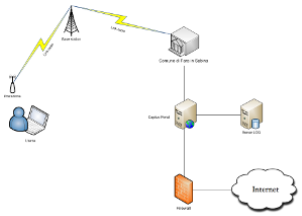
Networking

“Wifi in Fara”, un progetto di access point federati per l’accesso a internet gratuito.†

Angelo De Simone,[a] Giovanni Agostini,[a] Luca Ianniello,[a] Andrea Lora,[a] Giuseppe Nantista,[a] Augusto Pifferi.[a]



I presente documento descrive il progetto e la realizzazione di un sistema di punti di accesso wifi gratuito per i cittadini del Comune di Fara in Sabina. Illustreremo le linee guida di progetto, le postazioni selezionate e l’architettura di sistema.

Keywords: Captive Portal, Access Point, Mikrotik, VPN

1 Premessa

Un accesso ad internet disponibile gratuitamente per i cittadini è il primo passo che una amministrazione locale può compiere per abbattere il Digital Divide, il gap cioè che si pone fra i cittadini che hanno accesso e sanno utilizzare internet e quelli che non hanno queste possibilità.

In quest’ottica il Comune di Fara in Sabina, a fronte di numerose collaborazioni svolte in passato con il servizio reti dell’Area della ricerca RM1 del CNR, ha affidato allo stesso gruppo il compito di predisporre una piattaforma unica per consentire ai cittadini delle sue numerose frazioni di usufruire di questo servizio. Il progetto ha visto la luce nel luglio 2013 con il nome di “Wifi in Fara”.

2 Le postazioni

Su indicazione dell’amministrazione pubblica sono state predisposte postazioni nelle frazioni di:

Passo Corese, Prime Case, Corese Terra, Coltodino, Canneto, Borgo Quinzio, Fara In Sabina. Le postazioni sono sommariamente evidenziate nella mappa di figura 1.

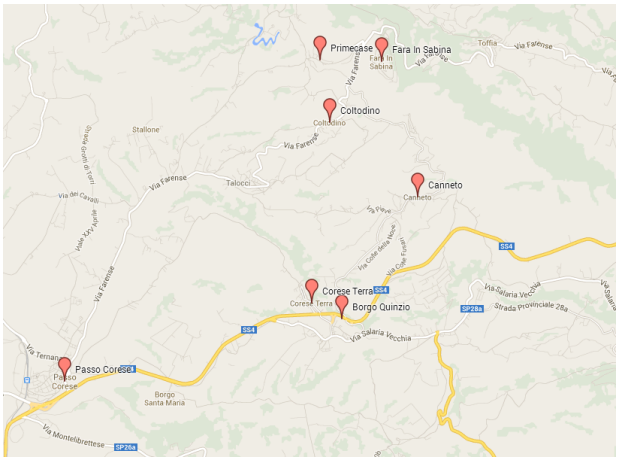


Fig. 1 Mappa delle postazioni.

3 Postazione tipo e rete di raccolta

In ogni postazione sono stati installati una CPE per la connessione alla rete wireless CNR e un Access Point per la distribuzione locale del segnale “Wifi in Fara”. Il primo collegamento viene realizzato in standard Hiperlan 802.11a, nell’intorno della frequenza 5Ghz, il secondo invece in standard Wifi 802.11b/g nell’intorno della requenza 2.4Ghz. Lo schema di connessione di rete, rappresentato in Fig.2 prevede che da ogni postazione venga instaurato un tunnel VPN verso la sede principale, dove gli utenti, previa accettazione delle condizioni di servizio, possono navigare verso internet liberamente.

[a] *CNR - Istituto di Cristallografia, Strada Provinciale 35/d, Montelibretti, Italia*

† rapporto tecnico IC 13/09 registrato con numero di protocollo IC/1879 del 20/12/2013

L'accettazione delle condizioni avviene tramite il meccanismo del captive portal, come già discusso nel precedente articolo,[1] ma grazie alla nuova normativa in vigore, il D.L. 21 giugno 2013 n. 69, è sufficiente che le connessioni effettuate da un utente siano riconducibili ad esso esclusivamente tramite il mac-address dell'apparato con cui si connette alla rete. Ogni dispositivo può usufruire di una banda massima di 2Mbit/s in download e può scaricare un massimo di 300 MByte di dati al giorno.

Per raccogliere tutte le connessioni provenienti dai vari hotspot è stato realizzato un unico dominio di broadcast, usando le funzioni messe a disposizione dagli apparati Mikrotik utilizzati per le funzioni di CPE e concentratore. Ogni CPE instaura una connessione pptp verso il concentratore e successivamente i tunnel così instaurati vengono collegati in bridge lato CPE con l'access point e lato concentratore con il server di Captive Portal.

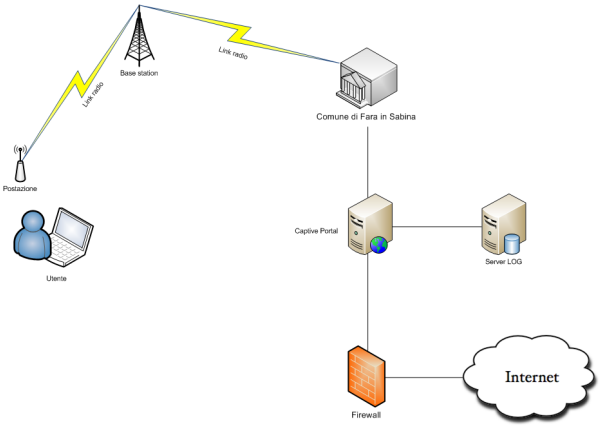


Fig. 2 Schema della connessione di rete.

Configurazione delle CPE:

Instaurazione del tunnel pptp:

```
[admin@c_farasabina.wifi_primecase] > int pptp-client add name="pptp-out1" \
connect-to=10.10.235.2 user="fara2-primecase" password=******** \
profile=default-encryption add-default-route=no dial-on-demand=no \
allow=pap,chap,mschap1,mschap2
```

Creazione del tunnel eoip:

```
[admin@c_farasabina.wifi_primecase] > int eoip add name="eoip-tunnel1" \
remote-address=172.31.31.1 tunnel-id=3112
```

Creazione del bridge:

```
[admin@c_farasabina.wifi_primecase] > int bridge add name="bridge1"
[admin@c_farasabina.wifi_primecase] > int bridge port add bridge=bridge1 \
interface= ether1
[admin@c_farasabina.wifi_primecase] > int bridge port add bridge=bridge1 \
interface= eoip-tunnel1
```

Lato concentratore sono presenti le regole gemelle di quelle appena descritte, il motivo per cui sono stati creati anche dei tunnel ethernet over ip (eoip) è che Mikrotik non consente di aggiungere ad una interfaccia virtuale bridge un tunnel pptp.

4 Il log dei dati sensibili

Come da normativa vigente i dati relativi alle connessioni effettuale dagli utenti, così come anche la corrispondenza mac-address - indirizzo IP, vengono salvati per un periodo di sei mesi (salvo comunicazioni dell'autorità giudiziaria) su un sistema di logging basato su syslog-ng.

Configurazione del syslog:

```
source s_net { udp (); };
destination df_captive { file("/var/log/captive.log"); };
filter f_captive { host( "IP_CAPTIVE_PORTAL_ROUTER" ); };
```

Configurazione Del Router Mikrotik Che Invia i Log

```
[admin@CAPTIVE_PORTALS] > ip firewall mangle add chain=prerouting action=log \
connection-state=new src-address=10.0.0.0/8
```

5 Il monitoraggio del sistema

Tutti gli apparati di rete impiegati dal sistema sono stati posti sotto monitoraggio tramite la piattaforma Istituto di Zabbix in uso presso l'Area della Ricerca RM1.[2] In caso di irraggiungibilità di uno di essi, un avviso via mail raggiunge lo staff tecnico, al fine di intervenire tempestivamente nella diagnosi e nella risoluzione del guasto.

Riferimenti

1 A. Pifferi, G. Nantista, L. Ianniello, C. Ricci, L. Rossi, M. Simonetti, Un Captive Portal per l'autenticazione su Reti Wifi dedicate agli Internet Access Point Liberi, SMART eLAB 2 (2013) 15–19. doi:10.30441/smart-elab.v2i0.55.

2 A. Pifferi, G. Nantista, L. Ianniello, A. Lora, M. Simonetti, Analisi e Implementazione di Sistemi per il Monitoraggio della Rete Wireless Relativa al Progetto ADD (Anti Digital Divide) e delle Infrastrutture di Campus AdR RM1., SMART eLAB 2 (2013) 1–9. doi:10.30441/smart-elab.v2i0.46.