**Elaborato**

**Brusarosco Matteo 5c**

**Introduzione**

La richiesta e’ quella di progettare una rete di gestione per un’azienda che vuole, tramite il sito web, esporre agli eventuali clienti tutti i prodotti messi in vendita e in che sede e’ possibile trovarli.L’azienda richiede un sistema di comunicazione attraverso il quale puo’ formire ai clienti assistenza.Si può quindi ipotizzare che l’azienda abbia la necessità di avere una rete locale LAN con almeno un server web e un mail server, due database e infine vari spazi per tutti gli altri eventuali dispositivi (pc, stampanti, ecc) utili all’azienda stessa, possibilmente divisi per sezione.

Per ipotesi presuppongo che l’afflusso dei clienti sia abbastanza grande e la quantità dei dipendenti contenuta. Da queste ipotesi ne ricavo le dimensioni e la struttura della rete interna, del server web e le altre caratteristiche necessarie per gestire il carico di richieste.

**Prima parte**

L’azienda dispone di diverse sedi, disposte in varie città diverse tra loro. Tutte le sedi hanno un software che si interfaccia con il database centrale (effettuando l’accesso con autorizzazioni adeguate). Ogni edificio è diviso in 4 sezioni, come la sede centrale, e da essa differisce solo per le dimensioni degli uffici.

**1.1 Architettura di rete e caratteristiche dei sistemi server**

Per la struttura della rete si possono fare alcune ipotesi:

1. Per erogare il servizio web e’ necessario almeno un server web dotato di ip pubblico e situato in una DMZ (per evitare accessi dall’esterno). All’interno della DMZ posiziono anche un mail server per le comunicazioni dell’assistenza.
2. Per la storicizzazione dei dati è necessario almeno 2 server con database, entrambi con un DBMS come MySql. Uno dei due database viene utilizzato per eseguire un backup periodico (settimanale o giornaliero) del database principale.
3. Tutti gli altri dispositivi come computer dei dipendenti, stampanti, ecc sono all’interno di una loro sottorete, protetta da un network firewall.
4. I dispositivi all’interno della sottorete dei dipendenti sono tutti collegati via cavo ethernet per avere un collegamento stabile.

Nella struttura reale della rete, considerando anche l’organizzazione interna, l’azienda viene divisa in 4 sezioni:

1. **Sezione server**: comprende la DMZ nella quale sono posti i due server che andranno ad interagire con l’esterno cioè il web server e il mail server.
2. **Sezione assistenza**: comprende i dispositivi che andranno ad interfacciarsi con il mail server per comunicare con i clienti.
3. **Sezione dipendenti**: comprende i dispositivi che andranno ad interfacciarsi solamente con i macchinari e la gestione interna. Nessun accesso alla rete esterna.
4. **Sezione manageriale**: comprende i dispositivi degli amministratori aziendali. Ha un collegamento con la rete esterna.
5. **Sezione database**: comprende i database e permette solamente operazioni di lettura ai suddetti archivi. Eventuali modifiche alla base di dati possono essere eseguiti dalla sezione dipendenti.

Questa soluzione prevede la divisione della LAN aziendale in molteplici sottoreti, ognuna con le sue caratteristiche, in modo da separare i dispositivi da usare all’interno da quelli che possono interfacciarsi verso l’esterno. I server per servizi esterni alla LAN sono posizionati all’interno di una DMZ.

Dato che l’azienda dispone di varie sedi, il numero di dipendenti per sede non e’ elevato. Si può proporre una soluzione con reti di classe C (che mette a disposizione 254 ip per sottorete).

|  |  |
| --- | --- |
| **Proposta con sottoreti di classe C** | |
| **Rete** | **IP** |
| Sezione dipendenti | 192.168.1.0 /24 |
| Sezione assistenza | 192.168.20.0 /24 |
| Sezione manageriale | 192.168.30.0 /24 |
| Sezione Database | 192.168.100.0 /24 |
| DMZ | 192.168.200.0 /24 |

Questo e’ un esempio per la rete principale ma, dato che le reti delle varie sedi sono tutte collegate alla principale con una VPN site to site, dovro creare delle sottoreti con ip diversi come per esempio:

|  |  |
| --- | --- |
| **Proposta con sottoreti di classe C** | |
| **Rete** | **IP** |
| Sezione dipendenti | 192.168.2.0 /24 |
| Sezione assistenza | 192.168.21.0 /24 |
| Sezione manageriale | 192.168.31.0 /24 |
| Sezione Database | 192.168.101.0 /24 |
| DMZ | 192.168.201.0 /24 |

Facendo cosi’ ho un range di ip nella quale poter mettere tutte le sottoreti senza creare conflitti.

Nel caso avessi bisogno di più’ ip (per future espansioni dell’azienda) potrei utilizzare una rete di classe B. In tal caso gli ip diventerebbero:

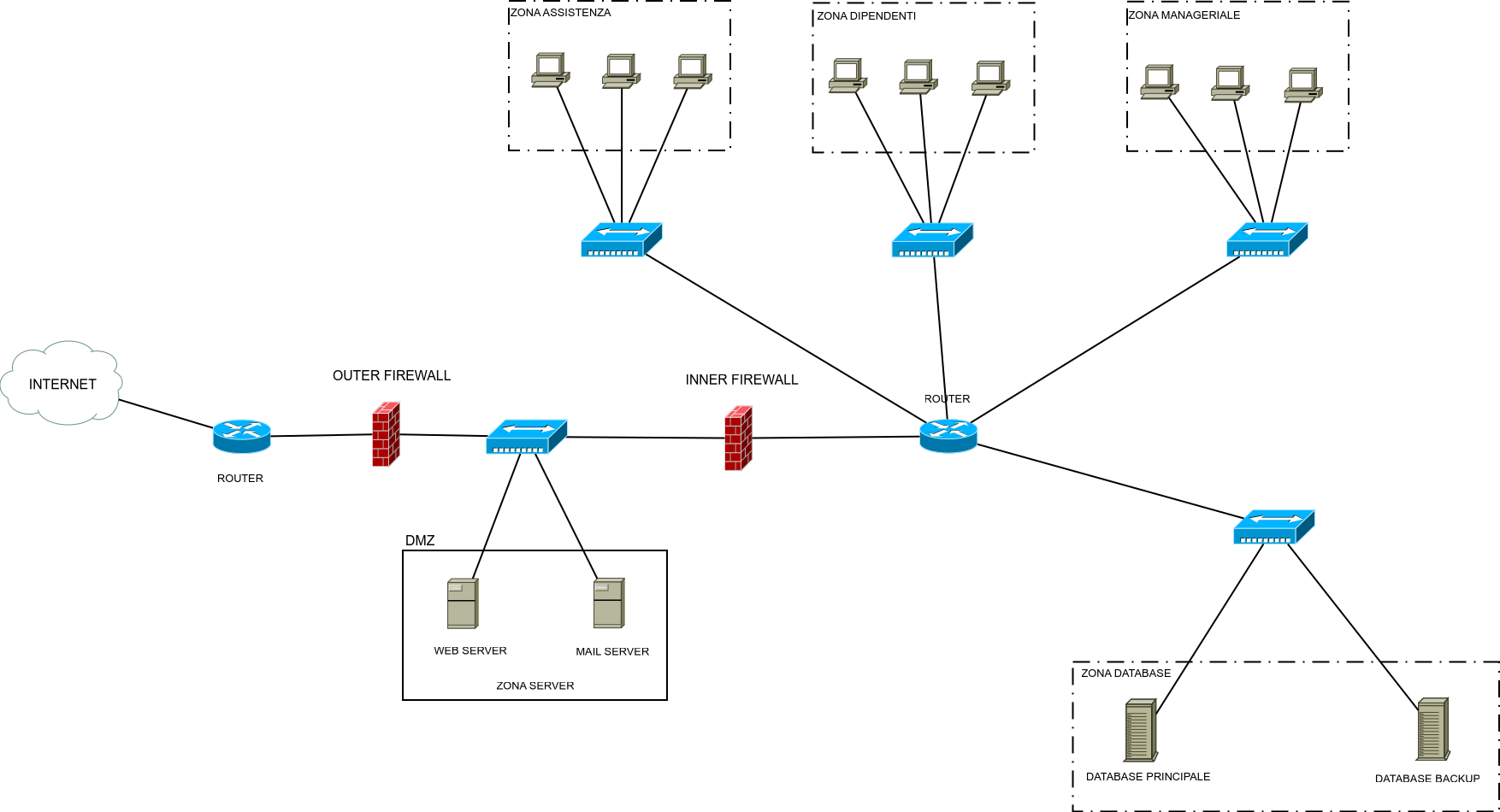
//forse sbagliato, chiedere

|  |  |
| --- | --- |
| **Proposta con sottoreti di classe B** | |
| **Rete** | **IP** |
| Sezione dipendenti | 152.1.0.0 /16 |
| Sezione assistenza | 152.2.2.0 /16 |
| Sezione manageriale | 152.3.3.0 /16 |
| Sezione Database | 152.20.0.0 /16 |
| DMZ | 152.50.0.0 /16 |

Per la struttura della rete si e’ deciso di utilizzare 2 firewall:

1. Il primo, posizionato verso l’esterno, protegge tutta la rete e ammette solo comunicazioni verso la DMZ. Questo firewall e’ di quarto livello cioe’ stateful (controllo attivo sulle connessioni in entrata ed uscita).
2. Il secondo, posizionato all'interno, ammette comunicazioni solo tra la LAN e la DMZ. Questo firewall e’ di tipo packet filter. Per risparmiare e’ possibile creare tramite la distribuzione pfsense un firewall packet filter, che comprende anche un servizio di vpn.

La soluzione potrebbe quindi essere schematizzata con la figura seguente, dove viene utilizzato un router per la connessione esterna e uno per le varie sottoreti interne. Sono presenti 2 firewall, quello esterno che ammette connessioni solamente verso la DMZ, e quello interno che ammette connessioni solo verso l’esterno.



volendo risparmiare: //aggiungi schema di rete.

//regole firewall. da fare

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Regole ACL in entrata e DMZ** | | | | | |
| Protocollo | Origine | Porte entr. | Destinazione | Porte dest. | Stato |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**//vpn e nat, da completare**

Per collegare le varie sedi sparse tra i vari comuni si e’ deciso di creare una **VPN** cioè una rete virtuale privata. La VPN permette di unire 2 reti private separate come fosse un’unica LAN e di fatto condividere i dispositivi di rete.

Con l’uso della VPN rendo possibile lo sharing del database tra le varie sedi, permettendo ad esse di sincronizzarsi, visualizzando i prodotti in magazzino e modificandoli (aggiungere e rimuovere).

**1.2 Modalità di comunicazione tra server e dispositivi, protocolli e servizi software per gestire la rete e fornire le pagine**

Per quanto riguarda il software lato server si può utilizzare XAMPP, una suite che comprende:

* Un DBMS free (MariaDB e SQLite)
* Web server Apache
* Mail server Mercury

Per l’email server si e’ scelto di utilizzare il protocollo IMAP in quanto permette di effettuare procedure di sincronizzazione delle email oltre a fornire operazioni in parallelo di invio e ricezione (utile per l’assistenza dato che viene utilizzato 1 account per tutte le richieste ma viene usato da diverse persone in contemporanea).

Per il web server si e’ scelto come protocollo l’HTTPS dato che fornisce una comunicazione sicura tra client e server tramite crittazione dei dati tramite TLS.

//da finire

**1.3 Gestione della sicurezza dei sistemi realizzati o utilizzati**

Per quanto riguarda la sicurezza, risulta possibile scomporla in più parti:

* **Rete**: Per prevenire attacchi dall’esterno sono stati inseriti nella rete 2 firewall: uno esterno e l’altro interno. Il firewall esterno permette l’accesso solo verso il web server dentro alla DMZ mentre quello interno solo connessioni in uscita verso la DMZ e la rete esterna. Le uniche persone che possono accedere all’esterno della rete sono i dirigenti, quindi imposto le regole del firewall esterno per accettare in uscita solo tutti gli IP appartenenti alla sezione amministrazione.
* **Database**: La sicurezza del database e’ quella incentrata sul preservare i dati da possibili problemi di natura casuale oppure intenzionale. E’ buona norma includere una backup policy per recuperare i dati in caso di perdita, corruzione o rottura, per eventi esterni, del database. Per il backup e gia’ stato predisposto un database secondario nella quale verranno copiati giornalmente, durante le ore notturne, i dati. Per quanto riguarda gli accessi non autorizzati al database c’e’ il bisogno di realizzare degli account specifici con i giusti permessi.
* **Comunicazioni**: Per la sicurezza delle comunicazioni si utilizza il protocollo TLS applicato all’HTTP. HTTPS fornisce autenticazione, integrità dei dati e confidenzialità.

//da finire

**1.4 Linguaggi di programmazione dinamica per il web**

Per realizzare un sito web interattivo che interagisce con un DBMS ci troviamo davanti a 2 scelte principali:

1. PHP
2. Java

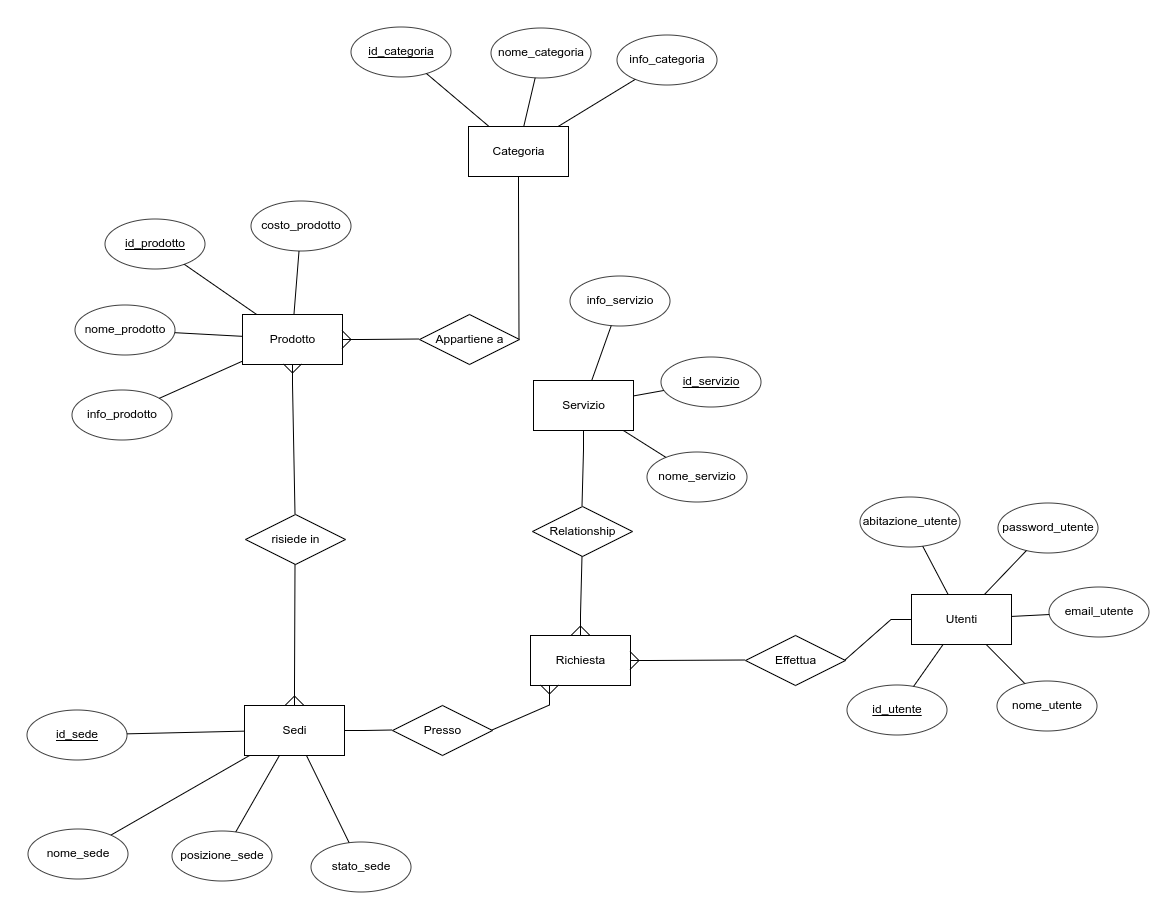
Per questo progetto e’ stato scelto PHP perché’ dispone di sintassi meno complesse.

//da finire

**1.5 modello concettuale e logico del database**

L’idea di fondo dello schema del database dovrebbe procedere in questo modo: un cliente può, tramite il sito web, richiedere un servizio (ad esempio consegna a domicilio, assistenza, ecc) ed ad una richiesta viene associata una sede di riferimento, che si occuperà del cliente. Nello stesso momento il cliente, sempre tramite il sito web, può visualizzare tutti i prodotti presenti nelle varie sedi. Del prodotto io posso vedere di che categoria fa parte e anche in che sede e’ posizionato (anche più sedi contemporaneamente).

Modello concettuale (E/R):

****

Lo schema logico risulterà quindi come segue:

**PRODOTTO** (id\_prodotto, nome\_prodotto, info\_prodotto, costo\_prodotto, categoria)

PK = id\_prodotto

FK = categoria riferito a **CATEGORIA**(id\_categoria)

**SEDE** (id\_sede, nome\_sede, posizione\_sede, stato\_sede)

PK = id\_sede

**PRODOTTO\_RISIEDE**(id\_collegamento, id\_prodotto, id\_sede)

PK = id\_collegamento

FK = id\_prodotto riferito a **PRODOTTO**(id\_prodotto)

FK = id\_sede riferito a **SEDE**(id\_sede)

**SERVIZIO** (id\_servizio, nome\_servizio, info\_servizio)

PK = id\_servizio

**UTENTE** (id\_utente, nome\_utente, email\_utente, password\_utente, abitazione\_utente)

PK = id\_utente

**UTENTE\_RICHIEDE\_SERVIZIO** (id\_richiesta, id\_utente, id\_servizio, id\_sede)

PK = id\_richiesta

FK = id\_utente riferito a **UTENTE**(id\_utente)

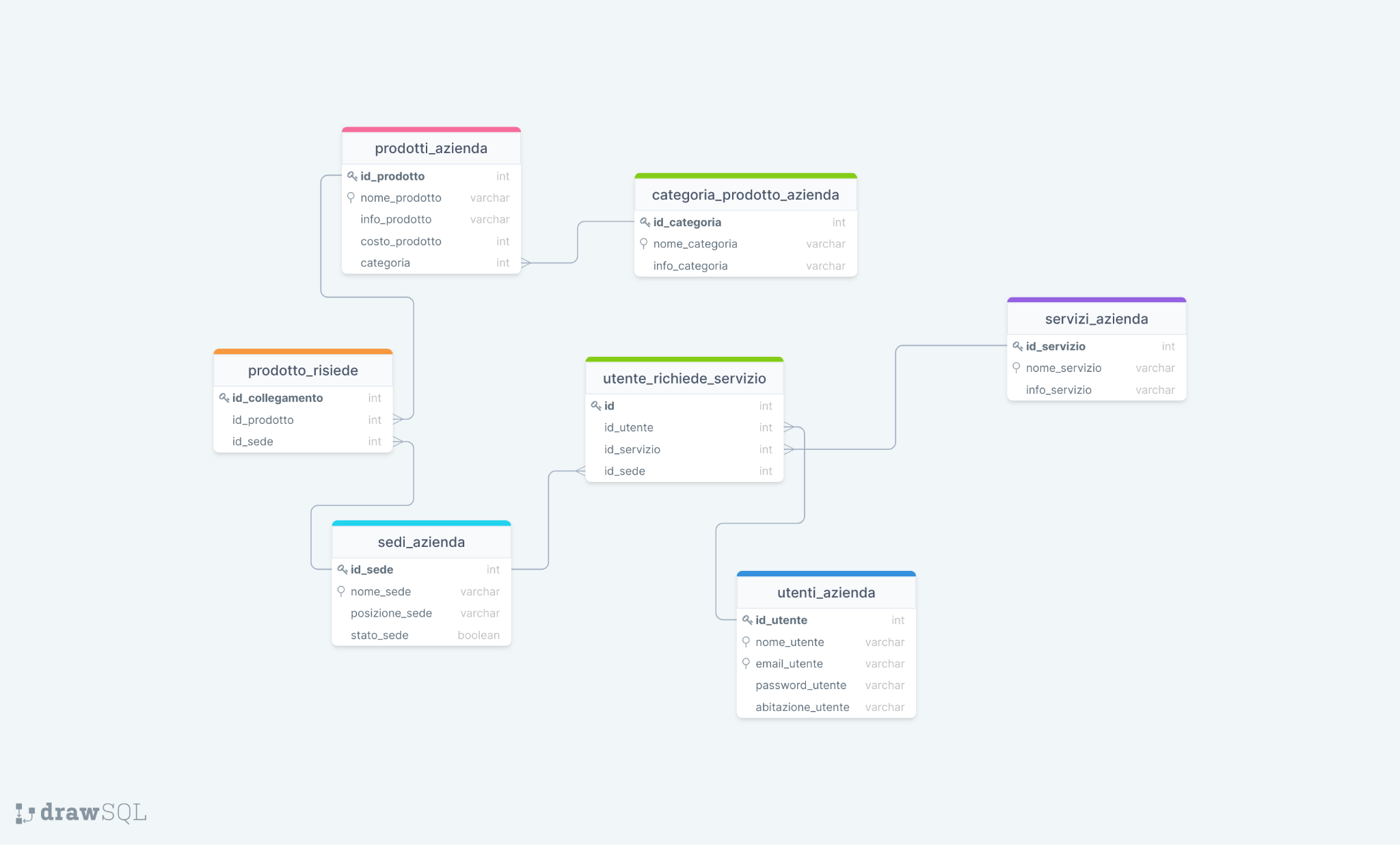
FK = id\_sede riferito a **SEDE**(id\_sede)

FK = id\_servizio riferito a **SERVIZIO**(id\_servizio)

**CATEGORIA** (id\_categoria, nome\_categoria, info\_categoria)

PK = id\_categoria

Modello logico:

****

//fare il punto 2 elaborato