Università degli Studi di Camerino

Scuola di Scienze e Tecnologie

Corso di Laurea in Informatica

Un Package sms per la gestione di Captive Portal

Laureando
Carlo Guerrini
Matricola 66987

Relatore
Prof. Fausto Marcantoni

A.A. 2010/2011

Questo lavoro è il completamento di quattro anni di studi ed è dedicato ai miei genitori

che in questo periodo mi hanno supportato in ogni aspetto.

Se ho potuto usufruire di questa opportunità e sono arrivato a questo punto lo devo a loro.

Mentre in fisica devi capire come è fatto il mondo,

in informatica sei tu a crearlo.

Dentro i confini del computer, sei tu il creatore.

Controlli – almeno potenzialmente – tutto ciò che vi succede.

Se sei abbastanza bravo, puoi essere un Dio. Su piccola scala.

[Cit. Linus Torvalds]

Indice

Introduzione

I calcolatori elettronici sono sempre più parte integrante della vita delle persone sia per hobby che per lavoro. Numerose attività dipendono dai calcolatori elettronici. Questa dipendenza viene ancora più accentuata dalla necessità di restare sempre e comunque connessi alla rete internet in ogni momento ed in ogni luogo. L'entrata in commercio dei tablet, dei pc portatili , degli smartphone permette proprio questo. Negli ultimi anni lo sviluppo delle tecnologie wireless unite alla banda larga hanno fatto nascere un nuovo concetto di connettività: gli *Hotspot*. Queste soluzioni permettono a qualunque utente dotato di un dispositivo per la navigazione in wifi, di connettersi ad internet in prossimità di questi spazi in modo del tutto legale e sicuro. I recenti cambiamenti sulle normative italiane dal 1° gennaio 2011 sulla liberarizzazione del WiFi in Italia lasciano ben sperare sull'evoluzione di questo standard. I precedenti vincoli del famigerato "Pacchetto Pisanu" introdotto nel 2005 ,nato per contrastare il terrorismo sulla rete internet, non ne ha permesso una rapida diffusione sul territorio nazionale per le sue restrittive condizioni. Resta comunque nell'interesse di chi mette a disposizione la propria connessione, come bar, ristoranti, aereoporti ,alberghi ecc , di fornire un servizio facile, accessibile a tutti, controllato, a basso costo, autonomo e nel rispetto delle regole. Per questi motivi l'autenticazione tramite SIM telefonica si presta bene a questo ambito.

La finalità della presente tesi è quello di fornire un *package* di sistema *standalone* per la libera condivisione internet completamente personalizzabile, rispettando il più possibile i principi di sicurezza informatica. L'integrazione di un *gateway* sms nel captive portal risulta una soluzione che fonde facilità e praticità d'uso con il rispetto delle normative per l'identificazione degli utenti. Il *software* che compone la tesi è completamente *open source* ed esente da costi di licenza. La parte di codice da me ideata e realizzata in fase di tesi è stata proposta alla comunità della distribuzione che ho utilizzato perché ritengo giusto, che come io ho potuto usufruire del lavoro degli altri, gli altri devono poter usufruire del mio lavoro secondo il principio di *software* libero.

Naturalmente la coesistenza di più utenti necessita la messa in sicurezza dalle insidie della rete e comporta un'azione di protezione della propria rete interna e dei propri dati. E' molto importante garantire l'integrità e la segretezza delle proprie informazioni, e non è raro che queste spesso vengano violate da malintenzionati utenti della rete. Da qui nasce l'impegno per mantenere la propria rete il più possibile sicura ed efficiente attraverso il *set-up* di strumenti addizionali, quali, un *proxy* dedicato al filtraggio degli elementi virali tramite l'accoppiata *havp + clamav*, un

altro *proxy server squid* per i controlli di accesso ed il *traffic management*, un controllo sulla risoluzione dei *DNS* ritenuti non appropriati, un servizio di NTP per la sincronizzazione dell'orario di sistema, un DHCP server per la LAN, il servizio di Captive Portal per la gestione degli utenti ed una procedura da me realizzata, per la registrazione tramite SMS di tutti gli utenti che vogliano usufruire dell'*hotspot.*

Struttura della tesi L'elaborato è stato organizzato in 5 capitoli. Nel primo si affronta il concetto di sicurezza informatica.

Il 2° capitolo è un'analisi al lato giuristico dell'infrastruttura allestita.

Il terzo capitolo è dedicato all'importanza di avere un firewall sulla rete, a riassumerne le principali tipologie ed a garantire un controllo di protezione tra la propria rete e quella esterna.

Il capitolo 4 riguarda l'implementazione di un sistema di autenticazione sms autonomo attorno al *Captive Portal*, ne illustra il funzionamento e la personalizzazione.

Il 5° capitolo prevede l'utilizzo ed il *set-up* di diversi strumenti disponibili in pfSense per un migliore funzionamento e controllo, i quali una volta completati, vanno a comporre il "pacchetto" *hotspot.*

Per l'argomentazione del tema trattato, sono state effettuate svariate prove in laboratorio e su *Virtual Machine*. E' stata appositamente realizzata una macchina fisica per verificarne il reale funzionamento ed i carichi di lavoro. Le caratteristiche verranno riportate dettagliatamente in seguito.

Abstract

Electronic calculators are becoming more and more important tools in human life both for work and pastimes.

Many activities depend on computers and so we are forced to access the internet wherever we are and at any time. The sale of tablets, laptop computers and smartphones allows everybody to do that. In recent times the development of wireless technologies together with the bandwidth has given birth to a new concept of connectivity :Hotspots. These resources enable WiFi system provided users to access the internet legally and safely when near these spaces. The recent Italian provisions dated 1st January 2011 in matter of Wi Fi deregulation in Italy give hope for a positive solution. The previous bindings of the ill-famous "Pacchetto Pisanu" introduced in 2005 to oppose internet terrorism, have not allowed a quick spreading of the net on our national territory because of its restrictive conditions.

However, providing an easy, controlled,approachable,independent, low cost and law-respectful service is the priority of those who place their connection at someone's disposal, such as bars,restaurants, airports, hotels etc. That's why the authentication by means of a SIM card will do the trick.

The aim of this thesis is to provide a package of standalone system for a free entirely-tailored sharing of the internet with the utmost respect for the principles of data processing security. The integration of a gateway sms in the captive portal is a solution combining ease and functional capacity while respecting the identification rules for users.

The software making up this thesis is completely open source and free of licence-fee. The part of the code I planned and carried out during my experience has been proposed to the community of the distribution I made use of; I deemed it right that as I was able to benefit from other people's work, so the others can take advantage of my own job according to the principle of free software.

Definitely the coexistence of several users requires precautionary measures against net traps implying a protection of your personal internal net and your own data. It is essential to guarantee the wholeness and secrecy of someone's information, quite often broken into by ill-intentioned users of the internet.

From this derives the commitment to keep your own net safe and efficient as much as possible by the set up of additional tools such as :

- a proxy intended to filter the viral elements by means of the coupling havp+clamav;
- another proxy server squid for access controls and traffic management;
- a controller on the resolution of non-appropriate DNS;
- a NTP service for the timing system synchronization;
- a DHCP server for the LAN;
- the Captive Portal system for users' management and a procedure I carried out in order to register all the hotpot users by means of SMS;

Structure of the thesis The thesis consists of 5 chapters.

Chapter 1 deals with the concept of security in informatics.

Chapter 2 is an analysis related to the juridical aspect of the accomplished infrastructure.

Chapter3 is devoted to the importance of having a firewell on the net as to sum up its main technologies and able to guarantee a protection control between your own net and the external one.

Chapter 4 deals with the implementation of an independent SMS authentication system around the Captive Portal, showing its working and its tailoring.

Chapter 5 implies the use and set-up of different devices available in pfSense for a better functioning and control; once they are completed they make up the hotspot package.

As far as the subject dealt with, several tests have been carried out both in laboratory and Virtual Machine. A special phisical machine has been accomplish to test the real operation and working load. The most outstanding features will be dealt with in detail later on.

Capitolo 1

Panoramica sulla sicurezza informatica

1.1 Il concetto di sicurezza

In un mondo in continua evoluzione quale quello della comunicazione digitale che presenta costi sempre più bassi di interconnessione, il concetto di sicurezza sta assumendo un ruolo sempre più importante, fino a diventare un requisito fondamentale per ogni software, sistema, rete semplice o complessa. Difatti, ogni comunicazione che attraversa internet o in generale una qualsiasi rete geografica, può toccare diversi nodi della rete stessa, dando quindi ad altri utenti l'opportunità di tracciare, intercettare o modificare i dati in transito.

Dobbiamo essere al corrente che tutto ciò che inviamo sulla rete internet non ha segretezza assoluta. Un'altra problematica fondamentale consiste nell'evitare accessi non autorizzati alla propria rete da parte di malintenzionati in grado di copiare, distruggere o modificare dati sensibili. Un ipotetico attaccante potrebbe compromettere la sicurezza di una rete utilizzando diverse metodologie oramai note.

La sicurezza di una rete è come la resistenza meccanica di una catena: corrisponde esattamente alla forza sopportata dall'anello più debole. Quando l'anello più debole viene rotto, il sistema può ritenersi in stato di *fail.* Ecco perché è necessario curare tutti gli aspetti, anche quelli più marginali. Prendere il controllo di un host sfruttando un *bug* di qualche servizio che gira su tale macchina, non sono tecniche da fantascienza, anzi, sono sempre più disponibili ad un numero maggiore di internauti.

In questo caso gioca un ruolo fondamentale la possibilità di effettuare gli *update* del software, infatti è buona norma mantenere installata l'ultima versione dei software in uso. Questo importante servizio, oltre alla possibilità di fornire nuove funzionalità al sistema, permette di correggere le eventuali falle del software successivamente rilevate dopo il rilascio. Si dice infatti che il testing può indicare la presenza di errori, ma non ne può garantire l'assenza.

Altro efficace metodo di protezione contro eventuali minacce, rimane la possibilità di trasmettere dati con un protocollo di criptazione per evitare che qualcuno nel percorso di comunicazione, si possa impossessare dei pacchetti che viaggiano verso destinazione. Successivamente, infatti, si potrebbe esplorare il traffico attraverso la tecnica del *packet sniffing* con un analizzatore di rete(cercando cioè di intercettare il più alto numero possibile di pacchetti che transitano sul mezzo fisico) e successivamente utilizzare macchine compromesse per attacchi a terzi per saturare il servizio sulla macchina vittima.

Con il crescere di internet, crescono anche la diffusione e lo sviluppo di nuove forme offensive quali virus, cavalli di troia, malware, exploit che vanno a mirare attività di interesse sempre piu comune quali *home banking* e carte di credito. Per queste categorie, la tendenza è far ricadere l'utente in un imbroglio. La cosi detta tecnica di *phishing* mira proprio a questo; dove non arriva il mezzo informatico può arrivare l'ingegneria sociale applicata al soggetto. Per questo tipo di attacchi sostanzialmente la parola d'ordine è una sola: diffidare.

La sicurezza informatica non è mai assoluta; per quanto ci si possa impegnare a considerare ogni aspetto, anche superfluo, non si raggiungerà mai la certezza dell'inviolabilità. Ogni dispositivo informatico connesso in rete ed avviato può essere soggetto a violazione del sistema.

La scelta dell' *OS* sulla macchina server che fornirà i servizi *hotspot,* è di fondamentale importanza; un sistema operativo solido e modulare è requisito indispensabile per una macchina che ipoteticamente è raggiungibile da chiunque.

L'installazione di un buon firewall, per questo tipo di applicazione, è basilare. Un firewall inserito nel punto di passaggio fra le due reti, quella interna e quella esterna, controlla i pacchetti che arrivano dall'esterno verso l'interno e viceversa e decide, in base a regole impostate dall'amministratore, quali pacchetti accettare e quali far cadere. Alcuni servizi di rete vengono limitati ed alcune porte non sono rese disponibili. Questo riduce il rischio di attacchi dall'esterno.

Solitamente è consigliabile mantenere un buon livello di sicurezza anche tramite stumenti quali: *antivirus, proxy, backup, IDS, IPS* e mantenere in esecuzione solo i processi necessari per i servizi da fornire.

In relazione alle questioni sopra analizzate, si può affermare che l'uso di una distribuzione firewall dedicata come pfSense è risultato estremamente vantaggioso grazie alla facilità gestionale, alla sua efficacia ed alla sicurezza che implementa.

Capitolo 2

Diritto e nuove tecnologie

La normativa italiana vigente in materia di connessione a Internet in ambiti aperti al pubblico si è orientata per diversi anni verso la regolamentazione dei mezzi attraverso i quali il collegamento viene veicolato. In particolare, diverse sono state le norme che hanno interessato in questi anni le reti wireless.

Fino al 2001 il riferimento legislativo per l'utilizzo delle apparecchiature operanti nelle bande di frequenza utilizzate per la trasmissione wireless LAN era dato dal DPR 447 del 5 Ottobre 2001. Il decreto stabiliva che tali frequenze potessero essere impiegate solo nell'ambito di LAN ad uso privato, mentre per connettere una WLAN alla rete pubblica occorreva un'autorizzazione generale del Ministero nonché il pagamento di un canone.

A partire dal gennaio 2002, il regolamento di attuazione dello stesso DPR 447 del 5 Ottobre 2001 consente l'utilizzo di dispositivi di rete wireless operanti sulle bande di frequenza appositamente assegnate senza più la necessità di richiedere alcuna concessione.

Il quadro regolamentare definitivo per l'utilizzo della tecnologia Wi-Fi in ambito pubblico è dato però dal cosiddetto decreto Gasparri del 28 Maggio 2003, che regola le condizioni per il rilascio delle autorizzazioni generali per la fornitura al pubblico dell'accesso Radio-LAN alle reti ed ai servizi di telecomunicazioni.

Sul tema degli accessi in ambiti aperti al pubblico una delibera dell'Autorità per le Garanzie nelle Comunicazioni (num. 102/03/CONS) precisa che non è necessario disporre di licenza o autorizzazione per l'erogazione di servizi di connettività di rete nel caso in cui l'attività commerciale non abbia come oggetto sociale principale l'attività di telecomunicazioni (es. bar, alberghi, centri commerciali contrapposti a Internet-point).

A limitare in misura minore la tendenza verso la liberalizzazione totale del servizio è recentemente intervenuto il Decreto "Misure urgenti per il contrasto del terrorismo internazionale", noto come decreto Pisanu, del 27 luglio 2005, con il quale alcune delle norme citate precedentemente sono state variate.

L'articolo 7 del Decreto, infatti, modifica la delibera dell'Autorità per le Garanzie nelle Comunicazioni (num. 102/03/CONS) precedentemente citata, indicando che è necessario dare comunicazione alla Questura qualora si mettano a disposizione del pubblico terminali telematici. In particolare, un'autorizzazione va richiesta solo per chi fa della fornitura di accesso Internet al pubblico la propria attività prevalente o esclusiva (ad esempio gli Internet point) o per chi ha più di tre terminali installati e destinati all'accesso pubblico alla Rete. La nuova norma prevede inoltre la "preventiva acquisizione di dati anagrafici riportati su un documento di identità dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili".

Il software di gestione di un *hotspot* deve sempre rispettare tutte le misure necessarie a fare in modo che i suoi sistemi rispettino in pieno le normative che si susseguono nel corso del tempo, al punto di aver anticipato anche le ultime variazioni intervenute sul tema dell'identificazione personale della clientela.

Tutte le infrastrutture di rete pubbliche devono essere, pertanto, pienamente compatibili con la legislazione vigente.

Successivamente riportiamo la normativa tutt'ora da seguire divisa per tematiche.

2.1 Il principio della "solidarietà sociale"

Art. 2 Costituzione espressamente tratta della Solidarietà politica, economica e sociale:

2.- *La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale.*

Gli stessi articoli di rinvio contenuti nell'art. 2 (artt. 41 e 42 Cost.) a loro volta ribadiscono il concetto.

21. — *Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione.*

33. — *L'arte e la scienza sono libere e libero ne è l'insegnamento.*

Gli articoli 41 e 42 Cost. sono complementari sull'iniziativa economica e la proprietà siano esse pubbliche o private.

41. — *L'iniziativa economica privata è libera. Non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana. La legge determina i programmi e i controlli opportuni perché l'attività economica pubblica e privata possa essere indirizzata e coordinata a fini sociali.*

42. — *La proprietà è pubblica o privata. I beni economici appartengono allo Stato, ad enti o a privati. La proprietà privata è riconosciuta e garantita dalla legge, che ne determina i modi di acquisto, di godimento e i limiti allo scopo di assicurarne la funzione sociale e di renderla accessibile a tutti. La proprietà privata può essere, nei casi preveduti dalla legge, e salvo indennizzo, espropriata per motivi di interesse generale.*

2.2 Condotta e regole

Alcuni comportamenti scorretti come usare un computer per danneggiare altre persone, interferire con il lavoro al computer di altre persone, curiosare nei file di altre persone, usare un computer per rubare, usare un computer per portare falsa testimonianza, utilizzare o copiare software che non è stato dovutamente pagato, usare le risorse di altri senza autorizzazione, appropriarsi del risultato del lavoro intellettuale altrui,sono regolamentati da articoli specifici:

- Legge sul diritto d'autore 633 (l. n. 633 del 1941);
- Legge a tutela del software 518 (d. lgs. N. 518 del 1992);
- Legge sulla privacy 196 (d. lgs. 196/2003);
- Legge sullo spamming 675 e 171(art. 29 legge n. 675/1996) e d.lg. 171 del 13/05/1998);
- Legge sulle banche dati 169 (Dlgs n. 169 del 1999);
- Legge sul commercio elettronico 70 (d. lgs n. 70 del 2003);

Ripensando ad alcune situazioni reali, non è difficile incombere in uno di questi reati ed è più facile di quello che si pensi.

Basta pensare a tutte le volte che un utente utilizza un software proprietario di cui non è stata acquistata una regolare licenza; la pubblicazione di una foto/video senza il consenso delle persone raffigurate sul web (comunissimo sui *social network*); informazioni trovate in rete e riutilizzate senza consenso o protette da *copyright;* pubblicizzazione di messaggi indesiderati in grande quantità per la vendita di un prodotto; e molte altre ancora.

Per cui, la persona che ricopre il ruolo dell'addetto informatico, deve considerare 2 aspetti principali: il *controllo* sicuro sui dati e l'*accesso* sicuro agli stessi.

Per controllo sicuro si intende la non possibilità di alterazione dei dati da parte di chiunque non sia autorizzato o a causa di eventi casuali.

Per accesso sicuro si garantisce la disponibilità all'utente della rete, delle informazioni, dell'accesso alle stesse e della fruizione corretta dei servizi di rete secondo le modalità ed i tempi previsti.

A completare questi 2 argomenti introduciamo altri concetti più specifici per la rete Internet:

- Riservatezza, intesa come protezione dei dati trasmessi attraverso la loro inaccessibilità a soggetti non autorizzati corrispondenti ad una identità (previa autenticazione);
- Integrità, intesa come protezione dei dati trasmessi attraverso la loro intoccabilità (senza possibilità di modifica) da parte di soggetti non autorizzati;
- Disponibilità, intesa come possibilità che i dati o i servizi di rete siano accessibili ed utilizzabili da parte degli utenti autorizzati;

2.3 Articoli in dettaglio

2.3.1 Frode Informatica

La violazione della normativa legata alla tecnologia da parte di individui può ricadere nel reato di *Frode Informatica* 640 (Art. 640 ter c.p.)

Art. 640 ter c.p.

"[1] Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da cinquantuno euro a milletrentadue euro.

[2] La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila (309.87€) a tre milioni (1549.37€) se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

[3] Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante."

Articolo aggiunto dall'art. 10, l. 23.12.1993, n. 547.I

2.3.2 Accesso abusivo ad un sistema informatico o telematico

In questo caso si fa riferimento all' Art. 615 ter.

615 Art. 615 ter.

Accesso abusivo ad un sistema informatico o telematico1

[1] Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

[2] La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesamente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

[3] Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica

o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. (omissis ...)

Articolo aggiunto dalla l. n. 547 del 1993

Inoltre, la sentenza della Corte di Cassazione (V Penale) del 6 dicembre 2001 afferma che non è importante il concetto di domicilio fisico in quanto ciò che conta è l'intento del gestore del sistema di ESCLUDERE soggetti non autorizzati ad entrare.

Risulta interessante trattare le condizioni in cui un individuo accede alla struttura informatica e non provoca danni o si giustifica col fatto che non erano state prese misure di sicurezza per l'accesso. In queste casistiche si ricade ugualmente nell' Art. 615 ter.

L'utilizzo di comandi di sistema come *ping* e *trace*route, infatti, può essere ugualmente finalizzato alla esecuzione di operazioni di manutenzione come alla preparazione di un assalto, e quindi essere considerato condotta propedeutica. La linea di confine diviene ancora più precaria con l'uso di programmi di *port scanning* che conducono a considerare come fine un attacco informatico.

2.3.3 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Proseguendo con l' Art. 615 quater 615 quater si ha che

[1] Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro cinquemilacentosessantaquattro.

[2] La pena è della reclusione da uno a due anni e della multa da euro cinquemilacentosessantaquattro a diecimilatrecentoventinove se ricorre taluna delle circostanze di cui ai numeri 1 e 2 del quarto comma dell'articolo 617 quater.

Viene considerata condotta incriminante quando il soggetto acquisisce codici di accesso, (parole chiave o altri mezzi utili per l'accesso), li procura ad altri o li diffonde pubblicamente.

2.4 Terrorismo internazionale e legge Pisanu

2.4.1 Perché viene introdotta

Nel 31 luglio 2005 il Parlamento italiano approva quasi ad unanimità una nuova legge in materia di "lotta al terrorismo internazionale". Il pretesto per questa operazione è stata la strage del 7 luglio 2005 a Londra, come precedentemente era avvenuto per le altre leggi sulla materia a seguito degli attentati dell'11 settembre 2001 a New York e dell'11 marzo 2004 a Madrid. La situazione internazionale ha influenzato così notevolmente la volontà di introdurre nuove leggi in materia di terrorismo, che il decreto legge del 22 luglio 2005, n.144, viene convertito in legge come 31 luglio 2005, n.155 155. ll primo dato, indiscutibile, è l'estensione dei poteri di intervento autonomo, anche precautelare, delle forze di polizia e l'inasprimento di norme già vigenti. Il secondo dato è l'introduzione di nuove forma di illegalità telematiche. Alcune di queste sono riservate a titolari o gestori di un esercizio pubblico o di un circolo privato di qualsiasi specie nel quale sono posti a disposizione del pubblico apparecchi terminali utilizzabili per le comunicazioni, anche telematiche conosciuti come *hotspot*. Rientrano in questo insieme attività come internet-cafè, alberghi, ristoranti, aereoporti, biblioteche, ospedali, università ecc. Con l'introduzione del "Pacchetto Pisanu" le precedenti attività sono costrette a mettersi in regola garantendo di:

- Acquisire preventivamente i dati anagrafici riportati su un documento di identità dei soggetti che andranno ad utilizzare postazioni pubbliche non vigilate per comunicazioni telematiche;
- Monitorare le operazioni dell'utente sulla rete;
- Archiviare i relativi dati mantenendoli per un anno;

Questo per garantire che gli utenti siano identificati, che si possa poter risalire a chi ha fatto cosa e che i dati di log siano conservati in sicurezza ed a disposizione delle autorità competenti.

Non esiste in nessun altro stato del mondo una normativa come il Decreto Pisanu.

2.4.2 Cosa impone la normativa

Informaticamente parlando nascono dei dubbi sulle tecniche con cui si possa monitorare il traffico e su cosa effettivamente "loggare". La normativa impone che siano conservati data e ora della comunicazione, "con chi" l'utente dell'*internet point* ha comunicato ed in che modalità. Più in dettaglio, la Direttiva 2002/58/CE, definisce i dati relativi al traffico come:

"i dati concernenti l'instradamento, la durata, il tempo o il volume di una comunicazione, il protocollo usato, l'ubicazione dell'apparecchio terminale di chi invia o riceve, la rete sulla quale la comunicazione si origina o termina,nonché i dati inerenti l'inizio, la fine o la durata di un collegamento".

Sulla base di questa specifica quindi i dati da mantenere sono:

- Data e ora di connessione;
- Data e ora di disconnessione;
- Il protocollo di rete usato per la comunicazione;
- La posizione del dispositivo che comunica in rete;
- Gli *IP address*(sorgente e destinazione) con cui è stata inizializzata la connessione;
- La porta(sorgente e destinazione) su cui è stato trasmesso il dato;

Per i log di archiviazione, bisogna prendere le giuste precauzioni perchè si stanno trattando dei dati sensibili che potrebbero essere richiesti in qualsiasi momento.

Nonostante la necessità di sicurezza il decreto Pisanu ha contribuito negativamente alla diffusione dei collegamenti rendendone troppo macchinosa la burocrazia.

2.5 Legge sulla privacy

In presenza di dati sensibili vanno garantiti i vincoli della legge sulla privacy.

Nel nostro caso,per usufruire di un servizio hotspot bisogna accettare delle condizioni che permettono l'elaborazione dei dati personali. In primo luogo :

- L'utente è tenuto a leggere e prendere atto dell'informativa del servizio 196 (art. 13 d.lgs 196/2003);
- L'utente è tenuto a consentire la stessa;[1]
- Il gestore è tenuto a conservare ed a garantire la sicurezza dei dati; si impegna cioè, ad attuare le misure minime di sicurezza e del modello DPS (artt. 33 e 34 d. e 132 dlgs. 196 del 2003 ed allegato per Dps);

Deve figurare un responsabile, che può coincidere con il titolare dell'impresa, a cui fa riferimento la persona giuridica. A sua volta,possono esserci delle persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Per misure minime di sicurezza si intendono quelle previste dal Disciplinare tecnico (Allegato B del Codice sulla privacy - Codice articoli 31-36 del Codice della privacy, spec. Artt. 33 Misure Minime di sicurezza - e 34 -DPS-) con particolare attenzione a quelle misure che riducono al minimo i rischi di distruzione o perdita, intercettazione e manipolazione dei dati personali.(art. 31 seconda parte Codice privacy).

[1] Il consenso non è necessario perché c'è un obbligo di legge che dice: se il soggetto si rifiuta di fornire il consenso ,il gestore può negare il servizio.

2.5.1 Documento di Programmazione della Sicurezza (DPS)

Il Documento Programmatico per la Sicurezza DPS è una "misura minima" prevista dalla legge e si traduce in un rapporto di analisi contenente la distribuzione dei compiti, l'analisi dei rischi sul trattamento dei dati e la documentazione di alcune soluzioni adottate. Garantisce la disponibilità, l'integrità, l'autenticità e la riservatezza dell'informazione e dei servizi per il trattamento. Prevede l'attribuzione di specifici incarichi, la certificazione delle fonti di provenienza dei dati e la previsione di istruzioni per le persone autorizzate ad effettuare i trattamenti.

Più specificatamente, le misure che debbono essere adottate devono riguardare determinate attività informatiche:

- Fase di autenticazione;
- Fase delle copie di Sicurezza;
- Fase della Protezione da accessi indesiderati (Internet);
- Fase della Protezione da programmi non autorizzati(Virus, Malware...);
- Fase dell'Aggiornamento Tecnologico;

Per la fase di autenticazione, l'adozione di un sistema con *Captive Portal* risulta perfettamente idoneo perché l'accesso è consentito con credenziali individuali(*username* e *password*) ed in maniera non concorrenziale(solo un utente per credenziali).

Per la fase di sicurezza è prevista la pianificazione di copie di backup (consigliata) a cadenza settimanale, per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

Per la fase di Protezione da accessi indesiderati, c'è obbligo di attivazione di programmi che permettano di difendersi da intrusioni provenineti dalla Rete. Nel nostro caso l'uso di un *firewall* quale PF (*Packet Filter*) è previsto nella distibuzione pfSense.

Per la fase della Protezione da programmi non autorizzati è previsto l'obbligo di attivazione di un sistema di rilevamento virale. L'uso di ClamAV come *package* di pfSense si rivela utile.

Per la fase d' Aggiornamento Tecnologico c'è l'obbligo di aggiornamento periodico dei programmi (compresi quelli antivirus; per questi ogni 6 mesi).

2.5.2 I documenti

Il garante della protezione dei dati personali distribuisce un Fac-simile da compilare ed una guida su cui creare il Documento Programmatico sulla Sicurezza. Questi strumenti permettono di snellire molto la burocrazia e di essere nel rispetto della legge.

Guida operativa per redigere il Documento programmatico sulla sicurezza - 11 giugno 2004 Guida

Obblighi di sicurezza e documento programmatico: al 30 giugno la redazione del "dps"- 22 marzo 2004 Obblighi DPR

2.5.3 Cosa si rischia

La responsabilità è diversa a seconda delle misure di sicurezza violate:

- Minime: Sono quelle misure che rispettano i parametri di sicurezza minimi individuati nel Codice (articoli 33, 34, 35 e 36 ed Allegato B);
- Idonee: Sono le misure che vanno "oltre" la previsione del Codice. "Tutte quelle misure" in grado di evitare il danno;

Per le violazioni minime la responsabilità è penale e per il reato è prevista la pena.

Per le violazioni idonee la responsabilità è civile ed il reato è punibile con un risarcimento del danno.

Sansioni penali: "Omissione di adozione delle misure minime di sicurezza"; Responsabilità penale RN: 169 Codice della privacy Reclusione fino a 2 anni o ammenda 10.000/50.000euro.[2]

Sansioni civili: "Omissione di adozione delle misure idonee di sicurezza"; Responsabilità civile RN: art. 15 Codice privacy = 2050 C.C. = Responsabilità prevista per le attività pericolose.

[2]N.B.: viene concesso un termine entro il quale è possibile regolarizzare la propria posizione. L'adeguamento estingue il reato.

2.6 Decreto "Milleproroghe"

Negli ultimi mesi del 2010 c'è interesse di cambiare la pesante normativa con lo scopo di abrogare la legge Pisanu. Viene introdotto un pacchetto sicurezza messo a punto dal ministro dell'Interno composto da un decreto legge (che contiene le modifiche all'articolo 7) e da un disegno di legge. Il disegno di legge presentato dal governo non parla di liberalizzazione del Wi-Fi, perché nel disegno si dispone anche che resteranno alcuni obblighi a tutela della sicurezza pubblica. E' interesse nazionale limitare le restrizioni introdotte cinque anni fa e che oggi sono superate dall'evoluzione tecnologica.

Dal 1° gennaio 2011 il Wi-Fi e le connessioni pubbliche in generale in Italia non saranno più soggette ai vincoli impostati dalla legge Pisanu del 2005 ma non senza alcun controllo. Milleproroghe 2011

- Al comma 1 dell'articolo 7, le parole: «fino al 31 dicembre 2010, chiunque» sono sostituite dalle seguenti: «fino al 31 dicembre 2011, chiunque, quale attività principale»
- I comma 4 e 5 sono abrogati.

2.6.1 Articolo 7

Integrazione della disciplina amministrativa degli esercizi pubblici di telefonia e internet.

1. A decorrere dal quindicesimo giorno successivo alla data di entrata in vigore della legge di conversione del presente decreto e fino al 31 dicembre 2011, chiunque, quale attività principale intende aprire un pubblico esercizio o un circolo privato di qualsiasi specie, nel quale sono posti a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni anche telematiche, deve chiederne la licenza al questore. La licenza non è richiesta nel caso di sola installazione di telefoni pubblici a pagamento, abilitati esclusivamente alla telefonia vocale.

2. Per coloro che già esercitano le attività di cui al comma 1, la licenza deve essere richiesta entro sessanta giorni dalla data di entrata in vigore del presente decreto.

3. La licenza si intende rilasciata trascorsi sessanta giorni dall'inoltro della domanda. Si applicano in quanto compatibili le disposizioni dei capi III e IV del titolo I e del capo II del titolo III del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773, nonché le disposizioni vigenti in materia di sorvegliabilità dei locali adibiti a pubblici esercizi. Restano ferme le disposizioni di cui al decreto legislativo 1° agosto 2003, n. 259, nonché le attribuzioni degli enti locali in materia.

4. [Con decreto del Ministro dell'interno, di concerto con il Ministro delle comunicazioni e con il Ministro per l'innovazione e le tecnologie, sentito il Garante per la protezione dei dati personali, da adottarsi entro quindici giorni dalla data di entrata in vigore della legge di conversione del presente decreto, sono stabilite le misure che il titolare o il gestore di un esercizio in cui si svolgono le attività di cui al comma 1 è tenuto ad osservare per il monitoraggio delle operazioni dell'utente e per l'archiviazione dei relativi dati, anche in deroga a quanto previsto dal comma 1 dell'articolo 122 e dal comma 3 dell'articolo 123 del decreto legislativo 30 giugno 2003, n. 196, nonché le misure di preventiva acquisizione di dati anagrafici riportati su un documento di identità dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili].

5. [Fatte salve le modalità di accesso ai dati previste dal codice di procedura penale e dal decreto legislativo 30 giugno 2003, n. 196, il controllo sull'osservanza del decreto di cui al comma 4 e l'accesso ai relativi dati sono effettuati dall'organo del Ministero dell'interno preposto ai servizi di polizia postale e delle comunicazioni].

Pertanto:

- Il requisito della "attività principale" aggiunto dal comma 19, infatti, fa si che tutti coloro che offrono connettività in via accessoria(come bar, ristoranti, ecc), possano ritenersi esclusi dalla richiesta di autorizzazione alla questura;
- L'obbligo di identificare gli utenti cade, invece, per entrambe le categorie, in quanto il comma 19 abroga espressamente i commi 4 e 5 dell'Art. 7 dove l'obbligo era previsto;
- Non c'è più obbligo di monitorare e conservare i dati relativi all'utente in capo al gestore, ma resta l'obbligo di proteggere la rete da intrusioni abusive e mantenere le misure minime di sicurezza;
- Con la liberalizzazione del WiFi non si intende l'accesso gratuito alla rete perché la gratuità o il pagamento del segnale dipendono dal soggetto o l'ente che lo mette a disposizione;
- Un possibile metodo per l'identificazione personale è la registrazione tramite messaggio SMS. In questo modo non è necessario fornire un documento d'identità perchè l'intestatario della scheda SIM registrata sarà la persona a cui fare riferimento;

Di seguito sono illustrate le differenze sostanziali tra il vecchio decreto Pisanu oramai abrogato e, dopo le modifiche del decreto "Milleproroghe", la attuale normativa vigente:

	pre 31/12/2010	post 1/01/2011
Per aprire un Internet Point	Necessità di licenza al questore, log del traffico e identificazione	Necessità di licenza al questore, log del traffico
WiFi per client di Bar, Ristoranti, Alberghi...	Licenza, fotocopia documento, log, obblighi conseguenti	Autorizz. generale, no fotocopia doc. no log, obblighi conseguenti
Condividere la propria linea ADSL	Vedi condizioni contratto consumer ADSL	Vedi condizioni contratto consumer ADSL
Il Wi-Fi sarà gratuito	La gratuità o il pagamento del segnale dipendono dal soggetto o dall'ente che lo mette a disposizione	La gratuità o il pagamento del segnale dipendono dal soggetto o dall'ente che lo mette a disposizione
Identificare gli utenti	Tramite carta d'identità	Tramite sms (ad esempio)

Tabella 2.1: Confronto tra vecchia e nuova normativa WiFi

2.6.2 Se un privato vuole condividere la propria linea con altri ?

Secondo il nuovo decreto, solo ai soggetti che hanno come attività primaria la messa a disposizione del pubblico di risorse di connettività è richiesta la licenza. Il ristorante/bar/lavanderia a gettoni/albergo che mette a disposizione un Access Point deve tuttavia tenere conto degli obblighi imposti agli operatori di telecomunicazioni, fra i quali la richiesta di autorizzazione generale al ministero e relative misurazioni e comunicazioni annuali da mandare all'AGCOM. L'alternativa è affidarsi a un operatore che eroga il servizio e si fa quindi carico di questi obblighi.

Discorso a parte merita l'ambiente *consumer*. Infatti, alla base del proprio servizio di accesso e fruizione di utenza ci sarà un contratto *flat ADSL* di connettività Internet. Solitamente questo contratto non lo consente, ma è necessario andare a vedere il contratto stipulato con l'ISP.

Capitolo 3

Firewall e Rete

3.1 Il firewall

Per difendere e controllare la propria rete è necessario un componente passivo che svolga funzioni di collegamento e filtraggio tra due o più segmenti di rete. Per la nostra infrastruttura la prerogativa fondamentale consiste nel decidere la politica di sicurezza da adottare prima della realizzazione fisica della rete. È di fondamentale importanza che l'amministratore sappia con assoluta precisione quali e quanti servizi offrire dall'interno all'esterno attraverso la propria rete, quali privilegi concedere agli utilizzatori dei terminali interni e come strutturare la rete stessa. Un sistema di protezione quale un firewall risulta complesso da configurare partendo da zero e richiede delle conoscenze tecniche che riguardano la struttura interna ed il funzionamento della rete, la conoscenza dei protocolli ed i meccanismi di comunicazione tra le diverse tipologie di reti.

Il *firewall* agisce sui pacchetti in transito da e per la zona interna potendo eseguire su di essi operazioni di:

- controllo;
- modifica;
- monitoraggio;

Data Unit	Layers	#	Description
data	Application	7	Network Process to Application
data	Presentation	6	Data Representation & Encryption
data	Session	5	Interhost Communication
segments	Transport	4	End-to-End Connections & Reliability
packets	Network	3	Path Determination & Logical Addressing (IP)
frames	Data link	2	Physical Addressing (MAC & LLC)
bits	Physical	1	Media, Signal & Binary Transmission

Tabella 3.1: Modello ISO/OSI

Il firewall più comune è il *packet filter*, che si limita ad "aprire" il pacchetto IP per leggere le informazioni presenti sul suo *header*, decidendo quali far passare e quali no sulla base delle regole configurate. Per *header* si intende la parte di pacchetto a livello network che contiene informazioni di controllo necessarie al funzionamento della rete.

I firewall di tipo *deep inspection* effettuano controlli fino al livello 7 della pila ISO/OSI, ovvero valutano anche il contenuto applicativo dei pacchetti, ad esempio riconoscendo e bloccando i dati appartenenti a virus o worm noti in una sessione HTTP o SMTP.

3.1.1 La struttura di rete

Un *firewall* in genere è composto da un computer che si pone tra le reti private e quelle esterne con lo scopo di controllare ciò che transita da una rete verso l'altra e viceversa. Usualmente la rete viene divisa in due sottoreti: una esterna detta WAN (*Wide Area Network*), comprende l'intera Internet mentre l'altra interna, detta LAN (*Local Area Network*), comprende una sezione più o meno grande di un insieme di computer locali. In alcuni casi è possibile che si crei l'esigenza di creare una terza sottorete detta DMZ (o zona demilitarizzata) adatta a contenere quei sistemi che devono essere isolati dalla rete interna ma devono comunque essere protetti dal *firewall*. Per come è realizzata la nostra struttura non utilizzeremo questo tipo di sottorete.

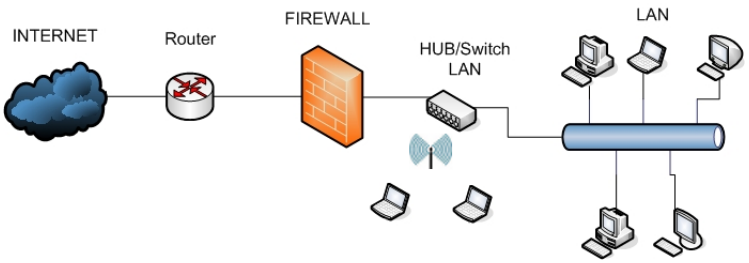


Figura 3.1: Esempio di rete con firewall

Un *firewall* può essere realizzato con un normale computer (con almeno due schede di rete e software apposito), può essere una funzione inclusa in un *router* o può essere un apparato specializzato. Come è possibile notare la figura in arancione è la macchina *firewall*. La macchina in questione è adibita principalmente al ruolo di *gateway* e *firewall* per gli utenti della LAN ed è infatti posta tra la rete interna e quella esterna. La LAN è composta da un numero arbitrario di host ed il traffico è smistato da un semplice switch con funzionalità WiFi. Questa ultima caratteristica fornisce la connettività alla rete senza fili. I computer della LAN interna non hanno particolari configurazioni. Sono dispositivi generici sui quali è installato un sistema operativo.

I due adattatori di rete sono stati configurati nel seguente modo:
L'interfaccia sulla LAN con:

- Indirizzo IP 192.168.0.1
- Maschera di Rete 255.255.255.0

L'interfaccia sulla WAN con:

- Indirizzo IP 193.205.92.225
- Maschera di Rete 255.255.255.0
- Indirizzo Gateway 193.205.92.2
- Server DNS 193.205.92.70
- Server DNS alternativo 193.205.92.1

L'interfaccia dell'access point con:

- 192.168.0.50
- Maschera di Rete 255.255.255.0

La connessione ad internet avviene tramite la rete Unicam e l'interfaccia WAN, sulla quale è abilitato l'assegnamento automatico dal server DHCP all'interno del dipartimento di informatica. Ogni macchina dall'interno del dipartimento "esce" in internet con un IP pubblico assegnatogli. A fini pratici, per usufruire del servizio gateway sms, ho avuto la necessità di ottenere sempre lo stesso IP *address* dal DHCP. Per ovviare al problema, l'amministratore di rete del dipartimento mi ha gentilmente impostato una regola di *reservation IP* in modo tale che ad ogni richiesta DHCP con MAC *address* della scheda WAN, corrisponda sempre lo stesso indirizzo IP.

Per la rete interna, il server ha un indirizzo fisso 192.168.0.1 ed a tutti i restanti *host* viene assegnato un indirizzo IP dal server DHCP del *firewall*. Il servizio di NAT (*Network Address Translation*) è abilitato di *default* per la rete LAN quindi le connessioni generate dall'insieme di host vengono "presentate" verso l'esterno con un solo indirizzo IP. Questo comporta un risparmio sulla linea (perché è necessario un solo IP pubblico) ed una condizione in sicurezza rendendo i calcolatori non direttamente raggiungibili da internet. Per i client della LAN, la macchina *firewall* fa anche da server DNS (*Domain Name System*) occupandosi della risoluzione nome-indirizzo.

3.1.2 Test di laboratorio

Per i test in laboratorio è bastato l'utilizzo di una macchina fisica ragionevolmente datata ma che si è dimostrata capace di gestire il sistema. Generalmente, infatti, una macchina per gestire un *hotspot* non necessita di potenze di calcolo particolarmente elevate, a patto che non debba trattare un numero elevato di utenti. La pratica di recuperare vecchio hardware, mettendo insieme anche pezzi di computer diversi e rendendoli di nuovo funzionanti è denominata *trashware*. Parte integrante del trashware è l'installazione di software libero, ad esempio i sistemi operativi GNU/Linux o BSD, che contribuiscono a portare avanti lo spirito di libertà dell'iniziativa.

Ad inizio test, la memoria installata sulla macchina era di 256MB di ram; tuttavia questo quantitativo è stato poi incrementato ad 1GB con l'aggiunta di servizi più onerosi in termini di risorse quali il *proxy* server e l'IDS.

Di seguito è riportato un elenco delle principali caratteristiche hardware:

- Processore pentium 4
- Ram 1GB DDR 400MHz
- HD 20GB 5400rpm
- 2 schede PCI Ethernet 10/100Mb
- Lettore CD-ROM 24X

Come OS si è deciso di utilizzare una distribuzione *firewall* dedicata di nome pfSense.

3.2 pfSense

pfSense[2] è un sistema operativo firewall software Open Source nato come *fork* di M0n0wall; ha lo scopo di fornire un potente, sicuro e completamente configurabile *firewall* utilizzando l'hardware di un comune PC. Al cuore del sistema c'è FreeBSD[5] ed il *firewall* PF (*Packet Filter*) in prestito da OpenBSD da cui ne deriva appunto la sigla.

Il sistema prevede un'installazione tramite CD da boot e successivamente può essere configurato tramite interfaccia web. Grazie all'aggiunta di ulteriori moduli è possibile estendere le funzionalità di base ed integrare funzionalità evolute come il web proxy, l'url filtering, l'antivirus/antispam e ulteriori funzioni.

Il progetto nasce nel 2004 da parte di due appassionati di networking di nome Chris Buechler e Scott Ullrich, entrambi statunitensi, partendo come base da M0n0wall il quale risultava troppo limitato come funzionalità. Per concetto M0n0wall è nato per girare su sistemi *embedded* mentre pfSense è più dedicato ad una pc vero e proprio. Allo stato attuale[1] è disponibile come versione stable la 1.2.3 , ed una versione Beta enumerata 2.0; per ragioni di sicurezza ed affidabilità precedentemente citate, è stata utilizzata la versione stabile.

Alla base del sistema pfSense c'è PF (*Packet Filter*), il sistema di filtraggio del traffico TCP/IP e *Network Address Translation* presente di default su OpenBSD. Tra tutti i filtri di pacchetto disponibili nel panorama UNIX, pf viene preferito in primo luogo per le prestazioni ed anche in condizioni di elevato carico, dimostra un buon comportamento senza abuso di risorse.

[1] maggio 2011

3.2.1 Perché usare pfSense

pfSense necessita di requisiti hardware veramente bassi:

- CPU - 100 MHz Pentium
- RAM - 128 MB
- Lettore CD-ROM
- 1GB di spazio libero sull'HD (solo per installazione)
- 512MB di spazio libero su un memoria flash (solo per *embedded*)
- Porta seriale per console (opzionale)

La distribuzione può essere lanciata anche in modalità *live* da CD-ROM, senza intaccare i dati presenti sull'*hard disk* e con la presenza di un dispositivo di archiviazione come un *drive USB* o un disco floppy per mantenere i file di salvataggio.

Come da tradizione UNIX, prestazioni ed affidabilità sono qualità irrinunciabili. Il server web lighthttpd consente di presentare una *WebGUI* in PHP veloce ed intuitiva con finalità di permettere una gestione abbastanza *user friendly* delle attività di rete. Quest'ultima è raggiungibile da qualsiasi *browser web* sia dal lato LAN che WAN(opzionale e non abilitato di *default*) e supporta la gestione tramite HTTPS. Ai fini di salvare agevolmente le impostazioni di sistema, la *WebGUI* genera un unico file XML in cui sono riportati tutti i settaggi al momento del backup.

pfSense è rilasciato sotto licenza BSD a matrice *Open Source* per essere libero e aperto. E' infatti, esente da costi di licenza che lo candida come uno dei *firewall* con il migliore rapporto qualità/prezzo. Utilizzabile anche in ambito commerciale permette a qualsiasi ditta o privato di implementare il proprio sistema. I *firewall* commerciali, solitamente, restano accessibili solo a poche aziende di medie o grandi dimensioni. Su richiesta è disponibile il supporto tecnico a pagamento da parte della comunità che continua a fornire in modo gratuito una completa documentazione composta da tutorials, wiki, forum[4] e IRC.

3.2.2 Funzionalità di sistema

pfSense dispone di innumerevoli servizi in continuo sviluppo:

- *Modulate state*: permette di rigenerare gli ISN (*Initial Sequence Number*) dei pacchetti prodotti dai dispositivi connessi ad internet. Alcune volte questi ultimi (soprattutto gli *embedded*) generano SN non molto casuali ed addirittura sequenziali;

- *SynProxy State*: questa opzione permette al *firewall*, in presenza di attacchi di tipo *Syn Flood* dove si genera una serie di pacchetti falsi (*Syn Spoofing*), di limitare il numero delle connessioni aperte da gestire contemporaneamente. Questa condizione permette al server di non allocare troppe risorse per soddisfare tutte le richieste TCP di *Three-way handshake* perché considera una connessione attiva solo dopo aver ricevuto il segmento *Acknowledgment* dal client;

- Supporto all'*Overload*: permette di inserire l'indirizzo IP di chi non rispetta alcuni limiti preimpostati dall'amministratore come limiti di tempo, limiti di connessione,ecc in una apposita tabella chiamata *abusive host*. Gli indirizzi figurano in questa speciale tabella se superano x connessioni totali o se aprono y connessioni ogni z secondi, dove x, y, e z sono 3 interi scelti a priori. Una volta presenti nell'*abusive host* si può scegliere se non offrire più connessione o se non offrire connessione per un tot tempo a quell'indirizzo sorgente;

- *OS Detection*: è in grado di effettuare un *fingerprinting* passivo che analizza i pacchetti in arrivo ed in base a come sono stati creati cerca di capire quale sistema operativo è in uso sul client. Questa non è una caratteristica che aggiunge sicurezza al sistema ma è comunque apprezzabile riuscire a distinguere i vari OS e poi creare delle specifiche *rules* in base a ciò che che gira sui client;

- *ALTQ*: è un pacchetto per le code di priorità ed implementazione di QoS (*Quality of Service*); ciò permette di gestire le priorità in base alla sorgente, alla destinazione ed al tipo di traffico. Per questo tipo di operazione pfSense ha un *frontend* di facile utilizzo che guida l'utente attraverso alcune pagine PHP; successivamente le scelte vengono tradotte ed inserite come *rules* di *firewalling*;

- *DHCP server*: assegna i parametri di rete ai client che vengono collegati sullo stesso segmento di rete. E' un servizio diffusissimo ed implementato in tutti i router casalinghi per la connessione ad internet. Ovviamente pfSense può svolgere la funzione anche di DHCP client e farsi assegnare da un altro DHCP server i dati di connessione;

- *VPN*: permette di creare *Virtual Private Network*; delle reti private virtuali attraverso internet che mettono in collegamento reti variamente disclocate su ampio territorio. Attualmente supporta IPSEC, OpenVPN e PPTP;

- *VLAN*: dà la possibilità di segmentare la rete; in dettaglio va a dividere il *dominio di broadcast* nelle reti locali. Risulta utile quando si vuole che alcune macchine inserite in una VLAN non siano visibili da altre macchine in un'altra VLAN;

- *Dyn DNS Client*: mantiene aggiornato un *hostname* anche se si ha un IP dinamico, tramite il servizio *DynDNS* o *RFC 2136*. E' quindi possibile risalire all'*host* desiderato utilizzando il nome precedentemente assegnato, anche se il suo IP dinamico è cambiato;

- *Caching DNS forwarder*: può memorizzare le risposte DNS per soddisfare instantaneamente richieste future. Infatti una volta che il server DNS (per esempio quello dell'ISP) ha risolto un indirizzo, il risultato viene memorizzato in una area di *cache* che sarà disponibile a tutti i client di pfSense senza effettuare una nuova risoluzione e senza attese;

- *SNMP*: *Simple Network Management Protocol* è un protocollo a livello applicativo che consente la gestione o la supervisione degli apparati collegati in rete. Crea e fornisce delle statistiche, prendendo informazioni dal sistema quali cpu, carico, memoria, ecc tutto in tempo reale;

- *Host/Network Aliases*: consente di stabilire degli *alias* ad host o gruppi di host per agevolare la configurazione del firewall. Una volta impostato un *alias* per un gruppo di host o per una rete, è possibile riferirsi a questo gruppo semplicemente riportando l'alias nelle regole di firewalling. A fini pratici, risulta molto comodo e veloce senza riscrivere la stessa identica regola per diversi host. In più, contribuisce a mantenere la tabella delle *rules* molto più leggibile;

- *Carp/pfSync*: si può creare, tramite *Common Address Redundancy Protocol* e pfSense, un *cluster* di firewall ad alta affidabilità che implementa il *failover*. Si può impostare una macchina firewall principale ed una macchina secondaria che intervenga nel caso in cui il primo firewall vada *down* per problemi hardware o perché sotto pesante carico. In questo caso l'apparato di riserva eredita da quello principale, tutte le connessioni attive e le regole attive fino a quel momento. E' possibile anche sincronizzare le due macchine per farle lavorare parallelamente dividendosi il traffico da gestire;

- *Traffic Shaping*: tramite ALTQ consente di stabilire chi o quali protocolli hanno la priorità, quali host devono poter avere più banda rispetto ad altri e da quali code si può prendere traffico;

- *RRD Graphs*: Questo servizio fornisce una serie di statistiche del sistema come cpu, memoria, disco, utilizzo e le rappresenta graficamente su un asse cartesiano ad aggiornamento dinamico;

- *PPPoE Server*: Tramite la connessione a diversi modem ADSL è possibile eseguire un *load balancing* tra le diverse linee e combinarle insieme ottenendone una molto più prestante. Questo può avere un ritorno a livello economico, ad esempio per una ditta, perché potrebbe essere vantaggioso mantenere 2 o 3 linee ADSL piuttosto che una HDSL simmetrica;

- *HostAP*: pfSense fornisce un supporto completo anche per il Wireless. Connettendo una scheda di rete compatibile PCI o USB con *chipset* Atheros, è possibile creare un *access point* a tutti gli effetti. Tuttavia, per la realizzazione si è preferito utilizzare un *access point* dedicato collegato alla scheda LAN di pfSense;

- *Packages*: possiede un sistema di packages avanzato che permette di installare software di terze parti in base alle esigenze dell'amministratore. Tramite GUI è possibile selezionare i nomi dei *packages* da installare seguiti da una breve descrizione. Al termine del setup, la GUI viene automaticamente aggiornata con nuove entry sotto le voci corrispondenti. Questi pacchetti permettono di espandere le potenzialità del sistema e vengono raggruppati per servizi, funzionalità di rete, sistema, firewall, diagnostica, sicurezza e rete;

- *Captive Portal*: è una tecnica che consente di forzare un client http connesso ad una rete a visitare una speciale pagina web, generalmente quella per l'autenticazione, prima di poter accedere alla connessione. La rete WiFi in questo modo può anche essere lasciata senza password d'accesso perché la navigazione è consentita solo tra le pagine inserite ed abilitate nel captive portal. Il controllo degli accessi, non è al layer 2 come WPA/WPA2 ma si sposta a layer 3 cioè a livello di protocollo IP. La realizzazione di un Captive Portal avviene mediante l'utilizzo di un gateway che funge da default router per la zona da proteggere. Tale gateway blocca il traffico IP diretto verso l'esterno mentre "cattura" qualsiasi richiesta http o https diretta alle porte TCP 80 e 443 e la redirige verso un web server che presenta all'utente una pagina di autenticazione in cui inserire le credenziali. Se l'utente ha le credenziali corrette, il Server verifica che l'host è autorizzato e vengono rimossi i filtri per il traffico di quel client. Ogni richiesta HTTP generata da un client non autenticato, viene risolta con un *redirect* sulla pagina di autenticazione. Questa unica e limitante regola permette comunque di allacciarsi alla rete e di ricevere i parametri di rete dal DHCP server.

Il quarto capitolo di questa tesi tratterà in dettaglio l'implementazione dell'autenticazione sms su Captive Portal.

3.2.3 Installazione del firewall

Prima di procedere con l'installazione, assicuriamoci che il disco che vogliamo utilizzare non contenga dati importanti, poiché in seguito dovrà essere formattato con file system *Unix File System* (UFS).

Sul sito di pfSense scegliamo l'immagine ISO stable v1.2.3 . Dopo averla masterizzata saremo pronti per iniziare l'installazione. Assicuriamoci di aver abilitato il boot con avvio da CD, ed avviamo la macchina. Comparirà una schermata simile alla seguente:

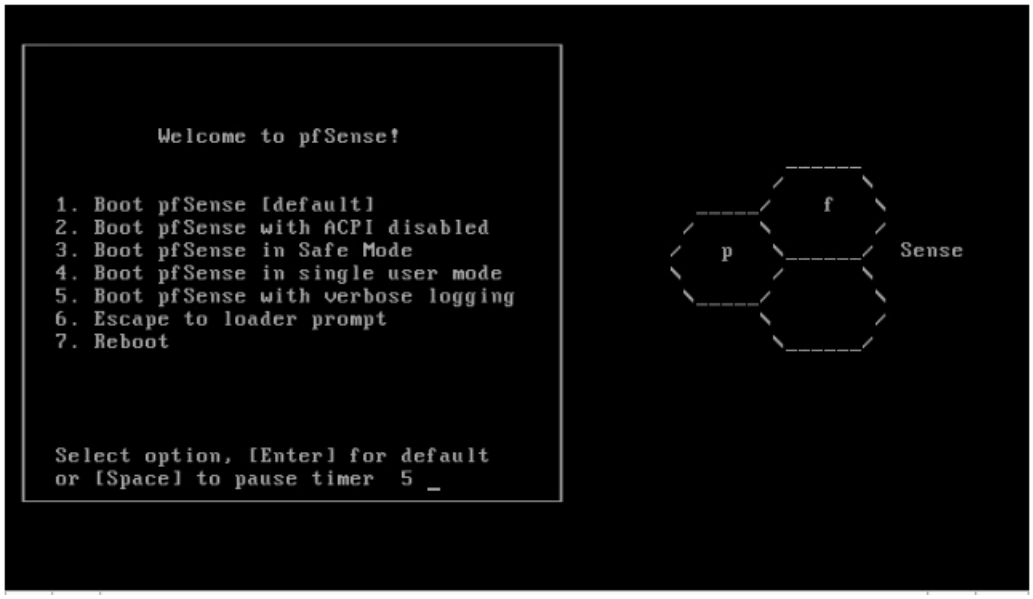


Figura 3.2: Pagina al boot di pfSense

Possiamo attendere il timeout del timer o premere il tasto "1". Dopo il caricamento del kernel FreeBSD verrà fatta partire un'istanza live di pfSense da CD-ROM.

Ora il sistema ci chiede se vogliamo lanciare subito l'installer, se procedere con un ripristino o se continuare con l'auto boot. A scopo dimostrativo, continuiamo con la normale procedura.

Figura 3.3: Scelta Recovery, Installer, Normal boot

Sta per iniziare la prima configurazione del firewall.

Viene mostrato un elenco delle schede di rete disponibili, e ci viene chiesto se si vuole eseguire la configurazione delle VLAN adesso. Questo perché è possibile fare in modo che un interfaccia del nostro firewall sia disponile su più VLAN, ovviamente previa opportuna configurazione di switch con supporto VLAN. Non avendo utilizzato tale servizio, digitiamo "n" ed a seguire INVIO:

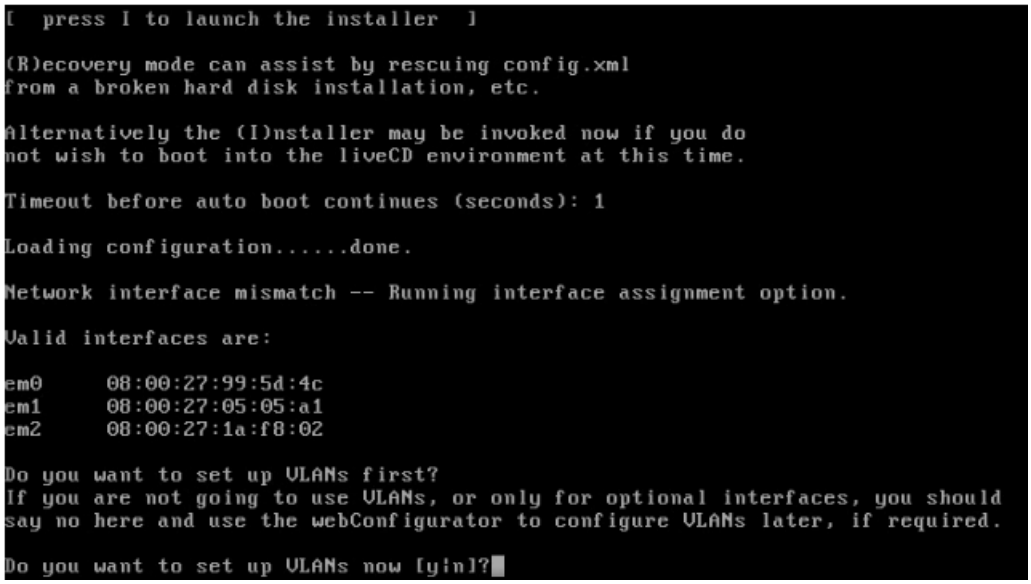


Figura 3.4: Setup di eventuali VLANs

Ora viene chiesto di assegnare i nomi alle 2 schede di rete LAN e WAN. Essendo pfSense basata su FreeBSD, la nomenclatura delle interfacce di rete è un po' diversa rispetto ai sistemi GNU/Linux. Mentre su Linux le interfacce di rete vengono nominate come eth0, eth1, ethX qualsiasi sia il tipo di scheda, sui sistemi *BSD il nome di un'interfaccia di rete dipende dal driver utilizzato. In questo caso abbiamo assegnato la scheda em0 sulla LAN e la em1 sulla WAN:

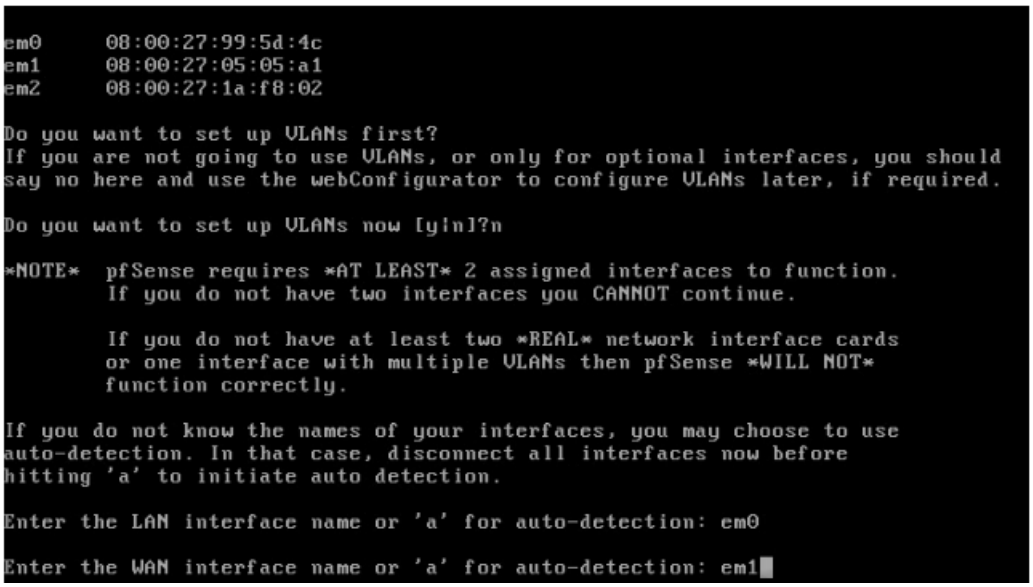


Figura 3.5: Assegnamento nomi alle schede LAN e WAN

Ci viene visualizzato un resoconto delle interfacce di rete ed una ulteriore conferma per proseguire:

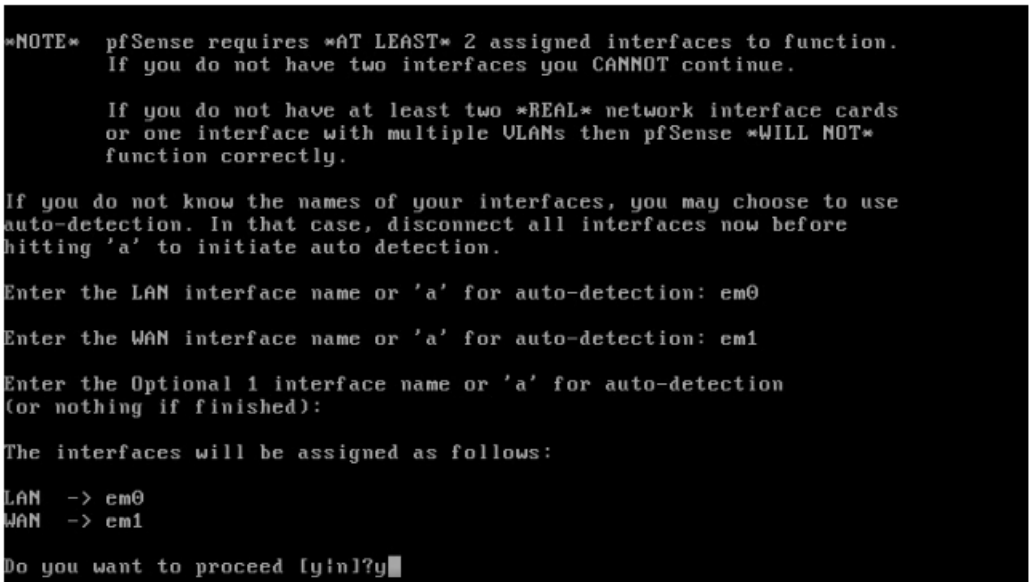


Figura 3.6: Conferma degli assegnamenti alle schede LAN e WAN

In questo momento abbiamo un firewall funzionante ed avviato da live. Per default la scheda LAN ha assegnato un indirizzo di rete 192.168.1.1 con NAT abilitato, mentre la scheda WAN riceve i parametri dal server DHCP (in questo caso Virtual Box[20]).

Per passare all'installazione su hard disk scriviamo "99" seguito da INVIO:

Figura 3.7: Digitando "99" si avvia l'installazione

E' possibile ora configurare il font dei caratteri, i settaggi per il display e la nazionalità della tastiera. Fatto ciò ci spostiamo sull'ultima voce per proseguire:

Figura 3.8: Impostazioni video e di tastiera

Per praticità scegliamo la tipologia di installazione più facile e veloce:

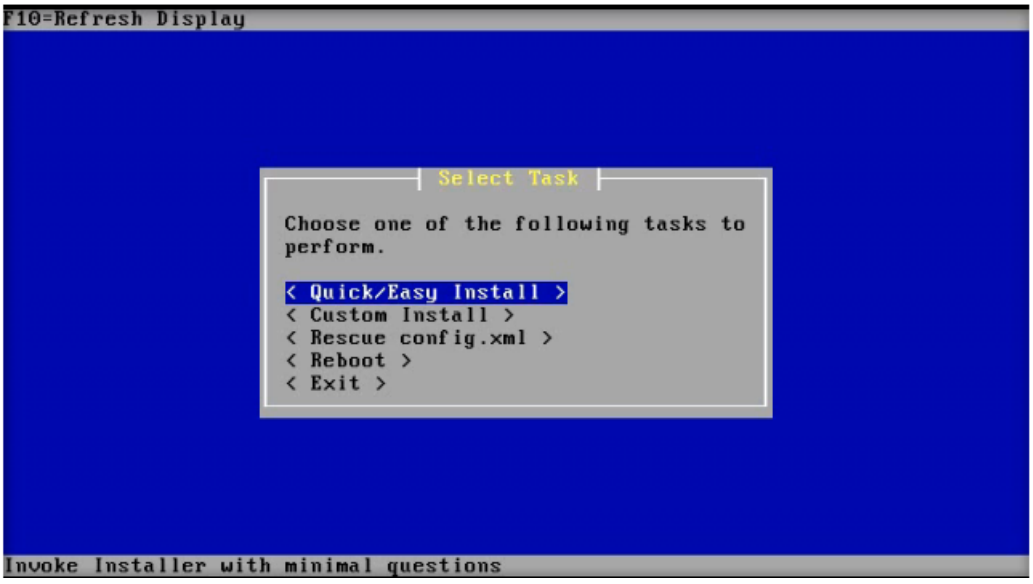


Figura 3.9: Tipologie di installazione

Un avviso ci informa che il sistema sta per installarsi sovrascrivendo il contenuto del primo hard disk:

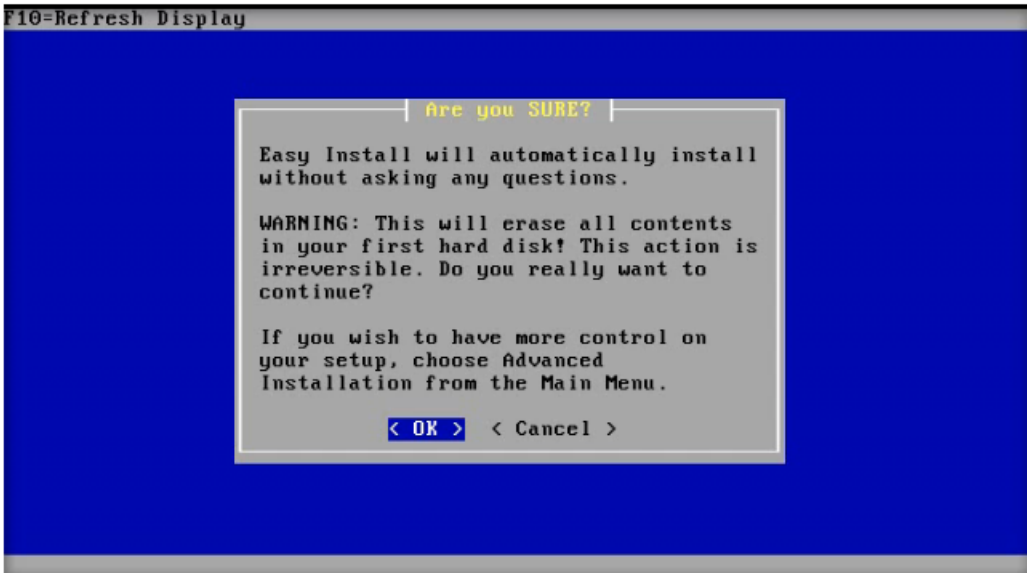


Figura 3.10: Avviso di sovrascrittura irreversibile

L'installer crea le partizioni e scrive i file di sistema:

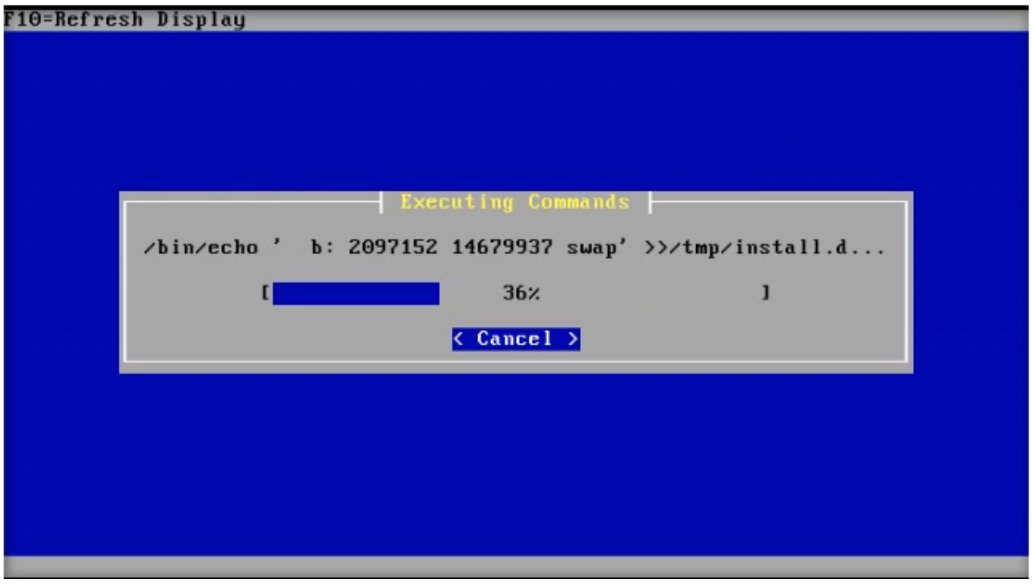


Figura 3.11: La procedura di installazione

Finita una prima fase di installazione, viene chiesto all'utente di selezionare il kernel corrispondente al tipo di architettura in uso. Per ragioni di compatibilità abbiamo scelto il kernel uniprocessore in presenza di architetture x86:

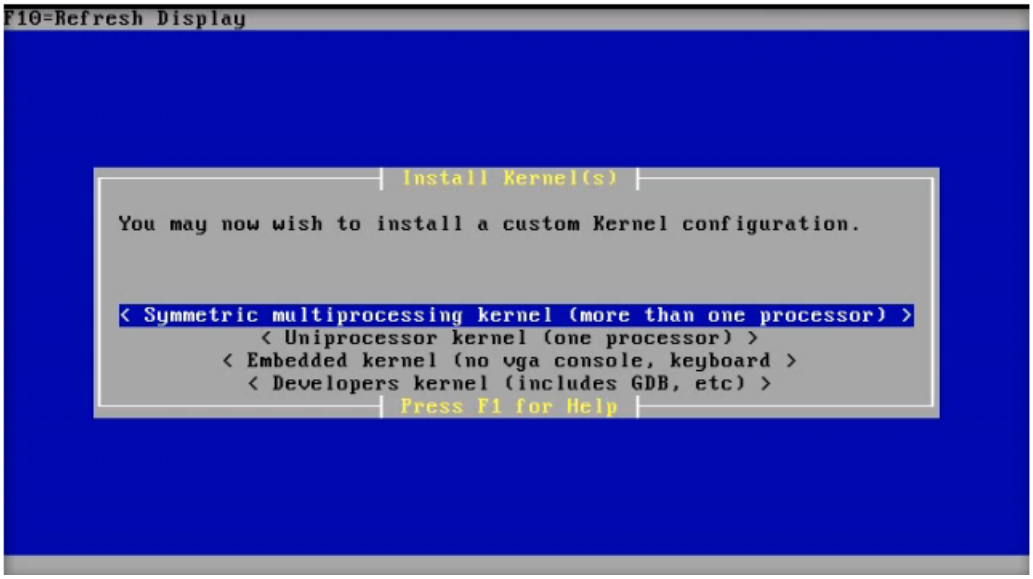


Figura 3.12: Scelta del kernel

Finita anche questa fase, il sistema è installato e richiede il riavvio:

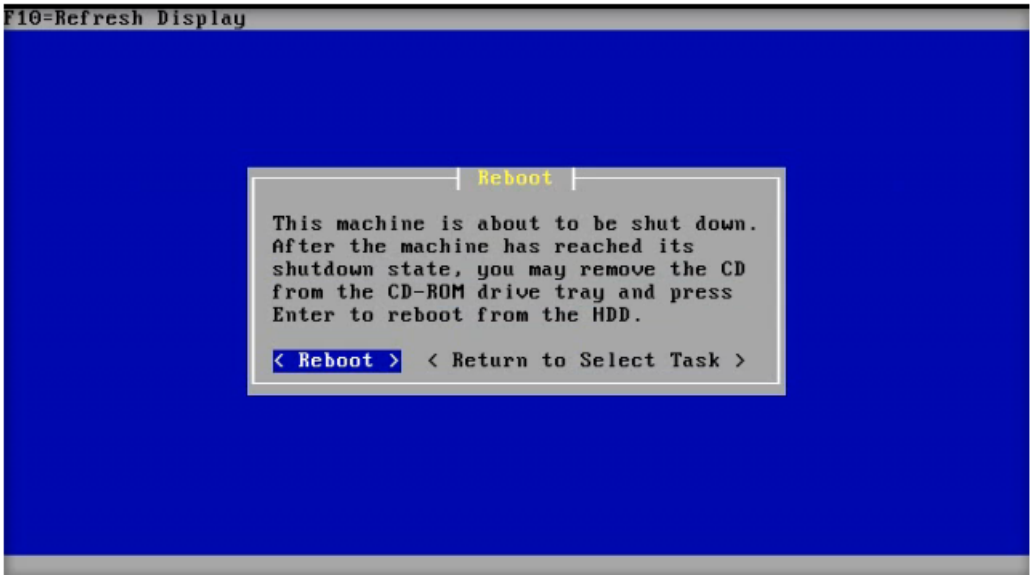


Figura 3.13: Richiesta di riavvio del sistema

Al successivo avvio, il firewall è completamente operativo e permanente. Si presenta in questo modo:

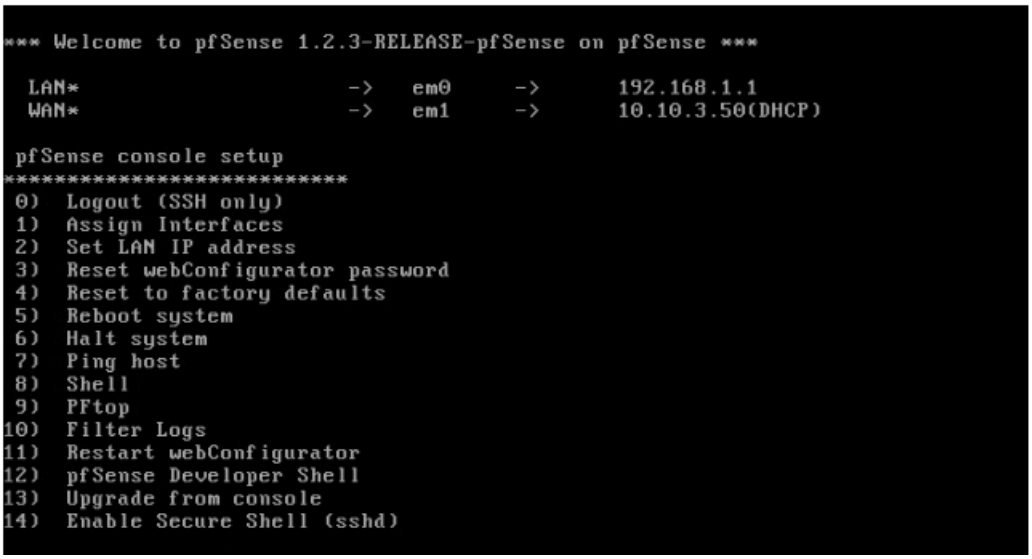


Figura 3.14: Sistema funzionante

pfSense mette a disposizione un'ottima interfaccia web per la sua configurazione. È possibile raggiungerla andando a puntare l'indirizzo http://192.168.1.1 inserendo come nome utente *admin* e come password *pfsense*.

Capitolo 4

Autenticazione SMS

L'autenticazione via Sms offre una serie di vantaggi sotto il profilo del miglioramento dei livelli di sicurezza e di massimizzazione della produttività, sia per gli utenti finali che per il personale amministrativo.

Se garantire un accesso immediato e affidabile è ormai un must, lo sono anche il controllo contro le violazioni e la conformità alle normative. In questo contesto una autenticazione forzata, che utilizza più accortezze per confermare l'identità dell'utente che esegue il login, diventa uno strumento strategico. Quando si trovano a valutare le alternative, molte aziende optano per l'uso dell'autenticazione via sms che offre, insieme, una tale comodità e sicurezza da renderla la soluzione ideale per numerosi scenari di utilizzo.

L' *sms authentication* si basa sulla sicurezza dell'autenticazione a due fattori e sulla comodità e semplicità dei dispositivi mobili e dei messaggi Sms. Sebbene il processo di autenticazione possa variare, in generale l'utente che ha bisogno di un accesso remoto richiede una password che gli viene inviata tramite sms direttamente sul cellulare da lui stesso autorizzato.

I vantaggi sono notevoli. Ad esempio l'aumento della sicurezza rispetto ai metodi basati su username e password, dal momento che si tratta di un'autenticazione a due fattori, oppure la riduzione dei costi, in quanto non è più necessario l'acquisto di token e/o di eventuali sostituzioni. Inoltre, dal momento che si avvale di uno strumento di uso quotidiano come i telefoni cellulari, la sms authentication trova applicazione anche in ambiti dove finora l'autenticazione a più fattori è stata poco praticata come l'online banking, l'e-learning, l'accesso a sistemi basati sull'autenticazione vocale, i siti dedicati alla sanità ed altro ancora. Prerequisito fondamentale è di possedere un telefono cellulare personale.

Questa non rappresenta una grande limitazione visto che l'Italia è al top della classifica europea per numero di contratti telefonici (alcune statistiche riferiscono 122 contratti di telefonia mobile su 100 cittadini) e per numero di sms inviati.

Una volta ottenuto l'sms di autenticazione, il sistema tiene i dati degli utenti registrati e può fornire il numero di cellulare salvato per risalire all'identità registrata alla SIM in caso di problemi. Per l'identificazione si fa riferimento all'autorità competente che provvederà a contattare il gestore telefonico della SIM stessa. In Italia, infatti, ogni numero telefonico mobile è associato ad un titolare. Questa convenzione tuttavia non può ritenersi sempre vera se considerata su scala europea, visto che alcuni paesi dell' UE rilasciano schede SIM senza una identità relativa.

Stiliamo alcune considerazioni sulla possibilità di autenticare gli utenti con un messaggio sms:

1. Comodità per l'utente finale: il successo di un metodo di autenticazione dipende da quanto gli utenti lo utilizzano senza che la loro produttività venga meno. A questo scopo i progettisti dovrebbero optare per soluzioni che offrono metodi di attivazione self-service in modo che gli utenti non debbano attendere l'assistenza di un operatore. Anche il processo di configurazione dovrebbe essere rapido, intuitivo e semplice.

2. Varietà di dispositivi supportati: i risparmi permessi dall'autenticazione tramite sms, senza la necessità di acquistare, distribuire e supportare nuovo hardware dedicato sono innegabili. Per questo è auspicabile cercare soluzioni che supportino il più esteso numero di modelli di dispositivi, con un occhio di riguardo al *mobile*.

3. Supporto reti Sms: in questo contesto gli utenti possono collegarsi ad una serie di reti in diverse aree durante il lavoro in ufficio o mentre si è in viaggio. Per essere davvero efficace, l'autenticazione via sms deve quindi supportare le reti sms di tutti i gestori.

4. Attivazione immediata: la velocità con cui viene evasa la richiesta una volta inviata, può determinare il successo o l'insuccesso del sistema. Possiamo considerare una buona attesa nell'arco di una diecina di secondi, tempo nel quale, l'sms arriva a destinazione.

5. Semplicità di gestione: una volta effettuata l'installazione, non necessita di operazioni di manutenzione. In un contesto aziendale, per esempio, l'incarico non viene assegnato a nessun dipendente contribuendo a snellire il carico di lavoro.

6. Rispetto delle regole: il Ministero dell'Interno, pur con le dovute precisazioni, ha ritenuto che queste soluzioni sono un più che accettabile compromesso fra le esigenze di sicurezza e controllo di cui regolamenta il Decreto Pisanu, e quelle di snellimento della procedura di autenticazione per ridare slancio al mercato HotSpot.

4.1 Il funzionamento

Inizialmente l'utente effettua uno scan delle frequenze WiFi dal suo dispositivo e nella lista dei risultati troverà un rete con SSID "hotspotPF". Ovviamente il nome impostato come SSID può essere personalizzato a piacere nei settaggi dell'access point incaricato di diffondere la rete wireless. L'utente effettua la connessione con l'access point che a sua volta inoltrerà la richiesta DHCP a pfSense. Quest'ultimo assegnerà un IP tra quelli disponibili al client il quale è ora associato alla rete. Si noti che la rete è volutamente sprovvista di crittografia per l'accesso e quindi accessibile a chiunque. Intanto nel server viene associato un IP al MAC address della scheda wifi che rimane nella client list del DHCP server.

In questo momento possiamo notare la funzione del Captive Portal. Tutto il traffico di ogni tipo è sottoposto ad un'unica e ferrea regola: viene dirottato su una particolare pagina web con porta di connessione 8000. L'unica pagina che l'utente può visualizzare è infatti la pagina di Login. Qualsiasi URL venga richiesta, verrà presentata sempre la stessa pagina web di autenticazione nominata come CP.html:

Figura 4.1: La pagina CP.html

In questa condizione l'utente può inserire le credenziali per accedere ad internet (se in suo possesso) o procedere con la registrazione cliccando sull'omonimo link.

Tutte le pagine internet create ad hoc e contenute all'interno dell'area cache del Captive Portal sono personalizzabili con la modifica di codice HTML.

In caso di credenziali errate, l'utente viene avvertito con una pagina dedicata:

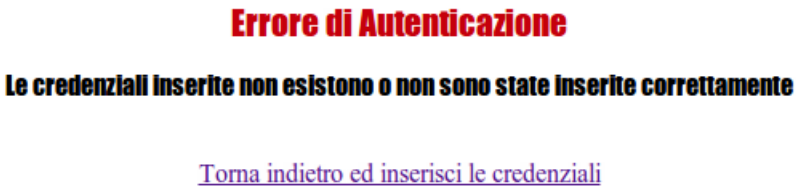


Figura 4.2: Pagina errore_auth.html

PfSense mette a disposizione una speciale area del Captive Portal nel quale è possibile inserire diversi file html abilitati all'accesso prima di essersi autenticati. E' proprio in questa area che abbiamo inserito tutti i file (ad esclusione di CP.html e di errore_auth.html). La procedura di registrazione si basa proprio su questo: guidare l'utente ad inserire i propri dati in maniera corretta passando da un file all'altro ed a finire con il login.

Un utente senza credenziali di login si troverà davanti la pagina di registrazione:

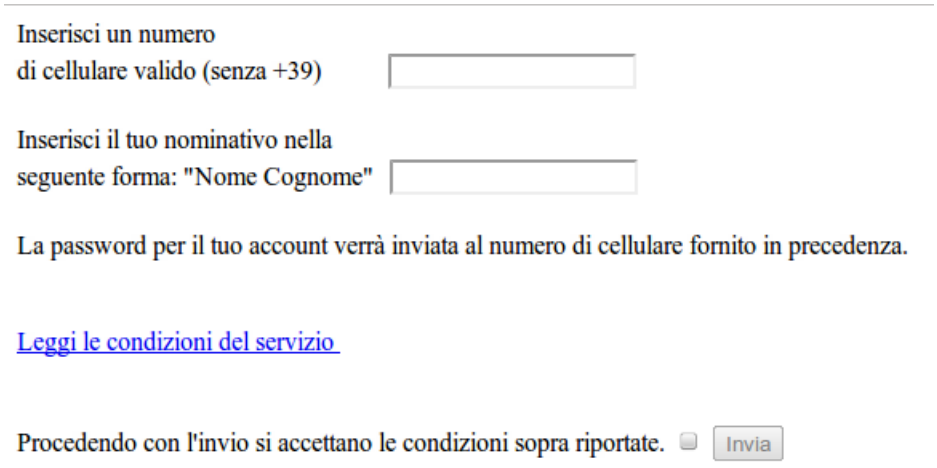


Figura 4.3: Pagina registrazione_utente.html

In questa fase l'utente è costretto ad inserire i dati per proseguire. Tecnicamente, la pagina è composta da una form html contenente 2 textarea. I valori inseriti verranno poi inviati, tramite metodo POST, alla successiva pagina inserisci_utente.php, la quale una volta ricevuti i campi delle textarea, ne valuta la correttezza.

Nella stessa pagina è presente un link al file clausule.html dove sono contenute tutte le condizioni da accettare per usufruire del servizio wifi. Un utente può anche non aprire questa pagina e non venire a conoscienza dell'informativa, ma proseguendo con la registrazione si accettano comunque le condizioni in tutte le loro parti.

Per procedere con il submit dei dati, è necessario spuntare la chechbox con un segno. Tale passaggio, infatti, è obbligatorio per poter interagire con il pulsante "Invia".

Dopo il submit dei dati, il codice dentro lo script php inizia ad essere eseguito con un determinato ordine:

1. E' necessario importare alcuni file e librerie per effettuare tutte le operazioni dello script.

2. Tramite il metodo POST vengono memorizzate in due variabili distinte, il numero di cellulare ed il nome completo. In particolare il numero di cellulare fungerà da username ed il nominativo sarà una descrizione dell'account creato. L'idea di utilizzare il numero di cellulare come username per i dati di accesso è vantaggioso per evitare errori di battitura da parte dell'utente.

3. Sulla pagina html, e quindi sul lato client, viene stampato a video un riepilogo dei dati precedentemente inseriti nelle textarea.

4. Ora lo script procede con la fase di controllo dei 2 valori. Per prima cosa si accerta che entrambi i campi non siano stati lasciati vuoti. Poi il controllo passa al numero di cellulare che deve essere di 10 cifre (escluso il prefisso +39) e deve essere un valore numerico intero. Successivamente il controllo passa sul nominativo, il quale non deve essere maggiore di 20 caratteri e non può essere un numero. Se un controllo solleva un errore, lo script termina e viene segnalato all'utente l'anomalia riscontrata.

5. Viene generata una password di 5 cifre alfanumeriche che sarà poi assegnata all'account dell'utente.

6. I dati vengono scritti su un file all'interno del file system di pfSense in base alla data ed ora della registrazione. Per ogni utente viene scritto anno, mese, giorno, ora, minuti e secondi della registrazione, seguiti da username (numero di cellulare), nominativo e la password generata per l'account criptata in md5. Questo file, oltre a mantenere una copia degli utenti registrati, può essere utile per inserire i log degli utenti ad esempio su un foglio elettronico.

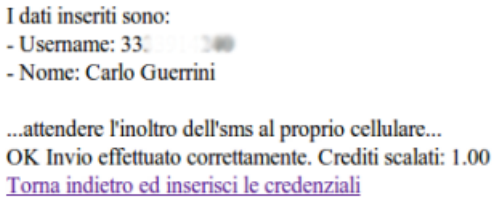
7. L'account viene creato e validato per accedere al Captive Portal secondo il metodo che utilizza pfSense per aggiungere un utente da webGUI. Questa fase dell'autenticazione è stata molto problematica perché solo dopo un accurato studio delle strutture dati di pfSense è stato possibile inserire un utente da script in modo del tutto automatico.

8. Viene composto il testo e la stringa d'invio per l'sms.

9. L'sms viene inviato al cellulare.

10. Viene stampato sulla pagina html l'esito d'invio del messaggio.

L'utente correttamente registrato visualizza una pagina web simile alla successiva:


I dati inseriti sono:
- Username: 33
- Nome: Carlo Guerrini

...attendere l'inoltro dell'sms al proprio cellulare...
OK Invio effettuato correttamente. Crediti scalati: 1.00
Torna indietro ed inserisci le credenziali

Figura 4.4: Registrazione avvenuta correttamente

Nel corso di qualche secondo, l'sms arriva a destinazione nella seguente forma:

Figura 4.5: Un esempio di messaggio ricevuto

Accertate le credenziali, sul browser dell'utente compare una finestra popup significativa che l'accesso è avvenuto correttamente:

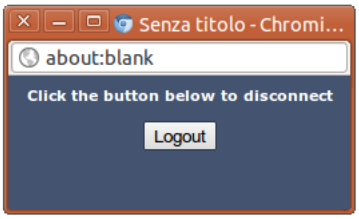


Figura 4.6: Popop di connessione

Per la disconnessione è sufficiente clikkare su "Logout" oppure chiudere semplicemente la finestra. Da pfSense è configurabile una soglia limite di inattività dopo il quale l'utente viene automaticamente disconnesso.

In seguito è riportato un diagramma riassuntivo per accedere ad internet:

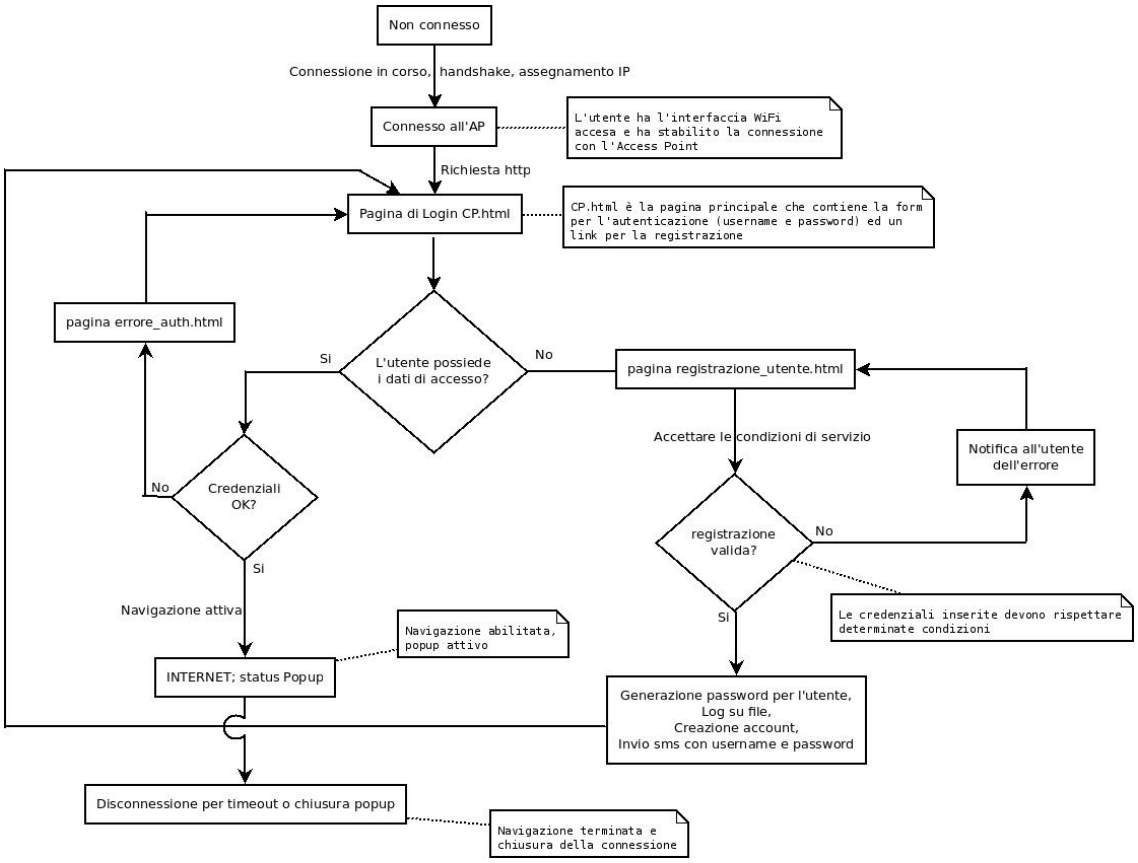


Figura 4.7: Flusso del Captive Portal

Ad ogni registrazione avvenuta correttamente, viene inserita una entry nella tabella utenti del Captive Portal in modo automatico:

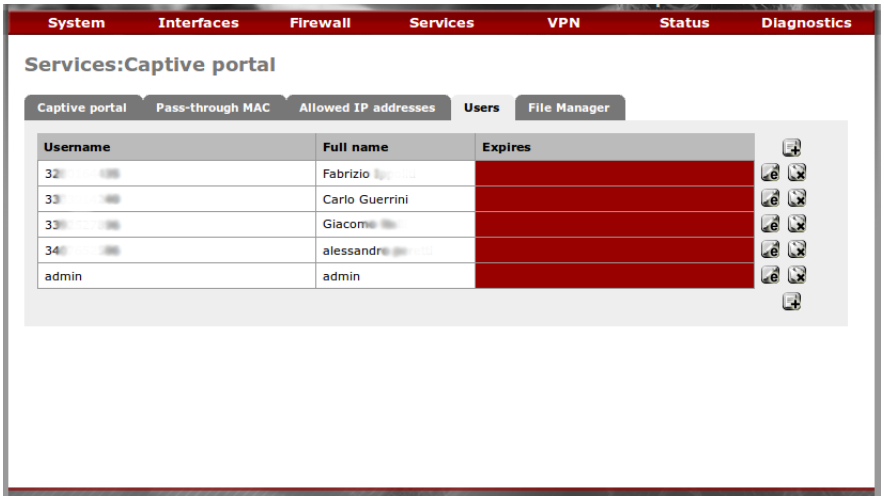


Figura 4.8: Tabella utenti abilitati al Captive Portal

4.2 Il gateway sms

Inizialmente l'idea principale era di collegare un telefono cellulare via cavo e sfruttare la rete GSM per inviare i messaggi. Proseguendo per questa strada abbiamo presto incontrato delle problematiche di compatibilità con il sistema operativo basato su BSD. PfSense, infatti, non ha installato uno stack per la gestione di questo tipo di periferiche e non dispone nemmeno di un applicativo in grado di gestire un telefono cellulare. Anche se il kernel di OpenBSD potrebbe fornire questo servizio, per la natura con cui è stato costruito pfSense, non risulta possibile utilizzare questa periferica.

Per l'invio degli sms, quindi, si è preferito scegliere uno dei tanti servizi di gateway sms online come TotalConnect.

La scelta è ricaduta su TotalConnect perché rende possibile automatizzare l'invio degli sms tramite uno script e perché il sito mette a disposizione 10 sms gratuiti al momento della registrazione. Non necessita di nessun canone o ulteriori prezzi fissi. Il listino prevede una somma di 30€ per 500 sms; un prezzo vantaggioso rispetto alla concorrenza.

Per l'implementazione di questo lavoro di tesi, lo spin off dell'Università degli Studi di Camerino e-Lios, ha messo a disposizione un pacchetto di sms dedicati a tale fine.

Molto utile, in fase di sviluppo, è stata la documentazione relativa all'invio di sms tramite script php.

Sono previsti 2 diversi metodi per l'uso dell'sms center di Totalconnect. Quello che più ci interessa è la possibilità di trasmettere messaggi SMS come parametri di un modulo HTML. Il servizio si basa su degli script di richiesta che vengono costruiti con i metodi descritti nella documentazione del gestore. I dati per le richieste devono essere trasmessi all'sms gateway attraverso richieste GET o POST via URL.

4.2.1 Abilitazione del servizio API

Per abilitare il servizio API di Totalconnect, il cliente, già registrato al

sito http://www.totalconnect.it, deve richiedere l'attivazione, telefonicamente chiamando un numero verde o aprendo un ticket al supporto tecnico direttamente dal pannello di gestione. Nella richiesta deve essere specificato il o gli indirizzi IP da attivare sull'account. L'indirizzo IP deve essere di tipo statico. Tuttavia, grazie alla *reservation* IP sulla rete unicam, abbiamo a disposizione sempre lo stesso indirizzo pubblico. I tempi di abilitazione del servizio sono brevi, solitamente lo stesso giorno in cui la richiesta è stata inviata.

4.2.2 Il pannello web di amministrazione

TotalConnect offre la possibilità di gestire vari servizi tramite un pannello web accessibile con le credenziali dell'account. Tutte le informazioni viaggiano sotto protocollo https per garantire la riservatezza dei dati.

La pagina è molto completa e chiara come si può vedere dall'immagine:

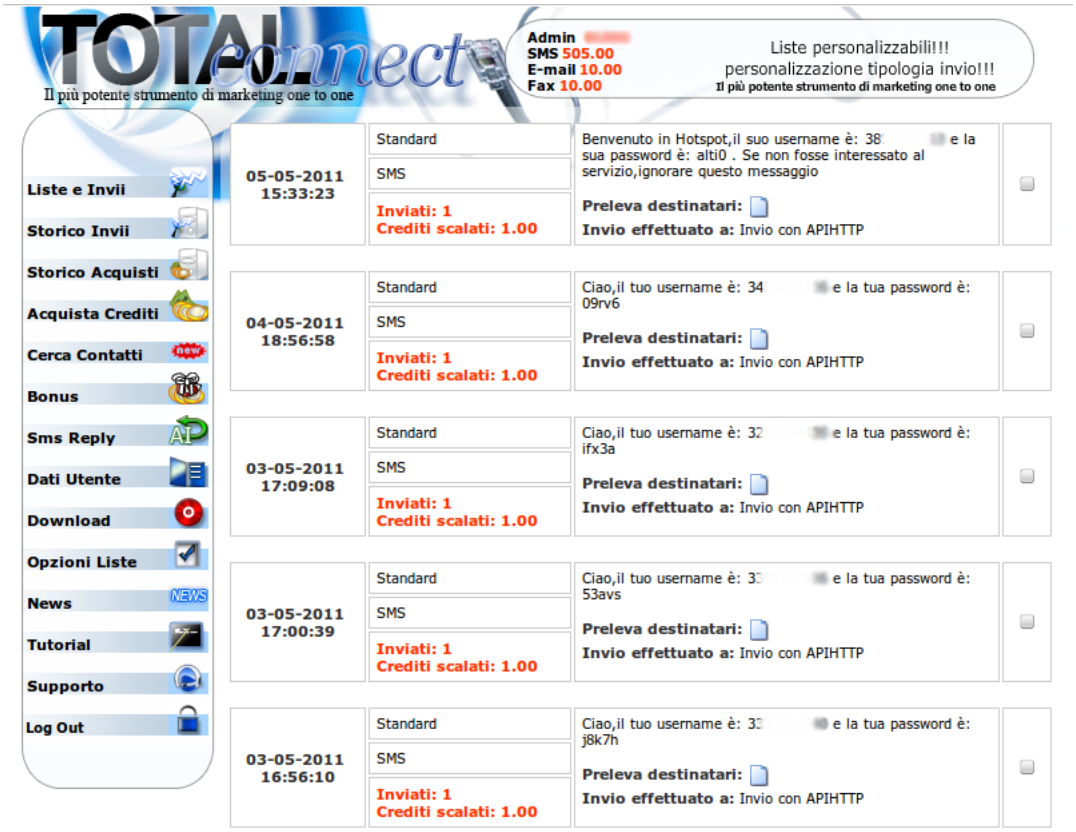


Figura 4.9: Il pannello di gestione di TotalConnect

In questo caso è stata selezionata la sezione "Storico Invii" dal quale è possibile visionare tutti gli sms inviati sia tramite pannello, sia tramite API HTTP. Con il motore di ricerca integrato è possibile risalire alla data e all'ora in cui è stata effettuata la registrazione, inserendo il numero di telefono identificativo dell'utente. Anche se queste informazioni sono scritte nel file di log del file system, rimane comunque utile avere un riscontro in questa pagina.

4.2.3 Composizione dell'URL di invio

Quando un messaggio viene inviato da API HTTP, è necessario comporre una stringa contente i parametri dell'account TotalConnect ed i dati relativi al messaggio da inviare:

I parametri base da impostare nell'URL sono:

1. username: Nome utente dell'account Totalconnect
2. password: Password dell'account Totalconnect
3. route: Tipologia gateway di invio, può essere: a) GW1 – per invii senza personalizzazione del mittente b) GW2 – per invii con mittente personalizzato. In base al tipo di parametro route vengono scalati dai crediti residui 1 credito per GW1 e 1.5 crediti per GW2
4. message: Il testo del messaggio da inviare. E' possibile inviare SMS fino a 160 caratteri. Il charset da utilizzare è latin1 ISO-8859-15. I caratteri accettati sono: []{}^'"&!?()*€#@%$£\/=+-_;,:.><A-Za-z0-9àèìòùÉ+
5. to: Il numero/numeri del/dei destinatari. In caso di più destinatari i numeri vanno separati dalla virgola senza spazi. Ogni numero deve essere riportato con il prefisso internazionale (per l'Italia +39).
6. from: Opzionalmente specifica il mittente del messaggio. La personalizzazione del mittente sarà tuttavia possibile solo utilizzando il gateway GW2. E' possibile inserire fino a 11 caratteri per un mittente alfanumerico o fino a 16 caratteri per un mittente solo numerico. Per i nostri test non abbiamo personalizzato il mittente per il suo maggior costo rispetto al mittente stardard.
7. flash: Opzionalmente manda un messaggio di tipo Flash. Questo tipo di messaggio appare direttamente sul terminale mobile del destinatario senza che venga aperto. Viene cancellato dalla memoria della SIM alla chiusura se non salvato esplicitamente. Siccome non tutti i cellulari possono risultare compatibili ed il messaggio non rimane permanente per una eventuale ridigitazione, non useremo questo parametro.

Una volta assegnate le giuste stringhe alle variabili sopracitate, vengono concatenate in una unica stringa url che sarà poi puntata dal file PHP. Dopo l'invio del messaggio, viene generato un valore di ritorno sullo status della consegna: "0" per la corretta consegna o "1" per mancata consegna.

Capitolo 5

Strumenti in dettaglio

5.1 Il proxy server Squid

5.1.1 Introduzione al server proxy

Un proxy è generalmente una macchina che si interpone tra un server e un client. Il client non si connette direttamente al server, ma al proxy. Sarà poi il proxy a gestire la connessione tra i due inoltrando le richieste al server e le relative risposte ai client.

Esistono 2 principali motivi per cui si utilizza un server proxy: il primo è quello di aumentare le prestazioni della rete, ed il secondo è il controllo e la limitazione del traffico.

Per velocizzare la rete si fa uso della funzionalità cache fornita dal server. La cache è un'area dell'hard disk dove vengono mantenute le informazioni che potrebbero essere richieste in futuro. Quando viene, ad esempio, richiesta una pagina web, il proxy controlla se questa è presente in locale. Nel caso non lo fosse, viene richiesta al server web in questione e successivamente fornita all'host che ne ha fatto richiesta. La pagina viene poi salvata e conservata sul disco rigido del server proxy a disposizione di chi la richieda. Ad una successiva richiesta, essa può essere immediatamente fornita, previa verifica di aggiornamenti senza doverne scaricare nuovamente il contenuto.

Il secondo vantaggio è che un proxy consente di controllare ed eventualmente filtrare il traffico. Un amministratore può bloccare le richieste a contenuti che ritiene dannosi o inappropriati per gli utenti. L'utilizzo di tali sistemi offre un notevole vantaggio in ambienti hotspot con un elevato numero di macchine interconnesse.

Una rete poco performante potrebbe significare una perdita di interesse nei confronti del servizio o, ancora peggio, nei confronti di chi lo gestisce. Allo stesso modo, una rete non adeguatamente protetta e monitorata potrebbe portare a problemi di sicurezza in primo luogo.

5.1.2 Squid su pfSense

Dopo aver installato il package Squid, abbiamo impostato il proxy server per l'interfaccia LAN. Una caratteristica fondamentale del pacchetto Squid, è la possibilità di lavorare in *transparent mode*. Se la modalità trasparente è attiva, tutte le richieste per la porta di destinazione 80 saranno trasmesse al server proxy, senza alcuna configurazione aggiuntiva necessaria sui client. Sarebbe improponibile, nonchè irrealizzabile, obbligare tutti i client a settare manualmente i dati di proxy sui rispettivi browser.

Squid, inoltre, permette di loggare il traffico di rete in un due file di testo dentro la cartella /var/squid/log.

Nello screenshot successivo è riportato il log di una pagina visitata (in questo caso http://www.pfsense.org/) da parte dell'IP 192.168.0.245. Ad ogni record possiamo notare l'intervento di scansione di havp su estensioni di file comuni quali *.html , *.gif, *.css, *.js, *.png :

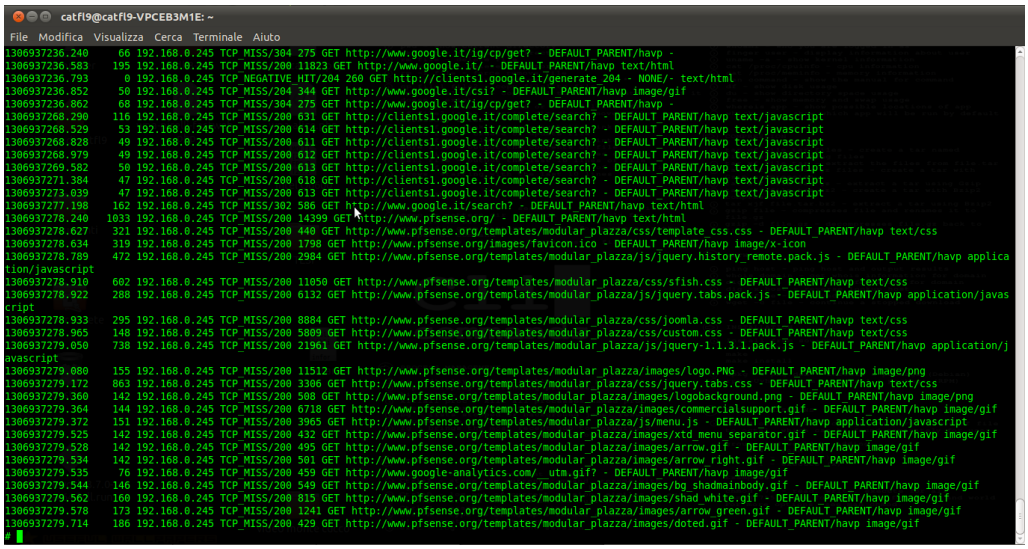


Figura 5.1: Log di Squid

Si è deciso di mantenere i log per 365 giorni. Alla scadenza i log vengono ruotati secondo la politica FIFO, permettendo a quelli che erano memorizzati da più tempo, di essere rimpiazzati dai nuovi.

Come dimensione di cache, il valore è stato aumentato ad 1GB in sostituzione degli originali 100MB visto le risorse disponibili.

Una sezione di Squid è dedicata al controllo degli accessi. In questa fase infatti possiamo andare ad impostare quali siti sono raggiungibili e quali no. L'inserimento di una URL o di una parola all'interno dell'URL nella textarea "Blacklist", non autorizza l'utente a visualizzare il sito. Sono considerati inappropriati i siti di file hosting e contenti pornografia. In seguito ad una richiesta non autorizzata, l'utente visualizzerà una pagina come la successiva:

Figura 5.2: Una pagina non abilitata

Inoltre, tramite Squid è possibile impostare una soglia massima di download per ogni host. Inserendo il valore in KB/s, questa sarà la banda che l'utente potrà utilizzare a suo piacimento.

Per correttezza, menzioniamo che in alternativa al proxy trasparente può essere utilizzato il protocollo WPAD[24]. Il *Web Proxy Autodiscovery Protocol* è un protocollo layer 7 che è stato elaborato da un gruppo di produttori software del calibro di Microsoft, RealNetworks, Sun Microsystem, InkTomi, che consente all'utente finale di configurare il proprio browser web in maniera trasparente, ovvero senza fare ricorso ad alcuna configurazione manuale.

5.2 L'HTTP proxy Havp e l'antivirus ClamAV

5.2.1 Antivirus di rete

I virus informatici costituiscono una grave minaccia per quanto riguarda la sicurezza di una rete ma soprattutto per i dispositivi ad essa connessi. Esistono software che tentano di proteggere da questa pericolosa insidia, conosciuti come Antivirus. Essendo soprattutto diffusi su piattaforme Windows, la maggior parte sono programmi a pagamento. Tuttavia esiste qualche soluzione Open Source. E' il caso di ClamAV[25], incluso come package installabile in pfSense. Per tradizione utilizzato su sistemi UNIX like, tale software non mira a proteggere la macchina su cui è installato, ma offre controllo per i file scaricati dalla rete hotspot. Molto spesso, infatti, capita che macchine server basate su UNIX si trovino a difesa di reti composte di host Windows. Bisogna, però, tenere a mente che non è sufficiente utilizzare una macchina per proteggere l'intera sottorete e quindi si presuppone che ogni macchina collegata alla rete dovrebbe essere munita di personal antivirus. Se un virus è contenuto in un archivio compresso scaricato da un sito o dalla posta elettronica, esso verrà intercettato dall'antivirus di pfSense senza arrivare ai client. In questa condizione, pfSense e ClamAV interrompono l'inoltro del file infetto ed informano l'utente con una speciale pagina web generata ad hoc:

Figura 5.3: Elemento virale intercettato da ClamAV

5.2.2 ClamAV su pfSense

Il package Antivirus HAVP è formato da un proxy http e dallo scanner ClamAV. Impedisce il download di file infetti e fornisce una scansione dinamica del traffico HTTP. I dati inizialmente passano attraverso il proxy havp e poi vengono sottoposti a scansione. In caso di esito negativo, sono resi disponibili alla rete. Il package può essere impostato come *Parent for Squid* oppure in modalità trasparente con o senza Squid.

Provando le varie configurazioni, si è deciso di utilizzare i 2 proxy uno consecutivo all'altro:

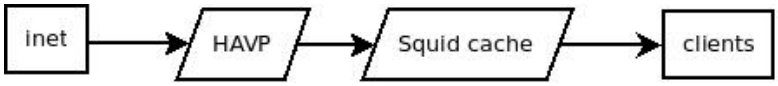


Figura 5.4: Schema HAVP e Squid

Tale soluzione è stata ottenuta impostando il proxy Squid trasparente (a contatto con i client) e HAVP come Parent for Squid. L'opzione "Parent for Squid" permette di dire al sistema che il proxy HAVP viene prima del proxy Squid e quindi una ipotetica pagina web richiesta, prima viene sottoposta a scannerizzazione e poi al controllo del proxy Squid.

Il motore ClamAV è impostato per effettuare l'aggiornamento automatico delle firme virali ogni 6 ore. Questa funzione permette di annullare la manutenzione per l'antivirus.

5.3 L'IDS/IPS Snort

5.3.1 Introduzione agli IDS

Un *Intrusion Detection System* è un sistema che permette di analizzare il traffico di rete alla ricerca di eventuali intrusioni ed attacchi informatici. Mi è sembrato giusto fornire alla rete questo tipo di servizio funzionante sulla scheda WAN. Riescono a riconoscere attività quali:

- Virus
- Troian
- Portscan
- Malware
- Exploit
- Worm
- Botnet
- Backdoor
- Dos
- P2P
- Tor

Una volta identificato un tentativo di attacco/intrusione, l'IDS registra le informazioni sull'accaduto generando un *alert* (IDS passivo) ed eventualmente intraprende una contromisura (IDS attivo meglio conosciuto come IPS - *Intrusion Prevention System*).

Solitamente gli IDS hanno un processo di aggiornamento delle regole di firewalling a cadenza programmata. L'update delle regole permette all'IDS di riconoscere nuove forme di attacco che altrimenti passerebbero ignare al controllo.

E' buona norma impostare una giusta politica nel riconoscimento delle minacce onde evitare falsi positivi. Infatti, un IDS che genera un numero spropositato di alerts perde di significato e di credibilità.

Il più noto software IDS Open Source è sicuramente Snort, che fa della vasta comunity e dell'applicazione multipiattaforma le sue armi vincenti. Quando si pensa a soluzioni di sicurezza difensiva si fa riferimento alla sua documentazione.

Una corretta analisi dei log e degli alert segnalati da Snort può evidenziare eventuali mancanze di sicurezza e permette successivamente di porre rimedio.

5.3.2 Snort su pfSense

Una volta installato Snort tramite il gestore dei pacchetti, per prima cosa è necessario impostare l'interfaccia su cui va ad operare. E' possibile impostare l'IDS anche su 2 o più interfacce di rete con differenti settings. La scelta più comune prevede la selezione della WAN dal menu interfaces e politica di scheduling "ac-bnfa" che risulta più adatta per hardware non particolarmente performante; teniamo anche conto che Snort è un package (insieme a DansGuardian) che fa molto uso di RAM e CPU.

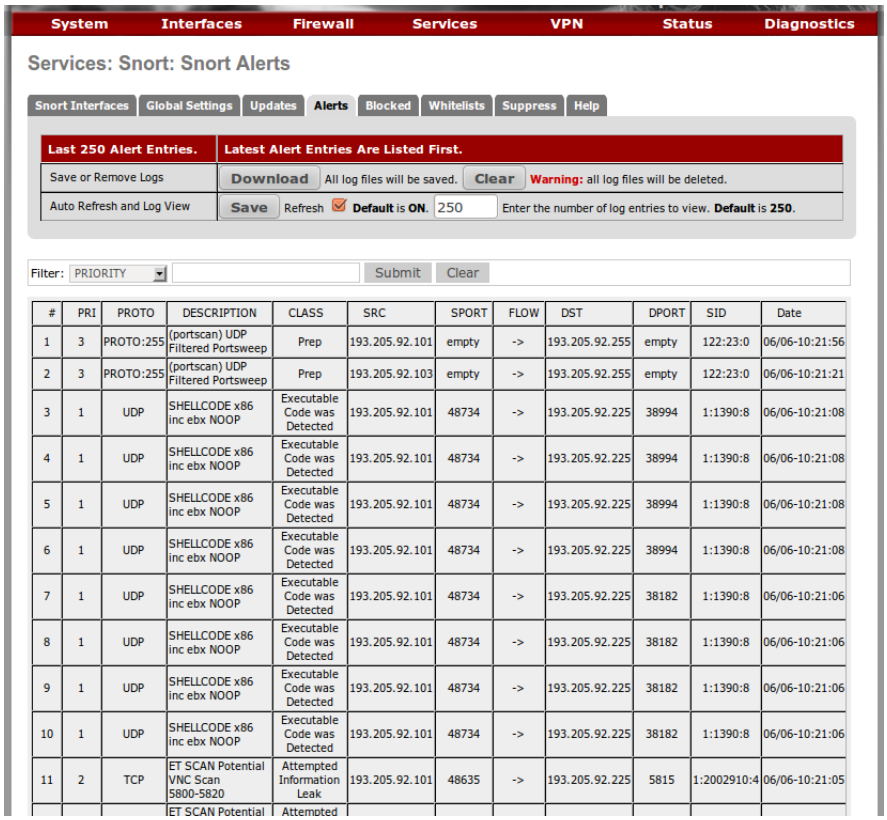
Per utilizzare l'IDS dobbiamo inserire una serie di regole su cui l'IDS stesso si baserà per riconoscere i pacchetti. Queste regole possono essere comodamente scaricate (ed aggiornate) tramite l'apposita sezione. Condizione necessaria per usufruire dello scaricamente delle rules è la registrazione al sito di snort.org per ricevere un *Oinkmaster code* Get an Oinkcode. Inserendo il codice nella relativa textarea, si può passare alla procedura di update che risulta facile e veloce. In seguito non sarà più necessario aggiornare manualmente le regole perché è disponibile un auto-update ogni 12 ore. Nello stesso pannello è possibile scegliere per quanto tempo viene negato il servizio ad un host bloccato; nel nostro caso si è scelto il minor intervallo di tempo disponibile (1 ora).

Snort raggruppa gli eventi per categorie. Selezionando una categoria, automaticamente importiamo una serie dei regole che vengono inserite nella pannello di Snort "rules". E' possibile modificare le regole di ogni categoria in base alla loro descrizione, abilitando o disabilitando manualmente le regole.

Nelle schede *Alerts* e *Blocked*, compaiono le attività dell'IDS. Gli alerts riportano gli eventi da segnalare classificati per priorità ma tale per cui l'host non viene bloccato, mentre una voce *entry* in "Blocked" segnala che un host è stato bloccato da Snort per il tempo stabilito di 1 ora. Gli alerts possono fornire molte informazioni come IP sorgente, IP destinazione, protocollo, descrizione, porta sorgente/destinazione che aiutano a capire cosa è successo nella rete.

Una scelta da valutare con attenzione è il flag per bloccare eventuali hosts che hanno generato alerts. Nelle prove condotte in laboratorio, questa opzione è stata abilitata per avere conferma dell'intervento di Snort.

Di seguito riportiamo i risultati dopo un port scan sull'interfaccia WAN:



#	PRI	PROTO	DESCRIPTION	CLASS	SRC	SPORT	FLOW	DST	DPORT	SID	Date
1	3	PROTO:255	(portscan) UDP Filtered Portsweep	Prep	193.205.92.101	empty	->	193.205.92.255	empty	122:23:0	06/06-10:21:56
2	3	PROTO:255	(portscan) UDP Filtered Portsweep	Prep	193.205.92.103	empty	->	193.205.92.255	empty	122:23:0	06/06-10:21:21
3	1	UDP	SHELLCODE x86 inc ebx NOOP	Executable Code was Detected	193.205.92.101	48734	->	193.205.92.225	38994	1:1390:8	06/06-10:21:08
4	1	UDP	SHELLCODE x86 inc ebx NOOP	Executable Code was Detected	193.205.92.101	48734	->	193.205.92.225	38994	1:1390:8	06/06-10:21:08
5	1	UDP	SHELLCODE x86 inc ebx NOOP	Executable Code was Detected	193.205.92.101	48734	->	193.205.92.225	38994	1:1390:8	06/06-10:21:08
6	1	UDP	SHELLCODE x86 inc ebx NOOP	Executable Code was Detected	193.205.92.101	48734	->	193.205.92.225	38994	1:1390:8	06/06-10:21:08
7	1	UDP	SHELLCODE x86 inc ebx NOOP	Executable Code was Detected	193.205.92.101	48734	->	193.205.92.225	38182	1:1390:8	06/06-10:21:06
8	1	UDP	SHELLCODE x86 inc ebx NOOP	Executable Code was Detected	193.205.92.101	48734	->	193.205.92.225	38182	1:1390:8	06/06-10:21:06
9	1	UDP	SHELLCODE x86 inc ebx NOOP	Executable Code was Detected	193.205.92.101	48734	->	193.205.92.225	38182	1:1390:8	06/06-10:21:06
10	1	UDP	SHELLCODE x86 inc ebx NOOP	Executable Code was Detected	193.205.92.101	48734	->	193.205.92.225	38182	1:1390:8	06/06-10:21:06
11	2	TCP	ET SCAN Potential VNC Scan 5800-5820	Attempted Information Leak	193.205.92.101	48635	->	193.205.92.225	5815	1:2002910:4	06/06-10:21:05
			ET SCAN Potential	Attempted							

Figura 5.5: Alerts segnalati da Snort dopo un port scan

Riconosciuta la minaccia, l'host viene inserito tra gli IP bloccati:

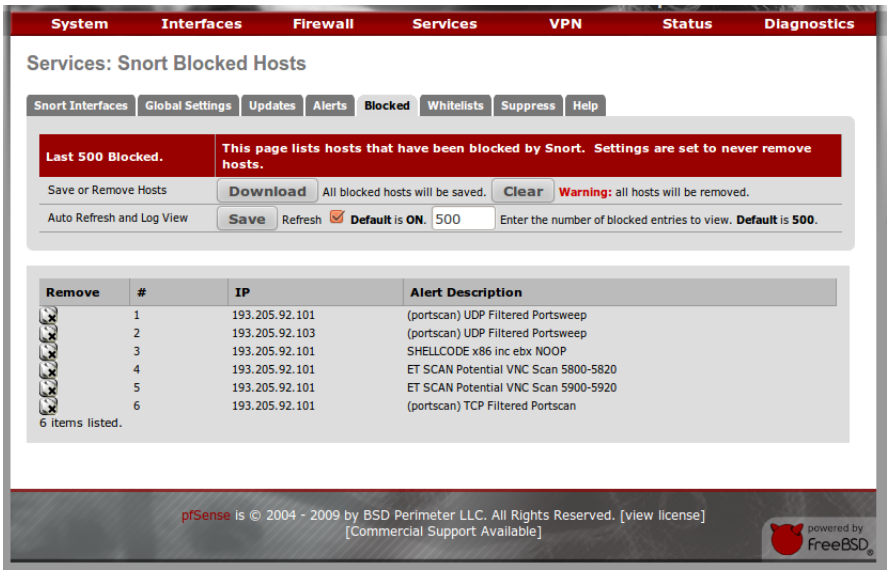


Figura 5.6: Blocked host dopo un port scan

5.4 Il DNS forwarder Dnsmasq

E' possibile impostare il firewall perché funga da server DNS o da DNS forwarder. Nel nostro caso, è il server DHCP che si occupa di assegnare i DNS ai client, ma c'è da dire che i DNS sono assegnati al firewall dalla rete WAN e quindi dall'ISP. Dnsmasq permette proprio l'inoltro del protocollo DNS: quando un client fa una richiesta DNS, dnsmasq la inoltra al server e la risposta contenente la mappa hostname-IP torna al client. In alcuni casi in cui i server DNS dell'ISP manifestino scarse performance, è preferibile impostare un server DNS per la LAN magari con funzione *caching*.

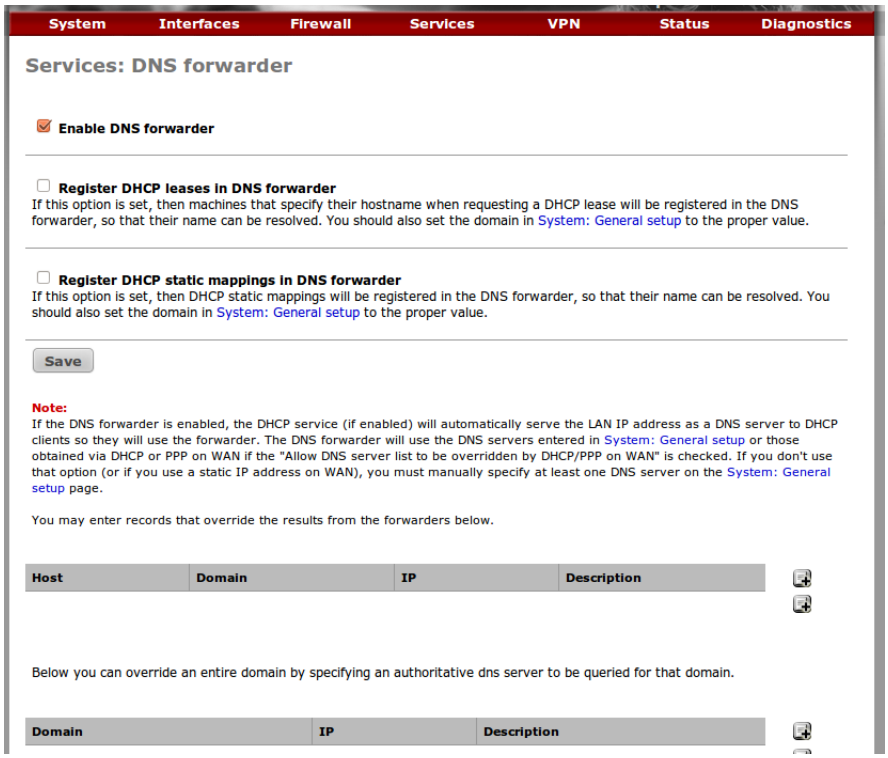


Figura 5.7: DNS forwarder su pfSense

5.5 La sincronizzazione clock Ntpd

Il *Network Time Protocol*, in sigla NTP[26], è un protocollo per sincronizzare l'orario dei computer all'interno di una rete ad intervalli variabili. L'NTP è un protocollo client-server appartenente al livello applicativo della pila ISO/OSI e di default in ascolto sulla porta 123. La sincronizzazione su questo tipo di installazione è utile per accettarsi che data e ora dei log registrati siano corretti.

La soluzione integrata in pfSense è il demone NTP, ntpd, facilmente configurabile dalla sua scheda. E' sufficiente, infatti, impostare il *timezone* in base alla nazionalità. In questo modo, oltre ad aggiornare l'orologio di sistema, ntpd ne stima l'errore sistematico evitando un andamento irregolare del tempo, migliorando la precisione quando il computer non è connesso alla rete. È anche possibile mettere ntpdate in *crontab* per mantenere automaticamente aggiornato l'orologio di sistema e sincronizzare i client tramite DHCP al momento della connessione.

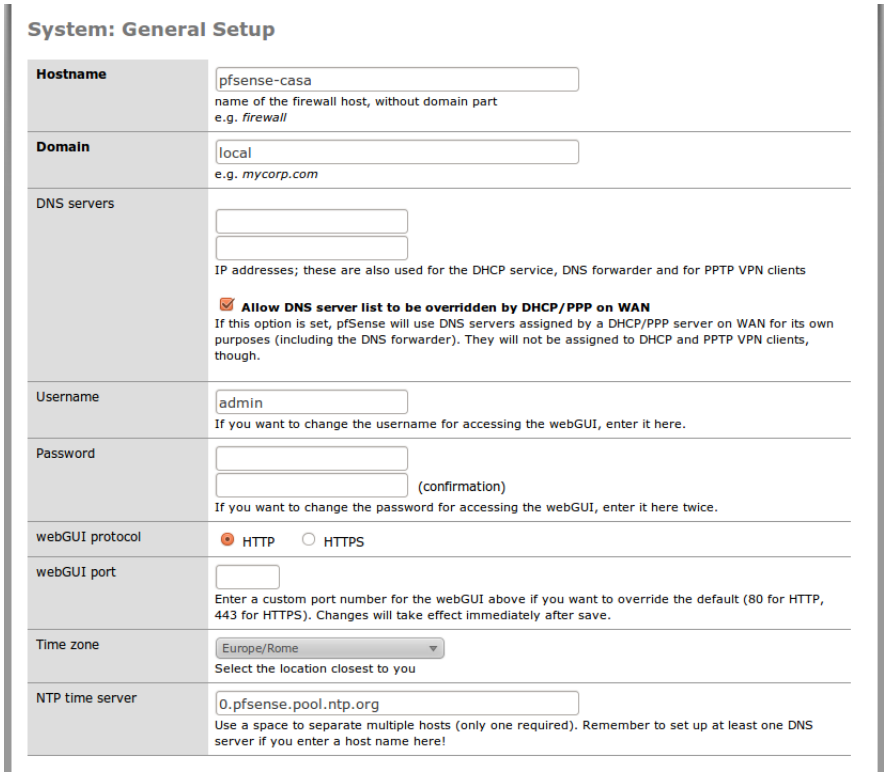


Figura 5.8: Impostazioni generali pfSense

5.6 Traffic Shaper

In pfSense è nativamente integrato un traffic shaper che intende gestire l'insieme di operazioni di controllo sul traffico di una rete in modo da ottimizzare/garantire le prestazioni di trasmissione, ridurre o controllare i tempi di latenza e sfruttare al meglio la banda disponibile tramite l'accodamento e il ritardo dei pacchetti che soddisfano determinati criteri. Lo shaping si realizza tipicamente mediante un sistema di accodamento e prioritizzazione dei pacchetti in uscita. Il meccanismo determina, sulla base delle condizioni di traffico istantanee, della priorità assegnata al pacchetto e dei limiti di banda prestabiliti, se un determinato pacchetto può essere trasmesso o deve essere accodato per essere trasmesso in un momento successivo.

Per ovvie ragioni, in condizioni di saturazione di banda sulla linea ADSL, tutto il traffico non può essere classificato allo stesso modo.

PfSense mette a disposizione una sequenza guidata da completare per lo shaping del traffico. Nella configurazione prima viene chiesta la disposizione delle interfacce di rete e poi la portata della connessione internet. La seconda fase chiede se si vuole priorizzare il traffico VoIP su tutti ed eventualmente riservare un certo quantitativo in Kb/s per tale servizio. In generale, rimane molto scomodo ricevere in ritardo la risposta di un interlocutore da una telefonata VoIP, quindi questa funzionalità può avere un riscontro pratico.

La terza fase è dedicata alla gestione della banda per i Peer-To-Peer; viene impostata la minima priorità e la minima banda per tutti gli specifici protocolli presenti nella lista. Ritengo opportuno che un servizio hotspot non debba fornire connettività da/verso P2P.

Un'altra scheda è per l'online gaming dove è possibile dare priorità ad alcune delle più famose piattaforme mondiali di videogiochi. Non è un nostro scopo quindi la priorità viene mantenuta a livello standard.

Per i restanti protocolli di rete, viene data priorità manuale al traffico:

Priorità	Protocolli
Alta	Html, IRC, Jabber, ICQ, AIM, MSN, Teamspeak
Defaut	RTSP, Streaming, SMTP, POP3, IMAP, SNMP e tutti i restanti
Bassa	MSRDP, VNC, PcAnywhere, PPTP, IPSEC e tutti i P2P

Tabella 5.1: Priorità Traffic Shaper

La pagina dedicata ai P2P si presenta nel seguente modo:

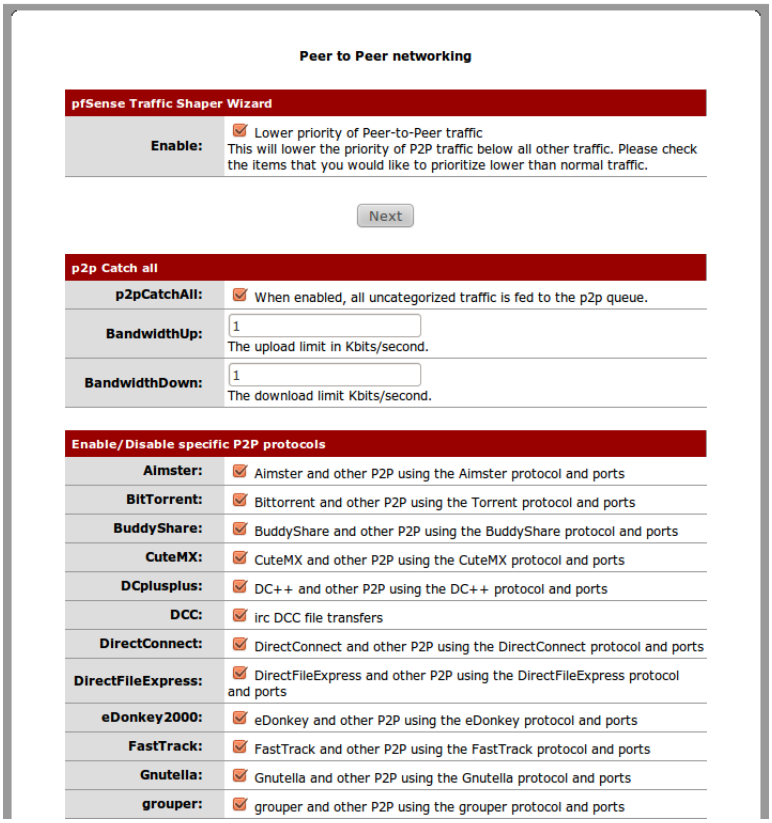
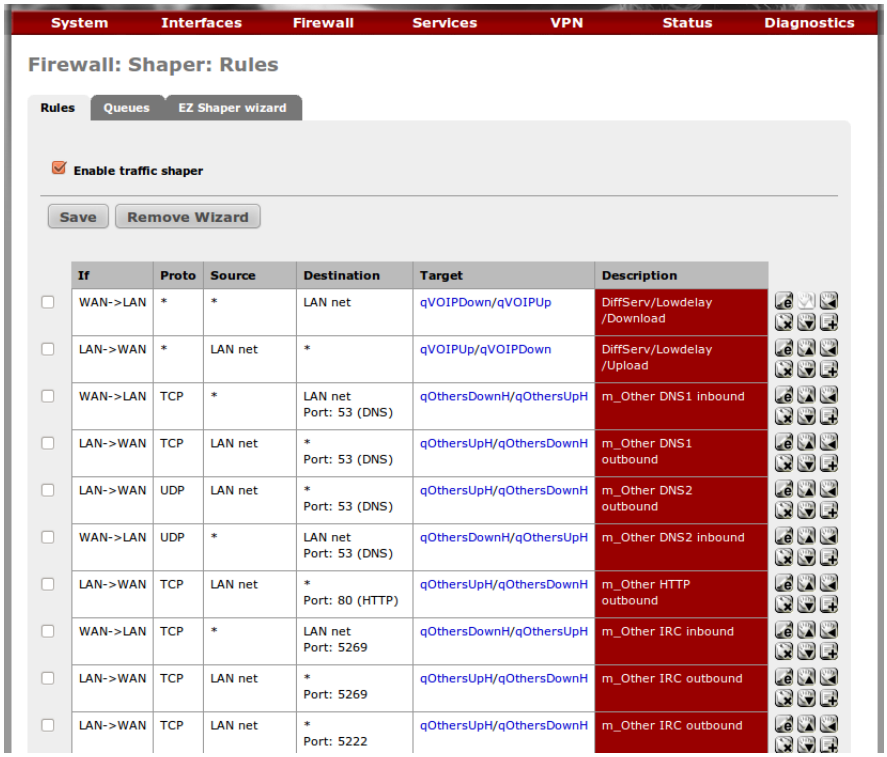


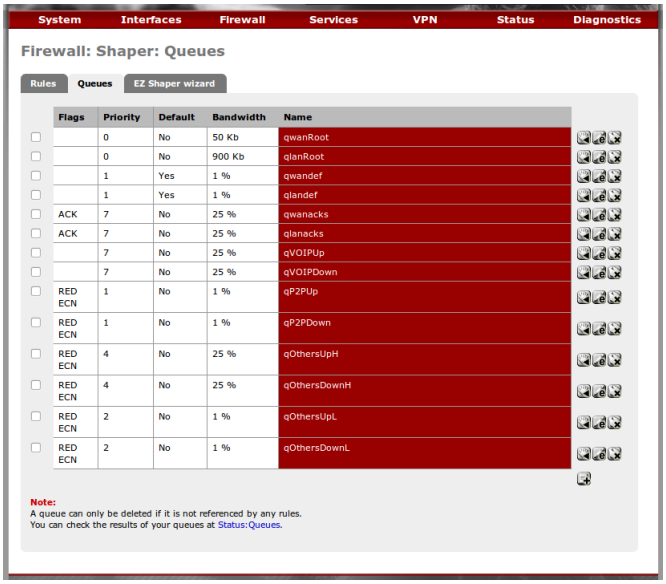
Figura 5.9: Gestione dei protocolli P2P con Traffic Shaper

Terminata la sequenza guidata otteniamo una serie di regole generate e le relative code di priorità:



If	Proto	Source	Destination	Target	Description
WAN->LAN	*	*	LAN net	qVOIPDown/qVOIPUp	DiffServ/Lowdelay /Download
LAN->WAN	*	LAN net	*	qVOIPUp/qVOIPDown	DiffServ/Lowdelay /Upload
WAN->LAN	TCP	*	LAN net Port: 53 (DNS)	qOthersDownH/qOthersUpH	m_Other DNS1 inbound
LAN->WAN	TCP	LAN net	* Port: 53 (DNS)	qOthersUpH/qOthersDownH	m_Other DNS1 outbound
LAN->WAN	UDP	LAN net	* Port: 53 (DNS)	qOthersUpH/qOthersDownH	m_Other DNS2 outbound
WAN->LAN	UDP	*	LAN net Port: 53 (DNS)	qOthersDownH/qOthersUpH	m_Other DNS2 inbound
LAN->WAN	TCP	LAN net	* Port: 80 (HTTP)	qOthersUpH/qOthersDownH	m_Other HTTP outbound
WAN->LAN	TCP	*	LAN net Port: 5269	qOthersDownH/qOthersUpH	m_Other IRC inbound
LAN->WAN	TCP	LAN net	* Port: 5269	qOthersUpH/qOthersDownH	m_Other IRC outbound
LAN->WAN	TCP	LAN net	* Port: 5222	qOthersUpH/qOthersDownH	m_Other IRC outbound

Figura 5.10: Regole Traffic Shaper



Flags	Priority	Default	Bandwidth	Name
	0	No	50 Kb	qwanRoot
	0	No	900 Kb	qlanRoot
	1	Yes	1 %	qwandef
	1	Yes	1 %	qlandef
ACK	7	No	25 %	qwanacks
ACK	7	No	25 %	qlanacks
	7	No	25 %	qVOIPUp
	7	No	25 %	qVOIPDown
RED ECN	1	No	1 %	qP2PUp
RED ECN	1	No	1 %	qP2PDown
RED ECN	4	No	25 %	qOthersUpH
RED ECN	4	No	25 %	qOthersDownH
RED ECN	2	No	1 %	qOthersUpL
RED ECN	2	No	1 %	qOthersDownL

Note:
A queue can only be deleted if it is not referenced by any rules.
You can check the results of your queues at Status: Queues.

Figura 5.11: Code di priorità

Capitolo 6

Conclusioni

La connettività è sempre più richiesta e ricercata dagli utenti. Fornire questo tipo di servizio al pubblico comporta una serie di accortezze raggruppabili in 2 grandi campi: legalità e sicurezza.

Una implementazione come quella realizzata è realmente candidata ad un utilizzo reale per l'elevata aderenza alle 2 condizioni da garantire. Ulteriori accorgimenti di natura tecnica possono essere aggiunti per completare la sicurezza dell'infrastruttura.

La semplificazione sulle normative ha contribuito notevolmente alla condivisione pubblica di internet. Speriamo che ciò possa farci risalire nelle classifiche per diffusione degli hotspot, in cui l'Italia è tra le ultime d'Europa.

Se in futuro ci sarà bisogno di comunicare con la pubblica amministrazione tramite internet, ad una ipotetica famiglia senza connettività per motivi tecnici o economici, gli viene negato il servizio. E' evidente che ciò non possa accadere.

L'autenticazione sms è un buon punto di incontro tra identificazione personale e rispetto delle normative mantenendo una facilità d'uso soddisfacente. Eventuali future revisioni al codice possono abilitare la registrazione anche a SIM non italiane.

La scarsa diffusione delle installazioni hotspot su scala nazionale, fa pensare anche una certa influenza da parte dei gestori di telefonia mobile. Chiaramente, una elevata copertura su territorio nazionale di hotspot wifi, non aumenta il fatturato di offerte e contratti per il traffico dati *mobile*. Non ci è dato sapere se i gestori di telefonia siano favorevoli o no, ma sicuramente suscita interesse nei loro confronti.

L'utilizzo di pfSense come firewall è molto più vantaggioso di un sistema Win Server/Linux/BSD per tutti le ragioni di facilità d'uso, rendimento e velocità di set-up.

PfSense è un ottimo prodotto, persino meglio di alcuni firewall commerciali, proposto ad un rapporto prezzo/servizi imparagonabile e potente strumento di network e security. Fornisce una eccellente personalizzazione grazie ai package aggiuntivi con facilità, facendo risparmiare ore di configurazione.

L'unica pecca che realmente manifesta è la mancanza di un filtro layer 7 per il filtraggio dei pacchetti. Ipoteticamente, infatti, utilizzando alcune tecniche per il mascheramento del traffico è possibile far transitare nella rete dei dati ritenuti non idonei. Il filtro a livello applicativo verrà integrato nella nuova release v2.0 terminato lo sviluppo, come dichiarato dalla comunità del progetto. Fa della stabilità uno dei punti di forza; la macchina fisica, pur non essendo un hardware specifico, non ha mai manifestato sintomi di affaticamento, simbolo della qualità del progetto.

Una anomalia che ho potuto riscontrare è che il proxy server Squid, dopo un riavvio, non viene lanciato automaticamente e necessita di click manuale sulla sua scheda di configurazione. Lasciando la macchina costantemente accesa, magari con un UPS, non si incombe in questa falla.

Mio malgrado non ho ancora potuto provare il sistema con un elevato numero di utenti, ma i risultati ottenuti finora lasciano ben sperare.

Per alcuni aspetti, l'attività di *logging* può essere delegata ad un server esterno se si vogliono ottenere maggiori dettagli e consistenza dei dati; magari con backup incrementali e controller RAID. Tuttavia la quantità di log prodotta da Squid, Snort e da SysLog risulta accettabile; è possibile infatti risalire alla data di registrazione, numero di cellulare, IP assegnato, MAC address, pagine visitate e data/ora di log sul captive portal di ogni utente.

Il package opzionale di pfSense "DNS Blacklist" non ha dato i risultati sperati. Questo pacchetto permette di selezionare per categoria i domini da "blacklistare" in modo che il DNS non fornisca una risoluzione di quei domini; una soluzione a prima vista molto vantaggiosa. Anche altri utenti del forum e del canale IRC di pfSense manifestano perplessità e malfunzionamenti. Per questi motivi non è stato utilizzato sulla nostra macchina.

Altri servizi quali Squid, Snort, Captive Portal, ClamAV ed il gateway sms, hanno svolto il proprio lavoro in maniera soddisfacente dopo una discreta fase di test.

La funzione di Traffic Shaping integrata in pfSense, a prima vista può risultare molto comoda per autogenerare una serie di regole, ma in realtà una quantità così elevata non lascia molta chiarezza per un eventuale intervento manuale. In mancanza del filtro layer 7 è utile per limitare i protocolli di P2P. Il traffico per questi ultimi, limitato ad 1Kb/s, non esclude totalmente il protocollo ma a scopo pratico lo rende comunque inutilizzabile.

Il codice da me realizzato sarà inviato, una volta completo di documentazione in lingua inglese, alla sezione di sviluppo di pfSense che manifesta sempre interesse verso qualsiasi ampliamento di funzionalità.

Appendice A

Appendice

Il codice sorgente di CP.html:

```
<img src="http://t1.gstatic.com/images?q=tbn:ANd9GcSDFtO98FEqmR4QNpM6Yz2162KdmCCPDASkJqJNL-RZWBryLt8P" alt="unicam" /><br><br>
Inserisci Username e Password per accedere alla connessione:<br>
<form method="post" action="$PORTAL_ACTION$">

        <input name="auth_user" type="text">
        <input name="auth_pass" type="password">
        <input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$">
        <input name="accept" type="submit" value="Accedi"> <br><br>

Se non possiedi i dati di accesso procedi alla
<a href="http://192.168.0.1:8000/captiveportal-registrazione_utente.html?redirurl=">  REGISTRAZIONE </a>
</form>
```

Sorgente di registrazione_utente.html:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta http-equiv="content-type"  content="text/html; charset=ISO-8859-1">
<title>registrazione_utente</title>
</head>
<body>
<form name="NomeForm" method="post" action="/captiveportal-inserisci_utente.php?redirurl=$PORTAL_REDIRURL$/" >
Inserisci un numero <br>
di cellulare valido (senza +39)         

        <input name="username" value="" type="text"> <br><br>

Inserisci il tuo nominativo nella <br> seguente forma: "Nome Cognome" 

        <input name="fullname" value="" type="text"><br><br>

La password per il tuo account verr&agrave; inviata al numero di cellulare fornito in precedenza. <br><br><br>


        <a href="http://192.168.0.1:8000/captiveportal-clausule.html?redirurl="> Leggi le condizioni del servizio </a> <br><br><br>

Procedendo con l'invio si accettano le condizioni sopra riportate.


        <input type="checkbox" name="ck" value="checkbox" onClick="document.NomeForm.Submit.disabled=! (this.checked); ">
        <input name="Submit" type="submit" disabled="true" value="Invia">

</form>
</body>
</html>
```

Codice sorgente di inserisci_utente.php:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>index</title>
</head>
<body>
<?php
require_once("config.inc");
require_once("functions.inc");
$username = $_POST['username']; //recupero il valore dal campo "nome" e lo metto in una variabile
$fullname = $_POST['fullname']; //recupero il valore dal campo "fullname" e lo metto in una variabile
echo "I dati inseriti sono:  <br> - Username: ".$username."<br> - Nome: ".$fullname."<br><br>"; //stampo a video i dati
// Due booleani di controllo
$account_creato = false; // l'account viene abilitato solo dopo la sua procedura
$errore = false; // l'errore di default è false
////////////////////////////////////////////
//////CONTROLLO DEI VALORI//
////////////////////////////////////////////
// controllo che nessun campo sia vuoto;
if( (!$username) || (!$fullname)) {
$errore = true;   // sollevo l'errore
echo " Non hai compilato tutti i campi! <a href=\"http://192.168.0.1:8000\">Torna indietro</a> ";
exit;
}
// controllo che il num di cellulare sia di 10 cifre e che sia un numero
$lungh_username=strlen($username);
if (($lungh_username != 10) || (is_bool($username)) || (is_float($username))) {
$errore = true;   // sollevo l'errore
echo " Non hai inserito un numero di cellulare valido! <a href=\"http://192.168.0.1:8000\">Torna indietro</a> ";
exit;
}
// controllo che "fullname" non deve essere un intero,un float,un booleano e maggiore di 20 caratteri
$lungh_fullname=strlen($fullname);
if (($lungh_fullname > 20) || (is_int($fullname)) || (is_float($fullname)) || (is_bool($fullname))){
$errore = true;   // sollevo l'errore
echo " Non hai inserito un nominativo valido! <a href=\"http://192.168.0.1:8000\">Torna indietro</a> ";
exit;
}
// se i controlli sono giusti arriva qui
else {
////////////////////////////////////////////
// GENERIAMO UNA PASSWORD DI 5 CIFRE ////////
////////////////////////////////////////////
function unaPasswordACaso() {
// setto la gamma di caratteri per generare la password
// attenzione - la l (L) e 1 (uno) nel risultato possono essere simili
// si possono togliere entrambi dalla stringa seguente
$gammaDeiCaratteri = "abcdefghiljkmnopqrstuvwxyz0123456789";
// inizializzo il generatore di numeri casuali
// la riga seguente può essere saltata se si usa PHP 4.2.0 o superiore
srand((double)microtime()*1000000);
// inizializzo la variabile $elaborazione
$elaborazione = '' ;
// in questo ciclo estraggo fino a 5 caratteri in modo casuale
// dalla variabile $gammaDeiCaratteri
// per modificare la lunghezza della password cambiare il numero 5
// con la lunghezza desiderata
for ($contatore=0; $contatore<5; $contatore++) {

        // prendo un numero casuale da 0 a strlen($gammaDeiCaratteri)-1
        // si parte da 0
        $numeroCasuale = rand(0, strlen($gammaDeiCaratteri)-1);
        // prendo dalla variabile $gammaDeiCaratteri un solo carattere
        // che è posizionato al numero $numeroCasuale
        // se per esempio il $numeroCasuale risultante è 4 il carattere
        // che prendero è "e"
        $carattere = substr($gammaDeiCaratteri, $numeroCasuale, 1);
        // aggiungo a $elaborazione il carattere risultante
        // mediante la concatenazione
        $elaborazione = $elaborazione . $carattere;
        }

// ritorn la stringa elaborata che conterrà una password casuale
return $elaborazione;
}
// chiamata della funzione e utilizzo
if ($errore == false) {
$password_generata = unaPasswordACaso();
}
```

```
//////////////////////////////////////
// SCRITTURA SU FILE //
//////////////////////////////////////
// acquistico data e ora
$data=date("Y m d");
$ora=date("H i s");
$write_file = fopen("/datiform.txt","a+");
$testolog= " ".$data."; ".$ora."; ".$username."; ".$fullname."; ".md5($password_generata)."  \n\n";
fwrite($write_file,$testolog);
fclose($write_file);
}
//////////////////////////////////////
// ACCOUNTING //
//////////////////////////////////////
if ($errore == false){
if (!is_array($config['captiveportal']['user'])) {

        $config['captiveportal']['user'] = array();

}
$a_user = &$config['captiveportal']['user'];
$id = "10"; // vecchio valore da POST
if (isset($id) && $a_user[$id]) {

        $pconfig['username'] = $a_user[$id]['name'];
        $pconfig['fullname'] = $a_user[$id]['fullname'];
        $pconfig['expirationdate'] = $a_user[$id]['expirationdate'];

}
if (isset($id) && $a_user[$id])

        $userent = $a_user[$id];

$userent['name'] = $username;
$userent['fullname'] = $fullname;
$userent['expirationdate'] = "";
$userent['password'] = md5($password_generata);
if (isset($id) && $a_user[$id])  $a_user[$id] = $userent;
else

        $a_user[] = $userent;

write_config();
$account_creato = true;
}
//////////////////
//  INVIO SMS //
//////////////////
// se non ci sono stati errori e se è stato creato l'account allora manda l'sms
if ($errore == false && $account_creato == true){

        echo "...attendere l'inoltro dell'sms al proprio cellulare...<br>";

// Imposto le variabili per l'autenticazione
$usernamesms = "●●●●●";
$passwordsms = "●●●●●";
// imposto altri dati
$type_user = "admin";
$route = "GW1"; // GW2 se si vuole il mittente personalizzato
$destinatario = "+39".$username;
$destinatario_corto = $username;  // sarebbe il numero del destinatario senza il +39
$messaggio = "Benvenuto+in+Hotspot,il+suo+username+è:+$destinatario_corto+e+la+sua+password+è:+$password_generata+.
+Se+non+fosse+interessato+al+servizio,ignorare+questo+messaggio";
// Compongo la url per l'invio del messaggio
$stringa = "https://www.totalconnect.it/send_sms/register.php?username=".$usernamesms;
$stringa .= "&password=".$passwordsms;
$stringa .= "&type_user=".$type_user;
$stringa .= "&route=".$route."&message=".$messaggio."&to=".$destinatario;
// Leggo la URL e determino l'esito dell'invio
$contents = file($stringa);
$risposta = trim(implode("",$contents));
echo $risposta."<br>";
// in presenza di errori con il gateway sms
if ($errore == false && $account_creato == true){
echo "<a href=\"http://192.168.0.1:8000\">Torna indietro ed inserisci le credenziali</a> <br>";
}
?>
</body>
</html>
```

Esempio di condizioni di utilizzo ed informativa del servizio hotspot:

Informativa ai sensi del D. Lgs. 30 giugno 2003, n. 196 sulla tutela dei dati personali

Gentile Utente, ti informiamo che per le finalità connesse alla fornitura del Servizio, la ditta XXXX di XXXX, P.IVA 0123456789, con sede a XXXXXXX, Via XXXXX 11, esegue il trattamento dei dati da Lei forniti, o comunque acquisiti in sede di esecuzione del Servizio.

Il titolare del trattamento è XXXXXX nella persona di XXXXXX. L'elenco dei responsabili del trattamento dei dati personali e dei terzi destinatari di comunicazioni è disponibile presso gli uffici di XXXXXX. Il trattamento dei dati avviene con procedure idonee a tutelare la riservatezza dell'Utente e consiste nella loro raccolta, registrazione, organizzazione, conservazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione, distruzione degli stessi comprese la combinazione di due o più delle attività suddette. Il trattamento dei dati, oltre alle finalità connesse, strumentali e necessarie alla fornitura del Servizio sarà finalizzato a: a) comunicare i dati a Società che svolgono funzioni necessarie o strumentali all'operatività del Servizio e/o gestiscono banche dati finalizzate alla tutela dei rischi del credito e accessibili anche a Società terze anche al di fuori del territorio dell'Unione Europea; b) raccogliere dati ed informazioni in via generale e particolare sugli orientamenti e le preferenze dell'Utente; inviare informazioni ed offerte commerciali, anche di terzi; inviare materiale pubblicitario e informativo; effettuare comunicazioni commerciali, anche interattive; compiere attività dirette di vendita o di collocamento di prodotti o servizi; elaborare studi e ricerche statistiche su vendite, clienti e altre informazioni, ed eventualmente comunicare le stesse a terze parti; cedere a terzi, anche al di fuori del territorio dell'Unione Europea, i dati raccolti ed elaborati a fini commerciali anche per la vendita o tentata vendita, ovvero per tutte quelle finalità a carattere commerciale e/o statistico lecite. Il conferimento del consenso al trattamento dei propri dati personali da parte dell'Utente è facoltativo. In caso di rifiuto del trattamento dei dati personali di cui alla lettera b) il trattamento sarà limitato all'integrale esecuzione degli obblighi derivanti dalla fornitura del Servizio, nonché all'adempimento degli obblighi previsti da leggi, regolamenti e normativa comunitaria. In caso di rifiuto del trattamento dei dati personali di cui alla lettera a) XXXXXXX non potrà fornire il Servizio. Il trattamento dei dati dell'Utente per le finalità sopraindicate avrà luogo prevalentemente con modalità automatizzate ed informatizzate, sempre nel rispetto delle regole di riservatezza e di sicurezza previste dalla legge. I dati saranno conservati per i termini di legge presso XXXXXX e trattati da parte di dipendenti e/o professionisti da questa incaricati, i quali svolgono le suddette attività sotto la sua diretta supervisione e responsabilità. A tal fine, i dati comunicati dall'Utente potranno essere trasmessi a soggetti esterni, anche all'Estero, che svolgono funzioni strettamente connesse e strumentali all'operatività del Servizio. Ti informiamo, inoltre, che, ai sensi dell'art. 7 del D. Lgs. 30 giugno 2003, n. 196, il Cliente ha il diritto di opporsi, in tutto o in parte, per motivi legittimi, al trattamento e può, secondo le modalità e nei limiti previsti dalla vigente normativa, richiedere la conferma dell'esistenza di dati personali che lo riguardano, e conoscerne l'origine, riceverne comunicazione intelligibile, avere informazioni circa la logica, le modalità e le finalità del trattamento, richiederne l'aggiornamento, la rettifica, l'integrazione, richiedere la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati in violazione di legge, ivi compresi quelli non più necessari al perseguimento degli scopi per i quali sono stati raccolti, nonché, più in generale, esercitare tutti i diritti che gli sono riconosciuti dalle vigenti disposizioni di legge.

Esempio di condizioni generali di contratto del servizio delegato a ditta esterna:

1. OGGETTO: Le presenti condizioni generali hanno per oggetto le norme per l'abbonamento al Servizio HotSpot Wireless, o come in futuro ridenominato, il quale è regolato, oltre che dalle presenti Condizioni Generali, dalla Richiesta di adesione al Servizio. Il Servizio offerto da XXXXXX di XXXXXX consiste in un accesso alla rete Internet attraverso un collegamento senza fili, altresì detto Wi-Fi (Wireless Fidelity). XXXXXX si riserva la facoltà di ampliare e modificare la gamma delle funzionalità offerte all'interno del Servizio, qualora, alla luce delle specifiche delle eventuali nuove funzionalità, sia necessaria un'integrazione alle presenti Condizioni Generali e alla Richiesta di adesione al Servizio, o un loro adeguamento, XXXXXX comunicherà le suddette innovazioni in modo opportuno. XXXXXX si riserva la facoltà di modificare le caratteristiche delle funzionalità del Servizio o eliminarne alcune. 2. DURATA DEL CONTRATTO: L'abbonamento al Servizio ha durata indeterminata salvo revoca da comunicare, per entrambe le parti, via email con un preavviso minimo di 30 giorni. 3. ATTIVAZIONE E SOSPENSIONE: Il contratto si perfeziona nel momento in cui XXXXXX fornisce il Servizio sulla base dell'accettazione on line delle condizioni di contratto da parte dell'utente. In caso di mutamento delle condizioni tecniche e normative per la fornitura del Servizio, XXXXXX avrà il diritto potestativo di sospendere in qualsiasi momento la fornitura del Servizio con un preavviso di quindici giorni notificato via posta elettronica all'indirizzo collegato al presente contratto di abbonamento. 4. RISERVATEZZA: L'accesso al Servizio è consentito mediante un codice di identificazione cliente (UserID) e una parola chiave (Password), tali elementi identificativi saranno unici per tutte le funzionalità ricomprese nel Servizio. Il cliente è tenuto a conservare la password con la massima diligenza, mantenendo segreti per tutta la durata dell'abbonamento sia il codice che la parola chiave. Inoltre, il cliente è tenuto a prestare la stessa diligenza con riferimento agli elementi identificativi delle ulteriori identità dell'abbonamento di cui è titolare eventualmente attivate. Il cliente sarà pertanto esclusivamente responsabile di qualsiasi danno causato dalla conoscenza, ovvero dall'utilizzo, della password o della UserID, anche delle eventuali multidentità attivate, da parte di terzi. Il cliente si impegna a comunicare immediatamente a XXXXXX l'eventuale furto, smarrimento, perdita ovvero appropriazione a qualsivoglia titolo da parte di terzi della password o UserID, anche con riferimento alle eventuali multidentità attivate. 5. GARANZIE: Il cliente garantisce che qualunque materiale o messaggio eventualmente immesso in aree pubbliche di XXXXXX riconducibile allo stesso in virtù della sottoscrizione del contratto è di propria titolarità e/o nella propria disponibilità giuridica, in difetto obbligandosi il cliente a manlevare e tenere indenne l'XXXXXX da ogni eventuale conseguenza pregiudizievole. Il cliente inoltre garantisce che detto materiale non viola o trasgredisce alcun diritto di autore, marchio di fabbrica, brevetto o altro diritto derivante dalla legge, dal contratto e dalla consuetudine. Il cliente prende inoltre atto del fatto che è vietato servirsi o dar modo ad altri di utilizzare il Servizio contro la morale e l'ordine pubblico o con lo scopo di recare molestia alla quiete pubblica o privata, di recare offesa, o danno diretto o indiretto a chicchessia e di tentare di violare comunque il segreto dei messaggi privati. Più in particolare è fatto espresso divieto per il cliente di utilizzare tecniche di "mail spamming" o equivalenti (invio di messaggi di posta elettronica non sollecitati e/o senza espressa autorizzazione del destinatario di qualsivoglia contenuto e verso qualsivoglia destinatario). È comunque esplicitamente vietato utilizzare il Servizio per contravvenire in modo diretto o indiretto alle vigenti leggi dello Stato italiano o di qualunque altro stato. Fermo il diritto di XXXXXX di invocare la risoluzione automatica del contratto ai sensi del seguente art. 9, è altresì in facoltà dell'XXXXXX sospendere a propria discrezione il Servizio ogni qualvolta sussista ragionevole evidenza di una violazione degli obblighi del cliente. 6. UTILIZZO DELL'ABBONAMENTO: Il cliente potrà utilizzare l'abbonamento secondo le specifiche relative ad ogni funzionalità. In particolare, la funzionalità Accesso potrà essere adoperata per un singolo accesso, non potranno essere effettuati più collegamenti contemporanei. Il sistema connesso a XXXXXX non potrà in nessun caso avere funzioni di raccolta di più utenti (LAN). In ogni caso, è espressamente esclusa la possibilità di cedere il contratto di abbonamento a terzi, a titolo gratuito o oneroso, temporaneamente o definitivamente, senza il consenso scritto di XXXXXX. 7. DOCUMENTAZIONE E IDENTIFICAZIONE CLIENTE: Con riferimento alle funzionalità che richiedono il collegamento in rete, il cliente prende atto e accetta l'esistenza del registro elettronico del funzionamento del Servizio (il Log), compilato e custodito a cura di XXXXXX. Il contenuto del Log ha il carattere della riservatezza assoluta e potrà essere esibito solo ed esclusivamente su richiesta delle Autorità competenti. Al fine di identificare con certezza la provenienza della connessione, il cliente prende atto del fatto che XXXXXX identifica l'utente nel momento del collegamento alla rete HotSpot Wireless mediante il numero identificativo del proprio telefono cellulare. 9. CLAUSOLA RISOLUTIVA ESPRESSA: In tutti i casi di inadempimento delle obbligazioni di cui agli art. 4,5,6,7 al presente contratto, XXXXXX avrà la facoltà di risolvere il presente contratto ai sensi dell'art.1456 c.c., fatta salva, in ogni caso, azione di rivalsa e risarcimento per i danni subiti. Il diniego e/o la revoca dall'abbonato al trattamento dei propri dati darà facoltà a XXXXXX di considerare risolto di diritto il presente contratto. 10. COMUNICAZIONI: Tutte le comunicazioni relative al contratto andranno inviate agli indirizzi di posta elettronica forniti dal cliente o predisposti da XXXXXX per il Servizio HotSpot Wireless.

In alternativa, per una attività che non fornisce connettività quale attività principale, è possibile inserire una informativa più snella e quindi più elastica:

Informativa ex art. 13 d. lgs. 196/2003

1. INDICARE IL SOGGETTO (DITTA + l'indirizzo e la partita IVA. Poi basta solo DITTA), come titolare del trattamento dei dati personali, ai sensi dell'art. 13 del d.lgs. 196/2003, informa che i dati personali riguardanti il Cliente, saranno trattati per finalità contrattuali, connesse o strumentali all'esecuzione delle prestazioni dedotte nel presente contratto di fornitura del Servizio in oggetto. In particolare la (DITTA) potrà compiere le suddette operazioni per: 1. dare esecuzione al Servizio richiesto dal Cliente, con tutte le eventuali attività connesse ed accessorie; 2. gestione gli adempimenti di carattere amministrativo-contabile, secondo quanto previsto dalle norme di legge vigenti in materia; 3. adempiere ad eventuali obblighi di legge compresa la collaborazione eventuale con le autorità giudiziarie e/o amministrative; 4. la comunicazione degli stessi dati alla rete di rivenditori e/o agenti della (DITTA) per fini amministrativi, tecnici e gestionali, qualora il contratto sia concluso per tramite di uno di essi. Inoltre, previo consenso, per: 5. iniziative di informazione commerciale e di marketing diretto da parte della (DITTA), nonché allo scopo dell'invio di proposte commerciali relative a servizi forniti dal medesimo o da altri partner commerciali. Un eventuale rifiuto a fornire i dati personali, dal parte del Cliente, relativamente ai punti 1 - 4, può comportare il mancato adempimento contrattuale da parte della (DITTA) o degli adempimenti di legge ad esso connessi. Per il punto 5 il consenso è invece facoltativo. Il trattamento dei dati avverrà mediante strumenti idonei a garantire la sicurezza nonché la riservatezza e potrà essere effettuato anche tramite l'ausilio di strumenti elettronici. 1.b. Il Cliente, interessato del trattamento dei dati personali, ha diritto ad esercitare i diritti di cui all'art. 7 del d.lgs. 196/2003 ed, in particolare, tra gli altri, di ottenere copia dei dati trattati, il loro aggiornamento, la loro rettifica o integrazione, la loro cancellazione, la trasformazione in forma anonima o il blocco per i trattamenti in violazione di legge. 1.c. La (DITTA), come titolare del trattamento, comunica che la lista completa e aggiornata di eventuali soggetti nominati responsabili è disponibile presso di sé. 1.d. I dati del Cliente potranno essere comunicati agli istituti di credito per l'effettuazione di pagamenti, alla compagnie assicurative per eventuali responsabilità per danni, ai professionisti commerciali e legali per finalità di consulenza, per obblighi fiscali, nonché per la tutela dei propri diritti in sede giudiziale e/o stragiudiziale. 1.e. La (DITTA) conserva i dati relativi al traffico telematico, per finalità di accertamento e repressione dei reati, a norma dell'art. 132 del d.lgs. 196/2003 (c.d. data retention).

Ringraziamenti

Desidero innanzitutto ringraziare il Prof. Fausto Marcantoni per la pazienza e per i preziosi insegnamenti durante tutto il periodo di studi, sempre figura di riferimento e grande disponibilità per la realizzazione della mia tesi.

Inoltre, ringrazio sentitamente la Prof. Maria Concetta De Vivo per il materiale e le delucidazioni sulla sezione giuridica.

Intendo poi ringraziare tutto il corpo docente che in questi anni ha contribuito a rendermi un informatico più competente.

Sottolineo la particolare disponibilità dei Dott.ri Francesco Maccari e Marco Maccari per avermi fornito materiale e servizi indispensabili per la realizzazione della tesi.

Credo sia doveroso ringraziare il Dott. Pietro Tapanelli per la revisione dell'informativa legale sul servizio hotspot.

Per la disponibilità di avermi fornito un account con dei sms prepagati ringrazio lo spin off e-Lios S.r.l.

Inoltre, vorrei esprimere la mia sincera gratitudine a tutti i miei compagni di corso, in particolare Andrea, David, Giacomo, Gabriele, Riccardo, Michele, Matteo, Fabrizio, Carlo ed Alessandro, per i bei momenti trascorsi dentro e fuori l'ambito accademico.

Ringrazio la mia splendida fidanzata Miriam, per il sostegno morale ed affettivo nei miei confronti con la sua spontanea dolcezza.

Infine, ovviamente, ho desiderio di ringraziare con affetto i miei genitori e mia sorella, senza i quali non sarei mai potuto giungere a questo punto, non solo per il sostegno economico, che sicuramente è stato fondamentale, ma per quell'aiuto, a volte tacito e a volte esplicito, indispensabile per superare i numerosi ostacoli incontrati nel cammino della vita e tutti quei momenti di stress, ansia e nervosismo che ne fanno parte.

Bibliografia

[1] Autori Vari, *pfSense Documentation site*, 2011 , http://doc.pfsense.org/index.php/Main_Page

[2] Sito ufficiale della distribuzione pfSense, *pfSense is a free open source customized distribution of FreeBSD tailored for use as a firewall and router*, http://www.pfsense.org

[3] Christopher M. Buechler and Jim Pingle , *The Definitive Guide to the pfSense Open Source Firewall and Router Distribution*, 2009 , Based on pfSense Version 1.2.3

[4] Official Forum pfSense, http://forum.pfsense.org/

[5] Comunità italiana di freeBSD, http://www.freebsd.org/it

[6] http://www.freebsd.org/doc/it/books/handbook/index.html

[7] Realizzazione di un firewall con pfSense, Stefano Sasso, http://www.pluto.it/files/journal/pj0704/pfsense.html

[8] *Build Your Own IDS Firewall With pfSense*, Greg Noel , 2 Febbraio 2011, http://www.smallnetbuilder.com/security/security-howto/31406-build-your-own-ids-firewall-with-pfsense

[9] Zeroshell & PFSense, iw5ek, 9 Luglio 2010, http://www.arezzonair.it/index.php?option=com_content&view=article&id=122:zeroshell-a-pfsense&catid=1:ultime&Itemid=50

[10] Interlex Diritto Tecnologia Informazione, http://www.interlex.it/index.htm

[11] Materiale didattico di sicurezza informatica, Prof.ssa Maria Concetta De Vivo, 2011, Università degli Studi di Camerino

[12] Wi-Fi, abolizione della Pisanu in Gazzetta Ufficiale , 22 Dicembre 2010 , Martina Pennisi , http://daily.wired.it/news/politica/wi-fi-libero-tutti.html

[13] 10 cose da sapere sul Wi-Fi (dopo l'abolizione della Pisanu), 31 Dicembre 2010, Martina Pennisi, http://daily.wired.it/news/internet/addio-pisanu-wifi-2011.html?page=1#content

[14] Gazzetta Ufficiale N. 173 del 27 Luglio 2005 , DECRETO-LEGGE 27 luglio 2005, n.144 , Misure urgenti per il contrasto del terrorismo internazionale, http://gazzette.comune.jesi.an.it/2005/173/1.htm

[15] *5 Open Source Wi-Fi Hotspot Solutions*, 7 giugno 2010, Eric Geier, http://www.linuxplanet.com/linuxplanet/reports/7087/1/

[16] Modificato il Decreto Pisanu: cosa cambia per gli hotspot Wi-Fi, 22 Gennaio 2011, http://www.wispot.it/blog/modificato-decreto-pisanu-cosa-cambia-hotspot-wifi/

[17] Wifi: nuova normativa 2011, Ing. Alberto Bellettato, http://www.innovationquality.it/nuovanormativawifi2011

[18] Sms Authentication: dieci cose da sapere prima di scegliere, Marco Costa, 11 Ottobre 2010, http://www.bancaemercati.com/sito/?p=978

[19] Come Integrare Gli SMS Nelle Web Application Grazie Agli SMS Gateway, Daniele Di Gregorio, 6 febbraio 2009, http://www.ikaro.net/articoli/cnt/sms_web_applications-00740.html

[20] Prodotto di virtualizzazione VirtualBox, http://www.virtualbox.org/

[21] *A free lightweight network intrusion detection system for UNIX and Windows*, http://www.snort.org/

[22] *Proxy Server Squid*, www.squid-cache.org/

[23] Enciclopedia aperta gestita da editori volontari, http://www.wikipedia.org/

[24] *WPAD protocol*, http://www.acmeconsulting.it/Squid-Book/HTML/sec-wpad-protocol.html

[25] *Antivirus Open Source*, http://www.clamav.net/lang/en/

[26] *Network Time Protocol project*, http://www.ntp.org/

[27] *PHP Manual*, http://php.net/manual/en/index.php

Elenco delle figure

Elenco delle tabelle