



Sistemisti indipendenti

Zeroshell b15: Accounting

Introduzione

Da tempo aspettavamo l'implementazione di questa funzione, per poter utilizzare pienamente ZS in situazioni in cui è necessario contabilizzare il traffico degli utenti ed accedere senza difficoltà da dispositivi mobili. Adesso ZS finalmente consente di effettuare questa configurazione in modo semplice ed efficace, la news recita così:

15 Luglio 2011 - La nuova release 1.0.beta15 contiene il modulo di Accounting RADIUS che permette di contabilizzare il tempo, il traffico e i costi di connessione sia per gli accessi su Access Point con WPA/WPA2 Enterprise che tramite Captive Portal. Si possono impostare limiti in traffico e tempo e gestire tariffe prepagate. Il Captive Portal è stato arricchito di nuove funzionalità come la protezione contro attacchi DoS e la possibilità di disabilitare la finestra Popup di accesso alla rete sui dispositivi Mobile.

Il mio obiettivo non pienamente soddisfatto dalla versione precedente (b14) era quello di abilitare un captive portal privo di autenticazione dal lato wireless, in una configurazione tipo internet point o aeroporto, in cui la connessione alla rete wireless avviene per tutti i dispositivi, senza autenticazione, ma l'accesso ad internet passa per un'autenticazione forzata attraverso la pagina web del captive portal. Inoltre la finestra di popup usata per mantenere e monitorare la connessione creava alcuni problemi per i dispositivi mobili, dotati di browser non in grado di gestirla, la mia necessità era quella di poterla eliminare almeno per i dispositivi tipo Iphone, Blackberry, Symbian, Android ecc ecc.

Ora tutti questi strumenti sono stati implementati vediamo se e come funzionano, facendo un po' di prove sul campo.

Ricordo che la mia configurazione standard prevede la box ZS tra un pool di access point senza autenticazione e una connessione ad internet tramite rete ADSL, per cui occorre configurare ZS con le sue interfacce di rete, il NAT abilitato, le funzioni di Proxy e Firewalling adeguate alle vostre necessità : per chi volesse approfondire può leggere gli altri Howto pubblicati, decisamente più dettagliati da questo punto di vista.

Configurazione Accounting

L'installazione è sempre la solita, che sia fatta da immagine ISO o da pen drive, non cambia, la vera differenza è già visibile in alcuni menu, quello dell'Accounting ora pienamente attivo e quello del Captive Portal. Per prima cosa ho creato una serie di utenti, a cui successivamente ho pensato di assegnare una CLASSE diversa per contabilizzare il tipo di accesso e di utilizzo del servizio.

USERS>Accounting



Dopo avere creato gli utenti ho creato le classi, accedendo alla sezione Accounting, basta cliccare su ADD. La schermata che si apre di Accounting Class, permette di dare un nome alla classe e poi inserire i valori per il pagamento (pre o post paid) ed i limiti di traffico (Traffic, Time Bandwidth)

Accounting Class Save Close

Class Name

BILLING

Type of Charge Postpaid ▼
Time and Traffic Limits take effect if specified

Cost per Megabyte (€)

Cost per Hour (€)

LIMITS

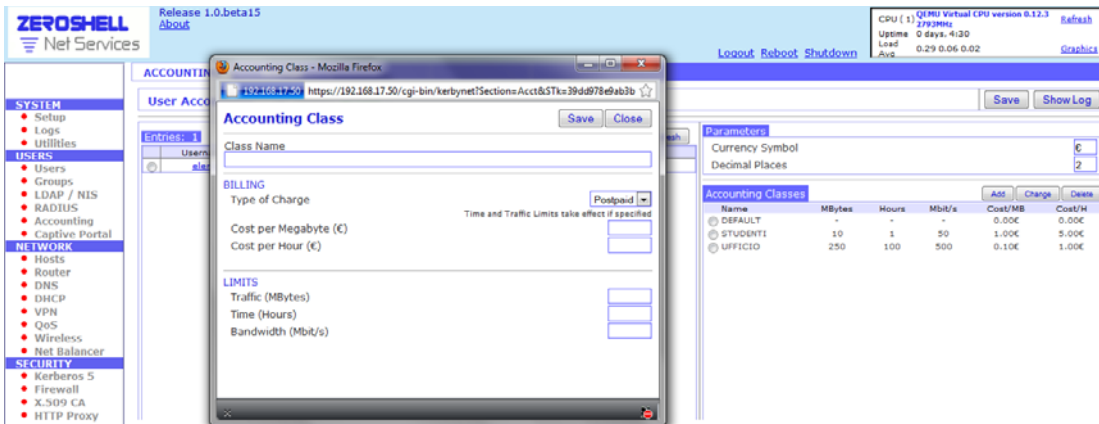
Traffic (MBytes)

Time (Hours)

Bandwidth (Mbit/s)

Se si sceglie *Prepaid* i limiti verranno calcolati in base al credito che si ha in partenza. Una volta esaurito il credito l'account non può più accedere al servizio.

Se invece si sceglie *Postpaid* i limiti impostati daranno luogo ad un conto finale da pagare, calcolato sulla base dei costi impostati al tempo e al traffico.



E' bene non confondersi tra i due metodi, il primo è quello da usare quando si "vende" il servizio e si vuole che scada automaticamente all'esaurimento del credito, il secondo invece è quello utile per contabilizzare il traffico degli utenti. In questo caso i conti si faranno alla fine.

Riepilogando i limiti possono essere impostati sulla base di valori:

- Tempo (h)
- Download (MB)
- Banda (Mbit/s)



Nel mio caso la necessità era quella di limitare l'accesso e fare in modo che gli utenti imparassero a gestire il loro traffico e a non abusarne, ho comunque dovuto creare due classi diverse, nel mio caso Postpaid, ma con limiti ben diversi.

Accounting Details - Mozilla Firefox
 https://192.168.17.50/cgi-bin/kerbynet?Section=Acct&STK=39d0978e9ab3ba7fe09779bfe7ba809179a3b3&Action=ShowDetails&Entry=elena

elena Refresh Close

Traffic : 12.94 MB
 Time : 0:08
 Cost : 13.63€ Credit: 0.00 €

Sessions : 2

	Client Identification	NAS	Start Time	Stop Time	RX (MB)	TX (MB)	Traffic (MB)	Time	Cost (€)	Last Update
1	192.168.150.151 / 00:21:5d:d3:7c:90	zeroshell	08/03/11 00:16:14	08/03/11 00:17:20	6.16	0.15	6.31	0:01:06	6.40	08/03/11 00:17
2	192.168.150.150 / 00:21:09:e6:d4:c0	zeroshell	08/02/11 20:01:08	08/02/11 20:08:24	6.43	0.20	6.63	0:07:16	7.24	08/02/11 20:10

Hours	Mbit/s	Cost/MB	Cost/H
-	-	0.00€	0.00€
1	50	1.00€	5.00€
100	500	0.10€	1.00€

Le mie due classi sono denominate in questo modo e sono di tipo postpaid e con limiti:

- STUDENTI 10 h, 250MB, 500Mb/s
- UFFICIO: 100 h, 1000MB, 1000Mb/s

A questo punto occorre tornare sulla scheda Utenti e associare gli utenti alle rispettive classi. Se volete fare un test usate due classi con limiti diversi, uno possibilmente basso, per mandarlo rapidamente in esaurimento.

USERS>Edit

/ /
 UFFICIO

Limits: 250 MB | 100 h | 500 Mb/s
 Costs (postpaid): 0.10€/MB | 1.00€/h

User Password
 Password:
 Confirm:

Authentication Protocol
 Kerberos 5
 RADIUS (VLAN)

Nella sezione RADIUS Accounting si può assegnare la classe all'utente.

Configurazione Captive Portal

A questo punto possiamo configurare il Captive Portal, che presenta delle belle novità.

USERS>Captive Portal

La schermata del CP presenta due nuove funzioni la Dos Protection di cui si può impostare il livello di forza e la finestra popup che può essere disabilitata per alcuni specifici dispositivi. Io consiglio di tenerla per i sistemi dotati di browser normale, come FF, IE o GC perché aiuta l'utente a visualizzare il suo traffico (cliccando sul tasto refresh), mentre per i dispositivi palmari e tablet, meglio lasciarla disabilitata, come da default.



Release 1.0.beta15
[About](#)

CPU (1) QEMU Virtual CPU version 0.12.3 Refresh
 Uptime 0 days, 4:30
 Load Avg 0.29 0.06 0.02 Graphics

[Logout](#) [Reboot](#) [Shutdown](#)

CAPTIVE PORTAL Gateway Authentication Accounting Language Graphics Bandwidth

GW Active on: ETH01 Interface: ETH01 MULTI Save Show Log

Connected Clients: 0 Disconnect Refresh

Username IP Address MAC Address

Network Access Popup - Mozilla Firefox
 192.168.17.50 https://192.168.17.50/cgi-bin/kerbynet?STk=39dd978e9ab3ba7fef09779bfe7ba809179a: ☆

Network Access Popup Save Cancel

Use the popup window for the browsers: All excluded the list below

Log the browser capturing requests Logs

Browser Exclusion List

- Mobile
- BlackBerry.*
- Nokia.*
- SAMSUNG.*
- Windows CE
- Windows Phone
- Windows Mobile
- Symbian.*
- SymbOS
- Palm.*
- Opera Mini
- Opera Mobi
- iPhone

Aug 03 00
 Aug 03 00

Gateway Parameters

DoS Protection Medium
 Client Identity IP and MAC address
 Simultaneous Connections Not allowed
 Authenticator Validity 5 minutes Popup

Free Authorized Services

Description	IP Address	Port
<input type="radio"/> Domain Name System	Any	53/udp
<input type="radio"/> DHCP and bootp	Any	67/udp

La prima cosa che noto una volta attivato il captive portal, tra la rete wireless e internet e che i miei dispositivi Symbian funzionano, si autenticano e accedono con il loro browser nativo ad internet. L'unica cosa che bisogna ricordarsi e di accettare il certificato SSL, selezionando la voce "Continua" solo per il primo accesso.

Verifica funzionamento Accounting

Nel mio caso per fare i test ho utilizzato prima il metodo Postpaid che non obbliga l'amministratore ad assegnare un credito prima della connessione. Se proviamo ad impostare un valore basso per il traffico ad esempio 5MB, possiamo verificare come sessione viene interrotta appena superato il limite, indicando che il limite è stato superato. Il messaggio in evidenza è "Traffic limit reached".

Network Access Close

elena@example.com not connected

Traffic limit reached

Time	:	0:01	Refresh
Traffic	:	6.31 MB	
Cost	:	6.40 €	

Powered by ZeroShell - Net Services

Se si tentasse di riconnettersi, il sistema lo impedirebbe in quanto l'account ha esaurito il traffico a disposizione. Quindi se il traffico è scaduto l'utente non può più collegarsi



Sistemisti indipendenti

Network Access

Access Denied !!!

elena@example.com not connected

Traffic limit reached

If you do not have an account, read the instructions by clicking on the follow link to obtain one. [Account](#)

Per poter dare nuova validità all'account occorre visualizzare lo stato dell'utente sotto la scheda Accounting, selezionare l'utente e cliccare sul bottone "Remove".

Release 1.0.beta15
About

ZEROSHELL Net Services

ACCOUNTING Manage

User Accounting Status: ACTIVE

Entries: 2 [Details] [Remove] Filter [] Refresh

Username	Traffic (MB)	Time	Cost (€)	Credit (€)	Last Update
elena	14.44	0:01	14.54	0.00	08/03/11 00:26
paolo	4.50	0:08	0.60	0.00	08/03/11 10:43

In questo modo i conteggi vengono azzerati e l'utente può tornare a ricollegarsi fino ad un nuovo esaurimento del suo credito.

Se si sceglie il metodo Prepaid occorre impostare un credito in partenza sufficiente a coprire i limiti, in caso contrario pur avendo un account il sistema ci risponde con "No credit available".

Per farlo occorre accedere alla scheda dell'utente ed assegnare in basso a destra nella sezione Credits, un valore in partenza. Quello sarà il totale che l'utente avrà a disposizione. Una volta esaurito gli sarà impossibile collegarsi.

RADIUS Accounting

Expiration (mm/dd/yyyy) [] / [] / []

Accounting Class [STUDENTI]

Credit: 100.00 € [+] [-]

Limits: 10 MB | 1 h | 50 Mb/s

Costs (prepaid): 100.00€/MB | 50.00€/h

Questo sistema è molto più restrittivo dell'altro, infatti indipendentemente dalla classe assegnata, che permette comunque di impostare i prezzi ed i limiti, senza il credito assegnato non si può assolutamente accedere.

Il metodo postpaid invece permette da subito l'accesso, e pur applicando i costi e le limitazioni della classe di appartenenza dell'utente, permette comunque di accedere fino alla scadenza dei limiti.

In questo caso la finestra di popup del browser, mostra ad ogni refresh il traffico effettuato ed il costo, permettendo di tenere sotto controllo il proprio credito. Una volta raggiunto il monte del proprio credito, il browser viene disconnesso, mostrando nel caso l'eccedenza.



Sistemisti indipendenti

Network Access

[Close](#)

elena@example.com not connected

Traffic limit reached

Time	:	0:07	Refresh
Traffic	:	11.65 MB	
Cost	:	12.30 €	
Credit	:	-1.97 €	

Powered by ZeroShell - Net Services

Il sistema si è rivelato piuttosto efficiente in entrambi i metodi di pagamento, una volta raggiunto il limite, o appena superato la connessione è stato interrotta.

Una funzione molto utile da assegnare è anche quella del tempo limite per la sessione. In questo modo si evitano che utenti possano lasciare attivi dispositivi a effettuare download prolungati.

Ovviamente anche dal lato amministrazione possiamo tenere sotto controllo questi dati e lo status di utilizzo del sistema da parte degli utenti, visto che ZS crea un piccolo ma molto utile file di log

```
root@zeroshell zeroshell> tail -f Accounting
```

```
Aug  3 00:20:43 zeroshell Accounting: Connection limit reached by the user elena@example.com (Traffic limit reached)
Aug  3 10:34:05 zeroshell Accounting: Connection limit reached by the user elena@example.com (Traffic limit reached)
Aug  3 16:40:45 zeroshell Accounting: Connection limit reached by the user elena@example.com (No credit available)
```

Questo file di log segna lo stato dell'accounting indicando per ogni utente eventuali superamenti di soglie sia per i limiti che per il credito.

La classe di default (accounting)

Questa classe è importante perché è quella cui appartengono gli utenti che normalmente non vengono assegnati a classi diverse. Non ha limiti impostati in partenza, una sorta di classe open, ma esistono casi, come quelli in cui si creano user a giornata che poi vengono resettati (alberghi, sale stampa), in cui può essere utile modificare i limiti di default di questa classe, per poter creare gli utenti senza necessità di doverli assegnare ad un classe particolare. E' molto utile in casi in cui si usano gli script di creazione automatica degli utenti, per cui non è necessario accedere manualmente all'interfaccia di ZS in amministrazione.

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.

Class	Description
DEFAULT	Default class for unclassified traffic

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.

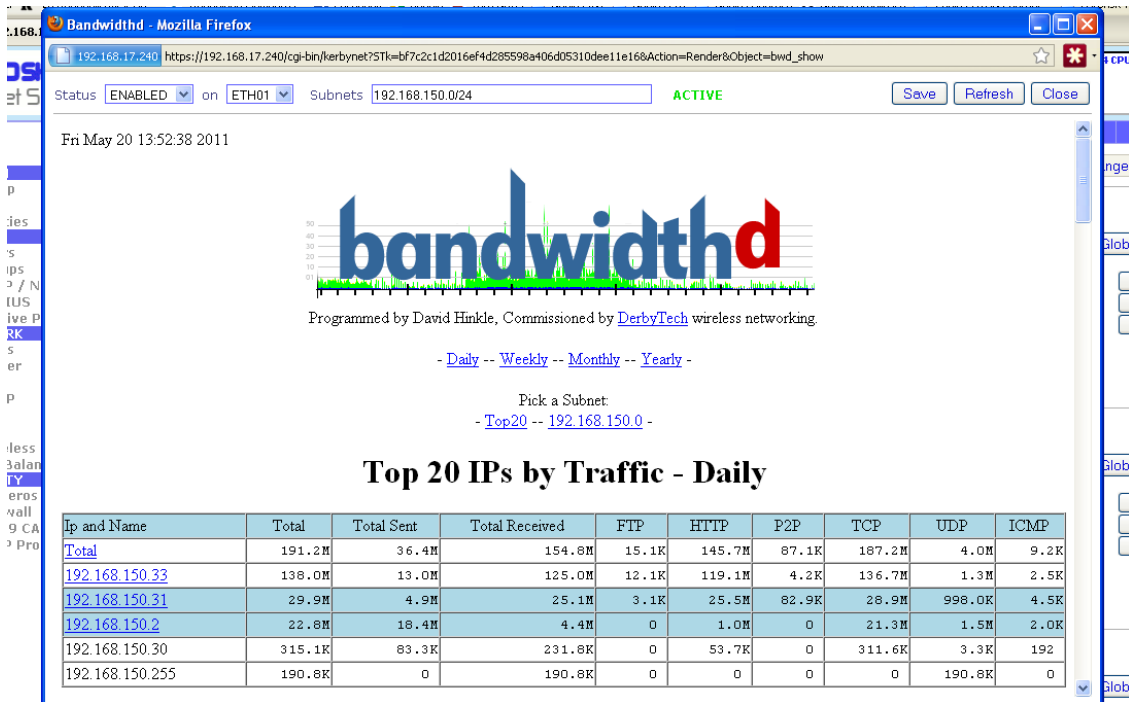
Facciamo qualche esempio se io assegno un valore massimo di 100 kbit, diviso 8 avrò la velocità di download in Bytes, quindi 12,5 KB. Basta fare qualche prova per rendersi conto che il filtro funziona ed è efficace. Occorre fare una valutazione attenta della propria banda a disposizione e decidere quanta 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 host (IP) e dei protocolli utilizzati.

NETWORK > Bandwidthd

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



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.

Il Quality of Service ben si accompagna ad uno strumento che in questo caso ha il compito di regimentare e contabilizzare l'accesso ed il traffico degli utenti.

Aggiornamento: da b14 a b15

Esiste un modo per effettuare un upgrade dalla b14 alla b15, consiste nell'usare uno script, `zeroshell-b14tob15.sh`.

Le istruzioni per effettuare l'operazione si trovano in questo utile thread del forum di Zeroshell.

<http://www.zeroshell.net/forum/viewtopic.php?t=3022>

Io personalmente trovo talmente semplice e automatico ZS da configurare che faccio prima a reimpostare le configurazioni e ricreare gli utenti. Comunque questa sembra un'ottima soluzione per effettuare upgrade su installazioni magari particolarmente complesse.

Conclusioni



Era da tempo che aspettavamo la funzione sull'accounting degli utenti. Adesso con le dovute cautele con un'installazione di ZS si possono gestire a pieno situazioni in cui gli utenti devono avere il traffico contabilizzato e a scadenza, quindi chioschi, internet point o zone wifi dove gli utenti acquistano del traffico a tempo. Inoltre l'eliminazione della finestra popup per dispositivi mobili, funzione adesso del tutto configurabile, rende la funzionalità Captive Portal altamente utilizzabile, eliminando le procedure di autenticazione wireless che sono normalmente le più complesse, e relegando la fase di autenticazione esclusivamente al Captive Portal. Consiglio a tutti quelli che intendono usarlo in produzione, di pianificare con cura l'ambito di utilizzo e la creazione delle classi di accounting, solo dopo aver ben chiaro il metodo di funzionamento e di contabilizzazione del traffico che questo sistema adotta.

Doc: **zeroshell-b15.pdf**

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

Data: *Luglio 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>