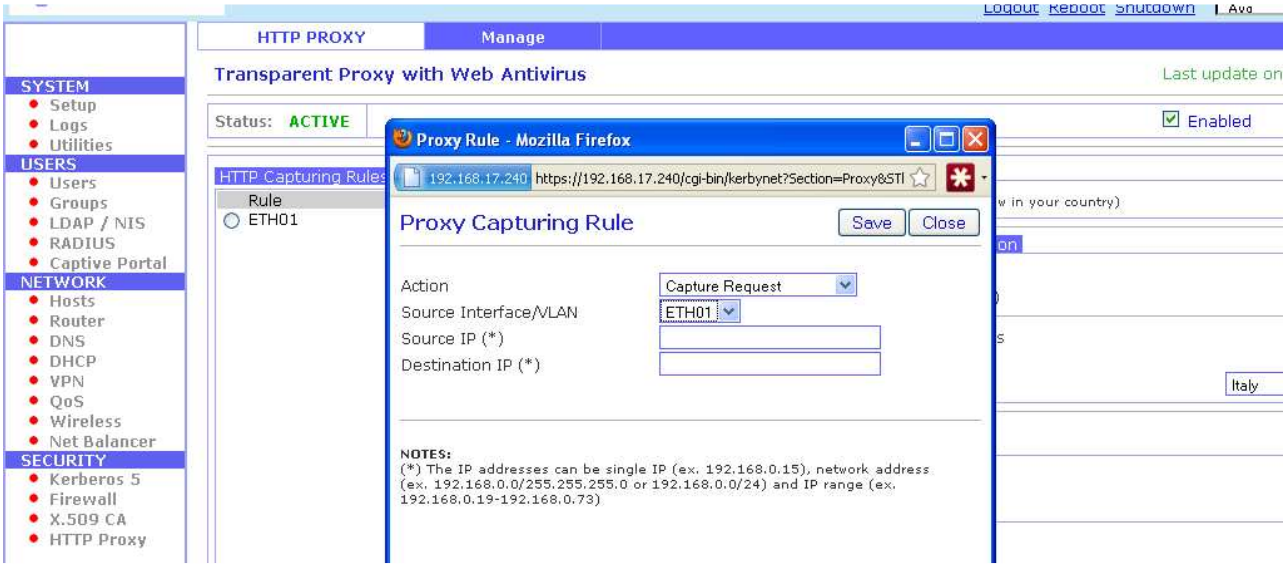
Attenzione!! La sezione "Free Authorized" permette di specificare porte o servizi che potranno bypassare il captive portal, senza autenticazione, si usa in genere per il DNS o il DHCP, attenzione che l'uso incauto permette ad utenti alle spalle del captive portal di bypassare l'autenticazione (ovviamente se Firewall e NAT lo consentono).

Nel caso in cui si vogliano monitorare le connessioni ad internet ed avere i LOG registrati delle connessioni occorre abilitare il Proxy, che in modalità trasparente intercetta le connessioni verso i siti web (solo porta 80), e permette anche di filtrarli secondo liste di siti.

SECURITY >HTTP proxy



Se si vogliono registrare i log occorre impostare sotto la voce Access Logging “Any Access” ed aggiungere sotto la sezione “HTTP Capturing Rules” una Proxy Capturing Rule, specificando quindi una regola che permetta al proxy di intercettare e scrivere nei log le richieste fatte per quella aspecifica regola.



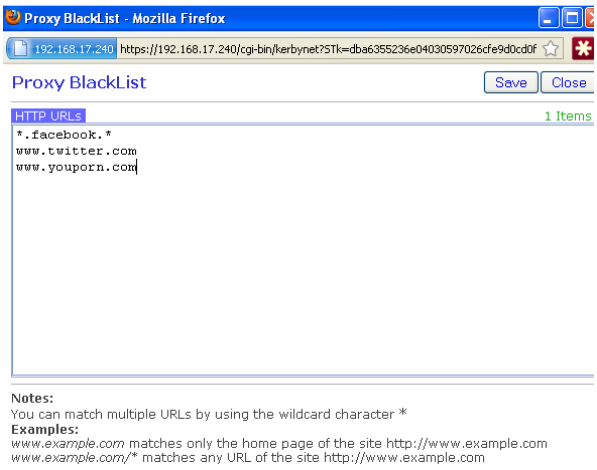
Nel mio caso ho detto di intercettare tutte le richieste su porta 80 per l’interfaccia ETH01, quella connessa alla rete wifi.

Blocco di siti

Se si utilizza l’http Proxy si può impostare una BL, indicando i siti che is vogliono bloccare. Allo stesso modo si può fare con una WL, per dare con certezza l’accesso a determinati siti

SECURITY >HTTP proxy>URL Management

Basta elencare i siti che si vogliono bloccare, anche con l’ausilio di caratteri jolly.



Attenzione che il filtro sui social network, facebook in primis, funziona solo su porta http, se avete abilitato l'http (come molti richiedono per ovvi motivi), nel caso in cui si voglia bloccarlo anche su https, si può agire sul Firewall, con una soluzione non elegante e che va aggiornata, perché si base sul DROP degli IP associati ai vari servizi.

```
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
LOG        tcp  --  0.0.0.0/0            66.220.156.0/24     tcp dpt:443 limit: avg 10/min burst 15 LOG flags 0 level 4
prefix `FORWARD/001'
DROP       tcp  --  0.0.0.0/0            66.220.156.0/24     tcp dpt:443
LOG        tcp  --  0.0.0.0/0            69.63.0.0/16        tcp dpt:443 limit: avg 10/min burst 15 LOG flags 0 level 4
prefix `FORWARD/002'
```

In questo caso basta aggiungere un drop su porta 443 dall'interfaccia ETH01 verso quella ETH00 e come destinatari mettere gli IP dei server di facebook.

Analisi dei LOG

Quando si imposta un Captive Portal, soprattutto quando alle sue spalle si ha una LAN aperta senza un meccanismo di autenticazione occorre essere certi del suo funzionamento, per cui occorre fare alcuni test e verifiche di sicurezza, proprio agendo dalla rete wireless.
Ma prima di approfondire questo aspetto vediamo come analizzare lo stato dei LOG, indispensabili per identificare in caso di necessità, o per fini statistici o per richiesta degli organi di sicurezza, abilitando il CP e il Proxy. I Log vengono salvati sul sistema nella cartella Database/LOG e archiviati per data.

```
root@zeroshell zeroshell> pwd
/Database/LOG/2011/May/16/zeroshell
```

I LOG del CP sono presentano sempre l'IP del client e sono associati allo user oppure ancora meglio al certificato questo, permette di collegare IP all'utente che ha avuto accesso alla rete. Ma vediamo al catena dell'identificazione del client. Intanto nel file dhcp troviamo il MAC address del client, anche se va detto che in assenza di un filtro questo parametro è facile da manipolare, in caso di attività malevoli.

```
root@zeroshell zeroshell> tail –f dhcp
```

```
May 16 18:31:39 zeroshell dhcpd: DHCPACK on 192.168.150.31 to 00:21:5d:d3:7c:90 (paolo-PC) via ETH01
```

➔ Da IP abbiamo nome host e indirizzo MAC

```
root@zeroshell zeroshell> tail –f CaptivePortal
ay 17 17:30:58 zeroshell CaptivePortal: AS: http session (Client: 192.168.150.31) captured for authentication (AS: 192.168.150.2)
May 17 17:31:01 zeroshell CaptivePortal: AS: Info: pavan@netlink.it (192.168.150.31) has the DN: /OU=Users/CN=paolo/emailAddress=pavan@netlink.it
May 17 17:31:01 zeroshell CaptivePortal: AS: Success: user pavan@netlink.it (Client: 192.168.150.31) successfully authenticated (X.509 Certificate)
May 17 17:31:02 zeroshell CaptivePortal: GW: Success: user pavan@netlink.it (IP: 192.168.150.31 MAC: 00:21:5D:D3:7C:90) connected
```

➔ In questo caso abbiamo user/IP/certificato

Attenzione alla data e l'ora, sono essenziali per poter analizzare ed incrociare i dati con i Log del Proxy. Utilizzando la data/ora di connessione e l'IP possiamo assegnare le consultazioni ad un determinato utente:

```
root@zeroshell zeroshell> tail -f proxy
May 17 17:30:42 zeroshell proxy[19593]: 192.168.150.31 GET 204 http://clients1.google.it/generate_204 147+0 OK
May 17 17:30:42 zeroshell proxy[19591]: 192.168.150.31 GET 404 http://lh4.ggpht.com/-2tI9V9BFjFA/TWPjGl1CbaI/AAAAAAAALIQ/IDFTe-EZnwU/e365/SDC12640.JPG 228+11854 OK
May 17 17:30:42 zeroshell proxy[10043]: 192.168.150.31 GET 204 http://www.google.it/ig/cp/fail? 225+0
```

→l'IP ci permette di risalire all'utente

Programmazione del Firewall

Sotto la sezione Security si trova il pannello di controllo per le regole del firewall

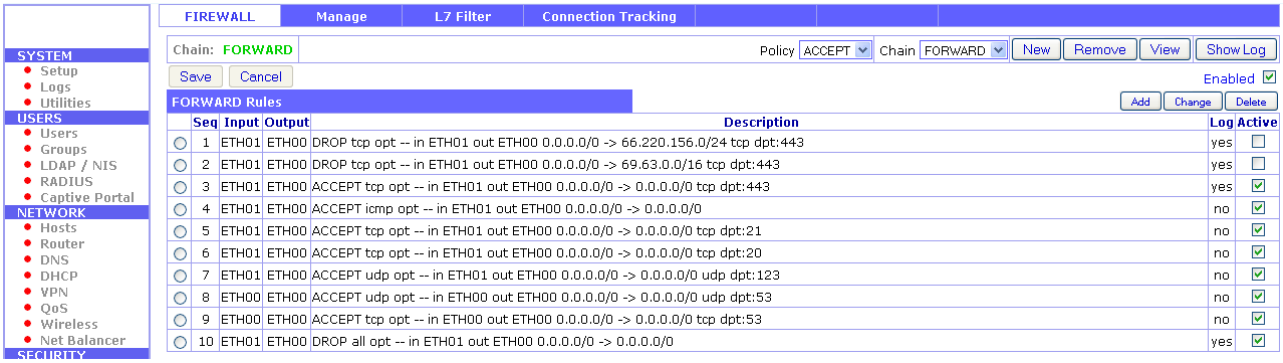
```
SECURITY >FIREWALL
```

E' essenziale conoscere la programmazione del firewall per evitare buchi e permettere accessi non autorizzati. Di default le tre CHAIN INPUT, FORWRD OUTPUT, sono messe in ACCEPT, questo significa che una volta autenticati si può accedere ad internet su qualsiasi servizio, ma solo dopo l'autenticazione.

```
root@zeroshell zeroshell> iptables -L -n  |grep Chain
Chain INPUT (policy ACCEPT)
Chain FORWARD (policy ACCEPT)
Chain OUTPUT (policy ACCEPT)
```

Questo spesso. non è quello che si vuole, nel caso in cui si vogliano abilitare solo i protocolli http e https, conviene specificarli nella catena del FOFWARD ed impostare come ultima regola (importante la sequenza) un nel DROP per tutto il traffico (0.0.0.0)

Vediamo un esempio:

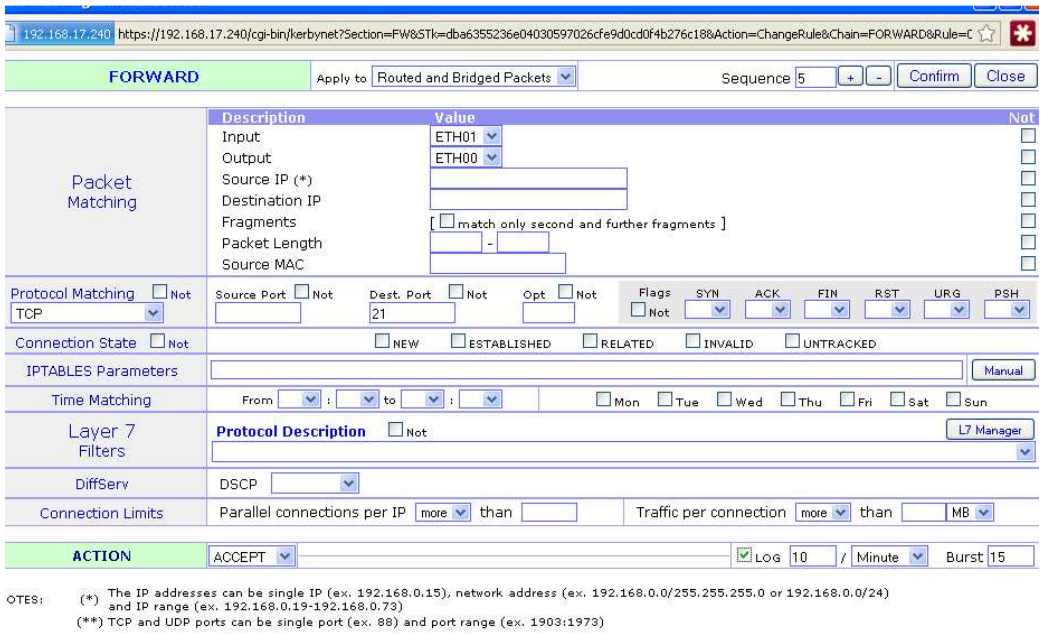


Una stampa delle regole della Catena di FORWARD

```
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
LOG        tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443 limit: avg 10/min burst 15 LOG flags 0 level 4
prefix `FORWARD/003'
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:21
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:20
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:123
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:53
LOG        all  --  0.0.0.0/0            0.0.0.0/0           limit: avg 10/min burst 15 LOG flags 0 level 4 prefix
`FORWARD/010'
DROP       all  --  0.0.0.0/0            0.0.0.0/0
CapPort    all  --  0.0.0.0/0            0.0.0.0/0
```

In pratica questa configurazione dice che tcp 443, 20, 21, 53 e ICMP sono abilitati ad attraversare le interfacce, mentre tutti gli altri protocolli sono bloccati. Un può decidere di restringere le connessioni anche degli host autenticati agendo quindi sull'interfaccia del firewall.

E' comunque possibile tracciare i LOG e quindi gli IP delle macchine abilitando il Logging quando si imposta una regola di ACCEPT nel firewall, l'ultima riga permette di abilitare i LOG.



Anche per la catena di INPUT si può irrobustire la sicurezza inserendo gli ACCEPT per le porte necessarie all'uso del Captive Portal e alla navigazione e mettendo un bel DROP ALL per tutti i protocolli sempre come ultima regola. Una configurazione funzionante può essere questa, che prevede in input le porte 80,443,123,53, 55559:

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  192.168.0.0        0.0.0.0/0          tcp dpt:22
ACCEPT     tcp  --  192.168.0.0/24     0.0.0.0/0          tcp dpt:80
ACCEPT     tcp  --  192.168.0.0/24     0.0.0.0/0          tcp dpt:443
ACCEPT     tcp  --  0.0.0.0/0          0.0.0.0/0          tcp dpt:80
ACCEPT     tcp  --  0.0.0.0/0          0.0.0.0/0          tcp dpt:443
ACCEPT     tcp  --  0.0.0.0/0          0.0.0.0/0          tcp dpt:55559
ACCEPT     tcp  --  0.0.0.0/0          0.0.0.0/0          tcp dpt:53
ACCEPT     udp  --  0.0.0.0/0          0.0.0.0/0          udp dpt:53
ACCEPT     tcp  --  0.0.0.0/0          0.0.0.0/0          tcp dpt:12087
ACCEPT     udp  --  0.0.0.0/0          0.0.0.0/0          udp dpt:67
ACCEPT     udp  --  0.0.0.0/0          0.0.0.0/0          udp dpt:68
LOG        all  --  0.0.0.0/0          0.0.0.0/0          limit: avg 10/min burst 15 LOG flags 0 level 4 prefix
`INPUT/012'
DROP       all  --  0.0.0.0/0          0.0.0.0/0
```

Ricordiamo che ogni volta che si modifica o crea una nuova regola bisogna salvare la configurazione del firewall. Il file kernel tiene traccia delle connessioni in forward, su cui abbiamo abilitato il log.

```
May  17  17:54:25  zeroshell  kernel:  FORWARD/005IN=ETH01  OUT=ETH00  SRC=192.168.150.31
DST=193.33.99.246 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=3477 DF PROTO=TCP SPT=20963 DPT=21
WINDOW=8192 RES=0x00 ACK URGP=0
```

May 17 17:54:25 zeroshell kernel: FORWARD/005IN=ETH01 OUT=ETH00 SRC=192.168.150.31 DST=193.33.99.246 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=3478 DF PROTO=TCP SPT=20963 DPT=21 WINDOW=8135 RES=0x00 ACK URGP=0

Con il comando arp possiamo risalire al MAC address del PC che ha aperto la connessione:

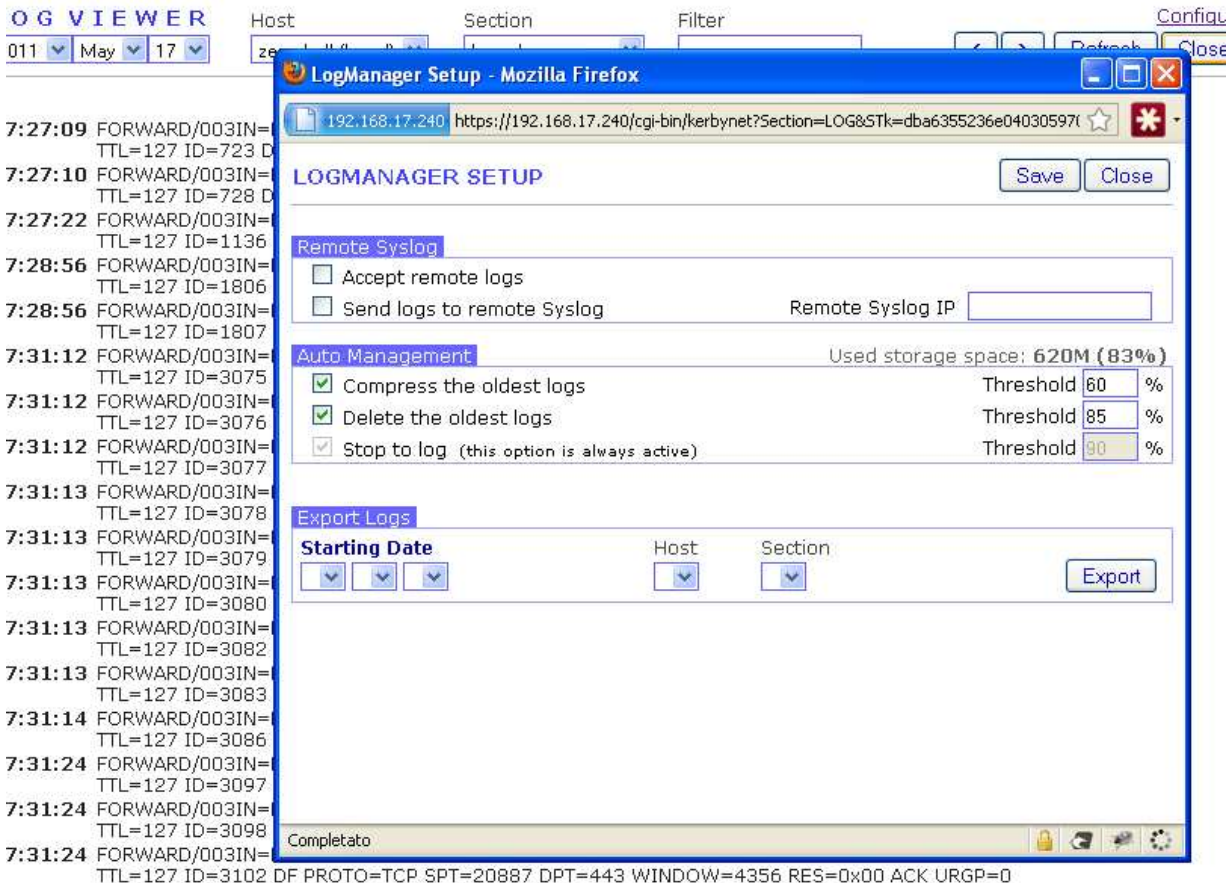
```
root@zeroshell zeroshell> arp -a
? (192.168.150.31) at 00:21:5D:D3:7C:90 [ether] on ETH01
```

Nel caso in cui si volesse usare il firewall e si volesse effettuare il debug delle connessioni consiglio, di impostare il loggin solo sulla o sulle regole dei DROP in questo modo possiamo capire cosa viene bloccato dal firewall. Ricordo che senza l'abilitazione del NAT le connessioni in forward non vengono fatte passare.

Configurazione ed esportazione dei LOG

Non l'ho sperimentato ma ZS supporta l'uso di un remote syslog server, per mettere al sicuro attraverso la rete dei file di LOG. Alternativamente i file di LOG possono essere copiati o sincronizzati con rsync dal host ZS verso un altro host della rete.

SYSTEM >LOGS>Configure



Abilitando il “Connection Tracking” vengono registrate le connessioni effettuate dal CP, in questo modo anche nei confronti della “Legge Pisanu” oramai abolita si aveva la possibilità di conservare i LOG necessari ad identificare l’utente e siti raggiunti, senza usare i log più espliciti del Proxy Trasparente.

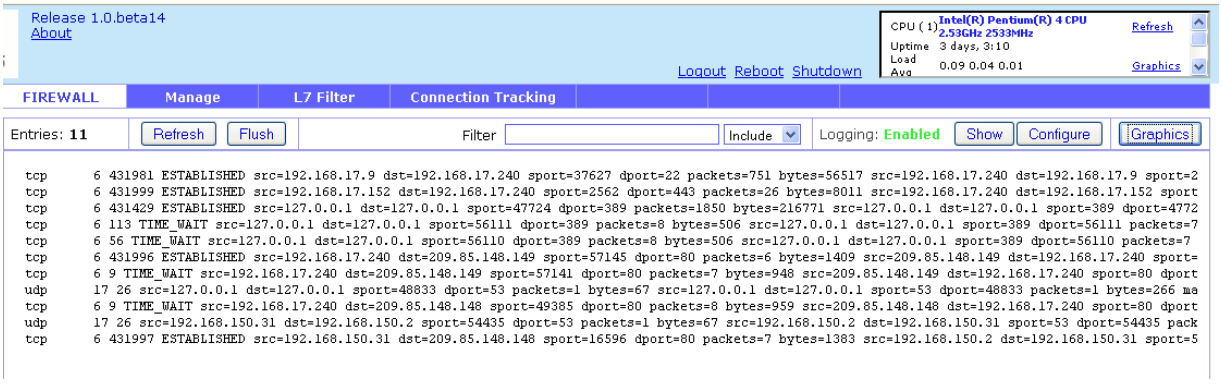
SECURITY >CONNECTION TRACKING

Si possono anche impostare dei filtri per includere od escludere eventi dalla registrazione. Ovviamente l’abilitazione dei Conn Track, aumenta di molto lo spazio usato per i log e occorre studiare un sistema per esportare i log all’esterno del CP.
Il file di Log in questo è il file *ConnTrack*, che conserva SOURCE e DESTINATION IP e anche lo stato della connessione, vediamo un esempio:

```
root@zeroshell zeroshell> tail -f ConnTrack |grep dport=80
May 23 15:42:43 zeroshell ConnTrack: [NEW] tcp 6 120 SYN_SENT src=192.168.150.31 dst=213.92.11.246 sport=16598 dport=80 [UNREPLIED] src=192.168.150.2 dst=192.168.150.31 sport=55559 dport=16598
May 23 15:42:43 zeroshell ConnTrack: [NEW] tcp 6 120 SYN_SENT src=192.168.0.2 dst=213.92.11.246 sport=39744 dport=80 [UNREPLIED] src=213.92.11.246 dst=192.168.0.2 sport=80 dport=39744
```

Assieme a questo file di LOG va conservato anche il file *CaptivePortal* che contiene IP e data della connessione e MAC Address del dispositivo che si è connesso:

```
root@zeroshell zeroshell> tail -f CaptivePortal
May 23 15:33:30 zeroshell CaptivePortal: GW: Success: user pavan@netlink.it (IP: 192.168.150.31 MAC: 00:21:5D:D3:7C:90) connected
May 23 15:39:30 zeroshell CaptivePortal: AS: Success: Captive Portal Authentication Server started
May 23 15:39:31 zeroshell CaptivePortal: GW: Success: Captive Portal Gateway started (1 clients connected)
```



Sicurezza del Captive Portal

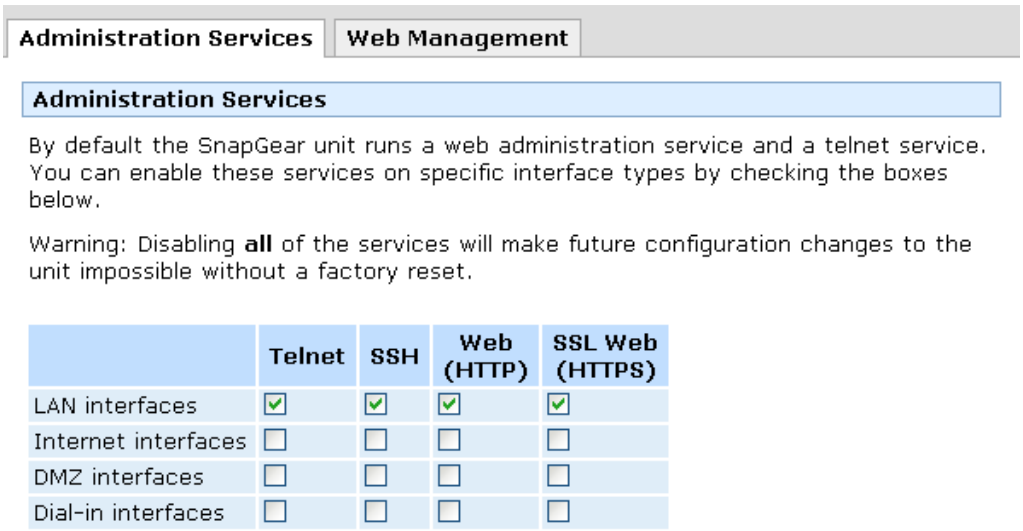
Per essere certi di aver fatto un buon lavoro di configurazione sul lato sicurezza, occorre prendere in considerazione questi aspetti:

- Programmazione firewall
- Scansione dalla rete wireless
- Sicurezza degli AP

- Controllo e monitoraggio costante del traffico e delle connessioni attive sul CP.

Dopo aver realizzato l'infrastruttura è bene fare ripetuti test di autenticazione e portscan dalla rete wifi alla ricerca di debolezze. Chiudete tramite il firewall (Catena INPUT) lo ZS ed impedite alla rete wifi di avere accesso al Captive Portal sulle porte di amministrazione come SSH, questo può essere configurato nella sezione SSH, dove si può specificare quali IP o subnet e da quale interfaccia possa collegarsi. Impostate per l'utente admin una password robusta, controllate con dei portscan, con tool come nmap, lo stato delle porte aperte sia in INPUT verso il captive portal che in FORWARD verso l'esterno.
Volendo le porte 80 e 443 in INPUT possono essere chiuse dal FIREWALL e tramite la sezione SETUP>HTTPS, in modo che i client della rete wifi non possano in alcun modo accedere all'interfaccia di gestione di ZS. Questo però impedisce l'accesso al CP per lo scarico dei certificati, nel caso in cui voglia usufruire di questa funzione, nel caso in cui non sia necessario è decisamente meglio chiudere tutto l'INPUT e blindare ZS.

Anche gli AP vanno configurati in modo da impedire l'accesso alle porte di amministrazione, in genere 80,443 e 22 da parte delle rete wifi. Fate in modo che possano essere raggiunti solo dalla rete LAN, oppure al limite dall'IP del CP, in modo che i client wifi non possano raggiungerlo direttamente, infatti anche se passivo e configurato in bridge è molto semplice scoprire il suo indirizzo IP. In genere ogni AP ha una sezione relativa alla limitazione degli accessi alla console di amministrazione o al limite si può agire sulla configurazione del Firewall presente bordo, nella catena di INPUT.
Nel mio caso ho limitato la possibilità di connettersi all'AP solo alla rete LAN, che può essere usata per il controllo diretto degli AP, e tolta a tutte le altre interfacce. Inoltre è bene mettere un bel DROP alle connessioni in INPUT dell'AP dalla rete Wifi, che fungendo solo da bridge, non avrà bisogno di erogare servizi, ma sarà solo attraversato dai pacchetti che transitano verso il CP.



Monitorate con costanza il CP, non lasciatelo abbandonato, controllate LOG, anzi impostate dei cron per esportare i LOG tramite rsync verso sistemi di backup della rete. Il monitoraggio costante dei sistemi è il miglior deterrente agli attacchi. Esistono tool come Nagios che ci permettono di controllare almeno le porte del sistema e intervenire tempestivamente in caso di disservizi.

Nel mio caso ho creato una partizione separata sul disco tramite Setup>Profiles, e ho impostato un cron job che imposti una sincronizzazione dei Log verso questa partizione. Mi sono scaricato ed installato il programma rsync nella directory /Database e schedulato una copia giornaliera della directory /Database/LOG su una partizione di backup:

Sul mio filesystem avrò:

```
root@zeroshell /> df -h|grep backup
/dev/sdb2             94G  440M   89G   1% /backup
```

In questa directory avrò tutti i LOG sincronizzati informa incrementale. Per conservare lo storico completo:

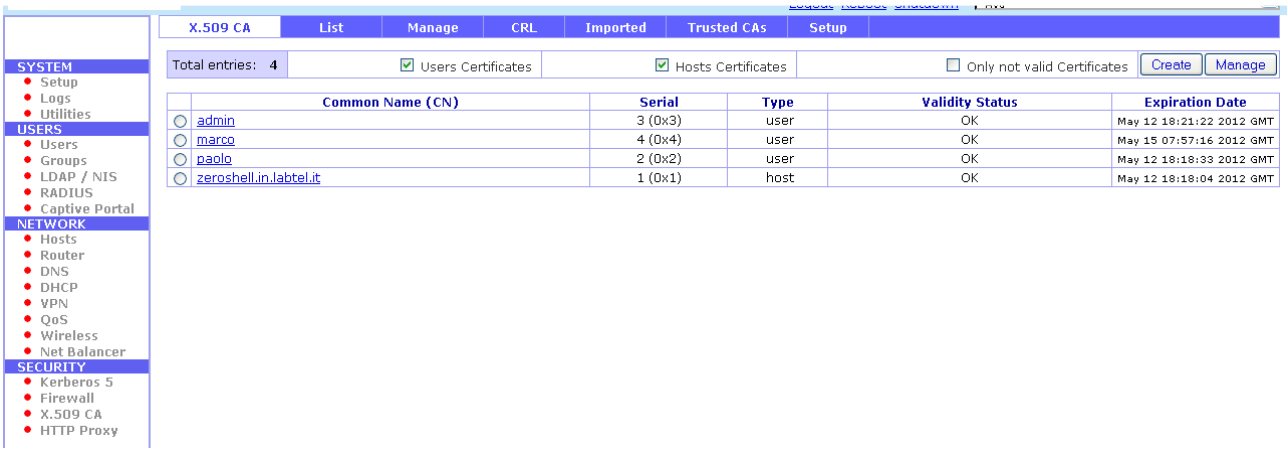
```
root@zeroshell > ls /backup/Database/LOG/2011/May/
24  25  26  27
```

Impostazione della CA ed emissione dei certificati

Uno dei motivi per cui ho scelto ZS è stata l'ottima gestione della Certification Authority, volendo io implementare un sistema che mi permettesse di autenticare gli utenti tramite un certificato, che una volta scaricato dovevano caricare nel loro browser.

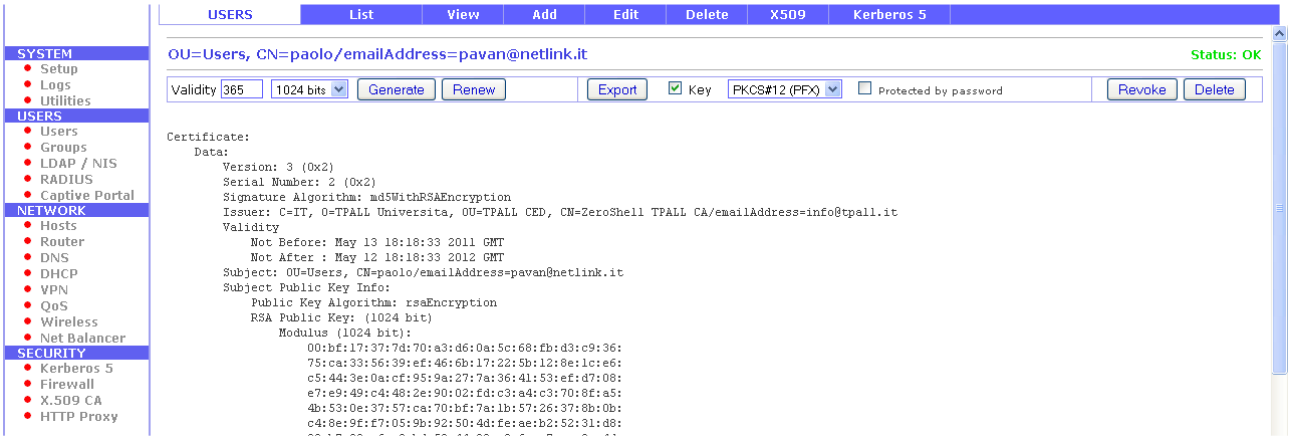
Vediamo la gestione della CA e l'emissione dei certificati X509 per i client. Sotto al sezione:

```
SECURITY >X509CA
```



I certificati vengono creati automaticamente quando si crea un utente e possono essere rinnovati o sospesi. Vanno esportati e caricati con il browser, con FF, IE e GC funzionano bene. Nel caso in cui un certificato venga revocato, deve essere rigenerato (Renew) e riesportato e riconsegnato all'utente per una nuova importazione. E' chiaro che un certificato revocato deve considerarsi non più utilizzabile.

USER >X509



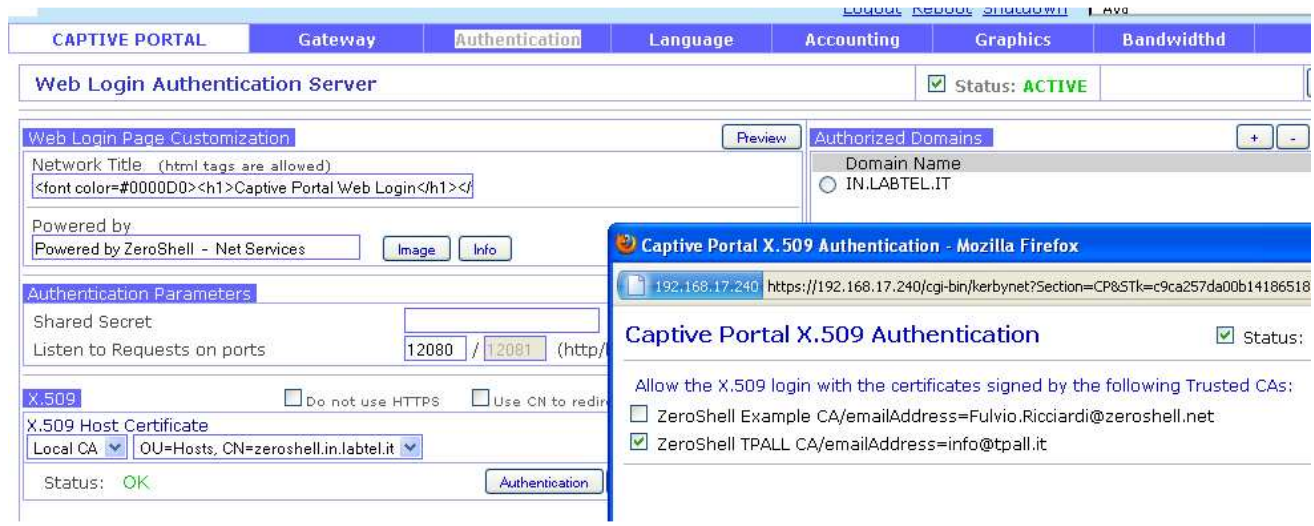
Attenzione!! Nel caso in cui si voglia rigenerare una CA per inserire parametri diversi da quelli di default occorre andare su :

SECURITY >X509CA>Setup

Inserire i propri dati e ricreare il certificato per la nostra CA. Ovviamente i certificati emessi smetteranno di funzionare, per cui attenzione.
Appena fatta questa operazione dobbiamo dire al nostro Captive Portal di usare la nuova CA, per cui accediamo a:

USER >Captive Portal> Authentication

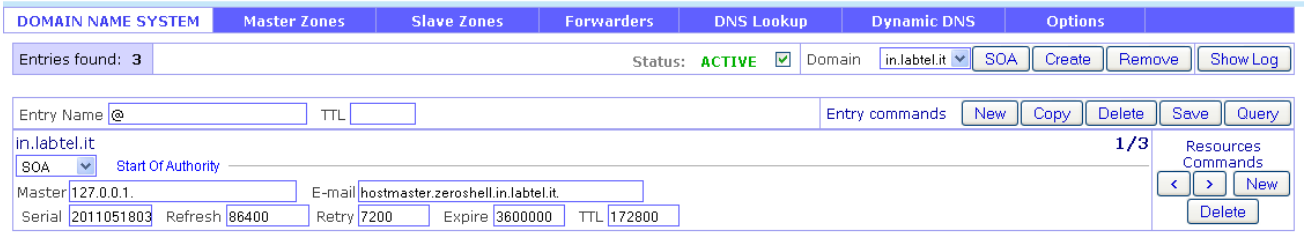
In basso nella sezione X509 clicchiamo sul bottone "Authentication" e selezioniamo la nostra nuova CA:

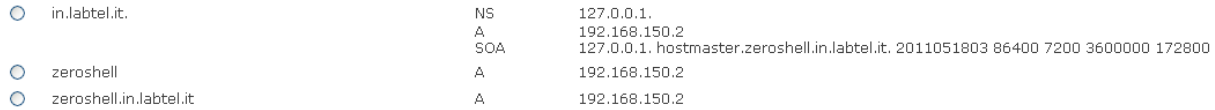


Senza questa modifica il CP rifiuterà i novi certificati emessi.

Da notare l'opzione "Use CN to redirect" che permette al CP di redirezionare le connessioni dirette a http e https verso il nome FQDN specificato nel certificato. Ovviamente il valore FQDN deve essere risolto dal DNS, in questo modo il browser accetterà il certificato dopo la prima conferma. Purtroppo IE, pretende il caricamento anche del certificato della CA, prima di smettere di segnalare che il certificato non è valido.
A tale proposito se si usa come DNS la box ZS, e si vuole usare un dominio interno o fittizio, lo si può creare come Master Zone nella sezione di gestione del DNS:

NETWORK >DNS



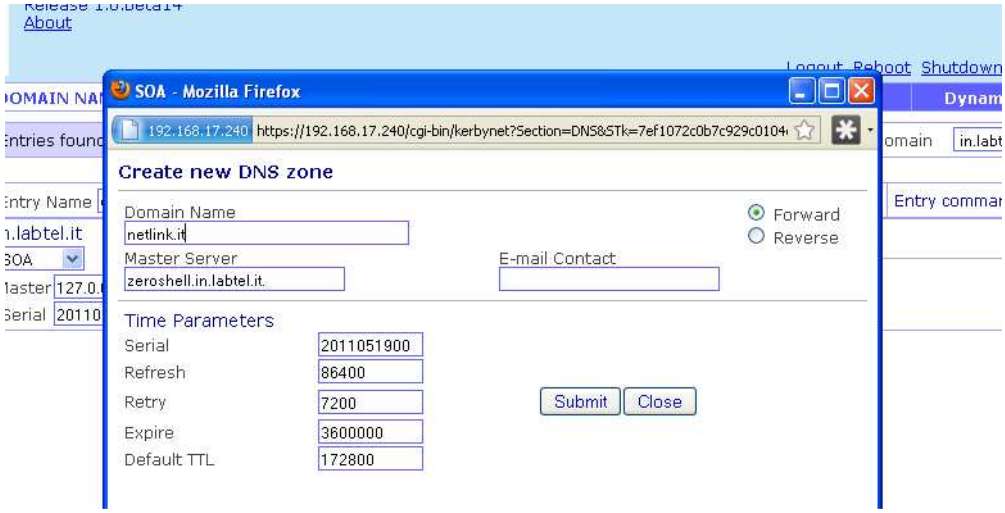


- Indicare nella maschera il nome del dominio
- Come Master Server indicare 127.0.0.1

Per aggiungere una nuova zona procediamo in questo modo:

NETWORK >DNS>Master Zones

Nella prima riga fianco di SOA, clicchiamo su CREATE:



Scegliamo il nome del dominio (zona) di tipo diretto (forward) In questo modo viene aggiunta la zona/dominio che vogliamo che venga risolto.

Se la zona è selezionata nella parte sottostante della schermata del DNS possiamo cliccare su NEW per inserire A RECORD oppure CNAME o PTR record a seconda delle nostra necessità. In genere inserendo una A RECORD, associato all'IP del CP possiamo poi verificare che venga effettivamente risolto dai client che usufruiscono del servizio di DNS dal Captive Portal stesso. Dopo avere inserito l'indirizzo IP cliccare sul bottone SAVE.

Se non vengono restituiti errori possiamo provare a vedere se il dominio viene risolto dai client della rete Wifi che usano il CP anche come DNS.

Attenzione!! Se si usa un bridge wifi alle spalle è importante inserire degli A RECORD che risolvano il nome del GW (ZS) con l'indirizzamento sulla subnet assegnata in bridge (192.168.150.0/24).

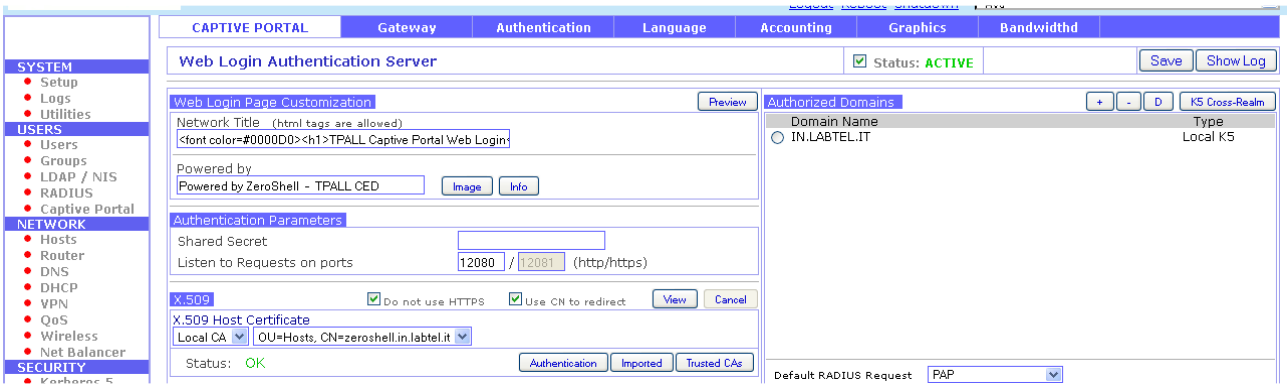
Il problema della CA non riconosciuta

Molti utenti lamentano il fatto che i browser soprattutto IE, producano quel fastidioso alert di sito non verificato, quando si collegano al Captive Portal e non solo la prima volta. Se Firefox permette al primo accesso di considerare valido il certificato e non avere più messaggi, una volta che lo si è considerato attendibile, su IE bisogna per forza importare anche il certificato della nostra CA autofirmata, e collocarlo tra le CA attendibili.

Per risolvere il problema ci sono tre soluzioni ovvero acquistare un certificato ufficiale per il nostro CP che sia tra quelli riconosciuto da IE e dagli altri browser e di conseguenza anche i certificati utenti dovranno essere emessi da quella CA, oppure si può optare per una soluzione, molto più semplice ma meno sicura, ovvero disabilitare l'HTTPS e affidarsi solo all'autenticazione utente.

USERS>Captive Portal >Authentication

Spuntare la casella *"Do not use HTTPS"*

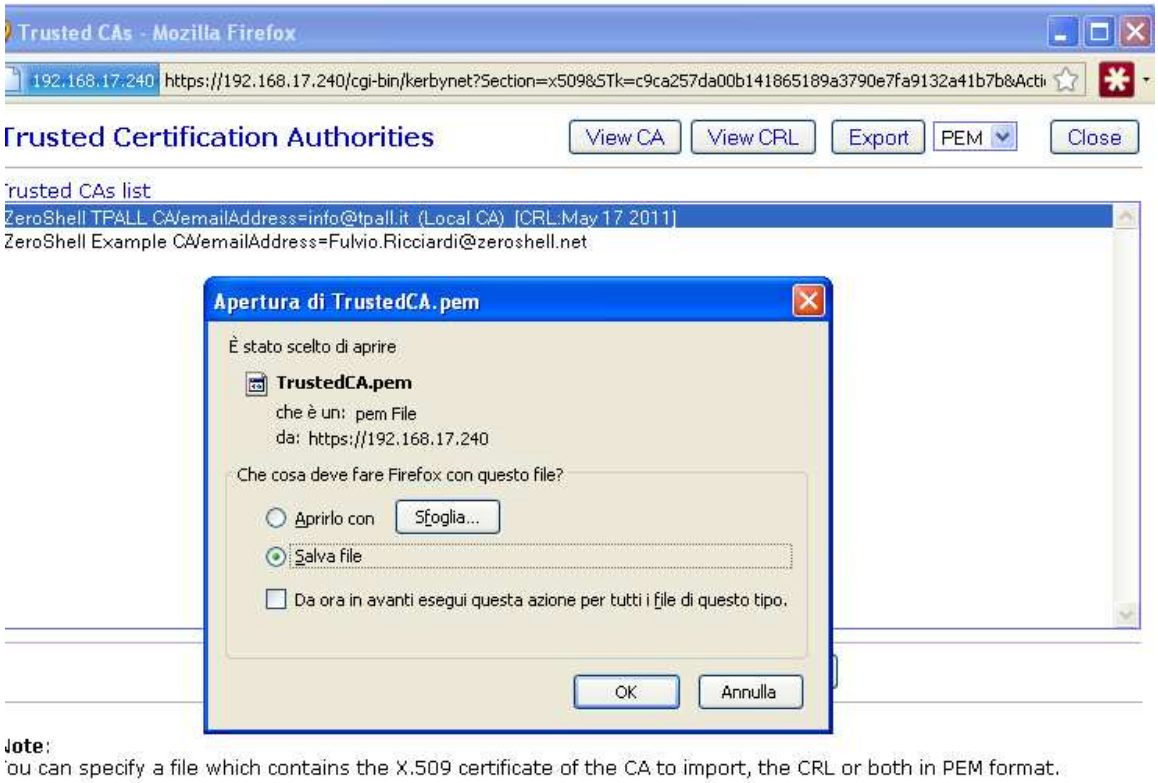


In questo modo tutti i dati viaggiano in chiaro, ma non vi sarà il fastidioso messaggio di certificato inaffidabile, che destabilizza molti utenti. Bisogna fare una scelta, in alcuni ambienti in cui la sicurezza non è essenziale (sembra una battuta) può anche andare bene fare questa scelta, ma nel caso di reti wifi open è meglio sicuramente impostare l'https e la conseguente cifratura delle sessioni.

L'ultima soluzione, che richiede un po' di istruzione degli utenti, ma che in molti casi è la più giusta da applicare, è quella di caricare il certificato della nostra CA, che si può scaricare direttamente dalla box ZS e mettere in distribuzione. Sotto la sezione Security:

SECURITY >X509CA> Trusted CAs

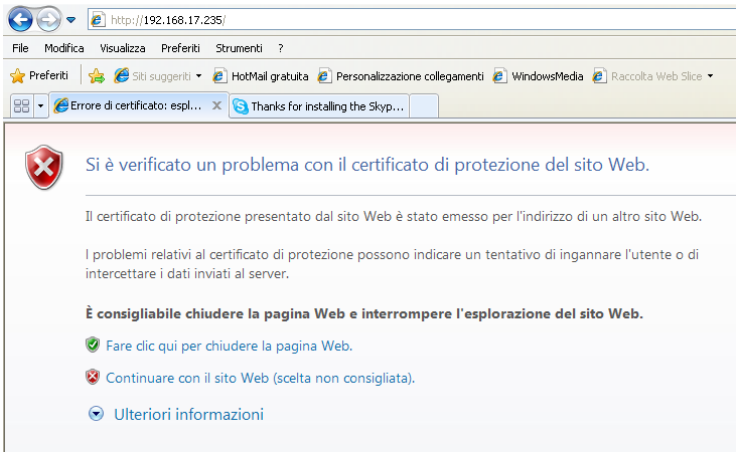
Selezionare la nostra CA e cliccare sul bottone Export:



Il file CA.pem (TrustedCA.pem) può essere importato da IE, nella relativa sezione dei certificati, vediamo i passaggi specifici:

Importazione della CA (only IE)

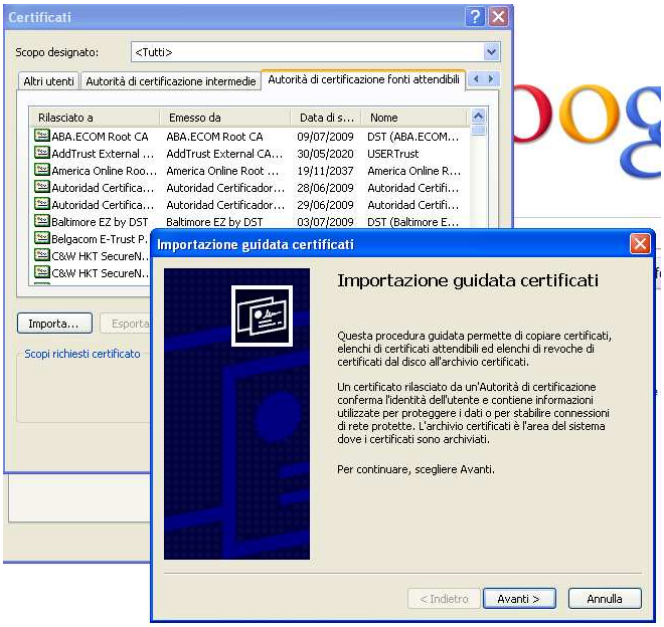
Per evitare la comparsa del fastidioso alert di IE per i siti di cui non possiede la CA caricata



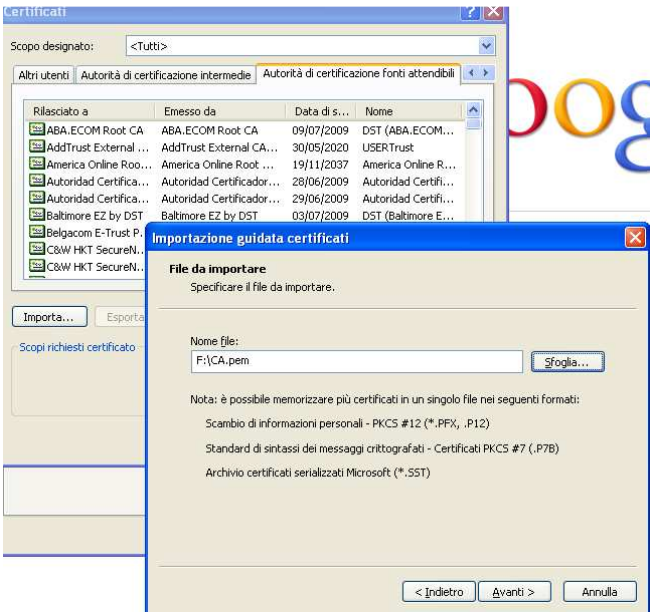
Occorre procedere in questo modo, ovvero scaricare sul proprio computer il certificato della CA che rilascia i certificati utenti, denominato CA.pem. Questo file può essere fornito con il certificato utente, su supporto removibile o scaricato direttamente dal Captive Portal.
Se compare questo messaggio, non è un errore e bisogna comunque scegliere “Continuare con il sito Web (scelta non consigliata).“

Comunque per caricare il certificato della CA occorre andare nel Menu di IE:

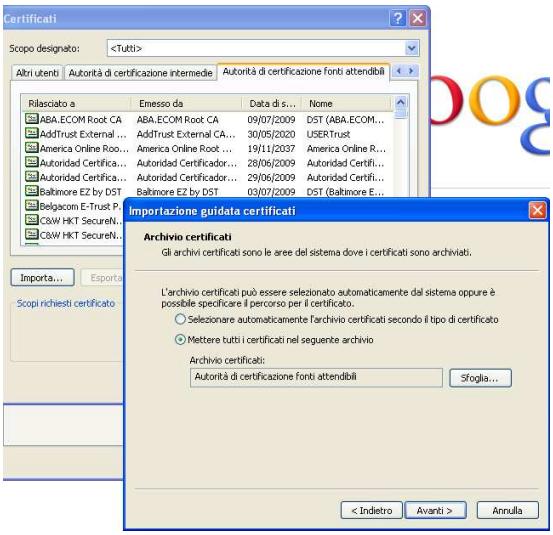
Strumenti>Opzioni Internet>Contenuto>Certificati>Autorità di Certificazione fonti attendibili>Importa



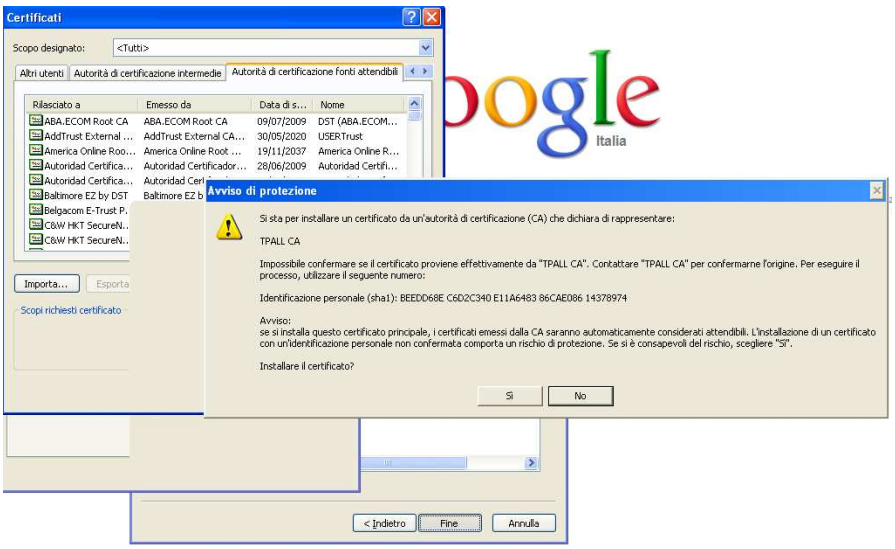
Scegliere “Tutti i file” e selezionare CA.pem



Mettere in “Autorità di certificazione fonti attendibili”



Viene mostrato il certificato cliccare su “Si”



A questo punto riavviamo IE e i nuovi accessi non dovrebbero più mostrare il fastidioso avviso.

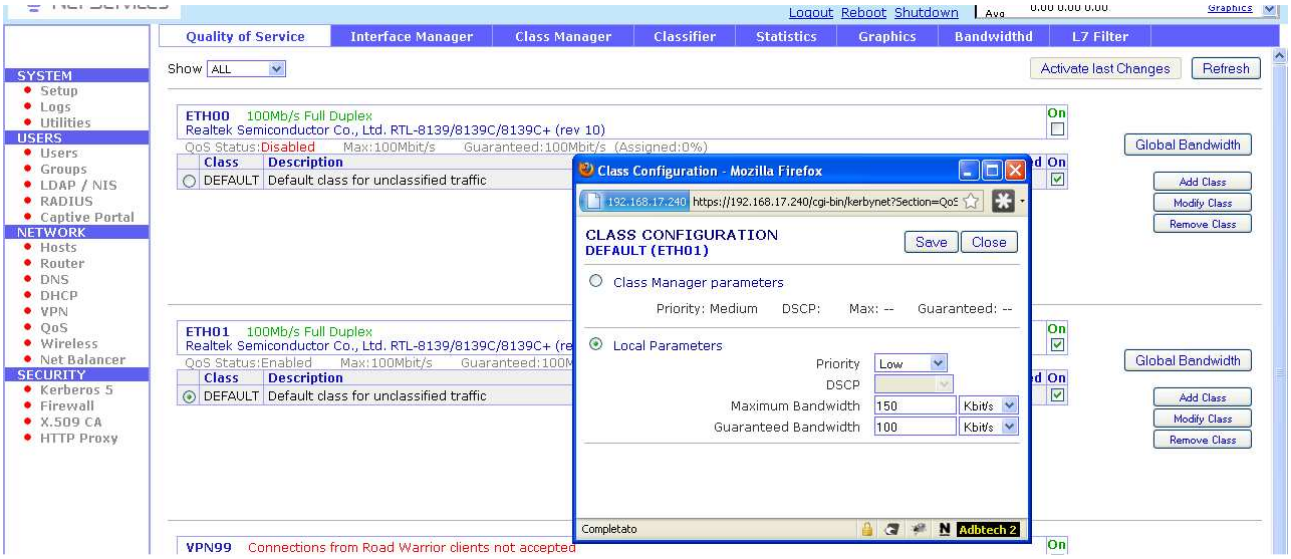
QoS e limitazione delle Banda

Un’altra importante funzionalità di semplice utilizzo di ZS è il QoS ovvero il Quality of Service, che ci permette di limitare la banda sulle diverse interfacce del nostro sistema.
Nel mio caso essendo la rete Wifi parte di un’unica rete che converge poi su un’unica linea ADSL in uscita, mi è stato chiesto di ridurre le possibilità di questa rete nel suo complesso di usufruire della banda totale.
Vediamo come fare, accediamo alla sezione

NETWORK >QoS

Qui selezioniamo la classe DEFAULT associata all’interfaccia ETH01 che è quella della rete Wifi da cui arriva il traffico che voglio regimentare. In questo modo non mi troverò la mia banda saturata da un utilizzo eccessivo da parte di questa rete.

Prima è bene ricordare che quando si applica una classe di QoS ad un'interfaccia di rete si intende controllare il traffico uscente da quella interfaccia. Nel nostro caso interessa regimentare il traffico uscente dall'interfaccia ETH01 collegata alla rete Wifi.

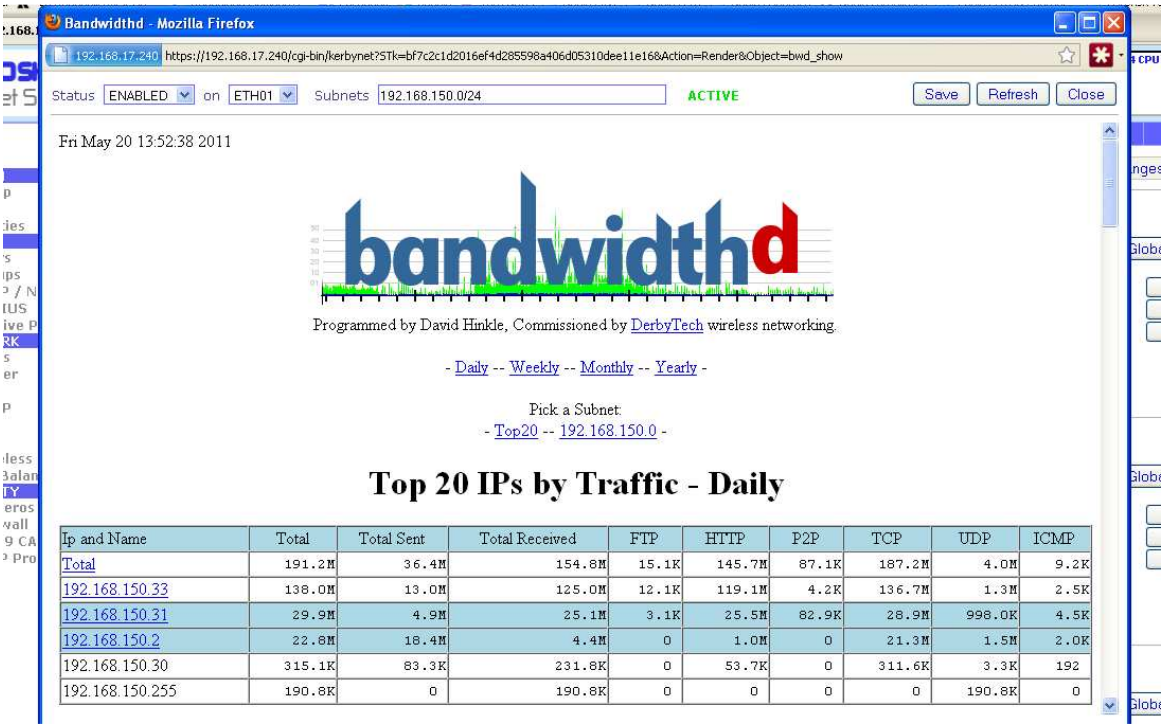


Selezionando la classe DEFAULT e cliccando sul bottone Modify Class, possiamo assegnare i nuovi valori espressi in kbit/s, saranno Maximum Bandwidth e Guaranteed Bandwidth, la prima è la banda massima a disposizione la seconda quella comunque garantita.
Facciamo qualche esempio se io assegno un valore massimo di 100 kbit, diviso 8 avrò la velocità di download in Bytes, quindi 12,5 KB. Basta fare qualche prova per rendersi conto che il filtro funziona ed è efficace. Occorre fare una valutazione attenta della propria banda a disposizione e decidere quanta lasciarne alla rete wifi. Io normalmente per un 1 MB di banda in download ne metto 500 kbit a disposizione della rete wifi, questo rende anche più sicuro il sistema ed evita pericolose saturazioni di banda.
Ogni modifica della banda richiede di cliccare sul bottone "Activate Last Changes", attenzione che lo shaping non è sempre preciso, ma è un valore medio che lo shaper stesso calcola in modo dinamico in base al flusso, cerca quindi di gestire il traffico sulle soglie impostate.

Assieme allo shaping ed al QoS può essere utile abilitare il modulo Bandwidth che permette di monitorare il traffico dei vari IP, e di generare report grafici per poter valutare l'uso della banda, il traffico dei singoli hot (IP) e dei protocolli utilizzati.

NETWORK > Bandwidthd

Sulla riga in lato della maschera che si pare occorre specificare la subnet che si vuole monitorare.



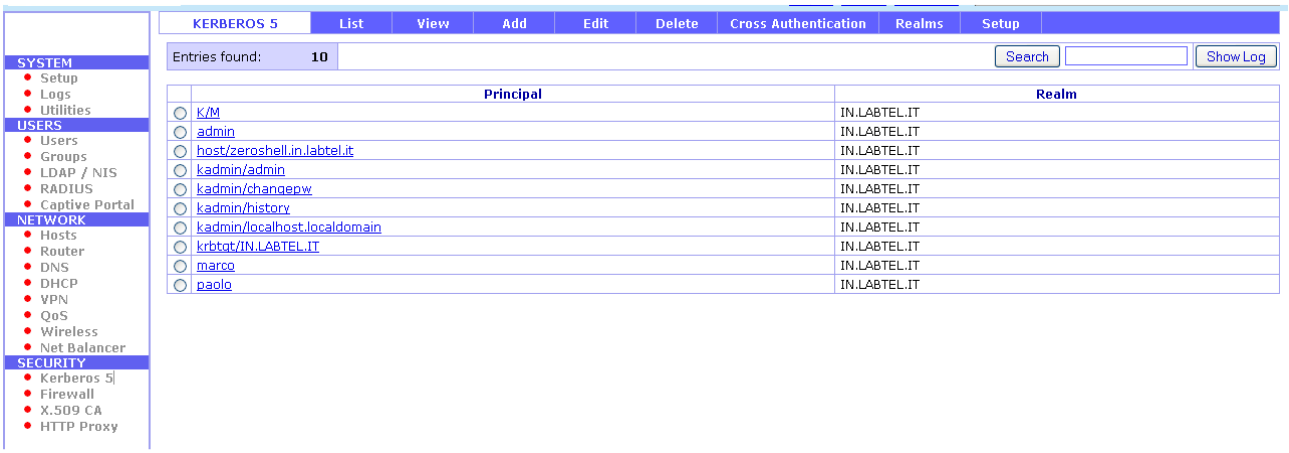
Ip and Name	Total	Total Sent	Total Received	FTP	HTTP	P2P	TCP	UDP	ICMP
Total	191.2M	36.4M	154.8M	15.1K	145.7M	87.1K	187.2M	4.0M	9.2K
192.168.150.33	138.0M	13.0M	125.0M	12.1K	119.1M	4.2K	136.7M	1.3M	2.5K
192.168.150.31	29.9M	4.9M	25.1M	3.1K	25.5M	82.9K	28.9M	998.0K	4.5K
192.168.150.2	22.8M	18.4M	4.4M	0	1.0M	0	21.3M	1.5M	2.0K
192.168.150.30	315.1K	83.3K	231.8K	0	53.7K	0	311.6K	3.3K	192
192.168.150.255	190.8K	0	190.8K	0	0	0	0	190.8K	0

L'elenco degli IP ed il grafico dei protocolli permette di tenere sotto controllo l'uso delle banda e di effettuare eventuali modifiche, ad esempio alla programmazione del firewall.

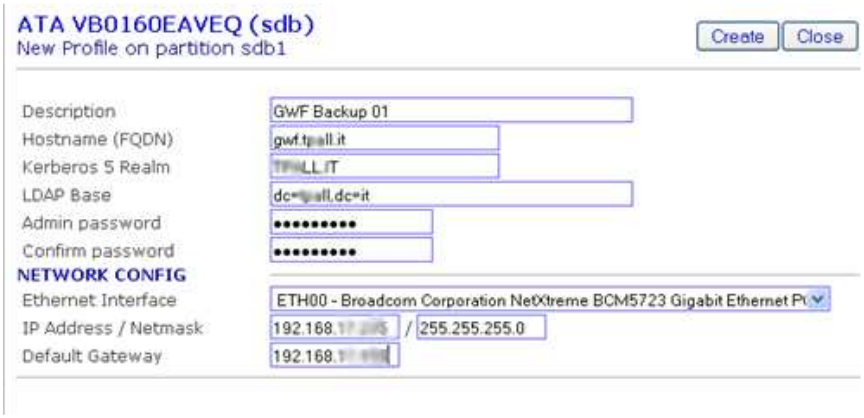
Kerberos

La parte relativa a Kerberos viene creata la momento dell'installazione, per cui conviene dare al sistema già un nome ed un dominio (DC) coerenti in modo da non dover apportare modifiche successive:

SECURITY >KERBEROS 5



Principal	Realm
K/M	IN.LABTEL.IT
admin	IN.LABTEL.IT
host/zeroshell.in.labtel.it	IN.LABTEL.IT
kadmin/admin	IN.LABTEL.IT
kadmin/changepw	IN.LABTEL.IT
kadmin/history	IN.LABTEL.IT
kadmin/localhost.localdomain	IN.LABTEL.IT
krbtgt/IN.LABTEL.IT	IN.LABTEL.IT
marco	IN.LABTEL.IT
paolo	IN.LABTEL.IT



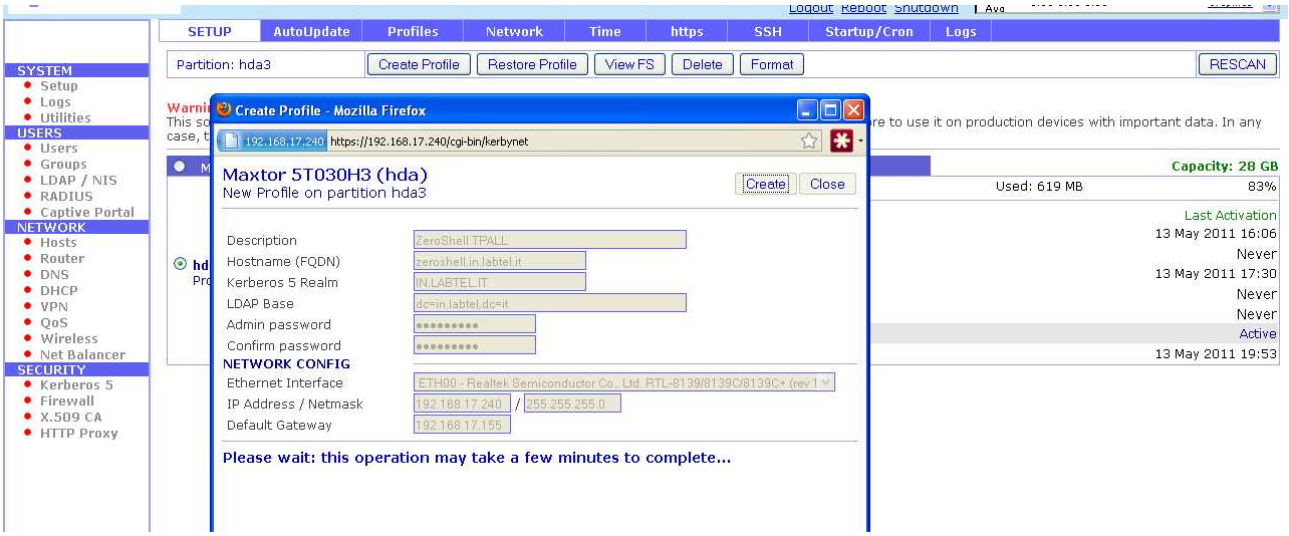
A questo punto si può rigenerare la CA con il nome a dominio corretto.

Salvataggio del Profilo

ZS mantiene attive le modifiche e le ricarica al reboot del sistema, ma per buona abitudine è bene salvare il profilo con tutte le ultime modifiche testate da considerare in qualche modo ufficiali.

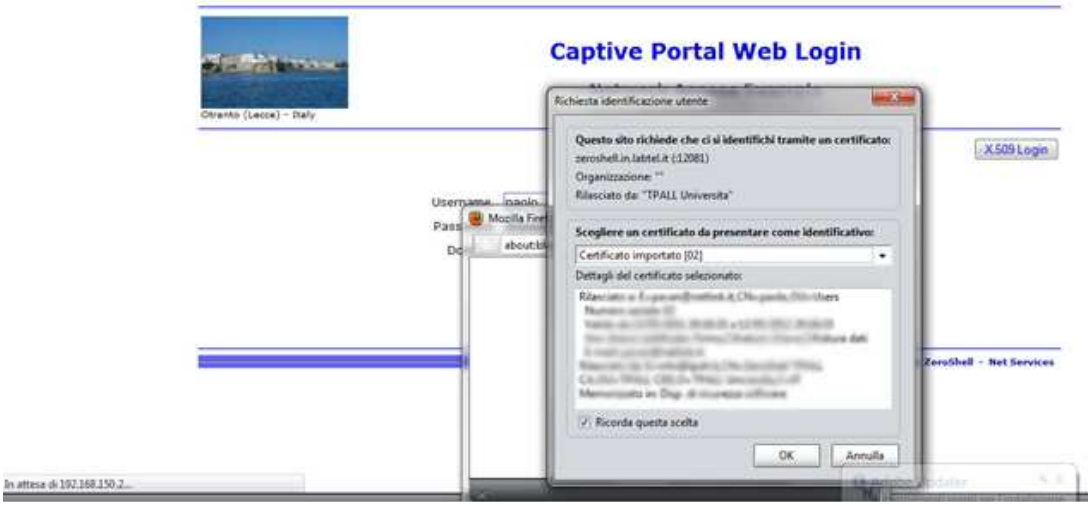
SYSTEM >SETUP>Profiles

Aggiungere i dati necessari e cliccare su “Create”.



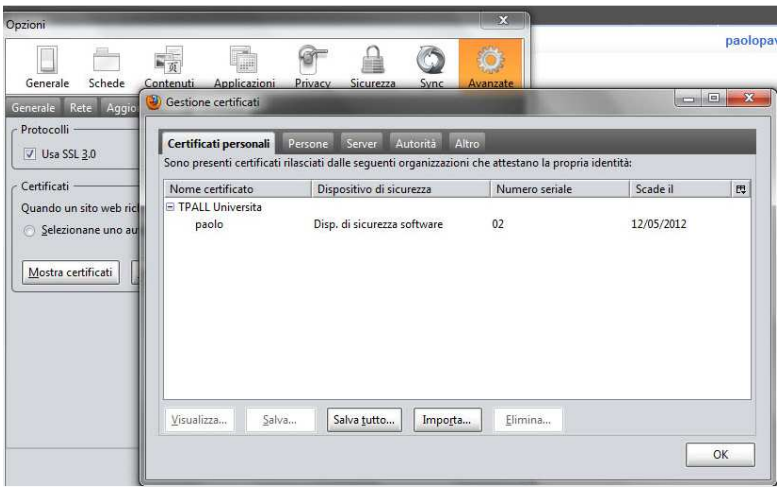
Client

Il client una volta associato alla rete Wireless, deve solo eseguire il browser e si troverà la richiesta di accesso del Captive Portal, che potrà espletare con user/password oppure con il certificato X509.
Indirizzo IP e parametri verranno forniti direttamente dal Captive Portal (ZS) collegato al bridge dell’Access Point.
E’ importante che il browser supporti e non blocchi l’aperture delle popup che sono necessarie per la negoziazione dell’autenticazione tra client e Captive Portal:



La finestra in popup permette di effettuare il refresh della connessione che in caso di inattività costringe a riloggarsi al sistema Captive Portal.

L'accesso tramite certificato, cliccando sul bottone "X509 Login" è possibile solo dopo aver caricato il certificato nel nostro browser. Il certificato va esportato e reso disponibile all'utente in qualche modo, attraverso la rete oppure su un supporto removibile (CD, chiavetta).
In genere sotto la sezione di Sicurezza/Certificati del browser si trova la possibilità di importare il certificato, che normalmente viene emesso senza una password, ma consegnato all'esclusivo destinatario, che da quel momento sarà responsabile del suo accesso e delle sue consultazioni.



L'accesso da dispositivi palmari o cellulari è limitato dall'uso della popup, non supportata dai browser di questi dispositivi. Pare che nelle prossime release vengano affrontati questi problemi. Nel caso servisse si può sempre abilitare il dispositivo autorizzando il suo indirizzo MAC, nella sezione del CP (Free Authorized>Clients), il client lascerà comunque tracce nei log del proxy o del Conntrack, ma non rappresenta certamente il sistema migliore dal punto di vista della sicurezza.

Tips&Tricks

Vediamo alcuni interessanti TIPS, trovati in giro sulla rete per ovviare ad alcuni problemi comuni:

Prestazioni havp

Non potendo disabilitare il supporto clamav per havp si può usare un ramdisk come partizione dove scrive i file temporanei havp.

Per farlo seguire questi semplici passaggi:

Step 0 – Disabilitare havp temporaneamente dall'interfaccia web
Questa è la directory dove scrive i temporanei havp
/Database/var/register/system/havp/tmp
Step 1 – Creare di 50MB ext2 file-system
> cd /Database
> dd if=/dev/zero of=HAVP.ext2 count=100000
> mkfs.ext2 HAVP.ext2
Step 2 - Preparare e HAVP.ext2 directory permissions per havp:
> mount -o loop HAVP.ext2 /mnt
> chown havp.havp /mnt
> umount /mnt
> gzip HAVP.ext2
Step 3 – Eseguire il mount da shell AND e aggiungerlo al pre-boot scripts:
> gzip -dc /Database/HAVP.ext2.gz >/dev/ram3
> mount -omand,noatime /dev/ram3 /Database/var/register/system/havp/tmp
root@zeroshell havp>

mount /dev/ram3 on /Database/var/register/system/havp/tmp type ext2 (rw,mand,noatime)
Riavviando havp dovrà essere in grado di scrivere dentro la directory
root@zeroshell tmp> ls
havp-4kc22p havp-CZiu5p havp-OSF18p havp-TlW29p havp-gYS9aq havp-gkJV6p havp-l7gacq

Risorse
http://www.zeroshell.net/eng/forum/viewtopic.php?t=1919

DB LDAP corrotto (soluzione)

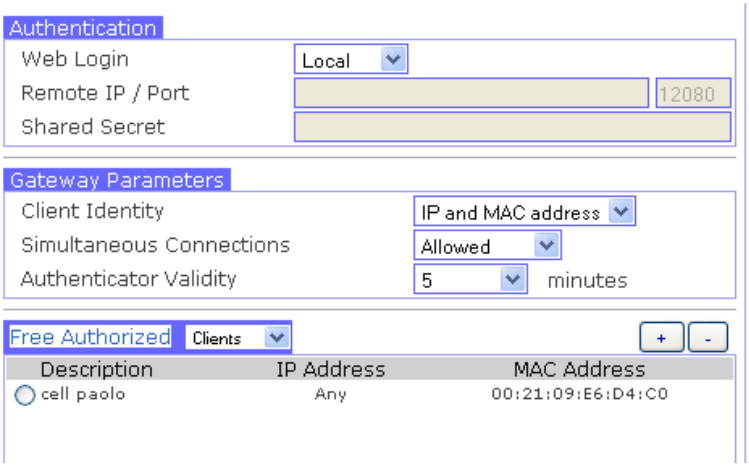
Mi è capitato di vedere bloccato ZS al boot con sula voce “Starting *LDAP* daemon"

Si può forzare il recover oppure usare questa procedura:

1. Effettuare l’avvio con un Live CD.
2. Montare la partizione che contiene la directory /var.
3. cd /mnt/sda1/_DB.001/var/openldap-data
4. sudo mkdir bak
5. sudo mv __.db.00* ./bak/
6. sudo reboot

Problema palmari, Ipad e Iphone

Iphone e Ipad non supportano la funzione di popup per l'autenticazione. Solo le vecchie versioni dell'iphone funzionano. L'unico modo per farli funzionare è di inserire il MAC nella sezione free authenticated service. Ho usato questo metodo per i miei cellulari Nokia (Symbian) ed ha funzionato correttamente.



Installare pacchetti su ZS

Esistono dei mods ovvero dei pacchetti disponibili a questo indirizzo per la nostra installazione di ZS:

http://0sh-mods.net/

Per aggiungere rsync al nostro sistema ZS:

```
cd /Database
wget http://0sh-mods.net/mods/0sh-mods-rsync-3.0.6-v1.0.tar.bz2
tar xfvj 0sh-mods-rsync-3.0.6-v1.0.tar.bz2
cd 0sh-mods-rsync-3.0.6-v1.0
./install.sh
```

Conclusioni

ZS come Captive Portal è un ottimo strumento, mi è parso stabile e ricco di funzionalità. Va ovviamente ricordato come si tratti di un prodotto rilasciato con licenza GPL, e non una soluzione professionale, dove c'è qualcuno incaricato a risolverci il problema perché previsto da un contratto di assistenza.
Chi lo utilizza lo fa sulla base delle proprie competenze e responsabilità, come del resto recita lo stesso ZS:

Warning:
This software is NOT guaranteed to be bug free. It is your responsibility to properly test it on scratch disks before to use it on production devices with important data. In any case, the author is not responsible for any data loss or damage caused by this software.

Esiste comunque il forum sia italiano che inglese che aiuta a risolvere molti problemi e che va consultato prima di chiedere magari aiuto su problematiche già affrontate e risolte.
Detto questo posso dire che si tratta di una'ottima distribuzione, ricca di funzioni e bootable anche con una semplice chiavetta USB. Molto facile e veloce da installare e configurare la trovo particolarmente adatta a quelle situazione in cui sono sufficienti alcune funzioni standard che non richiedano particolari modifiche, per cui lavorare su distro Linux complete può sembrare migliore. In realtà come Bridge/Firewall/Captive Portal l'ho trovato davvero flessibile e versatile e di facile implementazione.
Concludo con un ringraziamento per Fulvio Ricciardi, che ha fatto davvero un ottimo lavoro regalando alla comunità un prodotto di questo livello.

Risorse

- https://www.bottediferro.com/box/folder/15369
- http://www.uielinux.org/progetti/17-diffondere-linux/131-wi-fi-hotspot-tutto-opensource-grazie-a-zeroshell.html
- http://www.zeroshell.net/captiveportaldetails/
- http://www.renatomorano.net/?p=400

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

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