

Progetto per l'esame
Laboratorio di Reti



Università degli Studi di Perugia, Dipartimento di Informatica
A.A. 2007/2008



Realizzazione di una Rete Informatica
per
il Ministero della Magia

Rocchini Giovanni
D'Ambrosi Luca

Servizi richiesti

E' stato richiesto dal Ministero della Magia di progettare, configurare e gestire la rete telematica che permetta il collegamento dei principali edifici del mondo magico da sostituire al poco sicuro sistema dei gufi utilizzato fino ad ora per comunicare.

Il mondo magico comprende i seguenti edifici da collegare in rete: Ministero della Magia, Banca Gringott, Ufficio Auror, Archivio Pratiche.

La struttura che ci è stata presentata è la seguente:

1. Nel Ministero della Magia lavorano 270 persone, è diviso in 7 dipartimenti (un dipartimento per piano). Sono inoltre presenti un Server DNS, un Mail Server ed un Server WEB collegati con l'esterno.
2. Nell'ufficio Auror lavorano 100 persone, divise in 3 piani. Vi è inoltre un Mail Server per la posta interna.
3. Nell'ufficio Archivio Pratiche lavorano 50 persone esso è costituito da 2 piani. Vi è inoltre un Server DNS. L'intero ufficio ha copertura wireless.
4. Infine abbiamo la Banca Gringott. Essa ospita al suo interno 300 persone divise in 10 settori. Al suo interno vi è un Server Aziendale e un Server di Backup per il server aziendale. L'intera banca ha copertura wireless.

E' inoltre richiesto che tutte le postazioni siano connesse in rete ed abbiano a loro disposizione tutti i servizi disponibili necessari.

L'intera rete deve inoltre essere connessa ad internet e protetta tramite firewall per garantire la sicurezza di tutte le informazioni e dei dati, spesso anche molto sensibili, che viaggeranno su di essa.

Il Ministero della Magia è l'unico edificio con collegamento diretto ad internet. Qualsiasi host di uno qualsiasi degli altri edifici che si vuole connettere ad internet dovrà passare necessariamente attraverso le misure di sicurezza del Ministero prima di accedere all'esterno.

L'utilizzo del Server Aziendale interno alla Banca Gringott è riservato alla sola banca, in quanto contenente applicazioni inerenti alla gestione finanziaria e strettamente riservate. All'interno della banca è presente anche un server di Backup dove periodicamente viene copiato l'intero database che si trova nel server Aziendale. Sarà quindi riservata maggiore attenzione alla sicurezza del server stesso e del server di backup dato che contiene la copia degli stessi dati presenti nell'aziendale.

I server DNS presenti sono due. Uno interno principale che avrà la conoscenza di tutta la struttura e tutti i nomi delle sottoreti e uno secondario esterno (sulla DMZ) che avrà le informazioni relative solamente ai server visibili all'esterno e presenti nella DMZ.

Nella rete del mondo magico sono presenti inoltre due Server di Posta Elettronica. Uno interno per le missive e messaggi interni e uno per gestire il traffico postale con l'esterno attraverso Internet.

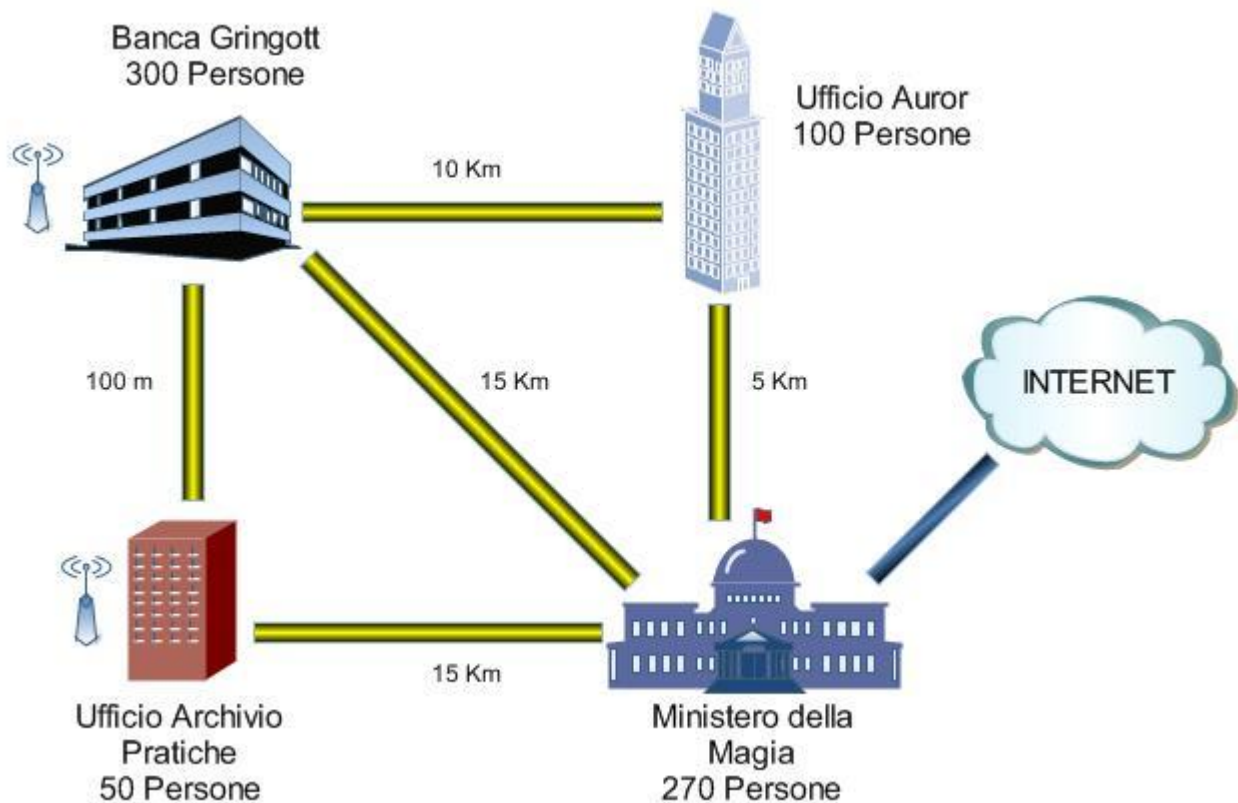
Infine sulla DMZ sarà presente anche un server WEB dove potrà esserci il portale con il quale i maghi possono interagire per usufruire dei servizi online del ministero.

Ci sono due edifici (Banca e Ufficio pratiche) che dovranno avere al loro interno anche un collegamento wireless per permettere a postazioni mobili di collegarsi alla rete. Questo aggiunge un problema di sicurezza dato che negli edifici, soprattutto nella banca sono contenuti dati sensibili.

Struttura della rete

Edificio	N° postazioni	Server	Copertura Wireless
Ministero della Magia	270	DNS, Web, Mail	No
Ufficio Auror	100	Mail	No
Banca Gringott	300	Aziendale, Backup	Si
Archivio Pratiche	50	DNS	Si

Distanze tra edifici e pianta della rete



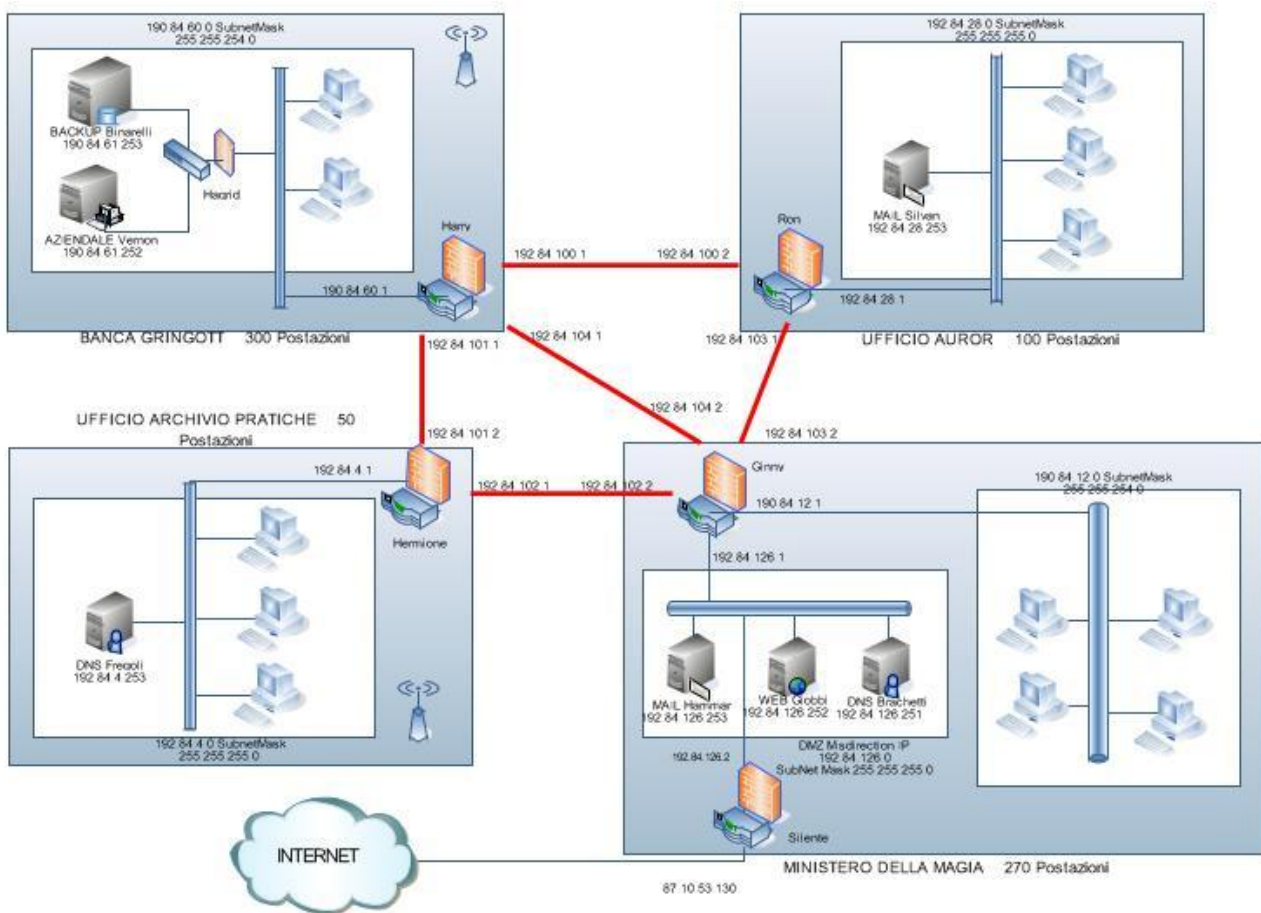
La grossa distanza tra gli edifici ci ha portato ad evitare la scelta di collegamenti diretti tramite fibra ottica o cavo Ethernet (costi elevati nel primo caso e distanze troppo grandi, con conseguente richiesta di ripetitori nel secondo caso).

Si è quindi deciso di creare dei collegamenti virtuali mediante la tecnologia VPN (Virtual Private Network). È una rete privata instaurata tra soggetti che utilizzano un sistema di trasmissione pubblico e condiviso come può essere Internet. Quando essi vogliono instaurare una conversazione richiedono ad un sistema di autenticazione di garantire l'esclusività del canale ed utilizzano un sistema di crittografia (in questo caso usiamo l'IPsec) per rendere sicura la trasmissione dei dati nel canale. I pacchetti della rete interna vengono così criptati e incapsulati all'interno di pacchetti adatti ad essere spediti via Internet e ricevuti dal router dell'edificio di destinazione che estrarrà da questi pacchetti i rispettivi pacchetti interni Lan che infine decifrerà.

L'utilizzo della VPN ci ha portato ad inserire un router per edificio, in modo da poter configurare il routing dell'intera rete. Si è scelto un router che supportasse la tecnologia VPN e con firewall interno per limitare i costi di progettazione e poter prevedere alla sicurezza della rete.

Si poteva decidere di collegare gli edifici della Banca Gringott e dell'Ufficio Archivio Pratiche tramite cavo Ethernet che è sufficiente a mantenere la qualità del segnale e la spesa dell'opera entro margini ottimali, data la modesta distanza che c'è tra di loro, ma si è scelto di continuare ad utilizzare la VPN per questioni di uniformità della rete senza intaccare né la qualità né la spesa.

Struttura fisica della rete



La connessione interna agli edifici tra i singoli piani è realizzata mediante Switch per portare la connessione ai singoli punti di accesso e gli switch tra di loro sono collegati ad una dorsale in fibra ottica che permette di massimizzare la velocità dei trasferimenti.

Un edificio, il Ministero della Magia, presenta 2 Router (entrambi con firewall). Questo perché il Ministero ha al suo interno la DMZ (DeMilitarized Zone) e quindi dovrà avere un router interno (Ginny), per collegare le varie sottoreti e gestire la sicurezza dei dati che le attraversano, e un router esterno (Silente), collegato ad internet per poter proteggere i server visibili all'esterno con una certa politica di sicurezza diversa da quella della rete interna.

Gli edifici dell'Ufficio Archivio Pratiche e della Banca Gringott avranno dispositivi (Access Point) che permettono, come già detto in precedenza, l'accesso wireless a postazioni mobili.

Struttura logica della rete

La struttura logica della rete appare quindi come una Lan che comprende 4 macro-zone, collegate attraverso internet da tunnel VPN criptati.

Si sono acquistati 5 IP pubblici statici di classe B. L'indirizzo 87.10.53.130 assegnatoci verrà usato per far collegare dall'esterno gli utenti ai servizi presenti nella DMZ (web,dns e mail) mentre gli altri 4 IP statici saranno necessari per poter utilizzare la VPN, verranno assegnati uno per ogni edificio. La VPN necessita di IP statici per funzionare dato che tutti gli edifici devono essere reperibili continuamente dagli altri edifici e per fare ciò, senza dover ogni volta riconfigurare tutti i

router, sono necessari gli IP statici.

Per la gestione della rete si è deciso di creare delle sottoreti date poi in gestione ad amministratori locali, per semplificare il lavoro ed aumentare la sicurezza, data anche la diversità dei vari edifici in quanto alle diverse esigenze che hanno.

In questo modo è stato inoltre possibile dividere i singoli edifici.

Per motivi di sicurezza si è inoltre inserita un ulteriore sottorete, cioè la DMZ, per permettere l'accesso ai server pubblici dall'esterno senza compromettere la sicurezza interna della rete.

All'interno della DMZ sono presenti un server DNS, un server WEB ed un Mail server.

Utilizzando la tecnica dell'IP masquerading si è inoltre provveduto ad assegnare indirizzi a scelta alle singole sottoreti.

Gli IP assegnati alle varie sottoreti sono i seguenti:

1. Ministero della Magia	190.84.12.0	SubnetMask 255.255.254.0
2. Ufficio Auror:	192.84.28.0	SubnetMask 255.255.255.0
3. Banca Gringott:	190.84.60.0	SubnetMask 255.255.254.0
4. Ufficio Archivio Pratiche:	192.84.4.0	SubnetMask 255.255.255.0
5. DMZ:	192.84.126.0	SubnetMask 255.255.255.0

L'identificazione dei router avviene appunto tramite i nomi dei 4 famosi maghi che hanno deciso di combattere in prima persona Voi-Sapete-Chi.

Per permettere la corretta comunicazione tra gli edifici, sono state create 5 ulteriori sottoreti, una per ogni coppia di router connessi

1. Harry-Ron:	192.84.100.0
2. Harry-Hermione:	192.84.101.0
3. Harry-Ginny:	192.84.104.0
4. Hermione-Ginny:	192.84.102.0
5. Ron-Ginny:	192.84.103.0

I server che si trovano nella rete sono identificati tramite i nomi di veri prestigiatori esistenti ed esistiti nel panorama artistico. (Binarelli, Fregoli, Silvan, Vernon, Hammar, Giobbi, Brachetti) Abbiamo aggiunto anche un firewall che ha il solo scopo di proteggere il server Aziendale Vernon ed il server di Backup Binarelli. Tale firewall è stato chiamato Hagrid per una identificazione più facile e veloce.

Gli host delle sottoreti sono invece identificati tramite dei generici nomi costruiti tramite le iniziali della rete di appartenenza seguito da un numero sequenziale in quanto l'assegnazione di nomi più originali porterebbe solamente confusione nella configurazione dei DNS o di altri servizi che prendono in considerazione il nome degli host anziché l'indirizzo IP. Nomi mnemonicamente più semplici sono stati riservati, come abbiamo visto, solamente ai server ed agli apparati di rete.

La struttura della rete per il mondo magico è molto complessa e ricca di collegamenti tra i vari edifici. Questi collegamenti creano degli "anelli" difficilmente gestibili da un semplice protocollo di routing statico. Per questo nella nostra rete abbiamo bisogno di implementare e configurare un protocollo di routing dinamico più complesso ma che permetta l'indirizzamento dei dati su diverse sottoreti anche in casi di guasti trovando sempre una buona strada tra i diversi collegamenti presenti.

Il protocollo scelto per questa rete è il RIP (Routing Information Protocol). Esso di basa sul conteggio dei numeri di salti (hop count) come metrica di routing.

Assegnazione degli indirizzi

DMZ:

- ✓ Server DNS: 192.84.126.251 (Brachetti)
- ✓ Server Mail: 192.84.126.253 (Hammar)
- ✓ Server WEB: 192.84.126.252 (Giobbi)

- ✓ Interior Router (interfaccia interna): 192.84.126.1 (Harry)
- ✓ Exterior Router (interfaccia interna): 192.84.126.2 (Silente)
- ✓ Exterior Router (interfaccia esterna): 87.10.53.133 (Silente)

Ministero della Magia:

- ✓ Router Harry: 190.84.12.1

- ✓ Host 1: 190.84.12.2
- ✓ Host 2: 190.84.12.3
- ✓ ...
- ✓ Host 270: 190.84.13.16

Ufficio Auror:

- ✓ Server Mail: 192.84.28.253 (Silvan)
- ✓ Router Ron: 192.84.28.1

- ✓ Host 1: 192.84.28.2
- ✓ Host 2: 192.84.28.3
- ✓ ...
- ✓ Host 100: 192.84.28.102

Banca Gringott:

- ✓ Server Aziendale: 190.84.61.252 (Vernon)
- ✓ Server Backup: 190.84.61.253 (Binarelli)
- ✓ Router Harry: 190.84.60.1

- ✓ Host 1: 190.84.60.2
- ✓ Host 2: 190.84.60.3
- ✓ ...
- ✓ Host 300: 190.84.61.46
- ✓ Host wireless 1: 192.84.61.47
- ✓ ...
- ✓ Host wireless 100: 192.84.61.147

Ufficio Archivio Pratiche

- ✓ Server DNS: 192.84.4.253 (Fregoli)
- ✓ Router Hermione: 192.84.4.1

- ✓ Host 1: 192.84.4.2
- ✓ Host 2: 192.84.4.3
- ✓ ...
- ✓ Host 50: 192.84.4.53
- ✓ Host wireless 1: 192.84.4.54
- ✓ ...
- ✓ Host wireless 20: 192.84.4.83

Sicurezza

DMZ: Per garantire la sicurezza necessaria all'intera struttura si è scelto di strutturare dei firewall Screened Sub Net utilizzando così appieno la DMZ inserita nel Ministero della Magia. Tramite la DMZ l'esterno della rete ha accesso solo ai server pubblici contenuti nella DMZ stessa, ma ha un "blocco" grazie al secondo firewall (quello interno), dotato di regole molto più restrittive del firewall esterno.

I due router (interno ed esterno) sono dotati di firewall che effettuano controlli sui pacchetti a livello 2 (Rete), permettendo così la protezione della rete da attacchi esterni. Per implementare i controlli si utilizza IPTABLES.

La sostanziale differenza dei 2 router è data dalla severità delle regole applicate. Il router esterno ha regole meno restrittive e si limita a filtrare gli accessi per garantire i servizi dei server pubblici, sia in ingresso che in uscita.

Il router interno incrementa un'ulteriore sicurezza restringendo le regole e impedendo accessi dall'esterno, essendo l'ultima difesa dei singoli host.

All'esterno della rete privata, nella DMZ, sono stati posti i servizi potenzialmente insicuri come il server di posta Hammar, il server Web Giobbi ed il server DNS Brachetti. Tali server se posti nella DMZ rimangono isolati dalla rete interna e non sono quindi dei punti critici per la sicurezza interna, non potendo accedere alla rete. Per restituire un po' di sicurezza a questi 3 server si è scelto di implementarli su Bastion Host (computer creati e configurati specificatamente per resistere ad attacchi esterni).

NAT: Per aggiungere un ulteriore livello di sicurezza alla rete interna, oltre al secondo firewall si è pensato di sfruttare la tecnica del Network Address Translation (NAT), che permette di accedere ad internet tramite un gateway (nel quale è realizzata la funzione di IP masquerading e quindi il NAT), e non direttamente con un IP pubblico. Infatti con il meccanismo del NAT, gli host della rete interna navigano all'esterno in maniera trasparente all'utente, (quasi) come fossero direttamente connessi ad internet, ma con un livello di sicurezza estremamente più elevato.

La tecnica dell'IP masquerading permette inoltre di risparmiare sull'acquisto di IP pubblici per i singoli host (all'interno la gestione è a scelta dell'amministratore della rete, all'esterno appare sempre lo stesso IP).

FIREWALL: Siccome ogni sottorete in ogni edificio è collegata direttamente ad internet per poter sfruttare la VPN (quindi per accedere ai servizi internet esterni bisogna comunque passare attraverso il Ministero della magia) si è trovato necessario per una maggiore sicurezza mettere su ogni router di accesso un firewall adeguatamente configurato che permettesse l'accesso alle sole connessioni provenienti dalla VPN stessa e, anche per queste, che siano autorizzate per quella parte di rete. I firewall sono stati configurati mediante IPTABLE. In ogni firewall si procede inizialmente a svuotare le catene ed impostare una politica di default di scarto dei pacchetti se non viene diversamente specificato successivamente tra le regole.

Si è deciso di utilizzare una politica statefull, in quanto i firewall statefull sono in grado di riconoscere le connessioni e le trasmissioni, e, tenendone traccia, sono in grado di prendere decisioni in base a parametri aggiuntivi, come le connessioni esistenti ed i protocolli utilizzati.

Una regola comune nei nostri firewall è quella di limitare la creazione di nuove connessioni per evitare saturazione della rete e, quindi, possibili attacchi DoS (Denial of Service). In aggiunta a tale regola, si limitano le connessioni diverse da quelle di syn (nuova connessione) alle sole connessioni esistenti.

I firewall procedono infine a controllare l'accesso alle reti in base alle porte richieste, verificando così che lo scambio di pacchetti tra le sottoreti avvenga solo per utilizzare i servizi interni alle sottoreti.

SERVER AZIENDALE: Si richiedeva inoltre un particolare riguardo per quanto riguarda la sicurezza del server aziendale che essendo all'interno di una banca ha dei compiti molto delicati da

svolgere e necessita della massima sicurezza.

Per fare ciò è stato innanzi tutto pensato di aggiungere un firewall utilizzato per la sicurezza del server. Esso ha il compito di far passare solamente le connessioni provenienti dalla rete interna vietando quelle provenienti da un qualsiasi altro edificio. Si è poi provveduto ad effettuare un hardening aggiuntivo sulla macchina mediante i file `host.allow` ed `host.deny`, che permettono un ulteriore filtraggio delle connessioni. Inoltre un superiore livello di sicurezza si potrebbe ottenere, ipotizzando che il server aziendale abbia un sistema operativo UNIX/LINUX, è quello di patchare il kernel utilizzando GrSecurity che aggiunge al kernel molti strumenti per garantire un alto livello di sicurezza del kernel come ad esempio l'ottima implementazione delle ACL Posix.

L'implementazione delle ACL è stata evitata per ora in quanto si ritiene che le metodologie di protezione attualmente implementate siano sufficienti.

L'Amministratore della rete che contiene il server aziendale avrà molto da fare contro gli aggressori che tentano di violare la sicurezza della rete. Per questo è possibile facilitargli il compito installando sul server un Host IDS e magari un Network IDS sulla rete che lo contiene. Gli IDS (Intrusion Detecting System) sono semplicemente degli strumenti di analisi del traffico che hanno il compito di registrare tutto quello che avviene all'interno e soprattutto di registrare il traffico più anomalo.

Il problema di sicurezza maggiore per il Server aziendale rimane per gli attacchi che partono da dentro la rete. Purtroppo questo è possibile non solo perché il Server si trova su di essa ("Il computer più sicuro è un computer spento") ma anche perché quella particolare rete accetta anche connessioni wireless. Un qualsiasi attaccante sufficientemente bravo che si trovi con un portatile nei paraggi della banca potrebbe facilmente collegarsi e quindi far passare tutto il suo traffico, agli occhi del firewall Hagrid, come traffico lecito proveniente da dentro la Banca.

Per risolvere tale problema abbiamo deciso di inserire nelle catene di iptable una speciale regola che permette di accettare un intervallo di IP, specificando come intervallo solo quello degli IP fissi, escludendo così a priori gli IP assegnati dinamicamente mediante DHCP alla rete wireless.

Possiamo inoltre rendere più sicuro il server aziendale conoscendo la porta su cui lavora il software installato. Il software infatti è stato creato ad hoc per la banca Gringott, e lavora sulla porta 4321.

Nel firewall Hagrid si accetta quindi solo la connessione su quella porta.

BACKUP: Nella stessa rete abbiamo anche un server di Backup che ha il compito di memorizzare una copia sempre aggiornata del database contenuto nel server aziendale. All'interno della richiesta di avere un particolare riguardo per la sicurezza del server aziendale quindi rientra anche quello di tenere sicuro e lontano da utenti non autorizzati l'accesso al server di backup e le informazioni che esso contiene. Per questo entrambi i server si trovano dietro il firewall Hagrid. Mentre al server aziendale possono accedere tutti gli utenti autorizzati, al server di backup potrà accedere solamente l'amministratore attraverso una ssh (shell dei comandi criptata con RSA) e solo lui potrà quindi andare a modificare le configurazioni del server Backup e gestire tutte le sue funzioni. Tale limitazione dell'accesso avviene abilitando solo sulla macchina 190.84.60.2 il protocollo ssh.

Componenti Hardware utilizzati e loro collegamenti

- **Router:** Vengono utilizzati per semplicità router Juniper tutti con 5 interfacce sia per gli edifici "Ufficio Archivio Pratiche" e "Ufficio Aurore" che avrebbero bisogno solamente di 3 interfacce sia per il router interno della DMZ che necessita di tutte e 5 interfacce. I router acquistati hanno firewall e vpn integrata.
- **Moduli adattatori GBIC:** Questi dispositivi sono degli adattatori di segnali che collegati a tutti gli switch e fanno sì che il segnale venga trasformato da ethernet a fibra ottica. Sono ottimi per creare una backbone, una dorsale, su cui i dati viaggeranno all'interno dello stesso edificio sviluppato su più piani.
- **Switch:** si utilizzano switch di tre tipi:
 - Per gli edifici che non richiedono wireless si hanno degli economici Telesis da 48 porte

- dove la wireless è presente andranno usati anche degli switch 3Com da 52 porte “PWR” che hanno la possibilità di alimentare gli Access Point attraverso l’ethernet senza necessita di cavi di alimentazione aggiuntivi.
- Infine nelle zone dove ci sono i server essi saranno collegati con degli switch da 10Gigabit in modo da rendere lo scambio di dati tra loro molto più veloce e performante da sole 12 porte (non ne servono di più). Questo switch ad alta velocità è necessario soprattutto tra il server Aziendale e quello di Backup.
- **Access point Wireless:** si crea una wireless interamente 3Com dato che si acquisteranno degli access point 3Com fatti appositamente per ricevere l’alimentazione via cavo ethernet dagli switch installati
- **Cavo Ethernet:** si sceglie un cavo di tipo STP, di costo maggiore all'UTP, ma che garantisce una sicurezza maggiore alle interferenze grazie alla schermatura.
- **Fibra ottica:** necessaria per creare una buona dorsale su ogni edificio.
- **Firewall:** Abbiamo necessita anche di un buon firewall (Cisco) per proteggere il nostro server aziendale Vernon

Tipologie di HARDWARE Acquistato			
SWITCH		Switch Allied Telesis AT-8000S/48 (Economici)	388,00 Euro
		Switch 5500-EI PWR 3Com 52 porte (per wireless autoalimentate)	2.021,00 Euro
		Switch 3Com 4200G 12 porte (da 10Gb per i server)	579,00 Euro
Moduli adattatori GBIC		Modulo 1000Base SX SFP 3Com (2 per ogni switch)	155,70 Euro
Cavo di Rete		RJ45 CROSSOVER SSTP 5mt cat.5	0,86 Euro al metro
Fibra Ottica		Cavo patch duplex FO ST-ST 20	6,00 Euro al metro
Router + Firewall		Juniper Networks SSG 20 a 5 interfacce (supportano vpn e firewall)	857,20 Euro
Acces Point Wireless		Access Point LAN wireless gestito 3150	239,52 Euro
Firewall		Cisco ASA5505-SEC-BUN-K9 (Hagrid)	840,00 Euro

Fonti: Hardware con relative prezzi presi dal sito: <http://www.bechtle.it/>

Disposizione dell'hardware necessario

- Nel **Ministero della Magia** lavorano 270 dipendenti su 7 dipartimenti (divisi da 7 piani).
Si richiedono:
 - ✓ 7 Switch semplici (uno per piano)
 - ✓ 1 Switch da 10Gb da collegare i 3 server della DMZ
 - ✓ 16 GBIC (due per Switch)
 - ✓ 2 Router (Interno ed Esterno)
- Nell'**Ufficio Auror** sono presenti 3 piani.
Si richiedono:
 - ✓ 3 Switch semplici (uno per piano)
 - ✓ 6 GBIC (due per Switch)
 - ✓ 1 Router
- Nella **Banca Gringott** sono presenti 10 settori.
Si richiedono:
 - ✓ 10 Switch PWR
 - ✓ 1 Switch da 10Gb da collegare i 2 Server
 - ✓ 22 GBIC (due per Switch)
 - ✓ 1 Router
 - ✓ 1 Firewall per l'hardering del Server Aziendale
 - ✓ 10 Access Point wireless per la copertura della rete wireless
- Nell'**Ufficio Archivio Pratiche** vi lavorano 50 persone su 2 piani
Si richiedono:
 - ✓ 1 Router
 - ✓ 2 Switch PWR
 - ✓ 4 GBIC (due per Switch)
 - ✓ 2 Access Point Wireless per la copertura della rete wireless

Preventivo

In totale avremo:

10	Switch economici	per un prezzo di	3.880,00	Euro
12	Switch PWR	per un prezzo di	24.252,00	Euro
2	Switch da 10Gbit	per un prezzo di	1.158,00	Euro
44	Adattatori GBIC	per un prezzo di	6.850,80	Euro
5	Router con firewall e vpn	per un prezzo di	4.286,00	Euro
12	Access Point	per un prezzo di	2.874,24	Euro
1	Firewall	per un prezzo di	840,00	Euro
320m	Fibra ottica	per un prezzo di	1.920,00	Euro
5000m	Cavo Ethernet	per un prezzo di	4.300,00	Euro
	Progettazione e installazione della rete	per un prezzo di	10.000	Euro

TOTALE = 60.361,04 Euro