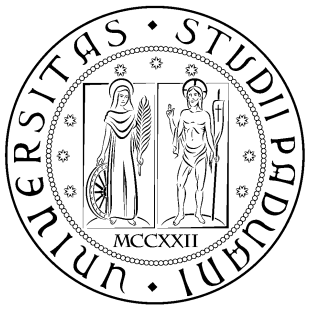
UNIVERSITÀ DEGLI STUDI DI PADOVA



Facoltà di Ingegneria

Corso di Laurea in Ingegneria delle Telecomunicazioni

Tesi di Laurea Triennale

Progettazione e configurazione di una rete LAN aziendale

RELATORE: Prof. Tomaso Erseghe

LAUREANDO: Davide Merzi

Padova, 25 Luglio 2013

Indice

Introduzione

Nella presente tesi verranno illustrati i procedimenti di progettazione e revisione della rete LAN dell'azienda Tech.Pa S.p.A. con relative configurazioni degli apparati e scelte software e hardware.

Nel primo capitolo è stata fornita una breve descrizione dell'azienda Tech.Pa, sede del tirocinio, e sono stati stabiliti gli obiettivi da raggiungere, tra cui l'implementazione di un firewall con la funzionalità di URL-filtering e la creazione e gestione di una VPN.

Nel secondo capitolo viene fatto un cenno storico sulla nascita delle reti LAN e successivamente una descrizione della tecnologia Ethernet dal punto di vista funzionale e materiale (cavi, connettori, prese ecc...); sono stati poi scelti gli apparati e l'indirizzamento IP dei dispositivi.

Nel terzo capitolo vengono presentati i criteri per la scelta sia del server aziendale che del sistema operativo e relativa configurazione. Sono stati inoltre stabiliti i tipi di backup del sistema con relativi software.

Nel quarto capitolo si procede alla scelta di un firewall per l'azienda con relativa descrizione della sua configurazione e delle problematiche relative all'implementaizone di un sistema di filtraggio del traffico web, con particolare attenzione per la modifica del sistema nanofreeBSD per poter accettare una blacklist.

Infine trovano spazio le conclusioni e gli sviluppi futuri.

In appendice possiamo trovare vari approfondimenti sui software e/o termini tecnici più importanti trattati nel corso di questa tesi.

Capitolo 1

Luoghi e obiettivi del tirocinio

1.1 Cenni storici relativi all'azienda Tech.Pa S.p.A.

Tech.Pa S.p.A. (fino al 2000 chiamata FI.PA.) nasce nel 1990 a Verona con l'obiettivo di diventare un punto di riferimento per l'automazione industriale, principalmente nel settore alimentare. Inizialmente si specializza nella realizzazione di impianti di formatura, cottura e confezionamento di prodotti alimentari, iniziando importanti collaborazioni con alcuni tra i leader italiani del settore.

Nel 2000 inizia a collaborare con ABB per l'installazione di robot antropomorfi e *pick and place*, espandendo le proprie competenze anche in questo campo.

Nel 2008 una sua applicazione viene scelta come rappresentante dell'Italia nella manifestazione organizzata in Svezia da ABB, in cui vengono presentati tutti i progetti più innovativi a livello mondiale eseguiti con i loro robot.

Nel 2009 Tech.PA S.p.A. esegue due importanti acquisizioni: la prima è un'azienda specializzata nella realizzazione di alimentatori switching, interfacce passive e a relé, la seconda è un'azienda specializzata nella realizzazione di quadri a certificazione UL e quindi destinati al mercato del Nord America.

Nel 2011, proseguendo il suo obiettivo di un sempre miglior servizio al cliente, si certifica ISO 9001:2008. Oggi può contare su 23 dipendenti, tra cui 6 ingegneri, ed una sede produttiva di 1.000 mq.

1.2 Descrizione della situazione iniziale e problematiche relative

Il problema iniziale è stato capire lo stato della rete, soprattutto per quanto concerne la topologia, in quanto questa è stata implementata e aggiornata durante gli anni di espansione e sviluppo dell'azienda.
All'inizio del tirocinio non sono stati forniti documenti e schemi relativi alla rete, ma con l'aiuto del titolare e dell'ing. Damiano Pasetto è stato possibile stabilire lo stato dell'arte iniziale nonchè definire gli obiettivi del lavoro.

Con l'utilizzo del programma LaNScan è stato possibile ottenere una lista di macchine e apparati presenti in azienda e relativo indirizzo IP associato, mentre per l'idividuazione dei cavi si è stato utilizzato uno strumento apposito chiamato *Network CableTracker* mostrato in Figura 1.1, di cui possiamo vedere le caratteristiche in Appendice. In Figura 1.2 si può notare come le risorse condivise siano decentrallizzate e senza un server: sviluppare un sistema di controllo accesso alle risorse basato sull'utente sarebbe quindi complicato da implementare e non elegante.

In Figura 1.3 possiamo notare lo stato del nodo principale prima della revisione della rete.

1.3 Richieste ed esigenze dell'azienda

Una volta stabilito lo stato della rete è stato pianificato come affrontare l'upgrade e le esigenze richieste sono risultate le seguenti:

- Creare un centro stella unico per la rete;
- Stesura di nuovi cavi cat.6 per ogni postazione;

- Installazione e configurazione di un nuovo server;
- Centralizzazione delle risorse condivise;
- Installazione di un firewall con servizio VPN per i dipendenti;

Figura 1.1: Cable Tracker

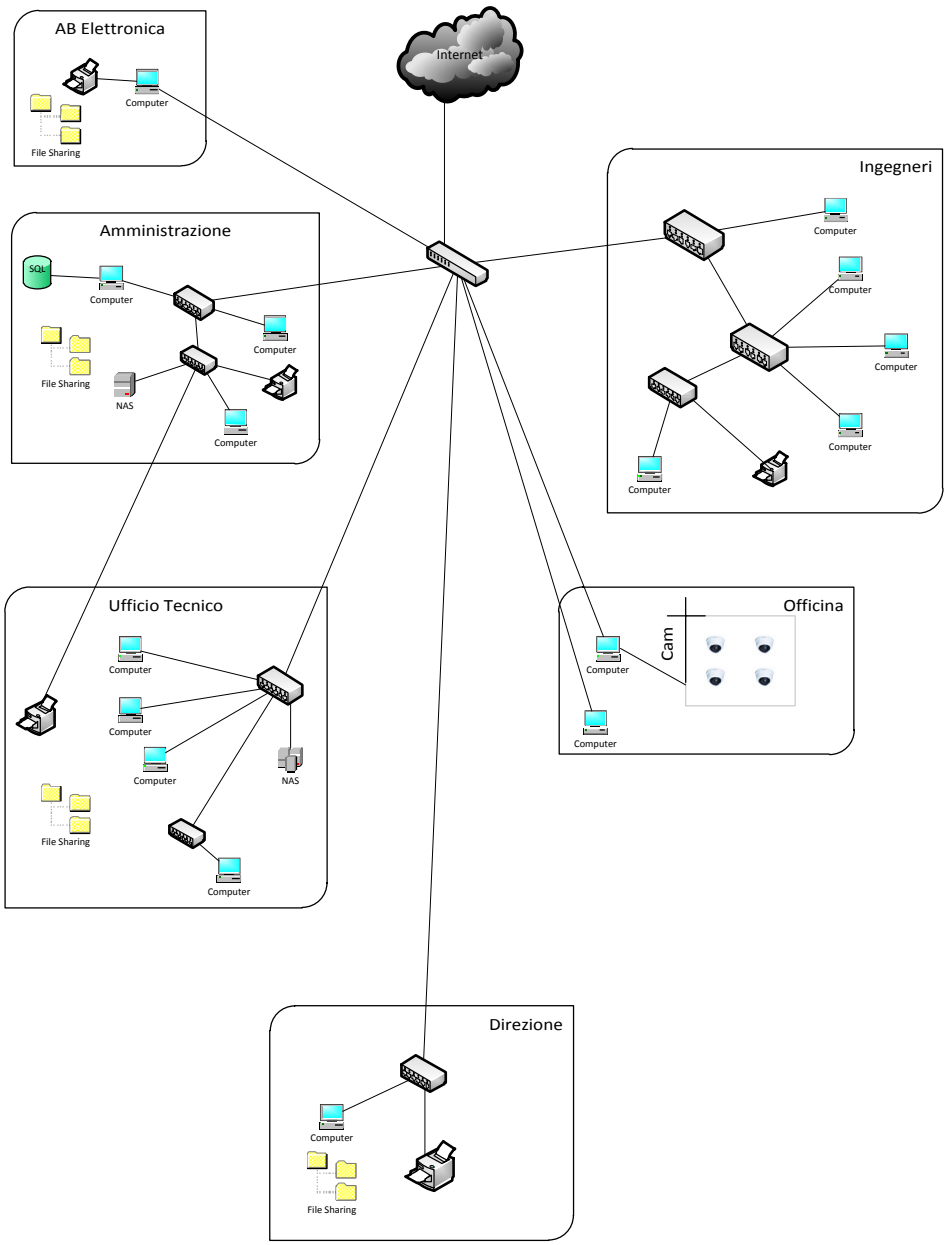


Figura 1.2: Situazione iniziale e distribuzione delle risorse

Figura 1.3: Nodo principale della rete

Capitolo 2

Le reti LAN

L'implementazione classica di LAN è quella che serve ad esempio un'abitazione o un'azienda all'interno di un edificio, o al massimo più edifici adiacenti fra loro. Quindi l'estensione territoriale limitata di una LAN favorisce la velocità di trasmissione dati, che inizialmente era tra i 10 Mbps e i 100 Mbps mentre le LAN più recenti operano fino a 10 Gbps presentando anche bassi ritardi e pochissimi errori.

2.1 Classificazione delle tecnologie

La tecnologia più popolare delle reti locali,che a oggi è la più diffusa, è chiamata **Ethernet**, sviluppatasi molto nel corso degli anni, in seguito verrando descritte le principali tecnologie disponibili. sectionEthernet La sua storia è iniziata nei primi anni '70 alle isole Hawaii, che all'epoca non avevano ancora un sistema telefonico funzionante. L'assenza di telefoni rendeva la vita più piacevole per i turisti, ma non per il ricercatore Norman Abramson e i suoi colleghi della università delle Hawaii che tentavano di collegare al computer principale di Honolulu gli utenti situati su isole remote. La posa nell'oceano di cavi dedicati era impensabile così cercarono una soluzione alternativa.

L'unica soluzione trovata fu la trasmissione a radio a bassa potenza. Il terminale di ciscun utente fu equipaggiato con un una piccola radio a 2 fre-

quenze: upstream verso il computer centrale e downstream dal computer centrale. Quando l'utente voleva collegarsi al computer, trasmetteva nel canale upstream un pacchetto contenente i dati. Se in quel momento nessun altro stava trasmettendo, il pacchetto probabilmente sarebbe arrivato a destinazione e confermato sul canale di downstream. In caso di non ricezione del riscontro il terminale avrebbe assunto che il pacchetto trasmesso fosse andato perso o colliso con un altro pacchetto, quindi ritentato la trasmissione. Questo sistema chiamato ALOHANET, funzionava decisamente bene in situazioni di di basso traffico ma le prestazioni diminuivano fortemente in caso di alto traffico.

All'incirca nello stesso periodo un dottorando chiamato Bob Metcalfe otteneva la laurea al M.I.T (*Massachusetts Institute of Technology*) e si trasferiva ad Harvard per ottenere il Ph.D. Durante i suoi studi conobbe il lavoro di Abramson e ne fu così entusiasta che dopo il Ph.D. decise di trascorrere l'estate alle Hawaii per lavorare con Abramson, prima di iniare il suo nuovo lavoro al PARC (*Palo Alto Research Center*) di Xerox. Quando arrivò al PARC, vide che i ricercatori avevano progettato e costruito ciò che in seguito presero il nome di Personal Computer ma questi computer erano isolati fra loro. Nel 1976 utilizzando quello che aveva imparato con il lavoro di Abramson e insieme al collega David Boggs progettò la prima rete locale.

Questa rete venne chiamata **Ethernet** citando *luminiferous ether* [3], mezzo attraverso cui un tempo gli scienziati immaginavano che si propagasse la radiazione elettromagnetica. Il mezzo trasmissivo non era il vuoto ma un cavo coassiale a grande diametro (*thick*), lungo fino a 2,5 Km con ripetitori ogni 200 metri. AL sistema si potevano collegare fino a 256 computer, tramite transceiver applicati al cavo. Il sistema fuznionava a 2,94 Mbps, e un esempio di questa tecnologia la possiamo vedere in Figura 2.1.

Ethernet offriva una importante miglioria rispetto all'ALHOANET: prima di trasmettere il dispositivo collegato al cavo ascolta la portante per verificare se qualcun altro sta già trasmettendo e in caso affermativo attende la fine della trasmissione poi tenta la trasmissione. Questo protocollo

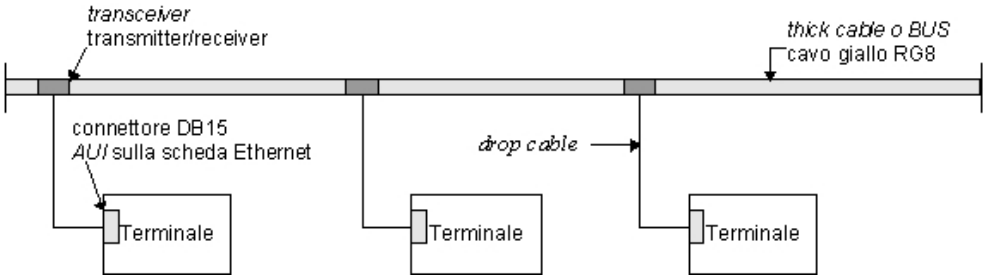


Figura 2.1: Bus Ethernet

venne chiamato **CSMA/CD** (*Carrier Sense Multiple Access with Collision Detection*).

Ethernet ebbe così successo che Intel e Xerox misero a punto nel 1978 uno standard per la versione a 10 Mbps, chiamato **DIX** che nell'1983 diventò lo standard IEEE 802.3.

Ethernet non è l'unico standard per le LAN; il comitato IEEE (*Institute of Electrical and Electronic Engineers*) ha standardizzato ache **token bus** (802.4), sviluppato da General Motors e **token ring** (802.5) sviluppato da IBM. Comunque ai nostri giorni Ethernet è la più diffusa.

Con il crescere della richiesta di velocità e capacità di banda, differenti gruppi industriali proposero due nuove LAN ottiche basate su tecnologie ad anello. Una fu chiamata **FDDI** (*Fiber Distributed Data Interface*) e l'altra fu chiamata **Fibre Channell**. Queste tecnologie portarono un aumento della velocità ma anche una crescita del costo degli apparati hardware in quanto più complessi e costosi. Fu così che nel 1992 IEEE riunì il comitato 802.3 dando il mandato di creare una LAN più veloce ma con costi contenuti.Il comitato 802.3 decise di procedere verso la definizione di una Ethernet semplicemente ottimizzata pre tre motivi fondamentali:

1. mantenere la compatibilità con le LAN Ethernet esitenti

2. il timore che un nuovo protocollo avrebbe potuto creare problemi imprevisti

3. il desiderio di raggiungere l'obiettivo prima che la tecnologia cambiasse.

Il lavoro fu svolto velocemente e il risultato, **802.3u**, fu approvato ufficialmente dall'IEEE nel giugno del 1995. Tecnicamente questo standard non è nuovo, ma si può considerare un'aggiunta allo standard 802.3 esistente per enfatizzare la retrocompabilità. In seguito questa nuova Ethernet fu chiamata da tutti **fast Ethernet** e non 802.3u.

Lo sviluppo dello standard fast Ethernet era stato appena ufficializzato quando il comitato 802.3 iniziò a lavorare a uno standard ancora più veloce del fast Ethernet, subito soprannominata **gigabit Ethernet**, con una capacità di banda fino a 1000 Mbps. Lo standard fu retificato dall'IEEE nel 1998 con il nome di 802.3z.

Gli obiettivi del comitato 802.3z erano essenzialmente gli stessi di quelli del comitato 802.3u: rendere Ethernet 10 volte più veloce mantenendo la compabilità con tutti gli standard Ethernet esistenti. Tutte le configurazioni Ethernet gigabit sono punto-punto, abbandonando il sistema multidrop dello standard 10 Mbps originale che oggi viene chiamato **Ethernet classico**. Nella configurazione più semplice di gigabit Ethernet è di due computer sono collegati direttamente fra loro. Il caso più comune, comunque, è dove uno switch o un hub si collegano a più computer e possibilmente ad altri switch o hub. In entrambe le configurazioni, ogni singolo cavo Ethernet è collegato a due e due soli dispositivi.

2.2 Cablaggio Ethernet

Relativamente alla rete Ethernet non solo la velocità nel corso del tempo è stata migliorata,come spiegato nel paragrafo precedente. Anche la tecnologia di cablaggio si è sviluppata ulteriormente. La più importante riguardava i tipi di cavi supportati. Un contendente era il doppino di categoria 3: a sui favore c'era il fatto che la maggior parte degli uffici del mondo occidentale, disponeva di almeno quattro doppini di categoria 3 o migliori collegati a una centralina telefonica distante non più di cento metri. Utilizzando questi

Nome	**Cavo**	**Lunghezza max. segmento**	**Vantaggi**
10Base5	Coassiale spesso	500 m	Cavo originale, ora obsoleto
100Base2	Coassiale sottile	185 m	Non occorre un hub
100Base-T4	Doppino intrecciato	100 m	UTP di categoria 3
100Base-TX	Doppino intrecciato	100 m	Full-duplex a 100 Mbps (UTP di cat.5)
1000Base-TX	Doppino intrecciato	100 m	Cat.6 o superiore
100Base-FX	Fibra ottica	2000m	Full-duplex a 100 Mbps; distanze elevate; immune alle interferenze

Tabella 2.1: I cavi fast Ethernet originali

doppini sarebbe stato possibile collegare con fast Ethernet i computer desktop senza ricablare l'intero edificio, con notevole risparmio per le aziende.

Lo svantaggio principale di questo doppino però è l'incapacità di trasportare segnali oltre i 100 m. Con cavi di categoria 5 questo problema si poteva aggirare. Il compromesso scelto fu di permettere tutte e tre le possibilità come mostrato in Tabella 2.1. Ad esempio la notazione **10Base5** è una specifica di livello fisico dello standard IEEE 802.3, caratterizzata da velocità di trasmissione di 10 Mbps in banda base e da segmenti di cavo di lunghezza non superiore ai 500 metri.

Un'altra importante evoluzione che ha avuto Ethernet nel corso degli anni è stato il connettore che permette di collegare il dispositivo alla rete. La prima versione prevedeva generalmente una **spina a vampiro**, spingendo con delicatezza uno spillo nel nucleo centrale del cavo coassiale come possiamo vedere in Figura 2.2. I primi tipi di connettori usati nello standard 10Base2

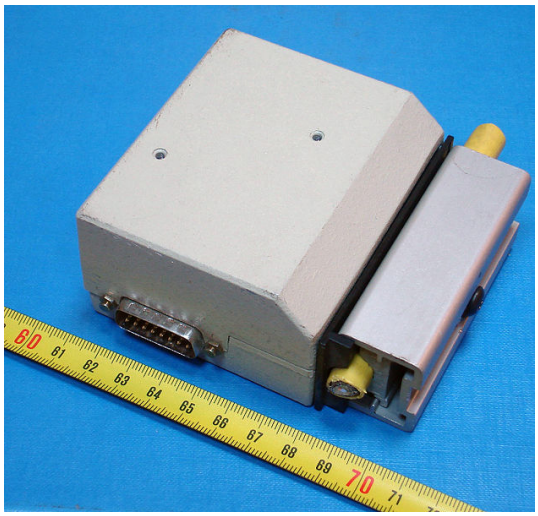


Figura 2.2: Spina a vampiro, standard 802.3 10Base5 [4]

invece sono stati i connettori **BNC** (*Bayonet Neill Concelman*), sono una famiglia di connettori unipolari a baionetta usati per l'intestazione di cavi coassiali. Possiamo vedere un'immagine in Figura 2.3. Infine il più moderno

Figura 2.3: Connettori BNC, standard 802.3 10Base2 [4]

e diffuso è il connettore **RJ-45**, mostrato in Figura 2.4, chiamati **8P8C** (8 posizioni e 8 contatti), che può essere utilizzato in varie applicazioni.

Figura 2.4: Connettori RJ-45, standard 100BaseT

Per le reti Ethernet cablate sono stati sviluppati 2 standard di cablaggio, EIA/TIA-568A ed EIA/TIA-568B, che differiscono fra di loro per l'inversione delle coppie 2 e 3. I due standard di cablaggio sono mostrati in Figura 2.5.

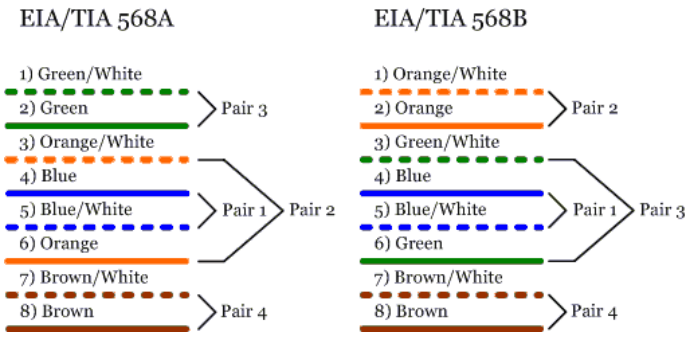


Figura 2.5: Standard EIA/TIA-568A ed EIA/TIA-568B

2.3 Scelta della tecnologia

Come visto nel paragrafo 1.3 caratteristica fondamentale che è stata richiesta dall'azienda è la velocità della rete, in quanto gli ingegneri e il personale dell'uffico tecnico lavorano con file di grandi dimensioni. Una rete a 100 Mbps non risultava quindi sufficiente ed è stato proposto di optare per una rete totalmente a 1 Gps.

La topologia, vista la possibilità di poter stendere tutti i cavi necessari, è stata a stella con un unico nodo centrale.

Un'altra scelta fondamentale è stata quella dei cavi. Per quanto riguarda il percorso dal nodo centrale alla presa a muro della postazione sono stati scelti cavi 1000Base-TX. Per quanto riguarda la schermatura, sono presenti varie tecnologie:

1. **UTP** è una sigla che sta per *Unschielded Twisted Pair* e che identifica un cavo composto da 4 coppie intrecciate di conduttori in rame.

2. **FTP** è invece l'acronimo di *Foiled Twisted Pair* ed identifica un cavo che, a differenza del cavo UTP, esternamente alle 4 coppie ha uno schermo composto da un foglio di materiale conduttore, generalmente alluminio.

3. **STP**, infine, è l'acronimo di *Shielded Twisted Pair*, un'ulteriore evoluzione del cavo FTP, nel quale sono avvolte da una schermatura anche le singole coppie, per un totale di cinque schermi.

Dato che in azienda sono presenti svariati disturbi di sorgenti elettriche e magnetiche si è optato per un cavo molto schermato, quindi STP di categoria 6.

L'unico punto in cui si sono usati cavi non schermati UTP è stato dal collegamento del patch pannel dell'armadio allo switch, comunque di categoria 5e e lunghezza massima di 50 cm.

Un esempio di questi tipi di cavi si può vedere in Figura 2.6.

Infine si è verificato che tutte le NIC dei dispositivi presenti fossero adatte a supportare un collegamento Gigabit Ethernet, in caso contrario è stata effettuata una sostituzione. Gli unici apparati presenti senza collegamento gigabit Ethernet sono stati 2 stampanti e un plotter, in quanto la sostituzione della NIC è risultata impossibile.

Figura 2.6: Cavi rispettivamente UTP, FTP, STP

2.4 Scelta degli apparati hardware

La rete, in quanto gigabit Ethernet, richiede apparati che supportino questa tecnologia, quindi la scelta più importante è stata quella dello switch principale.

Le postazioni previste, essendo in totale 31, hanno richiesto la scelta di uno switch a 48 porte. Il mercato offre svariati modelli di switch con queste particolari caratteristiche, quindi dopo aver richiesto il budget a disposizione per l'acquisto, l'attenzione si è focalizzata sul modello HP ProCurve 1810-48G 10/100/1000 Mbps con in più il supporto alle schede per il collegamento in fibra ottica. La scelta della fibra ottica risulta vincente perché, nel caso in cui l'azienda dovesse ampliarsi, non ci sarebbero problemi di capacità di banda e collegamento. In Figura 2.7 possiamo vedere la foto dello switch scelto.

Nella rete preesistente non era presente una zona di Wireless Area Network né per i dipendenti né per gli ospiti; in seguito viene mostrata una possibile ipotesi di configurazione futura:

1. Zona Wi-Fi protetta che permetta l'accesso a internet e alle risorse condivise sul server

2. Zona Wi-Fi guest protetta isolata dalla rete aziendale che permetta

Figura 2.7: HP ProCurve 1810-48G

solamente l'accesso a internet

Per la zona Wireless è stato proposto un Access Point, in particolare un CISCO Wireless-G Router con RangeBooster (Figura 2.8).

Figura 2.8: CISCO WRV210

2.5 Indirizzamento IP

Un'altra scelta importante è stata quella dell'indirizzamento IP degli apparati dell'azienda, in quanto inizialmente l'assegnagnazione degli indirizzi era stata fatta tramite un server DHCP senza nessuna regola impostata, rendendo difficile il riconoscimento degli apparati connessi e quindi una gestione macchinosa e talvolta impossibile. Come prima cosa quindi si è scelto di eliminare il servizio DHCP per gli apparati LAN e di impostare manualmete su ogni dispositivo presente sulla rete gli IP, così poi da avere una tabella con tutto registrato. Essendo una rete di piccole dimensioni la classe di indirizzi privati è stata la C del tipo con un range 192.168.1.0/24 in particolare l'idirizzo del gateway 192.168.1.1 e del server DNS 192.168.1.1 (per comodità). Per quanto riguarda la configurazione della zona Wi-Fi protetta riservata ai dipendenti si è scelto come SSID visibile **Wi-Fi Tech.Pa** e indirizzamento IP della classe C con rete 192.198.2.0/24 nattato sulla rete 192.168.1.0/24 sempre senza DHCP, e con protezione WPA2-PSK.

Per la rete riservata agli ospiti invece si è scelto come SSID **Wi-Fi Tech.Pa Guest** e come rete sempre la classe C ma con indirizzamento 192.168.3.0/24 e impostando una regola firewall in modo da bloccare l'accesso alla rete 192.168.1.0/24 e lasciando solo l'accesso a Internet. In que-s'ultimo caso si è abilitato un sever DHCP per facilitare la connessione alla rete e come chiave sempre una crittografia WPA2-PSK. Nella Tabella 2.2 viene mostrata una tabella generica riassuntiva dell'indirizzamento IP.

2.6 Schema finale

Di seguito possiamo vedere lo schema logico scelto per l'azienda Tech.Pa, dove vengono mostrati i device connessi alla rete e l'indirizzamento IP, mostrati in dettaglio nella Tabella 2.2.

In Figura 2.10, viene mostrata la situazione del nodo centrale della rete, sitemato in un armadio rack da 18 pollici.

Indirizzo IP	**Dispositivi**
192.168.1.1 - 192.168.1.10	Apparati rete e server
192.168.1.40 - 192.168.1.49	Telecamere e PC Officina
192.168.1.50 - 192.168.1.59	Dispositivi e PC Amministrazione
192.168.1.61 - 192.168.1.69	Dispositivi e PC Ufficio Tecnico
192.168.1.71	PC AB Elettronica
192.168.1.90 - 192.168.1.99	Stampanti e Plotter
192.168.1.100 - 192.168.1.200	Dispositivi e PC Ingegneri
192.168.1.250 - 192.168.1.253	Riservati Amministratore rete
192.168.2.100 - 192.168.2.250	Rete WiFi Tech.Pa (Opzionale)
192.168.3.100 - 192.168.3.250	Rete WiFi Ospiti (Opzionale)

Tabella 2.2: Indirizzamento IP Tech.Pa.

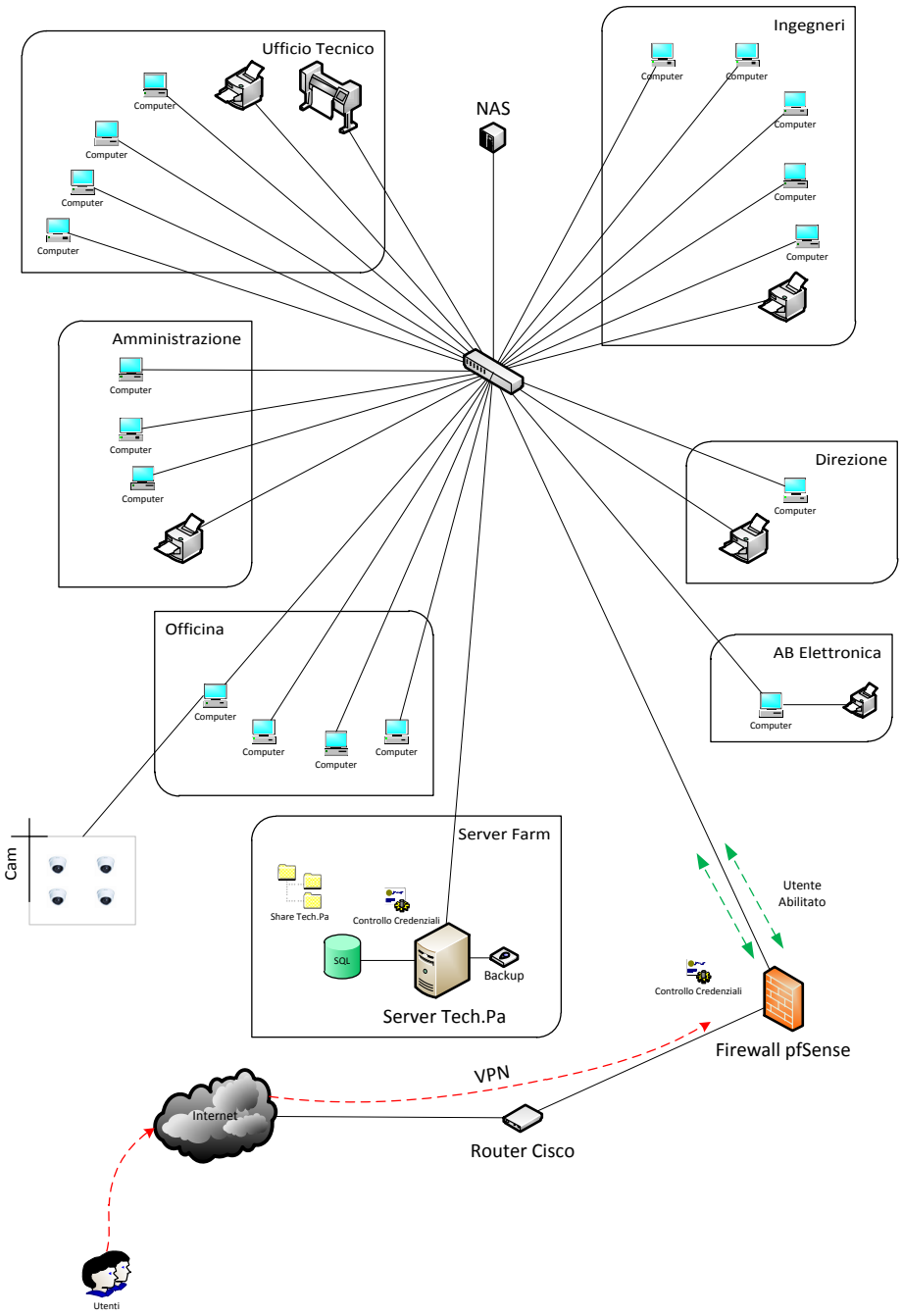


Figura 2.9: Schema rete LAN Tech.Pa S.p.A.

Figura 2.10: Quadro rack del nodo centrale della rete

Capitolo 3

Scelta del Server

In azienda inizialmente non era presente nessun tipo di server, in quanto come descritto nel paragrafo 1.2 le risorse condivise erano distribuite su vari PC e NAS senza alcun controllo. Si è quindi dovuto acquistare un server.

3.1 Scelta della macchina

Studiando le necessità aziendali è emerso che non servisse una macchina particolarmente potente; sarebbe stato sufficiente una buona Workstation. Tuttavia si è preferito prendere un server professionale IBM x3400 M3, mostrato in Figura 3.1. Non si è tenuta la configurazione di fabbrica ma si è estesa la RAM a 16 Gb e si è aggiunto un controller RAID che supportasse il RAID5 (Distributed Parity) (vedi appendice), in quanto implementazione più comune che ci permette, a parità di dischi, di avere una capacità maggiore rispetto ad esempio a un RAID0 o RAID1. La sceta del RAID5 pena la velocità di scrittura sui dischi rispetto a un RAID0 ma Permette di avere una capacità maggiore.

Figura 3.1: IBM X3400 M3

3.2 Scelta ed installazione del sistema operativo

L'azienda disponeva già di un software gestionale ERP (*Enterprise resource planning*) chiamato Impresa24. Questo software è un sistema che consente il controllo completo di tutti i processi aziendali, interni ed esterni.[10]. Impresa24 si basa su un database relazionale SQL (*Structured Query Language*), ed è scritto per il sitema Windows. Qindi in assenza di alternative si è installato sul server un sistema operativo Windows Server 2008 R2 Standard Edition e Microsoft SQL Server 2012 licenziati.

3.3 Configurazione

Per quanto rigurda la configurzione e l'installazione del sistema SQL Server 2012 è intervenuto un tecnico del software gestionale Impresa24.

La soluzione proposta in questo lavoro di tesi per quanto concerne il controllo degli accessi alle risorse condivise è la seguente:

1. Non si è scelto di implementare una architettura basata su Active Directory, anche se la gestione dell'intera rete sarebbe risultata più semplice, bensì una semplice condivisione delle risorse.

2. Il controllo dei permessi alle cartelle condivise è stato fatto creando degli utenti suddivisi in gruppi (Ingegneri, Amministrazione, Ufficio Tecnico, Officina).

3.4 Backup

Aspetto fondamentale è stato il backup delle risorse condivise e del sistema generale. Il backup generale è stato eseguito con l'utility presente in Windows Server 2008 R2 (*Windows Backup*) su un supporto removile, eseguito subito dopo la configurazione degli utenti e dei permessi associati.

Il backup della cartella condivisa generale, chiamata *ShareTechpa*, è stata fatta su un NAS (**Network Attached Storage**) collegato alla rete in una zona dell'azienda sicura e distante dalla sala server. Il sistema giornaliero di backup scelto è di tipo incrementale per riparmiare gigabyte di spazio sul NAS, mentre quello eseguito settimanalmente, ogni sabato notte alle ore 22:00, permette di conservare uno storico massimo di otto settimane.

Capitolo 4

Sicurezza

Un altro aspetto fondamentale su cui l'azienda ha voluto investire è la sicurezza. In seguito verranno esposti i criteri di scelta si un firewall.

4.1 Scelta del firewall

Esistono principalmente due tipi di firewall: software e hardware. I firewall di tipo software sono degli applicativi che vengono installati sulle macchine client, questi richiedono una configurazione per ogni computer e le loro prestazioni dipendono dallo stao della macchina client.

I modelli hardware invece hanno diversi vantaggi rispetto a quelli software:

- L'unico firewall puo proteggere tutta la rete, inserendolo tra router e switch;
- Non richiede l'installazione sulla macchina client;
- Non dipende dallo stato di salute della macchina client;
- Indipendenza dal sistema operativo del cliente;
- Non influisce sulle prestazioni della macchina client;

- Non viene eseguito sui client, quindi non può essere interrotto per errore di sistema o scorretto intervento da parte dell'utente;

In virtù di queste caratteristiche è stato proposto di acquistare un firewall hardware. Il mercato, offre molte scelte per tutte le esigenze e a tutti i prezzi. Marche come ZyXEL ZyWALL, Netgear ProSave, Symantec ecc... risultavano però sopra il budget messo a disposizione.

E' stato proposto allora di optare per un sistema operativo free e open-source e dopo svariate ricerche ci si è soffermati su queste distribuzioni:

- **Zeroshell** è una distribuzione GNU/Linux per server e dispositivi embedded il cui scopo è fornire i principali servizi di rete di cui una LAN necessita. È disponibile nel formato di Live CD o di immagine per Compact Flash ed è configurabile ed amministrabile tramite un browser web[5].

- **IPCop** è una distribuzione GNU/Linux con licenza GPL. É una delle distribuzioni più diffuse e nel 2007 ad IPCop è stato conferito il Premio Infoworld Magazine Bossie Award for innovation in Open Source, come miglor soluzione Open Source in campo di sicurezza informatica[6].

- **Pfsense** è una distribuzione open source basata sulla famiglia di sistemi operativi FreeBSD, è un sistema operativo libero di tipo UNIX, derivato dalla Distribuzione Unix dell'Università Berkeley (*Berkeley Software Distribution*)[7].

Tutte queste distribuzioni sono ideali per le aziende SOHO (*Small Office-Home Office*), quindi i criteri di scelta del sistema operativo sono stati i seguenti:

- Semplicità di utilizzo;

- Comunità di sviluppo attiva;

- Vasta scelta di estensioni;

4.1.1 Alix con pfSense

Dopo vari test svolti in azienda con l'utilizzo di un vecchio pc in dotazione, si è scelto di utilizzare la distribuzione **pfSense**.

Come descritto in precedenza pfSense è una *free distribution* basata su *freeBSD*; sua caratteristica peculiare è che permette di funzionare su dispositivi molto antiquati. I requisiti minimi di funzionamento sono:

- CPU 100 MHz - Pentium
- RAM 128 Mb
- 1Gb di HD
- minimo 2 schede di rete

Per questo si è cercato una soluzione hardware di tipo embedded con consumi molto limitati. Dopo svariate ricerche in rete è stata trovata un'azienda (PC Engines) che produce una scheda adatta alle nostre esigenze: la **Alix 2D13** mostrata in Figura 4.1. Per quanto riguarda invece una lista delle specifiche

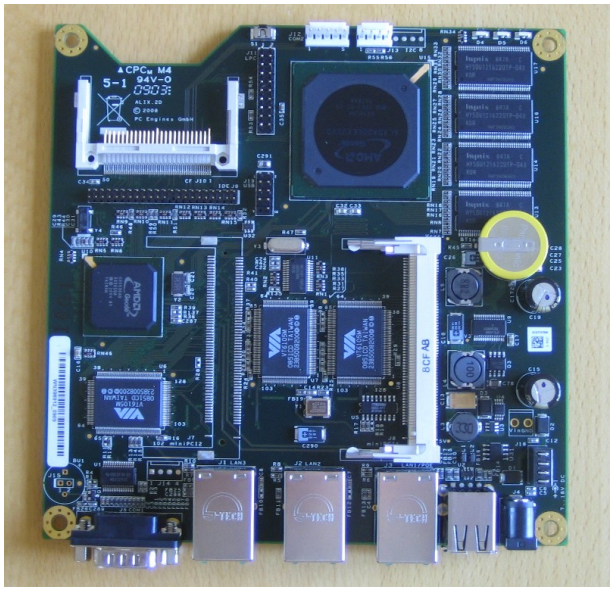


Figura 4.1: Alix board 2D13

hardware, queste sono esposte in dettaglio nella Tabella 4.1.1.

Hardware specifications
CPU: 500 MHz AMD Geode LX800.
DRAM: 256 MB DDR DRAM.
Storage: CompactFlash socket, 44 pin IDE header.
Power: DC jack or passive POE, min. 7V to max. 20V.
Three front panel LEDs, pushbutton.
Expansion: 1 miniPCI slot, LPC bus.
Connectivity: 3 Ethernet channels (Via VT6105M 10/100 Mbps).
I/O: DB-9 serial male port, dual USB port.
No video output. No audio output. Only serial console.
Firmware: tinyBIOS.

É stato trovato un fornitore italiano di questa scheda, il quale forniva anche un case su misura. L'azienda in questione, Firewall Hardware, si trova a Torino e possiamo trovare i suoi prodotti su `http://www.firewallhardware.it/index.html`. Una foto del firewall con il case è presente in Figura 4.2.

Figura 4.2: Alix board 2D13 - case

PfSense si basa su l'utilizzo di due o più porte Ethernet, per svolgere la funzione di firewall, distinte dalla seguente notazione:

- **WAN**: interfaccia sulla quale verrà configurato l'accesso a Internet;
- **LAN**: interfaccia sulla quale verrà configurata la rete aziendale;

- **OPT**: interfaccia opzionale sulla quale è possibile creare una DMZ o un altra rete.

Altro fattore fondamentale di cui dispone pfSense è una vasta disponibilità di *add-on*, rendendo possibile configurare il sistema per molteplici funzioni.

4.2 Configurazione del firewall

Subito dopo l'arrivo del firewall sono cominciati i test di configurazione dell'apparato. Come prima cosa abbiamo scaricato il sistema operativo dal mirror che troviamo sul sito pfSense[8], ultima versione disponibile al momento del tirocinio. Queta versione è per sistemi AMD Geode per Compact Flash da 4 Gb e senza VGA, quindi per installare il sistema operativo si è dovuto usare un lettore di schede Compact Flash.

A seconda del sistema operativo in possesso dell'utente, ci sono vari modi per installare pfSense su Compact Flash; in questo caso descriverò il procedimento per un sistema operativo Apple Mac OS X.

1. Inseriamo la Compact Flash nel lettore di schede e con lo colleghiamo alla porta USB;

2. Apriamo il Finder del Mac e entriamo in Utility-Utility disco;

3. Selezioniamo sulla sinistra dello schermo la Compact Flash e tramite il pulsante informazioni selezioniamo l'identificatore disco associato, e ci assicuriamo che la CF sia disattivata;

4. Apriamo il terminale e scriviamo:
   sudo dd if=nomeimmagine.img of=/dev/identificatore
   ci chiederà la password di *root*;

5. Finito il procedimento, che durerà circa una ventina di minuti, scolleghiamo la Compact Flash dal lettore e la inseriamo nella scheda Alix e, alimentandola, pfSense si avvierà;

6. Colleghiamo un cavo Ethernet alla porta di destra dell'Alix e ci assicuriamo di avere abilitato il DCHP sulla nostra scheda di rete;

7. Accediamo alla pagina `https://192.168.1.1/index.php`, inseriamo user e password, rispettivamente *admin* e *pfsense*, saremo reindirizzati sul *Wizard* iniziale di configurazione e ci apparirà una pagina come mostrato in Figura 4.3.

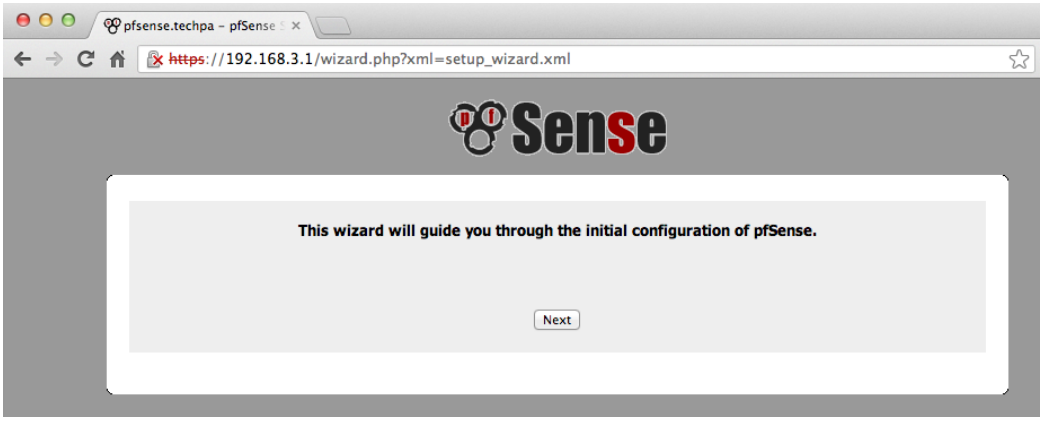


Figura 4.3: Wizard configurazione pfSense

Nel Wizard di configurazione vengono richieste le informazioni generali del firewall, quali hostname, dominio, tipo di accesso alla **WAN** (*DHCP, statico, etc...*) e indirizzo IP dell'interfaccia della rete **LAN** e infine un nuovo user e password per l'accesso alla pagina web di configurazione. In seguito sarà possibile configurare tutte le altre impostazioni richieste (*VPN, Firewall, Proxy, ecc...*) attraverso l'interfaccia web mostrata in Figura 4.4. Nel nostro caso, come descritto nel paragrafo 2.5, sono stati impostati i seguenti parametri:

- Interfaccia WAN statica con indirizzo 10.0.0.2/24, che si appoggia su un router Cisco di proprietà del fornitore di servizio aDSL (*Brennercomm*);
- Interfaccia LAN statica con indizizzo 192.168.1.1/24;
- Interfaccia OPT con indirizzo 192.168.10.1/24, nella quale verrà collegato il router WiFi Cisco per le zone WiFi richieste;

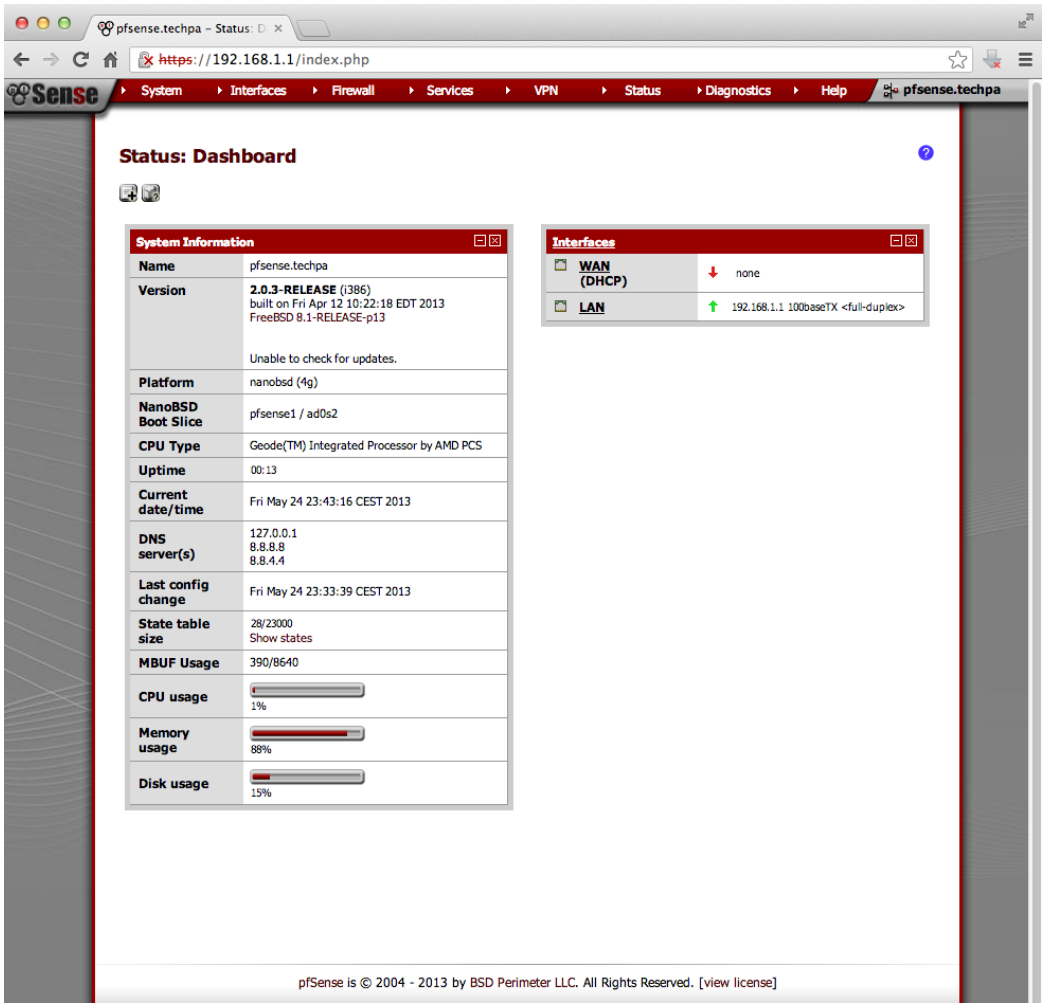


Figura 4.4: Web Configurator - Dashboard

- DNS liberi (Google) primario 8.8.8.8 e secondario 8.8.4.4.

Il server DHCP, per quanto riguarda la zona LAN e WAN, è stato disabilitato in quanto tutti gli indirizzi IP dei dispositivi associati sono stati assegnati staticamente secondo la Tabella 2.2.

Dopo queste configurzioni iniziali il firewall è pronto per essere installato nella rete LAN anziendale, ma i servizi richiesti non sono accora disponibili.

4.2.1 URL-Filtering

Il titolare dell'azienda ha espressamente richiesto che fosse implementato un sistema di filtraggio web senza intervenire con applicativi sulle macchine client. Per soddisfare questa richiesta è stato scelto un sistema sul firewall che svolgesse questo compito. Tra gli *add-on* di PfSense è disponibile un pacchetto molto utile e versatile chiamato **squid** che, abbinato con un altro *add-on* chiamato **squidGuard**, permette di implementare un server Proxy trasparente. Tale server, appoggiandosi su una Blacklist libera permette di fare un *URL-Filtering* sulla porta 80 *http*.

Di seguito verranni esplicitati i passaggi per l'installazione e configurazione dei pacchetti **squid** e **squidGuard**:

1. Apriamo il browser internet alla pagina `https://192.168.1.1/index.php`, inseriamo user e password impostati nel *Wizard* di configurazione iniziale, andiamo su *System - Packages* (Figura 4.5) e cerchiamo la voce **squid**, poi a destra sul pulsante installa pacchetto e verremo indirizzati su una pagina di stato dell'installazione;

2. Alla fine dell'installazione del pacchetto **squid**, andiamo nel menu di configurazione del pacchetto che troviamo in *Services - Proxy server* e abilitiamo le voci *Transparent Proxy* e come in Figura 4.6.

3. Come per l'installazione del pacchetto squid andiamo in *System - Packages* e installiamo **squidGuard**;

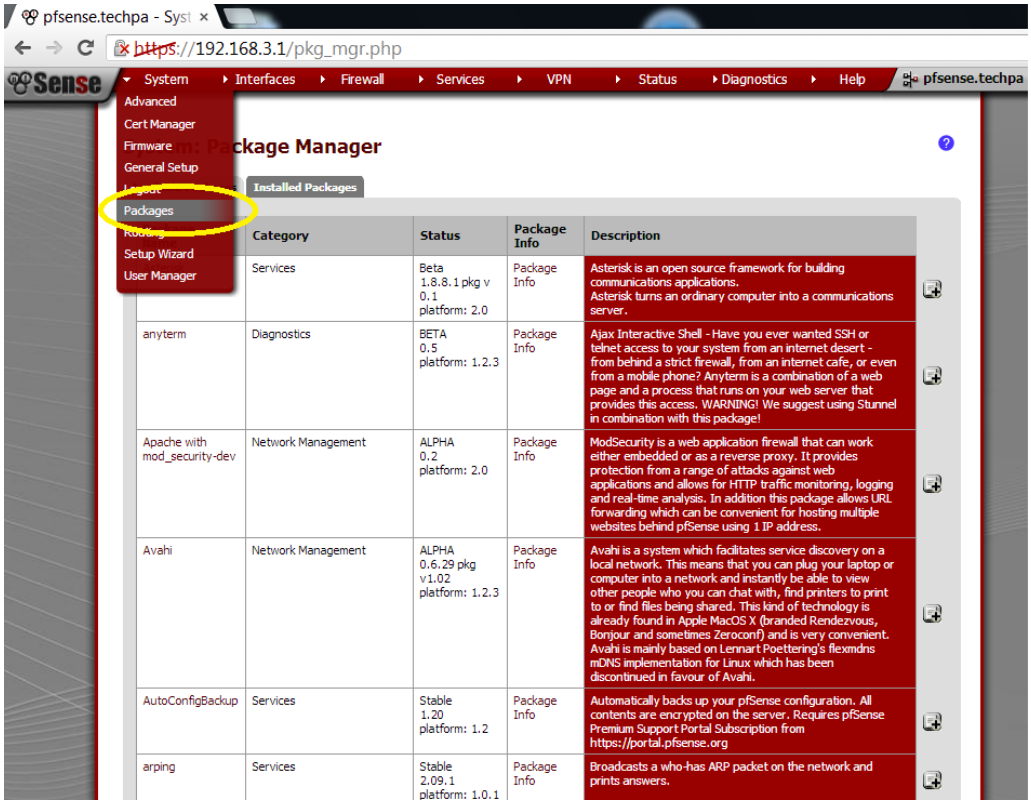


Figura 4.5: Installazione add-on

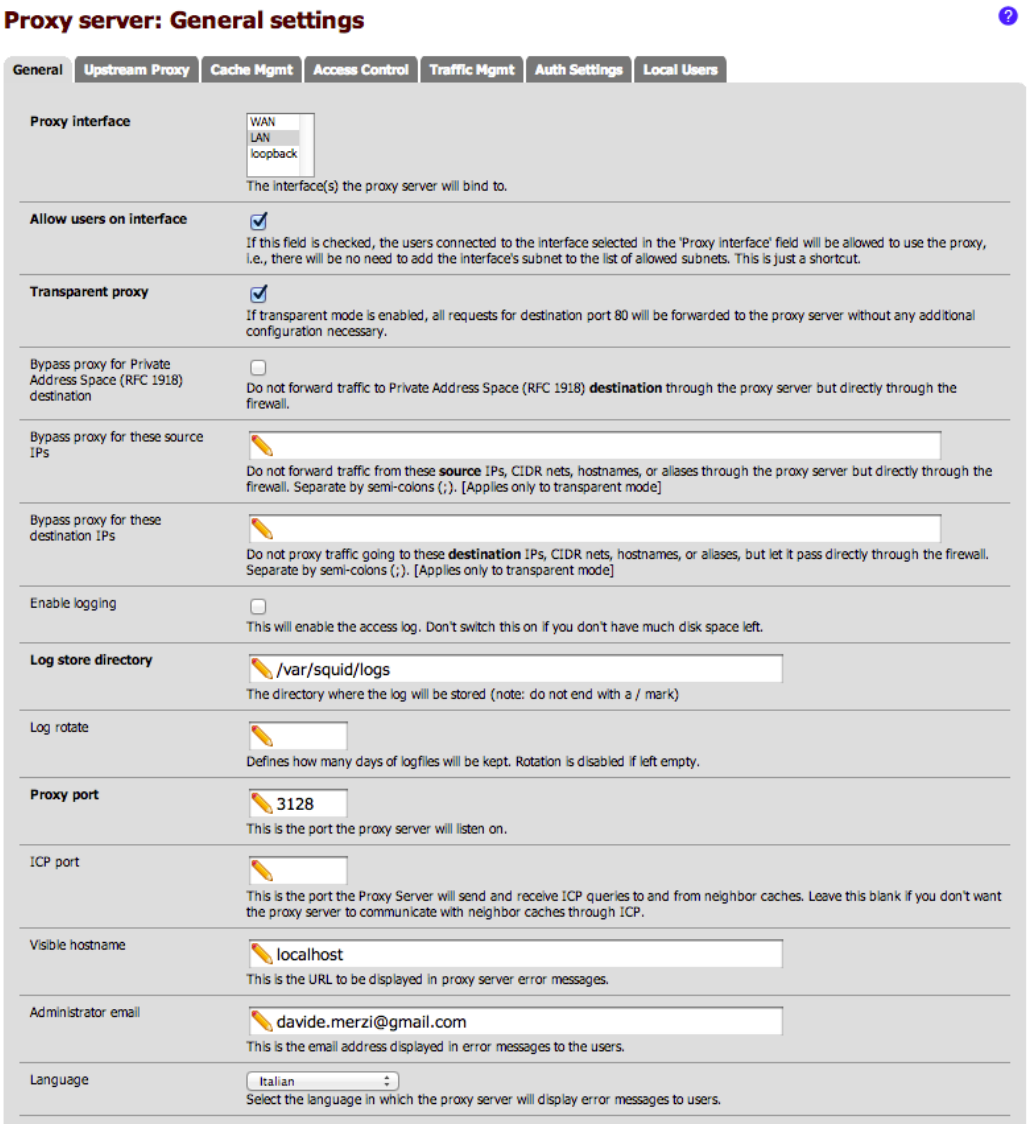


Figura 4.6: Pagina di configurazione del Trasparent Proxy

4. Accedendo alla voce *Services - Proxy filter* possiamo configurare le impostazioni dell'URL-filtering (Figura 4.7);

Il blocco principale richiesto deve essere fatto sui siti erotici, che possiamo aggiungere uno a uno nella sezione *Services - Proxy filter - Common ACL*. Ovviamente inserire a mano tutti i siti erotici presenti nella rete risulta impossibile quindi si è optato per l'utilizzo di liste contenenti un vasto elenco di pagine web suddivisi per categoria, chiamate **Blacklist**. In questo caso è stata usata una lista libera chiamata **Shalla's Blacklist** (vedi Appendice). Per caricare sul sistema le categorie dei siti da bloccare basta entrare sull'interfaccia web del firewall e dopo aver impostato le impostazioni generali (Figura 4.7) dalla voce *Blacklist* possiamo mettere url o il percorso locale della blacklist. Cliccando su download in automatico scaricherà la lista e dopo averla scompattata crea il database in `/var` che viene montato nella RAM del sistema. Il processo di download della blacklist è mostrato in Figura 4.8.

4.2.2 Blacklist su piattaforma Alix

La distribuzione di pfSense per la piattaforma Alix è di tipo *nanofreeBSD*; questa versione è stata disegnata per sistemi embedded con supporti di memorizzazione di tipo Compact Flash, impostando il filesytem in sola lettura sul disco mentre lettura e scrittura sulla RAM. Se il sistema fosse totalmente in scrittura il ciclo di vita della Compact Flash diminuerebbe drasticamente.

Con questa distribuzione di pfSense, quando andiamo a caricare la blacklist come mostrato in Figura 4.8, a un certo instante, controllando l'output del sistema dal cavo console, viene mostrato un errore (`/var: write failed, filesystem is full`). Il motivo di questo errore è dovuto al fatto che all'avvio le directory `/var` e `/tmp` sono istanziate di dimensioni troppo piccole per contenere il database creato da squidGuard. Per ovviare a questo problema si è scelto di procedere come segue:

- Prima di tutto si è cercato il file che definisce le dimensioni della directory `/var` e `/tmp`. Questo file denominato `rc.embedded` è situato in

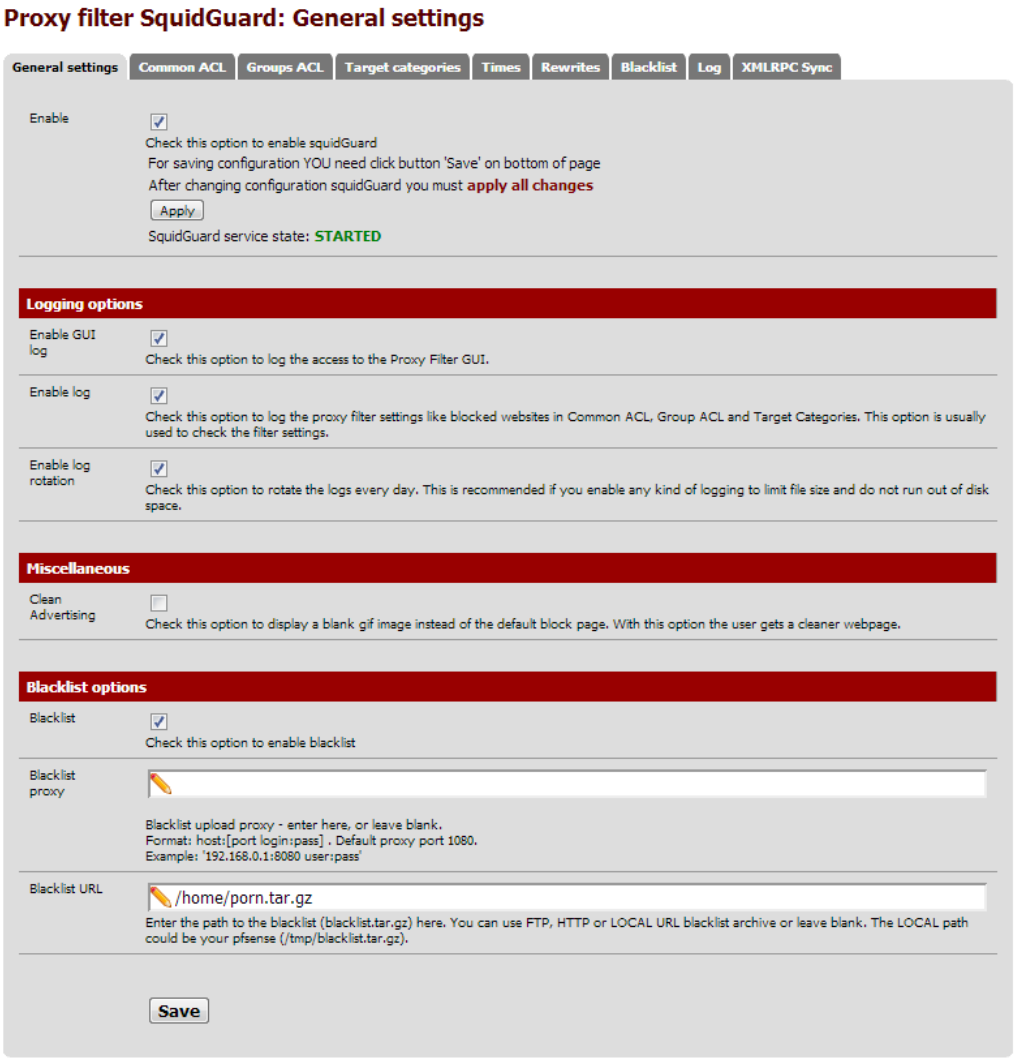


Figura 4.7: Configurazione di squidGuard

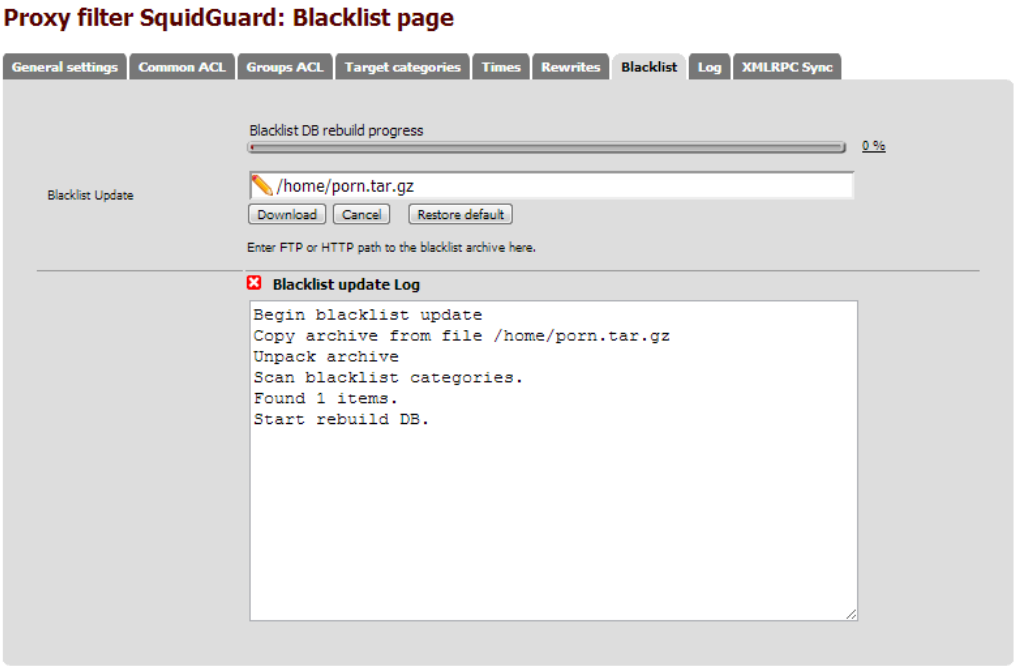


Figura 4.8: Processo di download delle Blacklist

`/etc` e le dimensioni delle rispettive directory vanno impostate grazie alle variabili `varsize` e `tmpsize` a 100Mb.

- La blacklist Shalla contiene moltissime categorie, ma a noi ne interessa solamente una: quella riferita ai siti erotici. Per caricare sul firewall solo questa categoria abbiamo scompattato il file della blacklist *tar.gz* e ricompattato lo stesso solo contenente le cartelle con la categoria *Porn*. In questo modo il file delle blacklist risulta di dimensioni notevolmente ridotte. Questo file è stato poi caricato nella directory `/home` del firewall.

- Sempre come illustrato in Figura 4.8, quando andiamo a caricare la blacklist personale, squidGuard crea il database sulla cartella `/var` e quindi nella RAM. Questo fa sì che i vari file di log possano oltre che essere letti anche scritti. Tuttavia al primo riavvio del sistema o spegnimento accidentale, questo database viene perduto e per ricrearlo bi-

sogna andare manualmente a cliccare il pulsante download dalla pagina delle blacklist.

Per poter mantenere il database anche dopo un riavvio della macchina si è scelto di procedere come segue:

- Creazione del database di squidGuard tramite il web configurator;
- Montaggio del sistema in scrittura con il comando `monut -w /`;
- Copia del database creato in `/home/blacklist_db` nella RAM cioè in `/var`;
- Montaggio del filesystem di nuovo in lettura.

Per automatizzare il tutto si è creato un semplice script bash chiamato *cp_database* che è stato messo nella cartella `/usr/local/etc/rc.d`, la quale contiene tutti gli script da eseguire all'avvio. Lo script *cp_database.sh* è mostrato di seguito:

```
#!/bin/sh
#copia il database creato da squidGuard in /var
#Riavvio del servizio squid
#Davide Merzi 04/06/2013

cp –R /home/blacklist_db/squidGuard/ /var/db/squidGuard
/usr/local/etc/rc.d/squid.sh
```

Infine un'altra richiesta da parte dell'azienda è stata quella di non permettere ai dipendenti la navigazione sul famoso social network Facebook. Per far ciò si è escluso l'utilizzo delle blacklist a disposizione, in quanto squidGiuard lavora con un proxy trasparente che filtra tutto il traffico *http* (porta 80/TCP). Facebook però instaura una connessione sicura attraverso il protocollo *https* (porta 443/TCP) [11], che fa sì che tra il protocollo TCP e HTTP si interponga un livello di crittografia/autenticazione come il Secure Sockets Layer (SSL) o il Transport Layer Security (TLS). In pratica viene

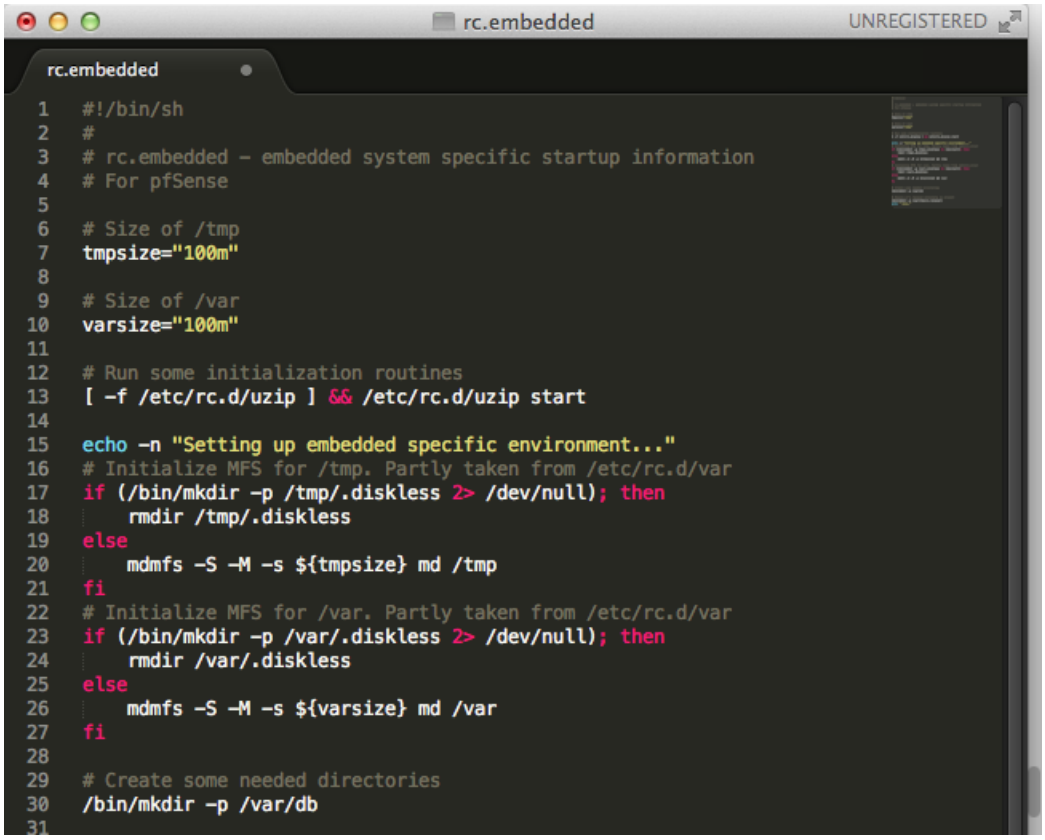


Figura 4.9: rc.embedded

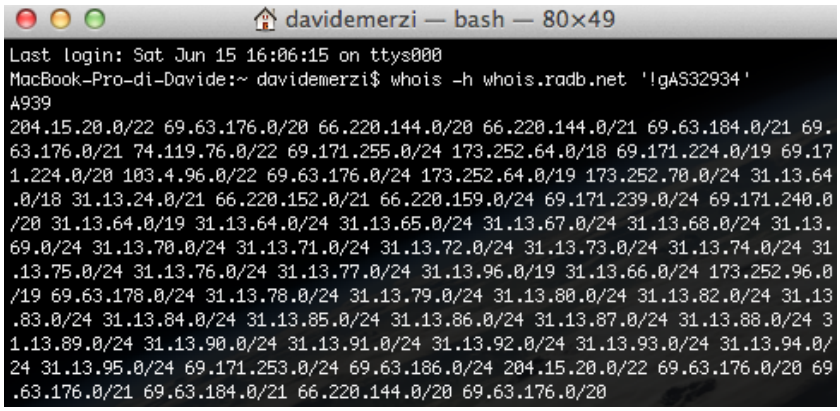


Figura 4.10: Whois sul social network Facebook

creato un canale di comunicazione criptato tra il client e il server attraverso uno scambio di certificati; una volta stabilito questo canale al suo interno viene utilizzato il protocollo HTTP per la comunicazione. Questo tipo di comunicazione garantisce che solamente il client e il server siano in grado di conoscere il contenuto della comunicazione. In questo modo squidGuard non riesce a andare a bloccare il traffico effettuato tramite https. Per risolvere questo problema si è scelto di intervenire configurando una regola firewall in modo tale che tutto il traffico in uscita dalla rete LAN aziendale verso gli indirizzi IP di Facebook fossero bloccati. Per risalire all'indirizzo IP di Facebook, o meglio alla classe di indirizzi IP, si è fatto un whois verso il codice '!gAS32934' che è un autonomous system number assegnato a Facebook usando il terminale del Macintosh. Si ottiene il risultato mostrato in Figura 4.10 (whois -h whois.radb.net '!gAS32934'). Ora accediamo al menù Firewall - Aliases e creiamo un nuovo alias così definito:

- Name: facebook_url;
- Description: fb_net;
- Networks(s): inseriamo tutte gli indirizzi di rete con la relativa CIDR risultate dal comando whois (Figura 4.10).

Un esempio di inserimento è mostrato in Figura 4.11.

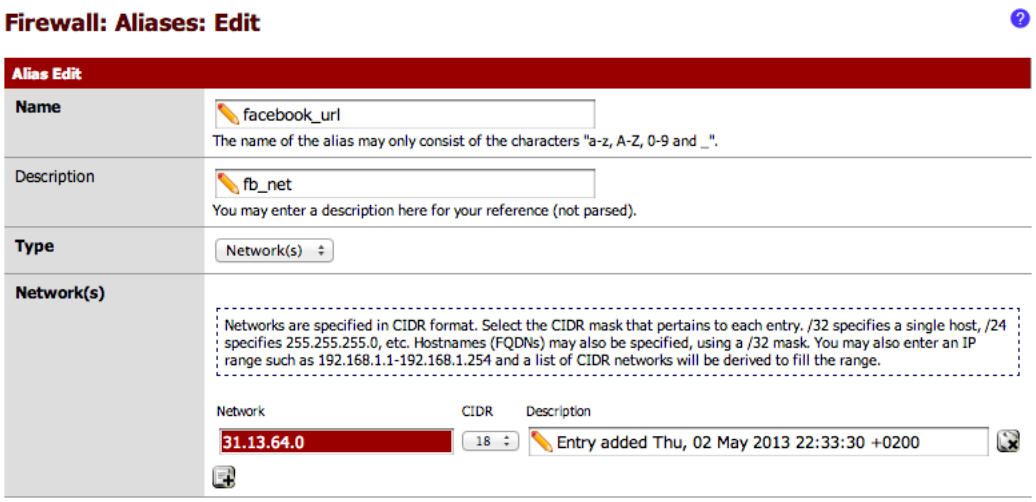


Figura 4.11: Inserimento classi IP di Facebook

Una volta concluso il processo di inserimento di tutte le classi di IP, creiamo la regola firewall per bloccare l'accesso a questi IP. Entriamo nel menù Firewall - Rules e selezioniamo l'interfaccia LAN. Clicchiamo su add new rule e impostiamo la regola firewall come mostrato in Figura 4.12.

- Aciton: Block;
- Interface: LAN;
- Protocol: TCP;
- Source: LAN subnet;
- Destination:
  - Type: Single host or alias
  - Address: facebook_url
- Destination port: Any.

Cliccare su **Save**.

Ora se proviamo ad accedere a Facebook da un computer interno alla rete LAN aziendale il risultato sarà una pagina bianca, che scaduto il timeout del browser ci restituirà un errore.

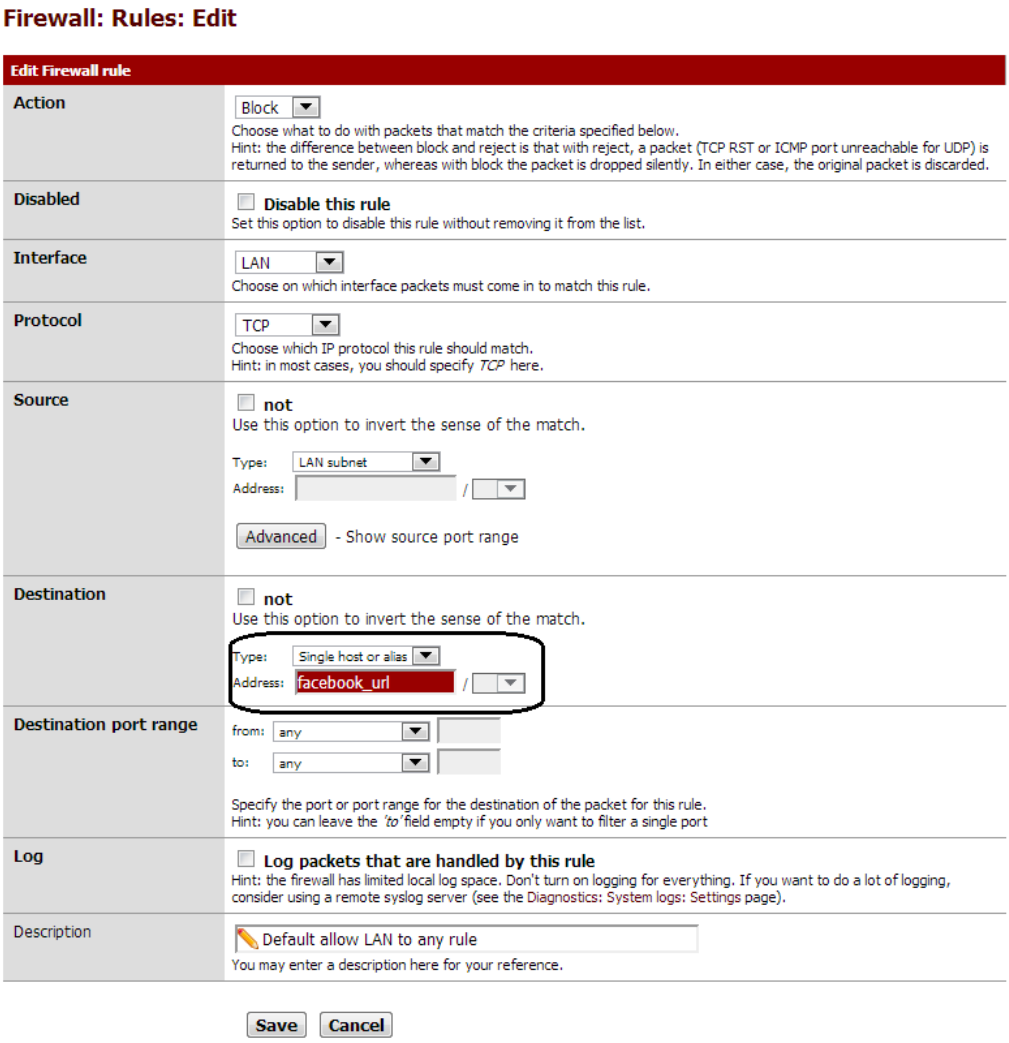


Figura 4.12: Creazione della regola firewall per blocco Facebook

4.3 Classificazione VPN

Le reti private virtuali o *Virtual Private Network* (VPN) consentono alle aziende di espandere le possibilità di accesso alle reti interne (LAN) a dipendenti esterni e partner attraverso reti internet pubbliche standard. La ragione principale per cui furono create le VPN era l'elevatissimo costo per linee in leasing offerte dai provider pubblici (ISP - *Internet Service Provider*).

Esistono principalmente due architetture d'implementazione di una VPN:

1. Le VPN di tipo **LAN-to-LAN** sono collegamenti cifrati attraverso Internet che collegano network geograficamente distanti. Come descritto prima, tali collegamenti trovano spazio in organizzazioni con sedi distribuite sul territorio dove l'utilizzo di linee di comunicazione dati dedicate risulterebbero troppo costose.

2. Le VPN di tipo **Host-to-LAN**, invece, collegano in maniera criptata singoli client ad una LAN. Tale esigenza è diventata sempre più sentita man mano che si è andato diffondendo l'utilizzo di firewall che impediscono l'utilizzo dall'esterno dei servizi più sensibili delle intranet aziendali: facendo uso delle VPN Host-to-LAN, un impiegato che è fuori sede può raggiungere tutti i servizi della sua intranet come se vi fosse fisicamente connesso.

4.4 Scelta e configurazione della VPN

Secondo le esigenze richieste dall'azienda è stato scelto di implementare un servizio di VPN del tipo Host-to-LAN.

La distribuzione pfSense mette a disposizione vari protocolli per l'instaurazione di una VPN:

- **OpenVPN**: è un software open source che implementa tecniche VPN per creare connessioni LAN-to-LAN o Host-to-LAN sicure. OpenVPN utilizza due modalità di autenticazione:

1. **Static-Key**: usa una chiave statica pre-condivisa;
2. **TLS**: usa SSL/TLS più certificati per l'autenticazione e lo scambio di chiavi.

In modalità chiave statica, una chiave pre-condivisa è generata e condivisa tra i due dispositivi con OpenVPN prima di avviare il tunnel. In modalità SSL/TLS, una sessione SSL viene stabilita con l'autenticazione bidirezionale (cioè ogni lato della connessione deve presentare il proprio certificato).

- **IPsec**: acronimo di *Internet Protocol Security*, è il protocollo di sicurezza più comunemente associato ad una VPN, è un protocollo di codifica che garantisce la trasmissione sicura dei dati codificati presso il Network Layer (livello 3 ISO/OSI). Due utenti che desiderano creare un tunnel IPSec devono prima di tutto stabilire una modalità standard per comunicare. Poiché l'IPSec supporta diverse modalità operative, entrambe le parti devono innanzitutto decidere la policy di sicurezza e la modalità da utilizzare e a quali algoritmi di codifica e quale metodologia di autenticazione ricorrere nella comunicazione. In questo protocollo, una volta che il tunnel IPSec è stato attivato, tutti i protocolli del network layer tra due parti in comunicazione sono codificati indipendentemente dalla sicurezza e codifica già esistenti (o non esistenti).

- **PPTP**: acronimo di **Point to Point Tunneling Protocol**, è un altro protocollo di rete che permette di implementare VPN. PPTP utilizza un canale di controllo su TCP e un tunnell con protocollo GRE, (*Generic Routing Encapsulation*, un altro protocollo di tunneling per incapsulare protocolli di livello rete sviluppato da Cisco), che operano per incapsulare pacchetti PPP.

Nel nostro caso abbiamo scelto OpenVPN, in quanto la sua configurazione risulta relativamente semplice ed è presente molto materiale di consultazione

nelle community. Inoltre è un software libero e multi piattaforma, dospobilie per la maggior parte dei sistemi operativi in commercio (*Linux, Mac-OSX, Windows, iOS, Android*). Un altro motivo importante per cui è stato scelto questo software è stato che nella repository di pfSense è disponibile un pacchetto chiamato *OpenVPN Client Export Utility*, che dopo aver configurato la VPN permette di esportare un pacchetto eseguibile che, a seconda del sistema operativo scelto, contiene il client OpenVPN già configurato con i parametri impostati nella pagina di configurazione della VPN, evitando quindi passaggi noiosi al cliente ed eliminando problemi di errata impostazione del client manuale.

Per la configurazione della VPN è stata seguita la seguente procedura: Entriamo nel gestore pacchetti come mostrato in Figura 4.5, e installiamo il pacchetto *OpenVPN Client Export Utility*. Prima di entrare nella configurazione vera e propria della VPN dobbiamo effettuare alcune operazioni preliminari che prevedono la creazione dei certificati digitali. Per iniziare dobbiamo creare 3 tipi di certificati:

1. Un certificato per la nostra Certification Authority (CA): Portarsi nel menù *System - Cert Manager - CAs* poi cliccare su **Add** e compilare in modo preciso i campi sotto riportati per la creazione del nostro certificato:

   ```
   Description Name: InternalCA
   Method: Create an internal CA
   Key length: 2048
   Lifetime: 3650 days
   State or Province: Italy
   City: Verona
   Organization: Techpa spa
   Email Address: admin@techpaspa.com
   Common Name: internal-ca
   ```

   Cliccare su **Save**.

2. Un certificato di tipo server per pfSense: Portarsi nel menù System - Cert Manager - Certificates, poi cliccare su **Add** e compilare in modo preciso i campi sotto riportati per la creazione del nostro certificato:

```
Method: Create an internal Certificate
Descriptive Name: Nome del certificato
Certificate Authority: Nome impostato nel CA
Key length: 2048
Certificate Type: Server Certificate
Lifetime: 3650 days
State or Province: Italy
City: Verona
Organization: Techpa spa
Email Address: admin@techpaspa.com
```

   Cliccare su **Save**.

3. Un certificato di tipo user per gli utenti che dovranno connettersi al server OpenVPN su pfSense. Portarsi nel menù System - Cert Manager - Certificates, poi cliccare su **Add** e compilare in modo preciso i campi sotto riportati per la creazione del nostro certificato:

```
Method: Create an internal Certificate
Descriptive Name: User Cert
Certificate Authority: Nome impostato nel CA
Key length: 2048
Certificate Type: User Certificate
Lifetime: 3650 days
State or Province: Italy
City: Verona
Organization: Techpa spa
Email Address: admin@techpaspa.com
```

   Clicchare su **Save**.

Ora i certificati sono pronti per l'uso, quindi passiamo alla configurazione del server OpenVPN:

1. Dal web-configurator ci portiamo alla voce VPN - OpenVPN - Server e clicchiamo su **Add** e impostiamo i seguenti campi:

   Server Mode: Remote Access (SSL/TSL + User Auth)
   Protocol: UDP
   Device Mode: tun
   Interface: WAN
   Local Port: 1194
   Peer CA: InternalCA
   Server Certificate: VPN Techpa
   DH Parameters Length: 1024 bits
   Encryption algorithm: BF–CBC (128 bit)
   Hardware Crypto: none
   Certificate Depth: One (Client+Server)
   Tunnel Network: 10.0.2.0/24
   Local Network: 192.168.1.0
   Compression: Yes
   Inter Client communications: Yes
   Dynamic IP: Yes
   Address Pool: Yes

   Cliccare su **Save**.

Dopo aver fatto ciò la configurazione del server OpenVPN è completata. Ora non ci resta che impostare una regola firewall per permettere il traffico UDP sulla porta 1194.

1. Ci portiamo sul menù Firewall - Rules - WAN;

2. Clicchiamo su Add e compiliamo i campi come in Figura 4.14:

   - Action - Pass;

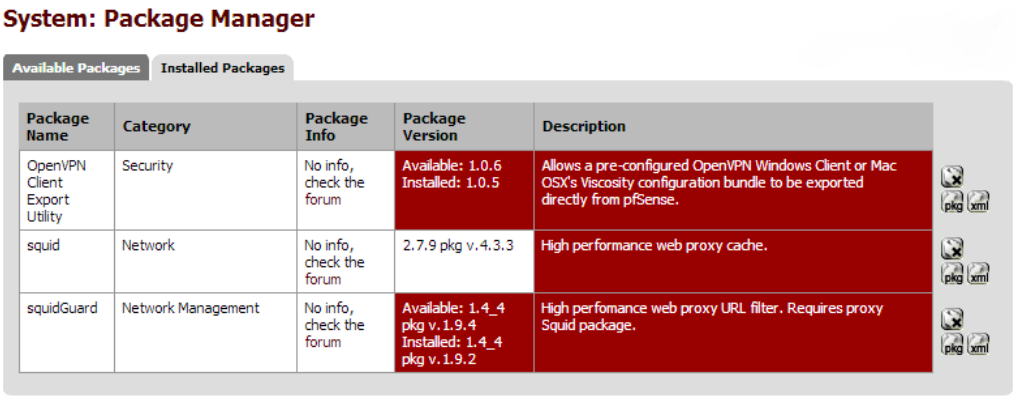


Figura 4.13: Pacchetti installati

- Protocol - UDP;
- Destination Port Range - From OpenVPN to OpenVPN.

In conclusione possiamo finalmente configurare il lato client, per il quale, come visto poc'anzi, possiamo utilizzare uno strumento chiamato *OpenVPN Client Export Utility*. Una volta installato possiamo andare nel menù di OpenVPN: VPN - OpenVPN - Client Export, e da qui selezioniamo il tipo di esportazione che ci interessa. Nel nostro caso utilizziamo il client di esportazione per Microsoft Windows in quanto tutti i computer (client) dell'azienda montano versioni di Windows XP o Seven. Questo strumento crea un pacchetto eseguibile autoestraente contenente un'interfaccia GUI del client OpenVPN già configurata e pronta all'utilizzo.

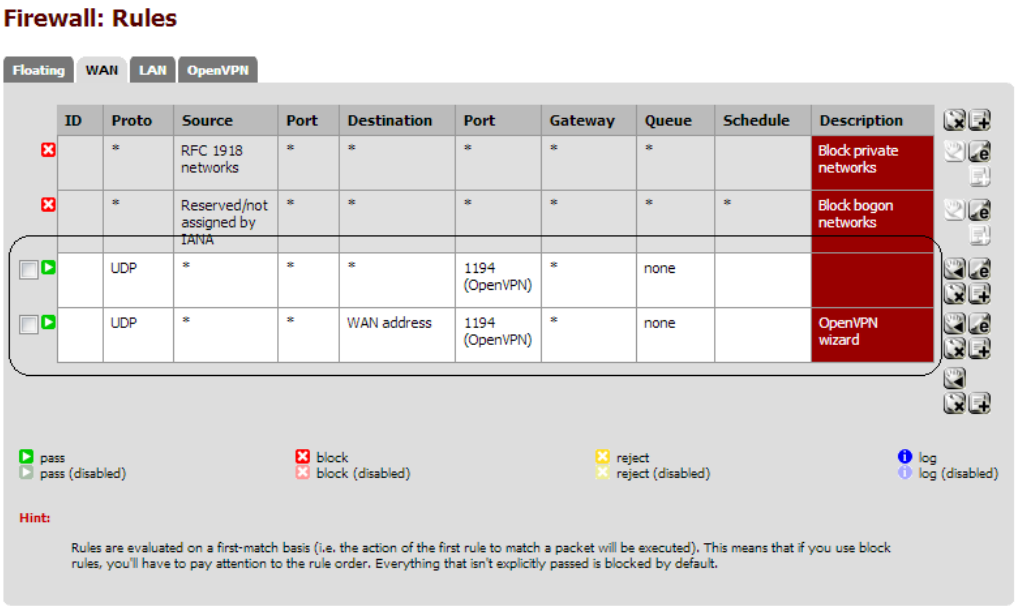


Figura 4.14: Configurazione porta UDP 1194

Conclusioni e sviluppi futuri

Tutte le esigenze dell'azienda sono state soddisfatte e durante la fase di test si sono registrati i vari miglioramenti. Il tempo di ping di un pacchetto verso il server dell'azienda è diminuito quasi del 50% e provando con la copia di un file di grandi dimensioni si raggiunge una banda utile di 80 Mb/s contro i 10 Mb/s iniziali con la rete Ethernet a 100 Mbps. Tutti gli utenti che utilizzano le risorse condivise sono registrati sul server con i relativi permessi.

In futuro è in programma di implementare un ulteriore backup di sicurezza esterno all'azienda, più precisamente in un'altra azienda situata a Vallese di Oppeano a una distanza di circa 11km. Questo backup sarà effettuato su un disco di rete dopo aver instaurato un altro servizio di VPN. Sarà poi schedulato una volta a settimana nel week-end in quanto usando la banda di Internet non abbiamo la capacità di una rete LAN ad alta velocità quindi il backup risulta molto più lento.

In futuro è in programma di installare anche un un sitema di Windows Server Update Services (WSUS) per facilitare gli aggiornamenti delle macchine windows in azienda [12].

Appendice A

Appendice

A.1 LanScan

LanScan è un semplice tool gratis per Mac OS X che permette di fare una scansione della rete locale indicando tutte le device attive sulle rete con relativo indirizzo MAC, indirizzo IP e tipo di venditore. Possiamo vedere un esempio di utilizzo in Figura A.1.

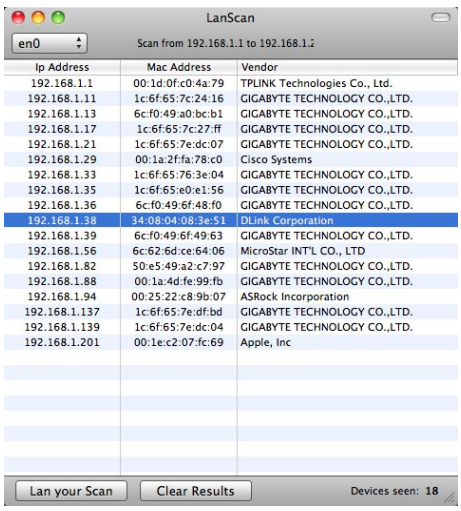


Figura A.1: LanScan

A.2 Modello OSI

Il modello OSI è mostrato in Figura A.2. Questo modello si fonda su una proposta sviluppata dall'*International Standards Organization* (ISO) come primo passo verso la standardizzazione internazionale dei protocolli impiegati nei diversi strati, ed è stato revisionato nel 1995. Si chiama modello di riferimento ISO OSI (*Open System Interconnection*). Questo modello ha 7 strati, ogni strato comunica con un altro attraverso una interfaccia. La completa riprogettazione di uno strato non deve influenzare gli altri.

Il modello OSI in sé non è un'architettura di rete, perchè non specifica quali sono esattamente i servizi e i protocolli da usare in ciscuno strato; si limita infatti a definire ciò che ogni strato deve compiere.

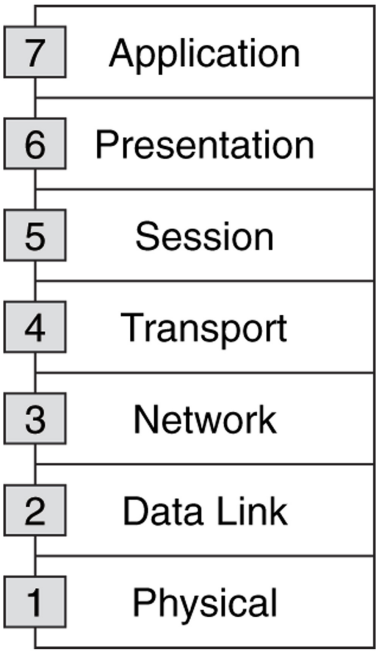


Figura A.2: Modello ISO/OSI

A.3 Cable Tracker 10

Il Psiber Network CableTracker è progettato per manager e tecnici di rete. Il Network CableTracker dispone di una funzione di Port ID che fa lampeggiare la spia dello switch del relativo al cavo collegato. Questa funzione fornisce inoltre un metodo semplice ed efficace per identificare le assegnazioni delle porte switch o hub su reti attive. Questo dispositivo permette anche di rintracciare un cavo emettendo un segnale nel cavo rilevabile tramite un tono emesso dalla sonda. [2]

A.4 WPA2-PSK

WPA2 è il modello di sicurezza Wi-Fi del momento. Si fonda su due protocolli principali:

1. Advanced Encryption Standard (AES), il protocollo di cifratura utilizzato dagli Stati Uniti e da altri governi per proteggere le informazioni riservate e dall'impresa per assicurare WLAN.

2. IEEE 802.1 X, uno standard ampiamente utilizzato nelle reti aziendali per fornire autenticazioni robuste e sofisticate funzioni di controllo di accesso alla rete. WPA2 è basato sullo standard IEEE 802.11i ed offre la crittografia basata su AES a 128-bit. Esso fornisce inoltre l'autenticazione reciproca con Pre-Shared Key (PSK, in modo personale) e con IEEE 802.1X / EAP (in modalità Enterprise). Nel 2004 la Wi-Fi Alliance ha introdotto la certificazione WPA2.

Nel 2006 la certificazione WPA2 è diventata obbligatoria per tutti i Wi-Fi CERTIFIED. Inoltre, nel 2007, la Wi-Fi Alliance ha introdotto il programma di installazione di Wi-Fi Protected per semplificare e favorire l'attivazione di WPA2 nelle reti residenziali.

Con WPA2, la tecnologia Wi-Fi ha raggiunto uno stato di maturità che gli consente di fornire eccellenti sistemi di sicurezza. La Wi-Fi Alliance è

impegnata ad ampliare i programmi di certificazione esistenti e crearne di nuovi per promuovere l'adozione di nuove soluzioni di sicurezza a beneficio di tutti gli utenti.[1]

A.5 Blacklist

Le Blacklist sono liste di siti raggruppati per categoria o contenuto, così da poterle usare per creare delle regole di blocco o accesso. Una delle più complete e aggiornata e soprattutto libera e usata in questo caso, è **Shalla's Blacklist** [9]. Oggi questa lista contiene più di 1,7 milioni di siti e le categorie sono visibili al sito `http://www.shallalist.de/categories.html`.

A.6 RAID

RAID è l'acronimo di Redundant Array of Inexpensive Disks, ed è un sistema informatico che usa un gruppo di dischi rigidi per condividere o duplicare informazioni. Il RAID può essere implementato sia con hardware dedicato sia con software specifico su hardware di uso comune. Con una implementazione software, il sistema operativo gestisce l'insieme di dischi attraverso un normale controller. Questa opzione può essere più lenta di un RAID hardware, ma non richiede l'acquisto di componenti extra. I livelli RAID più comuni sono identificati dal numero 1 al numero 6 sono mostrati in Figura A.3

Il sistema RAID permette di avere una ridondanza che nel caso di un guasto dei dischi permette il recupero dei dati. Il numero dei dischi difettosi ammessi a seconda del livello RAID scelto è mostrato in Firgura A.3.

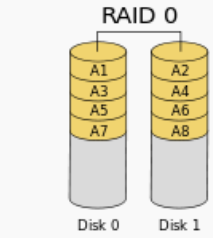
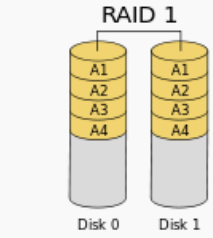
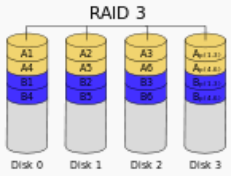
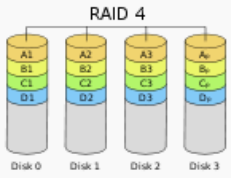
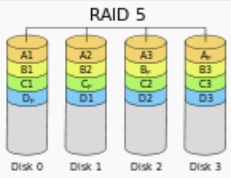
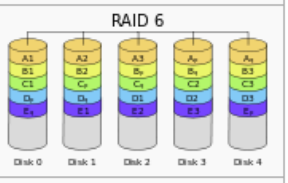
Livello	Numero minimo di dischi	Capacità	Max numero consentito di dischi difettosi	Schema
RAID 0	2	C × N	0	
RAID 1	2	C	N - 1	
RAID 3	3	C × (N - 1)	1	
RAID 4	3	C × (N - 1)	1	
RAID 5	3	C × (N – 1)	1	
RAID 6	4	C × (N – 2)	2	
C = capacità del disco più piccolo; **N** = numero di dischi				

Figura A.3: Livelli RAID più comuni

Bibliografia

[1] Wi-Fi Alliance http://www.wi-fi.org

[2] http://www.psiber.com/en/home/products/cable-tester/cable-tracker.html

[3] http://www.lhup.edu/~dsimanek/philosop/ether.htm

[4] http://it.wikiversity.org/wiki/File:ThicknetTransceiver.jpg

[5] Router/Bridge Firewall Linux http://www.zeroshell.net

[6] IPCop - The Bad Packets Stop Here http://www.ipcop.org

[7] Open Source Firewall Distribution - pfSense project http://www.pfsense.org

[8] Mirror pfSense http://pfsense.mirror.range-id.it/downloads/pfSense-2.0.1-RELEASE-4g-i386-nanobsd.img.gz

[9] Shalla Secure Services http://www.shallalist.de/

[10] Impresa24 - Il Sole 24 Ore http://www.impresa24.ilsole24ore.com/impresa24.html

[11] Lista delle porte assegnate dall'ente IANA http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml

[12] http://technet.microsoft.com/it-it/library/cc645571.aspx

RINGRAZIAMENTI

I miei più grandi ringraziamenti vanno a tutta la mia famiglia, in particolare a papà Paolo, mamma Stefania e alla sorella Sara per avermi sempre sostenuto e dato la fiducia necessaria per arrivare fino a questo traguardo, insieme a zii e tutti e cugini, in particolare a mio zio Luca per avermi supportato tecnologicamente in questi anni.

Un doveroso ringraziamento al Prof. Erseghe che si è sempre dimostrato disponibile per ogni chiarimento o correzione.

Come non ricordare e ringraziare tutti i colleghi di corso e di studio (e non solo...)? Daniele, Alberto, Damiano, Checco, Myriam, Giulio, Paolo, Cassy, Marty, Viviana e Francesca.

Un ringraziamento particolare ai coinquilini con cui ho condiviso la mia esperienza a Padova: Red, Mario, Gibo, Piz, Alberto, Fabio, Eugenio e Fabione.

Un grazie anche a tutti gli amici di Verona, Giovanni, Vale, Anna, Gabri, Chiara, Mago, Ludovica, Anselmo, Karol, Ciccio, Hannah, Signo, Mitch, Pado, Azzurra, Eros, Nicolò, Sara, Conzu, Giulia, Matteo, Daiuz, Manza, Zambo, Manto e Zanna.

Come non ricordare la mia squadra di calcetto Real Verona e gli amici del "Bar della Poli" che mi ha aiutato a distrami e divertirmi in quest'ultimo anno di Università.

Un ringraziamento particolare va al mio amico Luca per tutti questi anni di amicizia.

Un affettuoso ringraziamento alla mia ragazza Ilaria, per avermi aiutato nei momenti più difficili in questi ultimi mesi di Università.

Grazie a tutti per aver reso questi anni indimenticabili !!!

Davide Merzi