UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Facoltà di Ingegneria

Corso di Laurea in Ingegneria Informatica

GESTIONE DELLA RETE INFORMATICA AZIENDALE

a.a. 2009/2010

Nome: Nicola

Cognome: Lanza

Matricola: 563087

Tutore aziendale: Ing. Paolo Penzo

Tutore universitario: Prof. Ing. Fabrizio Dughiero

PREFAZIONE

Il seguente lavoro nasce dall'esperienza del tirocinio svolta presso l'azienda "Alveare" di gestione e progettazione reti informatiche nella sede dell'ospedale di Chioggia.

Il tirocinio ha avuto una durata complessiva di 6 mesi, strutturato in 500 ore suddivise in circa 25 settimane, dall'8 Marzo 2010 al 28 Agosto 2010.

Il lavoro svolto è stato quello di monitorare e gestire una grande rete privata contenente una grande quantità di dati, permettendo l'implementazione di innumerevoli servizi per la buona gestione dell'ospedale.

L'opportunità datami dall'azienda e dai collaboratori mi ha permesso di applicare le conoscenze apprese durante gli studi in un ambito diverso da quello universitario e più vicino all'ambito lavorativo futuro.

CAPITOLO 1 : SCENARIO APPLICATIVO

1.1 ORGANIZZAZIONE DEL LUOGO E DEL LAVORO SVOLTO

L’ufficio del CED (Centro Elaborazione Dati), dove si è svolto il mio tirocinio, è situato all’interno dello stabile di Villa Verde sede dell’ULSS 14 di Chioggia.

All’interno di tale stabile, oltre all’ufficio del CED, si trovano numerosi reparti dediti alla buona gestione e manutenzione dell’ospedale.

I compiti da me svolti all’interno del CED, sotto supervisione del tutore aziendale, sono stati di vario genere in base alle esigenze dell’azienda.

In particolare le principali attività svolte sono state:

- Gestione di Sistemi Operativi del CED e consulenza per strutture Client-server UNIX, Linux,Windows;
- Gestione software e hardware dei server del CED.
- Gestione della rete locale.
- Cura dei seguenti servizi di rete: posta elettronica, web server internet e intranet, IP e DNS, server FTP, server di accesso, server proxy http, server firewall, stampa in rete e connettività locale e geografica col protocollo TCP/IP.
- Monitoraggio attività dei server del CED, del traffico di rete e archiviazione di questi dati.
- Gestione di periferiche: Stampanti, X-Terminal, Terminal server, Print server, bridge wireless, Scanner e Plotter.
- Gestione delle memorie di massa e dei backup dati sui server del CED.

- Gestione delle chiamate di assistenza per interventi su hardware e corrispondente assistenza durante le operazioni di riparazione.

Il lavoro di monitoraggio della rete è stato effettuato da remoto, oppure fisicamente accedendo alla sala Server, situata in un’apposita sala di Villa Verde.

1.2 OBIETTIVO TIROCINIO

Durante il mio tirocinio ho avuto l’opportunità di mettere in pratica le nozioni imparate durante il percorso di studi, di relazionarmi con la realtà del mondo del lavoro come quello di un’azienda che gestisce la rete informatica dell’ente ospedaliero.

L’esperienza del tirocinio ha completato il mio percorso formativo di studi, in cui la parte teorica della materia viene applicata per la gestione, progettazione, e risoluzione della rete per il corretto funzionamento della struttura.

1.3 MOTIVAZIONI TIROCINIO

Le motivazioni che mi hanno spinto ad intraprendere questa esperienza sono state molte, in particolare la possibilità di capire come funziona il mondo del lavoro, e la possibilità di mettere in pratica tutto quello che ho studiato nel corso degli anni di università.

CAPITOLO 2 : DESCRIZIONE

2.1 STRUTTURA DELLA RETE

L’ospedale è composto da più sedi, distrettuali e ospedaliere, che hanno la necessità di essere collegate fra loro per l’utilizzo dei servizi informatici.

Ogni sede ha un collegamento con la sede centrale tramite una rete privata, grazie ad apposite VPN (Virtual Private Network), viene così a formarsi una rete a tipologia a “STELLA”.

Tutte le varie sedi possono comunicare tra loro passando per la sede centrale, che ne controlla i vari flussi di dati ed i vari accessi, compreso l’accesso ad internet.

La comunicazione tra le varie sedi e la sede centrale avviene tramite VPN (Virtual Private Network).

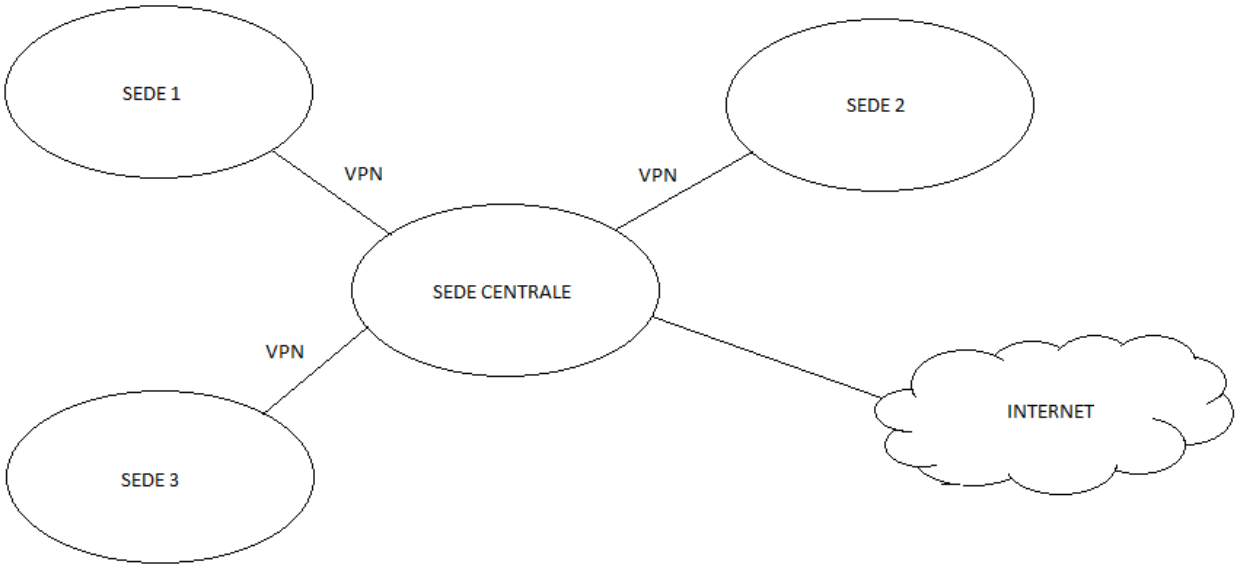

Figura 1.1: Comunicazione tra le varie sedi.

La protezione della rete interna da quella esterna è affidata al Firewall che agisce sui pacchetti in transito da e per la zona interna potendo eseguire su di essi operazioni di : controllo, modifica, monitoraggio.

La funzionalità principale in sostanza è quella di creare un filtro sulle connessioni entranti ed uscenti; in questo modo il dispositivo innalza il livello di sicurezza della rete e permette sia agli utenti interni che a quelli esterni di operare nel massimo della sicurezza.

Tra la rete esterna e la rete interna viene creata una speciale area chiamata DMZ (Demilitarized Zone) che è una zona demilitarizzata in cui sia il traffico esterno che quello interno sono fortemente limitati e controllati per poter implementare alcuni servizi che comunicano con l'esterno. All'interno di quest'area sono presenti tutti i server detti front-end, a cui corrispondono i relativi back-end nella rete interna.

La rete privata interna è costituita dalla LAN (Local Area Network) che permette la gestione dei dati aziendali.

La LAN principale è segmentata in più VLAN (Virtual LAN), tramite switch, in modo da poter limitare gli accessi alle varie risorse.

All'interno dei SERVER vengono conservati e gestiti i dati destinati ai vari servizi per i client della rete.

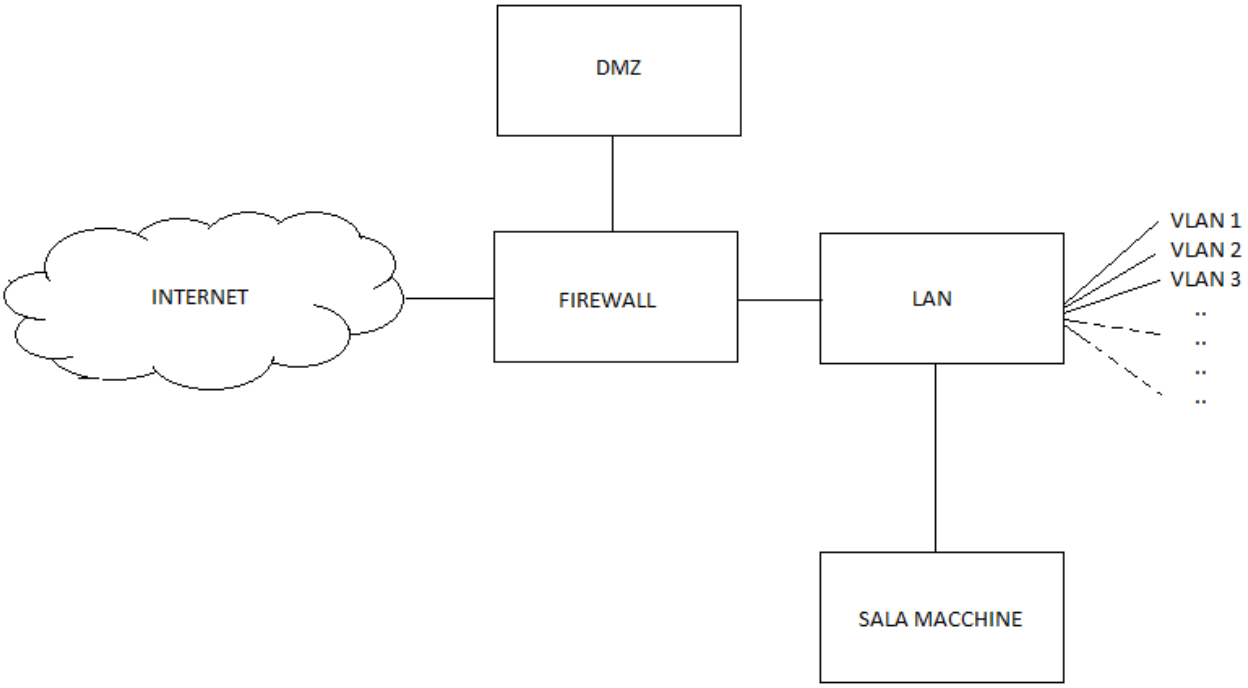

Figura1.2 : Rete interna di ogni sede.

2.2 SERVIZI E VANTAGGI OFFERTI DALLA RETE

La rete interna dell'azienda offre numerose opportunità per l'impresa, come ad esempio la disposizione di numerose applicazioni per la gestione amministrativa remota dell'azienda con un alto livello di protezione.

I vantaggi apportati dalla rete sono molti, tra i quali:

- Accesso protetto migliorato alle risorse aziendali. La connessione VPN migliora la protezione di accesso alla rete tramite una rigida conformità ai requisiti di aggiornamento antivirus e della protezione.
- Amministrazione e manutenzione semplificate dei servizi. Le organizzazioni possono uniformarsi agli standard delle tecnologie più sicure e aggiornate. Inoltre possono rimuovere le implementazioni VPN hardware, ad esempio i sistemi di computer di accesso remoto specializzati dell'infrastruttura di rete, semplificando in questo modo strumenti di supporto, documentazione e processi di connessione. Questa semplificazione consente di migliorare il supporto operativo quotidiano della soluzione di accesso VPN e di bilanciare i costi di gestione relativi all'implementazione di una soluzione di quarantena.
- Affidabilità e usabilità migliorate dell'accesso remoto**.** I miglioramenti apportati ad affidabilità e usabilità favoriscono l'utilizzo del servizio VPN da parte dei dipendenti, fornendo maggiori garanzie per la protezione di risorse aziendali critiche e di attività importanti.
- Costo totale di proprietà ridotto**.** Poiché i computer remoti devono essere conformi a rigidi criteri di affidabilità, vengono ridotti i costi complessivi di supporto e amministrazione. Questo risparmio deriva dalla riduzione delle chiamate di supporto e del tempo speso per bloccare gli attacchi di virus e worm.

- Protezione migliorata delle informazioni critiche per l'azienda. Le informazioni sui clienti hanno un'importanza fondamentale per la maggior parte delle organizzazioni, in particolare per quelle che operano in ambienti regolamentati. Assicurando la maggiore protezione possibile a queste informazioni vengono garantiti i requisiti di conformità alle norme.

- Processi aziendali migliorati. L'implementazione di una soluzione di connessione VPN consente di migliorare la disponibilità dei processi e delle applicazioni aziendali per i responsabili di vendita esterni, i responsabili della clientela e i consulenti. Questa disponibilità migliorata garantisce tempi di decisione più rapidi e una maggiore flessibilità nella fornitura di prodotti e servizi.

CAPITOLO 3 : GESTIONE

In questo capitolo vengono spiegate le fasi più importanti per la gestione della rete aziendale, i problemi ed gli eventuali metodi di risoluzione che ho affrontato quotidianamente durante il tirocinio.

Una nota importante è data dal fatto che la rete è formata da molti server e pc, i quali possono essere di dominio diverso come Linux o Microsoft, con relative diverse versioni.

Di seguito verrà spiegata la gestione della rete sotto dominio Microsoft, poiché la maggior parte delle macchine si trova sotto tale dominio; anche se l'implementazione della gestione nel dominio Linux non è molto diversa, se non per i software utilizzati.

3.1 GESTIONE ENTITA' ED ACCESSI

L'autenticazione degli utenti è necessaria per vari motivi nel corso del lavoro quotidiano; l'accesso alla rete, alle applicazioni, ai dati e alla posta elettronica ne sono esempi tipici.

Gli utenti possono collegarsi tramite un unico accesso a tutte le risorse, applicazioni e dati a cui l'utente è autorizzato ad accedere. Per gestire questi accessi controllati è necessaria, in una rete basata su prodotti Microsoft, un'infrastruttura di Active Directory che fornisca il supporto di base per molti servizi richiesti dall'organizzazione, tra cui messaggistica e collaborazione, gestione dei sistemi e servizi di protezione.

All’interno del sistema informatico dell’azienda, l’Active Directory è il servizio directory incentrato sulla rete incluso in Microsoft® Windows® 2000 e Windows Server® 2003.

A causa delle differenti competenze e ruolo ricoperto da ciascun utente,come ad esempio medici, infermieri, etc.., è necessario gestire le informazioni relative ad ogni utente e il loro utilizzo delle risorse informatiche con un unico sistema di autenticazione coerente che possegga le caratteristiche necessarie per rendere il più efficace possibile la gestione di queste informazioni. Per far questo il sistema di autentificazione :

- È organizzato e presentato come una directory.
- È supportato un metodo comune di richiesta, indipendentemente dal tipo di dati richiesto.
- Le informazioni con caratteristiche simili sono gestite in modo analogo.

Progettazione del servizio directory:

Il servizio viene implementato mediante l’uso di cinque categorie di directory:

- Directory ad uso specifico
- Directory delle applicazioni
- Directory incentrate sulla rete
- Directory a scopo generale
- Metadirectory

L’ amministratore Active Directory ha il controllo completo sul modo in cui vengono presentate le informazioni nella directory, queste informazioni sono raggruppate in contenitori denominati unità organizzative (OU), spesso organizzati in modo da semplificare l'archiviazione gerarchica dei dati. I tipi di dati archiviati nella directory vengono definiti tramite uno schema che ne specifica le classi

denominate oggetti. Un oggetto utente, ad esempio, corrisponde alla classe Utente definita nello schema, gli attributi dell'oggetto utente contengono informazioni, quali nome, password e numero di telefono dell'utente. L'amministratore può aggiornare lo schema in modo da includere nuovi attributi o classi, quando ve ne è la necessità.

Progettazione della struttura di Active Directory:

La struttura logica di Active Directory è considerata come una serie di directory logiche denominate domini. L'insieme dei domini è denominato foresta poiché i dati della directory in ogni dominio in genere sono organizzati in una struttura ad albero che rispecchia l'organizzazione.

L’implementazione e la progettazione della struttura logica consiste nelle seguenti operazioni:

1. Requisiti di progettazione della struttura logica. Le funzionalità di Active Directory per la delega amministrativa sono fondamentali nella progettazione della struttura logica. L'amministrazione delle OU organizzative può essere delegata per ottenere l'autonomia o l'isolamento di un servizio o dei dati. La delega amministrativa viene effettuata per soddisfare i requisiti legali, operativi e organizzativi della struttura.

2. Progettazione della foresta. Un modello di progettazione della foresta viene selezionato dopo aver determinato il numero appropriato di foreste nel processo di progettazione del servizio; ad esempio, quando sono necessarie diverse directory o le definizioni degli oggetti cambiano all'interno di un'organizzazione.

3. Progettazione del dominio. Viene selezionato un modello di dominio per ogni foresta.

4. Progettazione radice della foresta. Le decisioni relative alla radice della foresta si basano sulla progettazione del dominio, se viene selezionato

un modello di dominio singolo, quest'ultimo funziona da dominio radice della foresta, se viene selezionato un modello di dominio regionale, il proprietario della foresta deve determinare la radice della foresta.

5. Pianificazione dello spazio dei nomi di Active Directory. Una volta determinato il modello di dominio per ogni foresta, è necessario definire lo spazio dei nomi per la foresta e i domini.

6. Infrastruttura DNS per supportare Active Directory. Dopo aver progettato le strutture di dominio e la foresta di Active Directory, è possibile completare la progettazione dell'infrastruttura Dynamic Name System (DNS) per Active Directory.

7. Creazione della progettazione di un'unità organizzativa. Le strutture delle OU sono univoche per il dominio a differenza della foresta, quindi ogni proprietario di dominio è responsabile della progettazione della struttura della OU per il proprio dominio.

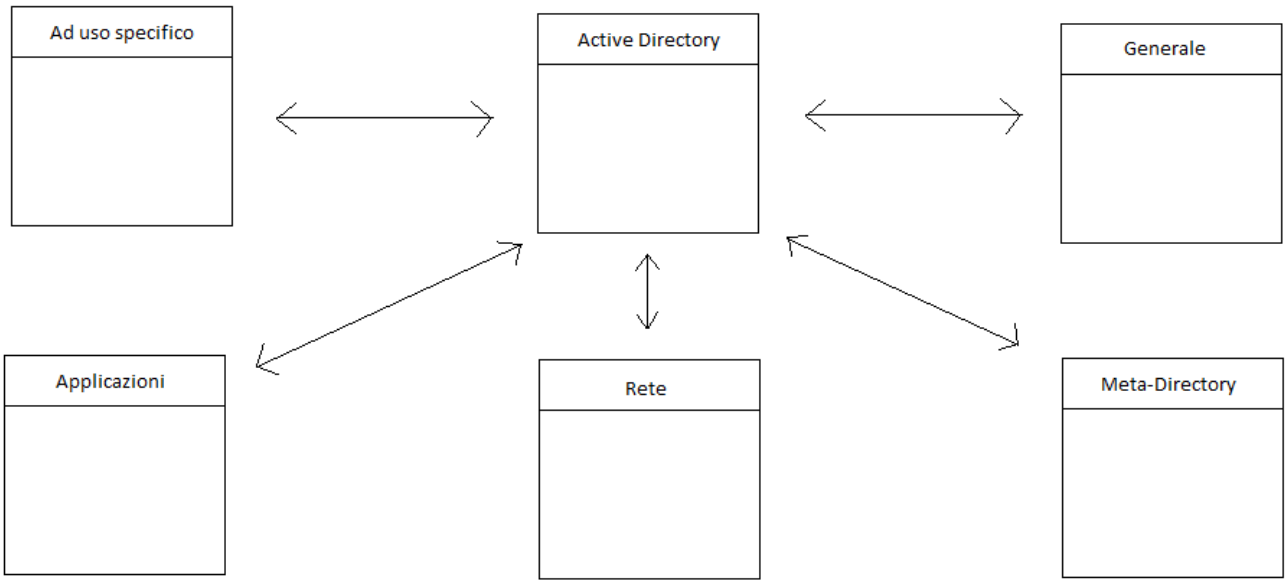

Figura 1.3 : Suddivisione della Active Directory.

3.2 DEFINIZIONE POLITICHE DI SICUREZZA E PRIVACY

L’azienda gestisce una grande quantità di dati personali relativi ad ogni utente, e tali dati sono soggetti alla legge sulla privacy.

Dal 1 Gennaio 2004, approvato con decreto legislativo del 30 giugno 2003 n.196 la nuova legge sulla privacy è stata creata in sostituzione della vecchia legge 675/1996 in modo più semplificativo e armonizzato per non aggravare le aziende e le persone fisiche di vincoli burocratici molto forti.

In particolare il terzo articolo cita:

“I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente dati anonimi od opportune modalità che permettono di identificare l'interessato solo in caso di necessità.”

(Codice privacy, d.lgs 196., Articolo 3)

Il Codice prevede, per chi intende trattare dati, una serie di obblighi e di diritti. Infatti chiunque voglia utilizzare i dati personali di un soggetto deve informarlo, preventivamente, indicando con chiarezza le finalità per cui prevede di utilizzare tali dati e le relative modalità di utilizzo. Inoltre deve avere il consenso da parte del soggetto interessato. In base a tale legge, l’azienda deve adempiere l’obbligo della protezione e trattamento dei dati dei singoli utenti.

Per fare ciò ogni utente appartiene ad un gruppo (per esempio gli utenti vengono divisi in medici,infermieri, etc….) ed ogni gruppo può accedere, tramite username e password, solo ad alcune risorse che vengono affidate in base alle competenze del loro ruolo all’interno dell’azienda.

Anche le risorse, dati e servizi, vengono suddivisi in gruppi, il cui accesso verrà permesso o negato ai vari gruppi in base alla necessità.

Le regole di accesso vengono implementate tramite una lista di controllo degli accessi, spesso chiamata col nome inglese di Access Control List (ACL), che ne permette appunto le politiche d'accesso.

Questa suddivisione avviene grazie alle VLAN (Virtual Local Area Network) le quali segmentano la LAN principale in diverse parti, alle quali i gruppi possono accedere; in questo modo ogni VLAN permette l'accesso a particolari risorse e servizi in base alle politiche adottate.

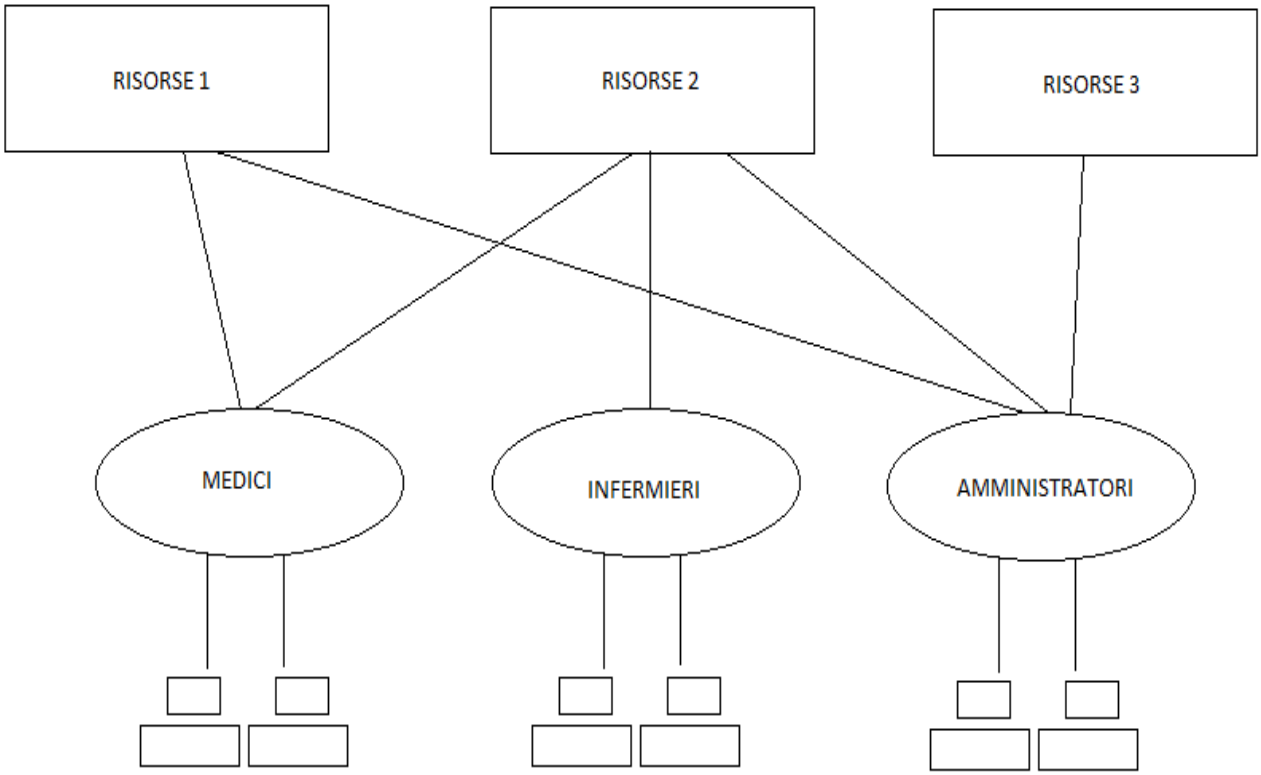

Figura 1.4 : Suddivisione utenze e risorse in gruppi

3.3 AGGIORNAMENTI

Il controllo degli aggiornamenti, rappresenta la gestione della distribuzione delle patch ed eventuali aggiornamenti.

Per la gestione di questo servizio, l'azienda utilizza una serie di strumenti, utilities e prodotti Microsoft che semplificano la fase di valutazione del controllo e distribuzione delle patch in modo centralizzato.

Queste tecnologie includono:

- Microsoft Windows Server® Update Services (WSUS)

All'interno dell'azienda, per la gestione della stessa, vengono usati numerosi software, i quali ogni periodo di tempo sono soggetti ad aggiornamenti. Uno dei problemi più importanti che nasce da questa operazione di aggiornamento, è il fatto di creare conflitti tra questi software a causa degli aggiornamenti che vengono installati. Per questo tutti gli aggiornamenti vengo scaricati in un server dedicato dal sistema WSUS di Microsoft, il quale grazie a politiche adottate dai tecnici dell'azienda, decide quali aggiornamenti inviare ai vari pc e server.

Gli obiettivi della fase di identificazione e selezione degli aggiornamenti sono i seguenti:

- Individuare in maniera affidabile i nuovi aggiornamenti software.
- Stabilire se gli aggiornamenti software sono pertinenti per il proprio ambiente di produzione e che non costituiscono motivo di conflitto fra software.
- Ottenere i file di origine degli aggiornamenti software e controllare la loro sicurezza e che vengano installati correttamente.
- Determinare se gli aggiornamenti software debbano essere considerati urgenti.

L'obiettivo nella fase di stima e pianificazione consiste nel prendere una decisione sulla distribuzione o meno dell'aggiornamento software, nello stabilire le risorse necessarie per la sua distribuzione e nel “testare” l'aggiornamento software in un ambiente simile a quello di produzione per controllare che non comprometta le applicazioni e i sistemi critici per l'attività dell'azienda.

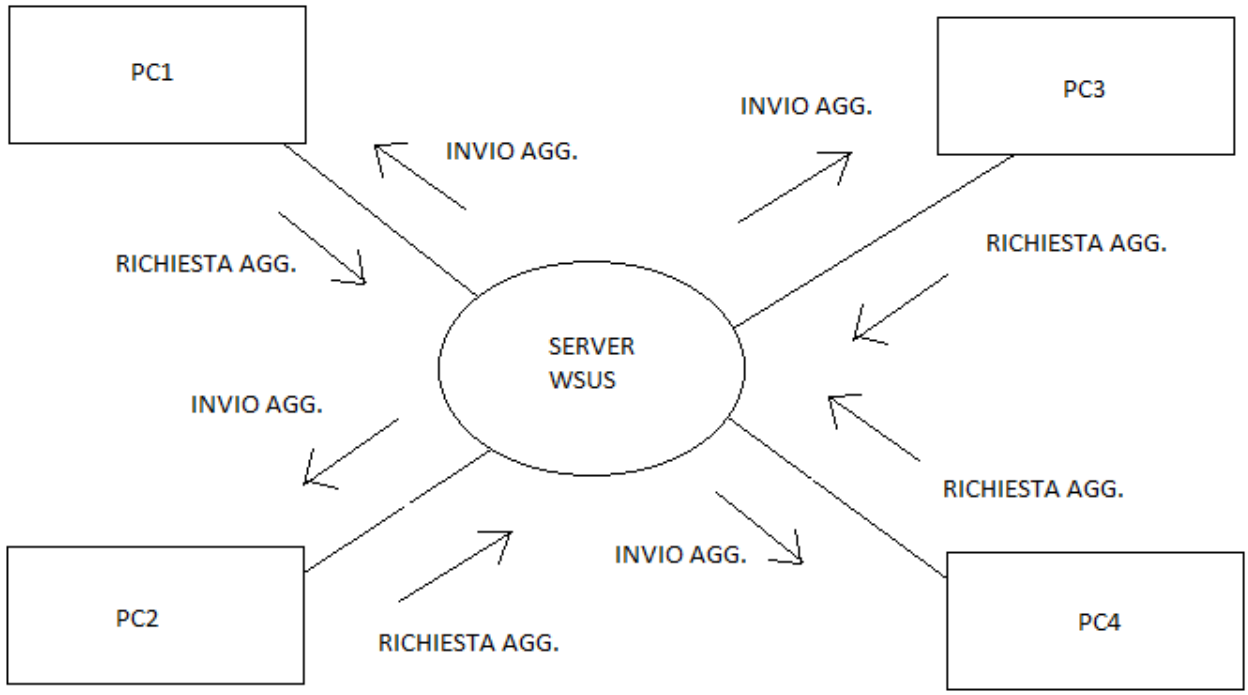

Figura 1.5 : Funzionamento richiesta e distribuzione aggiornamenti.

L'obiettivo durante la fase di distribuzione invece è quello di distribuire correttamente l'aggiornamento software approvato nell'ambiente di lavoro, grazie ad una serie di strumenti e prodotti come WSUS, con il quale è possibile automatizzare la distribuzione e l'installazione degli aggiornamenti software.

3.4 BACKUP

L’azienda gestisce una gran quantità di dati, quindi l'archiviazione, il ripristino e il recupero dei dati sono attività di gestione dell'archiviazione essenziali.

I centri dati possono utilizzare componenti ridondanti e tecnologie per la tolleranza di errore (quali il clustering di server e il mirroring del software o dell'hardware) per assicurare un'elevata disponibilità tramite la replica dei dati fondamentali. Può essere necessario che le informazioni vengano archiviate per motivi di controllo o legali all’interno di SERVER dedicati a tale scopo, ed è necessario disporre di una strategia di protezione dei dati che includa un piano completo di backup e recupero per proteggere i dati da qualsiasi tipo di interruzione o danno non previsto.

Per salvaguardare la conservazione di tali dati, l’azienda predispone di particolari supporti per la memorizzazione di massa, come Storage e cassette.

In modo ciclico a distanza di un lasso di tempo preciso, i server subiscono un BACKUP che può essere di vario tipo in base alla politica adottata per la macchina:

- Backup completo (o Full backup): un backup di tutti i file del sistema. A differenza della disk image, un full backup non include le tavole di allocazione, le partizioni ed i settori di boot.
- Backup Differenziale: backup cumulativo di tutti i cambiamenti effettuati a partire dall'ultimo backup completo (o full backup). Il vantaggio è il minor tempo necessario rispetto ad un backup completo. Lo svantaggio è che i dati da salvare aumentano per ogni giorno trascorso dall'ultimo backup.
- Backup Incrementale: backup che contiene tutti i file cambiati dall'ultimo backup (completo e incrementale). Il backup incrementale è più rapido di quello differenziale ma richiede tempi di restore più lunghi poiché è

necessario partire dall'ultimo backup completo e poi aggiungere in sequenza tutti i backup incrementali.

In questo modo, utilizzando una delle tre metodologie di backup, l’azienda predispone un piano di ripristino e protezione dei dati, che le consente la reperibilità di tutti i dati, persi a causa di guasti o imprevisti.

3.5 PROTEZIONE INFORMATICA DELLA RETE

La rete interna dell’azienda è protetta dalla rete esterna dal Firewall, il quale monitorizza i pacchetti dall’esterno verso l’interno e viceversa; ma l’intrusione oppure lo svilupparsi di un virus può avvenire anche dall’interno della rete. Per questo motivo, all’interno della rete vengono adottate diverse politiche per la protezione interna, utilizzando alcuni componenti, tra cui:

- Software antivirus per computer desktop e server
- Servizi firewall centralizzati
- Monitoraggio della disponibilità dei server critici

L’azienda dispone di un software antivirus standard installato su ogni computer client, un firewall perimetrale centralizzato, servizi di monitoraggio della disponibilità per i servizi critici.

Quando un'applicazione software dannosa raggiunge un computer host, i sistemi di difesa sono mirati a proteggere il sistema host e i relativi dati impedendo la diffusione dell'infezione. Queste difese non sono meno importanti delle difese a livello di protezione fisica e di rete del proprio ambiente.

Il firewall personale o basato su host rappresenta un importante livello di difesa dei client, in particolare sui computer portatili che potrebbero essere portati dagli utenti all'esterno degli usuali sistemi di difesa della rete. Questi firewall filtrano tutti i dati che si tenta di immettere o di prelevare da uno specifico computer host.

I firewall costituiscono un elemento principale del mantenimento della protezione e della sicurezza dei computer della rete. Tutti i computer necessitano della protezione di un firewall, sia che si tratti dei numerosi server o desktop che costituiscono la rete dell’azienda.

L’implementazione della strategia Firewall all’interno dell’azienda, avviene per l’esigenza di conservare e proteggere informazioni riservate della rete.

La rete offre numerosi servizi legati anche alla rete Internet, per fornire anche il più comune di questi servizi, ad esempio la posta elettronica, la rete interna deve collegarsi a Internet. Facendo questo, tali sistemi diventano accessibili da fonti esterne e, quindi, vulnerabili ad attacchi.

Per questo motivo tali servizi vengono inseriti all’interno di una DMZ (Demilitarized Zone) che è un segmento isolato di LAN (una "sottorete") raggiungibile sia da reti interne che esterne che permette, però, connessioni esclusivamente verso l'esterno.

I firewall di rete proteggono un'intera rete controllandone il perimetro, inoltrano il traffico proveniente e diretto ai computer su una rete interna e filtrano tale traffico in base ai criteri impostati dall'amministratore.

Quelli all’interno dell’azienda, sono basati sia su hardware che su software. I firewall basati su software possono essere eseguiti anche sullo stesso server di altri servizi quali la posta elettronica e la condivisione di file, permettendo un miglior uso dei server esistenti.

I Firewall che proteggono la rete interna da quella esterna sono di tipo hardware e sono due, entrambi clusterizzati per garantire il servizio anche in caso di guasto.

Per la gestione di tale servizio di protezione, i Firewall implementati forniscono vari servizi come ad esempio il bloccaggio oppure lo scorrimento del traffico mediante un’ampia gamma di tecniche che garantiscono gradi diversi di protezione.

Le seguenti funzionalità firewall, attraverso le quali la rete può essere protetta, sono elencate in ordine crescente di complessità:

- Filtri di input della scheda di rete

- Filtri di pacchetti statici
- Network Address Translation (NAT)
- Stateful Inspection
- Controllo a livello di circuito
- Filtraggio a livello di applicazione

Grazie a tali funzionalità la rete può essere protetta.

Gli amministratori della rete aziendale, nel valutare la connettività della rete protetta, considerano:

- Protezione
- Complessità gestionale
- Costo

Ed in base a questi tre punti fondamentali, viene decisa la politica da adottare per la rete aziendale.

Per il monitoraggio della rete invece vengono utilizzati anche altri sistemi, come ad esempio il filtraggio dell'input della scheda di rete, filtri di pacchetti statici.

Il filtraggio dell'input della scheda di rete consente di esaminare gli indirizzi di origine e di destinazione e altre informazioni del pacchetto in ingresso per bloccarlo o lasciarlo passare. Questo tipo di filtraggio viene applicato solo al traffico in ingresso, Network Address Translation (NAT), Proxy e filtraggio a livello di applicazione.

I filtri di pacchetti statici associano le intestazioni IP per determinare se consentire o meno il passaggio del traffico attraverso l'interfaccia. Questo tipo di filtraggio viene applicato sia al traffico in ingresso che in uscita.

La tecnologia NAT converte un indirizzo privato in un indirizzo Internet. Sebbene NAT non sia propriamente una tecnologia firewall, l'occultamento del reale indirizzo IP di un server impedisce agli autori degli attacchi di acquisire informazioni importanti sul server.

Il firewall proxy raccoglie le informazioni per il client e restituisce i dati ricevuti dal servizio al client.

Il livello più sofisticato di controllo del traffico del firewall è rappresentato dal filtraggio a livello di applicazione, un buon filtro applicativo consente di analizzare un flusso di dati relativo a una determinata applicazione e garantisce particolari attività di elaborazione.

L’azienda inoltre possiede anche un sistema di antispam hardware suddiviso in due elementi clusterizzati, che permettono il filtraggio e quindi il monitoraggio della posta in arrivo.

In conclusione, all’interno dell’azienda, vengono utilizzati tutti questi servizi, per garantire la protezione della rete, sia dall’esterno che dall’interno.

Oltre a tutti questi metodi di protezione, la rete utilizza anche il sistema ISD (Intrusion Detection System) il quale può essere sia hardware che software e permette l’identificazione d’accessi non autorizzate alla rete.

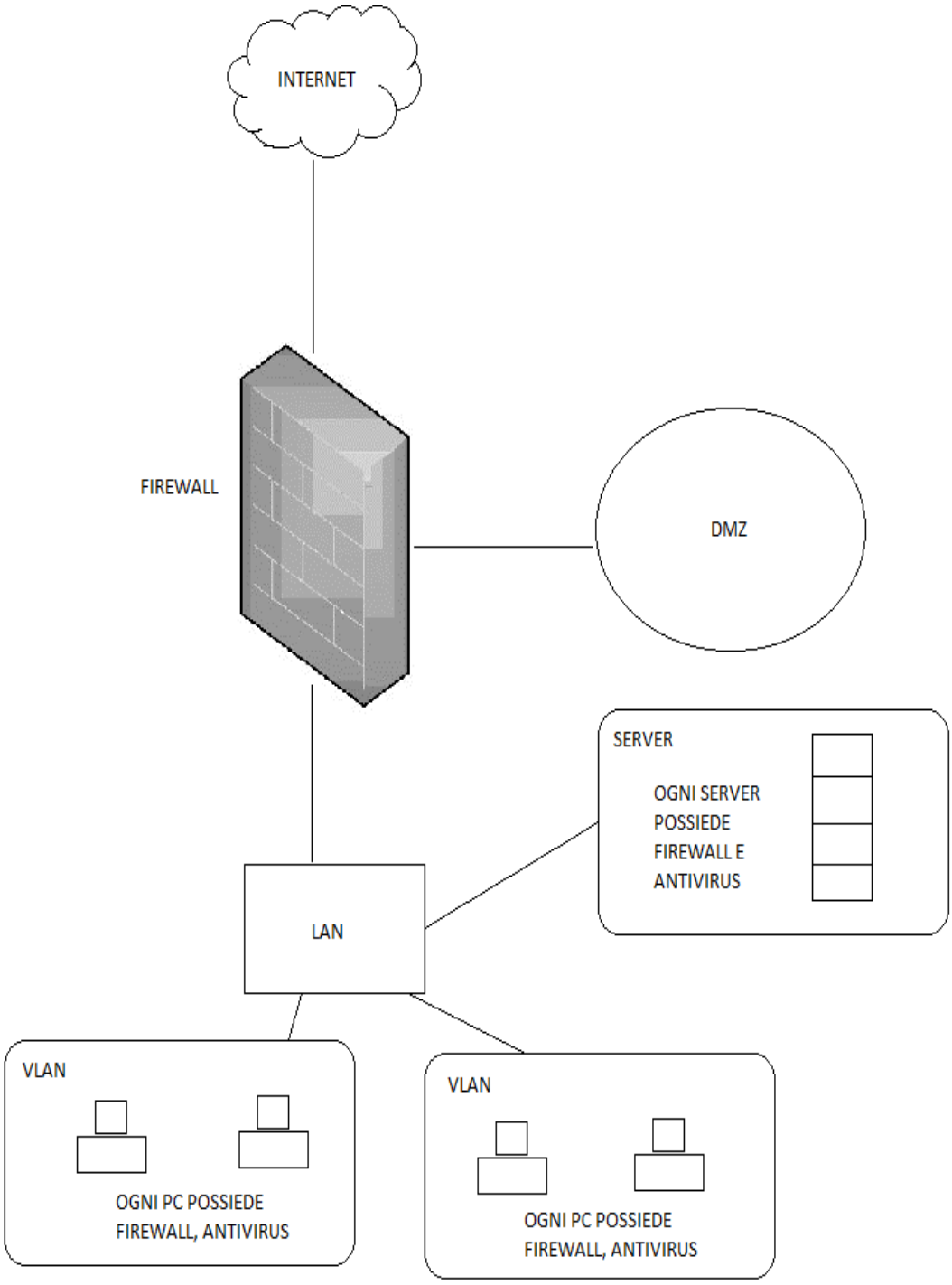

Figura 1.6 : Protezione della rete

3.6 PROTEZIONE FISICA DELLA RETE

La sicurezza informatica della rete è affiancata dalla sicurezza fisica che ne garantisce un'ulteriore livello di protezione. Questo è dovuto al fatto che i dati contenuti ed il traffico sulla rete sono soggetti alla legge sulla privacy e quindi devono essere protetti e tutelati dal gestore della rete.

I cablaggi ed i cavi, che collegano le varie sedi, per questione di sicurezza non si appoggiano su quella regionale ma su appositi supporti. In questo modo l'accesso alla rete esterna può avvenire solo attraverso il firewall riducendo al minimo la possibilità di intrusioni esterne.

I server, che contengono i dati dell'azienda, si trovano all'interno di un'apposita stanza climatizzata per evitare il surriscaldamento delle macchine e sono raggiungibili mediante un sofisticato sistema d'accesso controllato a serratura elettronica.

Tale sistema d'accesso, viene usato anche per proteggere i locali aziendali implementando anche un sistema di videosorveglianza.

Inoltre per evitare un possibile black out delle rete energetica oppure di guasto agli organi della rete, esiste un sistema di ridondanza che permette di offrire il servizio richiesto anche in caso di guasto, in particolare tutti i cavi che collegano le varie sedi sono doppi ed ogni sede dispone di un gruppo elettrogeno che si attiva in caso di necessità per garantire comunque il buon funzionamento della azienda, oppure il clustering del firewall e dell'antispam il quale suddivide il compito affidato a tale componente a due organi separati ma identici in modo da poter usufruire di uno dei due se l'altro si danneggia.

In questo modo la sicurezza fisica unita a quella informatica permette una protezione adeguata della rete da attacchi esterni ed interni alla rete.

3.7 GESTIONE DELLA RETE

La rete è composta da numerosi computer e da molti server, che hanno la necessità di comunicare tra di loro sulla rete LAN, per fare questo ogni dispositivo deve disporre di un'identità che può essere il nome del dispositivo logico o l'indirizzo che identifica in modo univoco il dispositivo e la sua posizione nella rete.

La distribuzione dei nomi e degli indirizzi, poiché la rete dispone di molti dispositivi, non può essere gestita manualmente, per questo la rete dispone di DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol) e WINS (Windows Internet Naming) che sono tre meccanismi essenziali per la fornitura di servizi di gestione e assegnazione di indirizzi IP dei PC dell’azienda.

Lo scopo principale di DNS è quello di convertire nomi host facili da leggere e da ricordare in indirizzi IP numerici. Tra le tante funzionalità, DNS risolve anche indirizzi di posta elettronica per individuare lo specifico server di scambio di posta elettronica del destinatario.

DHCP è un protocollo che consente a un computer, un router o un altro dispositivo di rete di richiedere e ottenere un indirizzo IP univoco e altri parametri come una subnet mask da un server che contiene un elenco di indirizzi IP disponibili per una rete.

WINS è un servizio di risoluzione dei nomi NetBIOS che consente ai computer client di registrare i nomi NetBIOS e gli indirizzi IP in un database dinamico e distribuito e di risolvere i nomi NetBIOS delle risorse di rete nei relativi indirizzi IP.

WINS e DNS sono entrambi servizi di risoluzione dei nomi per reti TCP/IP. Mentre WINS risolve i nomi nello spazio dei nomi NetBIOS, DNS risolve i nomi nello spazio dei nomi del dominio di DNS. WINS principalmente supporta i client

su cui sono in esecuzione le precedenti versioni di Windows e le applicazioni che utilizzano NetBIOS.

All’interno della rete i servizi e gli host di rete vengono configurati con i nomi DNS affinché possano essere individuati nella rete. Vengono anche configurati con i server DNS che risolvono i nomi dei controller di dominio di Active Directory.

Stabilire i server DNS interni consente di avere massima flessibilità e controllo sulla risoluzione dei nomi dei domini interni ed esterni. Ciò riduce il traffico di rete Internet e Intranet.

All’interno della rete è stato anche predisposto un server DHCP il quale fornisce i seguenti vantaggi:

- Configurazione affidabile dell'indirizzo IP**.** DHCP consente di ridurre al minimo gli errori di configurazione causati dalla configurazione manuale dell'indirizzo IP, come gli errori tipografici o i conflitti di indirizzo provocati dall'assegnazione dello stesso indirizzo IP a diversi computer contemporaneamente.

- Amministrazione della rete ridotta**.** DHCP comprende le seguenti funzionalità che consentono di ridurre le attività di amministrazione della rete:

    1. Configurazione TCP/IP automatizzata e centralizzata.

    2. Possibilità di assegnare una gamma completa di valori di configurazione TCP/IP aggiuntivi tramite le opzioni DHCP.

    3. Inoltro dei messaggi DHCP iniziali tramite un agente di inoltro DHCP che risulta nell'eliminazione dell'esigenza di disporre di un server DHCP su ogni subnet.

I componenti di Windows Server 2003 che richiedono la risoluzione dei nomi tenteranno di utilizzare questo server DNS prima di provare a utilizzare il precedente servizio di risoluzione dei nomi Windows predefinito, WINS.

Se l'organizzazione dispone di computer su cui sono in esecuzione sistemi operativi precedenti a Windows 2000, viene implementato WINS per questi sistemi.

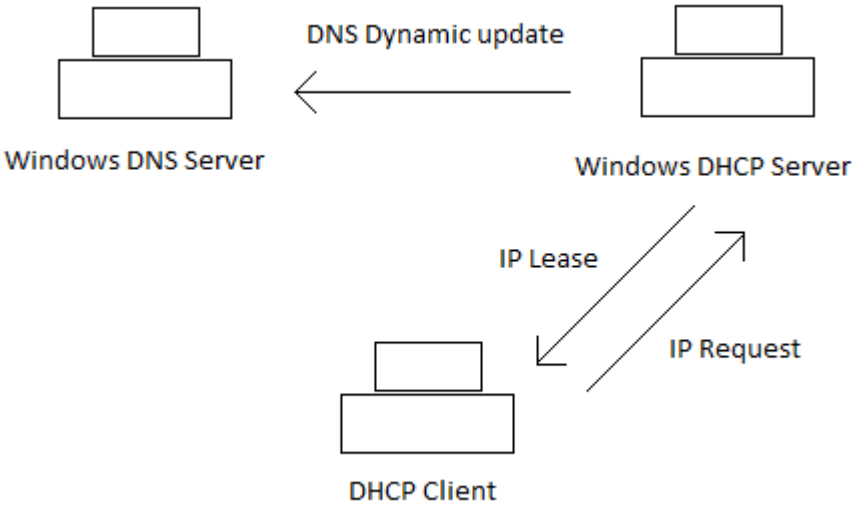

Figura 1.7 : Richiesta dell’indirizzo IP da parte di un client.

3.8 GESTIONE DELLA RETE WIRELESS

All’interno di ogni sede è stata implementata una struttura wireless per garantire l’accesso alla rete dati interna da parte dei propri operatori e la contemporanea possibilità di offrire ai pazienti, ai visitatori ed agli utenti esterni l’accesso alla rete internet con il massimo grado di sicurezza attualmente possibile in unione ad un’ampia flessibilità di utilizzo. La rete wireless inoltre è stata progettata in modo da potersi adattare dinamicamente alle esigenze di una moderna rete mobile multiservizi.

La gestione di tale rete è centralizzata tramite uno specifico modulo wireless posizionato nel cuore della rete, mentre gli apparati radio, chiamati Radio Port, sono dislocati nei vari reparti e sono semplici ricetrasmittenti complete di antenne ma senza configurazioni personalizzate. Tali Radio Port funzionano in abbinamento con il modulo wireless per offrire servizi wireless avanzati, sono dotate di antenna integrata ed offrono una soluzione economica per la rete wireless. In questo modo tramite uno switch, l’amministrazione della rete diventa centralizzata per la gestione della rete wireless unificata; tale approccio centralizzato semplifica la configurazione dei dispositivi e l’amministrazione della sicurezza e delle policy utente basate su identità che sono applicate alla periferia della rete indipendentemente da come e dove l’utente si connette.

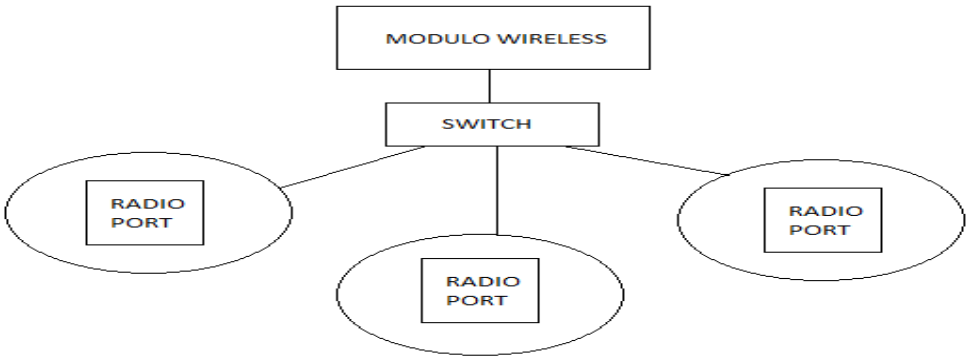

Figura 1.8 : Rete Wireless

Tale rete permette una disponibilità di accesso a tutti gli apparati provvisti di scheda wireless con standard 802.11, con una fruibilità riportata in tabella:

Standard	Frequency	Data rates	Typical maximun throughput*
802.11b	2.4 Ghz	1, 2, 5.5, 11 Mbps	5 Mbps
802.11g	2.4 Ghz	6, 9, 12, 18, 24, 36, 48, 54 Mbps	22 Mbps
802.11a	5 Ghz	6, 9, 12, 18, 24, 36, 48, 54, Mbps	22 Mbps

La soluzione supporta il roaming ‘layer 2’ tra le celle. Il tempo massimo di passaggio tra una cella ed un’altra è inferiore ai 50 millisecondi. Queste tempistiche sono fondamentali soprattutto in presenza di connessioni *time-sensitive* quali possono essere la telefonia su IP o le applicazioni video.

Viene fornito un solo punto, il modulo wireless, per configurare a livello di sistema il setup e le operazioni della LAN wireless, incluso SSID, sicurezza, opzioni di autenticazione e servizi avanzate wireless. Le impostazioni LAN wireless vengono assegnate automaticamente alle rispettive Radio Port, eliminando i costi e i tempi associati alla configurazione individuale degli access point.

In caso di guasto di una radio port, il modulo adegua automaticamente la potenza di trasmissione e la velocità di trasferimento dei dati alle Radio Port adiacenti per mantenere la copertura LAN wireless. Il sistema ricalibra automaticamente l’assegnazione dei canali alle radio port per evitare interferenze di tipo ambientale o altre interferenze wireless basate su 802.11. L’obbiettivo che si vuole raggiungere è la massima sicurezza nell’accesso a la possibilità di assegnare diritti e policy personalizzate in base alle diverse tipologie di utente. Ad esempio il visitatore potrà solo navigare previa assegnazione di istruzioni del caso (password, smart card o altro). Il personale medico potrà invece avere un accesso più completo compreso

l’utilizzo dei software a lui necessari. Per tale motivo la soluzione prevede differenti modalità di autenticazione alla rete wireless elencati di seguito.
Elenco delle modalità di autenticazione possibili:

- Sicurezza tramite SSID (4 BSSID/16 SSID per radio):

domini multipli di broadcast wireless con sicurezza, autenticazione e configurazione di policy separate per SSID che forniscono controllo dell’accesso alle risorse di rete in base all’autenticazione dell’utente e al livello di sicurezza affidabile tra utente wireless e rete.

- Scelta tra IEEE 802.11i, Wi-Fi Protected Access 2 (WPA2) o WPA:

blocco di accesso wireless non autorizzato mediante autenticazione degli utenti prima di garantire accesso alla rete; la robusta crittografia Advanced Encryption Standard (AES) o Temporal Key integrità Protocol (TKIP) garantisce l’integrità dei dati del traffico wireless.

- IEEE 802.1X: autenticazione degli utenti con supporto per il protocollo EAP (Extensible Authentication Protocol) MD-5, TLS, TTLS e PEAP con scelta tra AES, TKIP e crittografia WEP statica o dinamica per la protezione del traffico wireless tra client autenticati e access point.
- Autenticazione Web: come per l’autenticazione 802.1X, l’autenticazione Web fornisce un ambiente basato su browser per l’autenticazione di client che non supportano il supplicant 802.1X.
- Autenticazione MAC: il client è autenticato con il server basato sull’indirizzo MAC del client, utile per client che hanno interfaccia utente minima o nessuna interfaccia utente.
- Rilevamento di access point non autorizzati: il modulo Wireless offre una vista a livello di sistema di tutti gli access point rilevati nell’area di copertura della LAN wireless. Gli access point rilevati sono facilmente classificati come autorizzati o non autorizzati per semplificare il monitoraggio di rete. Ciascuna Radio Port effettua una scansione simultanea

per rilevare la presenza di altri access point mentre fornisce servizi ai client wireless.

Per il monitoraggio della rete wireless le Radio Port sono configurate in modo da controllare continuamente il buon funzionamento della rete:

- Accesso sicuro alla gestione: tutti i metodi di accesso come CLI, GUI o MIB sono crittografati in modo sicuro mediante SSHv2, SSL e/o SNMPv3.
- VLAN di gestione: segmentazione del traffico verso e dalle interfacce di gestione, incluse
  - CLI/telnet
  - interfaccia browser
  - Web
  - SNMP
- Blocco del traffico tra stazioni: prevenzione della comunicazione tra dispositivi client associati alla stessa porta radio.
- Sistema chiuso: restrizione del broadcast di SSID come misura di sicurezza per mascherare la presenza della rete wireless.

La gestione della rete wireless con questo approccio permette di usufruire di innumerevoli vantaggi per l'amministrazione e per l'azienda:

➢ Flessibilità e disponibilità elevata

• Rete con funzionalità self-healing : in caso di guasto di una radio port, le radio port adiacenti adeguano la potenza di trasmissione e la velocità di trasmissione dei dati per mantenere la copertura LAN wireless.

• Rilevamento rete wireless e prevenzione di interferenze: le radio port ricalibrano automaticamente l'assegnazione dei canali per evitare interferenze di tipo ambientale o altre interferenze wireless basate su 802.1.

➢ Protezione

• Scelta tra IEEE 802.11i, Wi-Fi Protected Access o WPA: blocca l'accesso wireless non autorizzato autenticando gli utenti prima che possano accedere alla rete.

• Autenticazione basata sul Web: come per il modello 802.1X, fornisce un ambiente basato su browser per l'autenticazione di client che non supportano supplicant 802.1X .

• Autenticazione MAC : un client wireless è autenticato con un server in base all'indirizzo MAC del client; questa soluzione è utile per i client con un'interfaccia utente minima o privi di interfaccia utente

• Rilevamento di access point non autorizzati : Ciascuna radio port effettua una scansione simultanea per rilevare la presenza di altri access point mentre forniscono servizi ai client wireless.

• Blocco del traffico tra stazioni: prevenzione della comunicazione tra dispositivi client associati alla stessa radio port.

• Access control list (ACL): fornisce filtro IP layer 3 basato sul campo sorgente/destinazione dell'indirizzo IP ed inoltre dei campi sottorete e sorgente/destinazione del port number TCP/UDP.

• Network Address Translation (NAT): la scelta di NAT statico o dinamico conserva il pool di indirizzi IP di una rete o nasconde l'indirizzo privato delle risorse di rete, quali server Web, resi disponibili per gli utenti di una LAN wireless pubblica o per ospiti.

• Sistema chiuso: restrizione del broadcast di SSID come misura di sicurezza per nascondere la presenza della rete wireless.

➢ Connettività

• Architettura ad accesso radio singolo IEEE 802.11g : offre una soluzione estremamente economica per installazione LAN wireless.

• Antenna diversity integrata con copertura onnidirezionale: valida copertura LAN wireless per uffici con ambienti aperti.

• Configurazione internazionale: configurate centralmente sul modulo Wireless, tutte le radio port si adattano automaticamente per soddisfare i requisiti normativi.

• Selezione automatica del canale (ACS): consente di ridurre l'interferenza radio sullo stesso canale mediante selezione automatica di un canale radio non occupato.

• Corrente in uscita regolabile: controllo dimensioni cella per implementazioni di access point ad alta densità di utenti.

➢ Qualità di servizio (QoS) avanzata

• Supporto WMM Wi-Fi : garantisce funzionalità QoS nella rete wireless grazie a priorizzazione del traffico wireless di diverse applicazioni.

➢ Gestione

• Gestione centralizzata: viene fornita una soluzione di accesso centralizzato per configurare a livello di sistema il setup e le operazioni della LAN wireless, incluso l'SSID (Service Set Identifier), la sicurezza, le opzioni di autenticazione ed i servizi avanzati wireless. Le impostazioni LAN wireless vengono assegnate automaticamente alle rispettive radio port, eliminando i costi ed i tempi associati alla configurazione individuale degli access point.

3.9 GESTIONE SERVER

L’azienda possiede numerosi server implementati per varie funzioni, ma poiché i costi di manutenzione e di sviluppo di ogni server sono elevati, è stato deciso di utilizzare la virtualizzazione di tali componenti.

Con virtualizzazione si intende la possibilità di poter gestire più macchine virtuali con un unico server, quindi l’implementazione di più server in un’unica macchina.

I vantaggi principali offerti da tale metodo sono:

1. Ottenere il massimo dalle risorse esistenti: raggruppamento in pool delle risorse d'infrastruttura comuni ed eliminazione del vecchio modello di corrispondenza univoca tra applicazioni e server ("una sola applicazione su ciascun server") grazie al consolidamento server.

2. Ridurre i costi del data center mediante la riduzione dell'infrastruttura fisica e ottimizzare il rapporto server gestiti per amministratore: meno server e relative risorse hardware significa ridurre le esigenze di spazio e le esigenze di alimentazione e raffreddamento. Con l'ausilio di strumenti di gestione ottimizzati è possibile migliorare il rapporto server gestiti per amministratore e, di conseguenza, ridurre le esigenze di personale.

3. Incrementare la disponibilità di hardware e applicazioni per migliorare la business continuity: esecuzione di backup sicuri e migrazione di interi ambienti virtuali senza interruzioni operative.

4. Acquisire la flessibilità operativa: superiore capacità di risposta ai cambiamenti del mercato con la gestione dinamica delle risorse.

5. Monitoraggio di ambienti desktop sicuri cui è possibile accedere in locale o in remoto, con o senza connessione di rete, da quasi tutti i desktop, laptop o tablet PC dell'azienda.

La virtualizzazione avviene grazie alla creazione di più macchine virtuali sulla stessa macchina, con macchina virtuale si intende un contenitore software totalmente isolato in grado di eseguire i propri sistemi operativi e applicazioni come fosse un computer fisico. Una macchina si comporta esattamente come un computer fisico ed è dotata dei propri componenti (CPU, RAM, disco rigido e schede di rete) virtuali, vale a dire basati su software. Un sistema operativo non è in grado di distinguere una macchina virtuale da una macchina fisica, né possono farlo le applicazioni o altri computer in rete.

Implementando tale sistema l'azienda riesce a ridurre i costi di capitale e operativi migliorandone nel contempo l'efficienza operativa e la flessibilità.

Il software usato per la gestione della virtualizzazione dei server è VMWARE creando una infrastruttura virtuale la quale consente di condividere le risorse fisiche di più macchine nell'intera infrastruttura aziendale. Una macchina virtuale consente di condividere le risorse di un singolo computer fisico fra più macchine virtuali per ottenere la massima efficienza.

Le risorse vengono condivise tra più applicazioni e macchine virtuali. L'ottimizzazione delle risorse garantisce maggiore flessibilità all'organizzazione con conseguente riduzione dei costi di capitale e operativi.

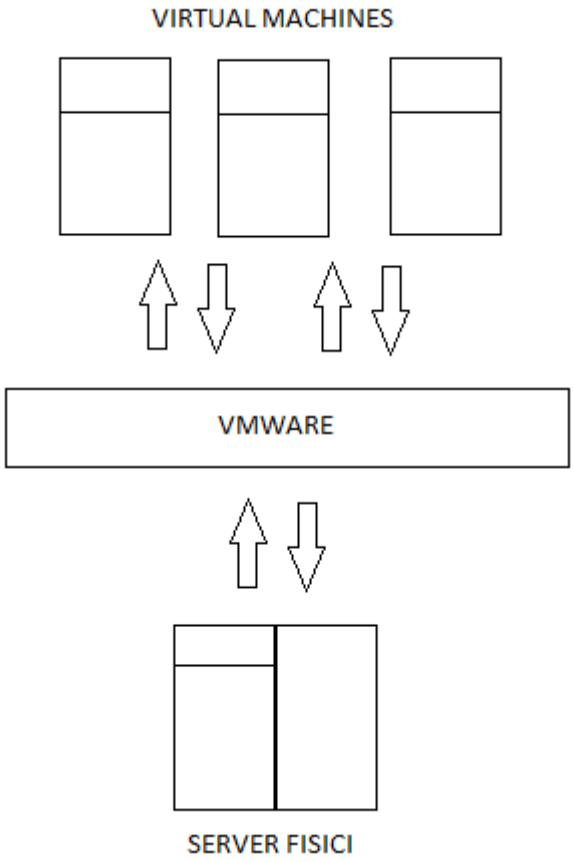

Figura 1.9 : Funzionamento virtualizzazione server.

L'ambiente software è separato dall'infrastruttura hardware sottostante per consentire l'aggregazione di più server, è quindi possibile allocare le risorse alle applicazioni in modo dinamico, sicuro e affidabile, in base alle esigenze. Grazie a questo approccio si possono usare le componenti dei server standard per creare un data center ottimizzato e garantire livelli elevati di utilizzo, disponibilità, automazione e flessibilità.

Questo sistema permette di disporre di disporre di più server virtuali rispetto a quelli fisici, utilizzati per vari servizi aziendali.

Uno dei server più utilizzati all’interno dell’azienda è il server di posta, creato per agevolare il compito di ogni dipendente che permette ad ogni utente di poter accedere tramite username e password ad una propria mail box personale.

La scelta adottata per l’implementazione di tale servizio, è stata quella di installare un server SMTP dedicato a tale scopo. La gestione di tale server avviene grazie al software MDaemon che è in grado di sincronizzare gli utenti e le password con Active Directory. Quando si aggiunge un utente in Active Directory MDaemon si “accorge” del cambiamento e crea un utente con lo stesso nome, login e password all'interno della lista utenti di MDaemon.

Gli aggiornamenti portati agli utenti in Active Directory, come il cambio password, sono portati automaticamente anche all'interno del server di posta; mentre quando si rimuove un utente da Active Directory, MDaemon può cancellare l'utente o disabilitarlo.

Per la gestione della mailbox ogni utente accede tramite Web con World Client gestibile direttamente da ogni browser di ogni postazione dell’azienda.

Per proteggere la posta in arrivo ad ogni utente il sistema adotta un filtro antispam che permette di ridurre il numero di email contenenti spam in maniera significativa; inoltre un sistema antivirus effettua la scansione dei messaggi in tempo reale durante la trasmissione del messaggio stesso in modo che nessun messaggio infetto possa essere memorizzato sul disco del server nemmeno per un istante.

L’amministrazione del servizio avviene da remoto tramite terminal server collegandosi al server di posta MDaemon.

CAPITLO 4 : CONCLUSIONI

Dopo circa sei mesi di Tirocinio, posso fissare alcuni punti , i quali rappresentano gli obiettivi fondamentali per il mio arricchimento formativo acquisito da questa esperienza:

- Capacità di applicare in un caso specifico, come la rete ospedaliera, tutto ciò che ho imparato dal mio percorso di studi;
- Capacità di relazionarmi con l'ambiente lavorativo, con i colleghi, con il personale e con gli organi amministrativi;
- Acquisizione di responsabilità che il ruolo impone;

Questi sono gli obiettivi fondamentali raggiunti, che erano anche quelli prefissati.

L'azienda "ALVEARE" mi ha dato la possibilità di imparare molto, affidandomi ad una equipe composta da personale altamente qualificato e competente, tra cui il tutore aziendale ed altri collaboratori.

Le mansioni che mi sono state affidate sono passate dalle più semplici, fino ad arrivare a compiti con maggior responsabilità; ma non è mai mancato il supporto del tutor e dei colleghi.

In conclusione posso affermare che l'esperienza del tirocinio ha completato il mio percorso formativo, arricchendo con aspetti pratici lo studio universitario.

CAPITOLO 5 : INDICE DELLE FIGURE

La figura 1.1 rappresenta la struttura della rete che collega le varie sedi tra loro e con Internet. Le sedi da collegare sono tre le quali si basano su di un collegamento VPN per isolare e proteggere la rete aziendale.

La figura 1.2 descrive la rete interna di ogni singola sede, la cui protezione è affidata al FIREWALL che la collega con l'esterno e dove alcuni servizi di comunicazione tramite Internet sono isolati in un'apposita area chiamata DMZ. I vari calcolatori all'interno della rete comunicano tramite LAN tra loro e con i server situati nella SALA MACCHINE.

La figura 1.3 è lo schema della suddivisione dell' Active Directory in 5 Directory principali per la corretta gestione degli accessi alla rete.

La figura 1.4 rappresenta la suddivisione del personale in vari gruppi, i quali hanno la possibilità di accedere solo ad alcune risorse.

La figura 1.5 esprime il funzionamento del sistema centralizzato WSUS il quale scarica, controlla e distribuisce gli aggiornamenti.

La figura 1.6 descrive come avviene la protezione della rete attraverso FIREWALL e software antivirus, i quali vengono implementati sia per proteggere la rete interna da quella esterna, sia le macchine interne da minacce interne.

La figura 1.7 riproduce invece il meccanismo di richiesta da parte di un client di un indirizzo IP ad un server DHCP, il quale dopo aver ricevuto la richiesta dal client ne assegna uno di default che però dovrà essere riconfermato dopo un certo periodo di tempo. Inoltre il server DHCP comunica con il server DNS per la risoluzione dei nomi di dominio.

La figura 1.8 è la rappresentazione della struttura della rete Wireless, composta da un modulo centrale e da più radio porte, le quali permettono di propagare il segnale per tutta l'area della rete. La gestione della rete è centralizzata tramite uno switch posto tra il modulo principale e le varie radio porte.

La figura 1.9 riproduce il funzionamento del software VMWARE per la virtualizzazione dei server dell'azienda.

CAPITOLO 6 : APPENDICE

ACL : Access Control List

AES : Advanced Encryption Standard

BIOS : Basic Input-Output System

CED : Centro Elaborazione Dati

DHCP : Dynamic Host Configuration Protocol

DMZ : Demilitarized Zone

DNS : Domain Name System

EAP : Exstensible Autentication Protocol

FTP : File Transfer Protocol

IP : Internet Protocol

ISD : Intrusion Detection System

LAN : Local Area Network

MAC : Media Access Control

NAT : Network Address Translation

OU : Unit Organizzation

SMTP : Simple Mail Transfer Protocol

SSH : Secure SHell

SSID : Service Set Identifier

TCP : Transmission Control Protocol

TKIP : Temporal Key Integry Protocol

ULSS : Unità Locale Socio Sanitaria

VLAN : Virtual LAN

VPN : Virtual Private Network

WINS : Windows Internet Naming

WPA : Wi-Fi Protected Access

WSUS: Windows Server Update Services

CAPITOLO 7 : BIBLIOGRAFIA E SITOGRAFIA

Bibliografia:

Autore: Peter Norton

Titolo: Sicurezza di rete

Casa Editrice: Apogeo

Anno in cui è uscita l'Edizione: 2000

Autore: Larry L. Peterson, Bruce S. Davie

Titolo: Reti di calcolatori

Casa Editrice: Apogeo

Anno in cui è uscita l'Edizione: 2005

Autore: Tanenbaum Andrew S.

Titolo: Reti di calcolatori

Casa Editrice: Pearson Education Italia

Anno in cui è uscita l'Edizione: 2003

Autore: Tanenbaum Andrew S.

Titolo: Reti di calcolatori. Un approccio strutturale

Casa Editrice: Pearson Education Italia

Anno in cui è uscita l'Edizione: 2006

Sitografia:

Microsoft : http://technet.microsoft.com/it-it/library

Google Immagini : http://www.google.it/img

Wikipedia Informatica : http://it.wikipedia.org/wiki/Categoria:Informatica

VMware : http://www.vmware.com/it/

MDaemon : http://www.altn.com/