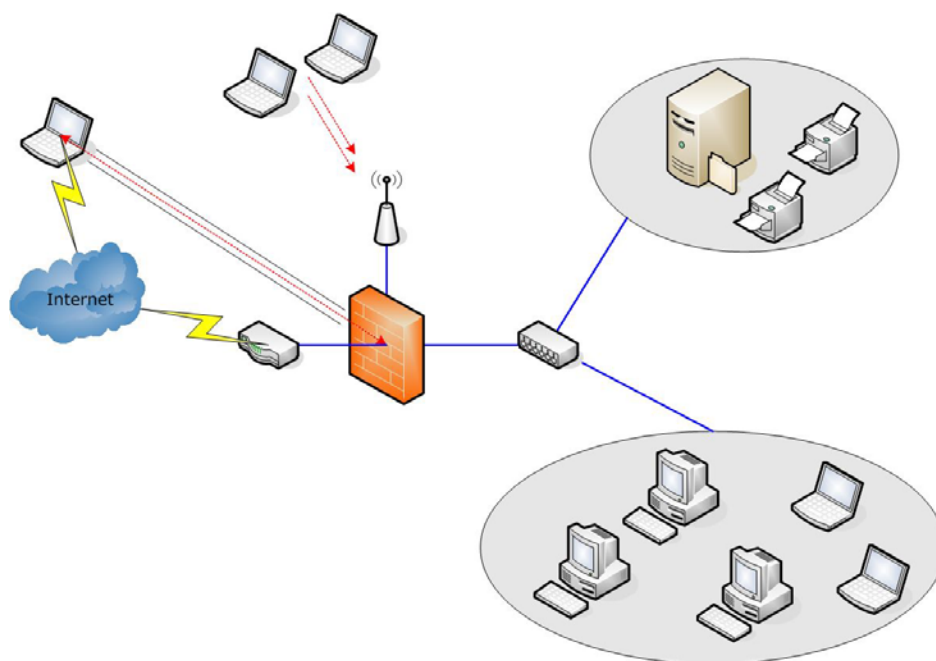


# LA RETE INFORMATICA NELL'AZIENDA

Capire i benefici di una rete informatica nella propria attività.



- ✓ **I componenti di una rete**
- ✓ **I dispositivi utilizzati**
- ✓ **I servizi offerti**

## **LA RETE INFORMATICA NELL'AZIENDA**

Copyright © 2006 Paolo Valsecchi

Tutti i diritti riservati. La riproduzione totale e parziale del presente documento deve essere autorizzata dall'autore.

### **NOTE**

Il contenuto è da intendersi orientato esclusivamente al progetto proposto.

Il linguaggio utilizzato per il documento è volutamente semplice e non tecnico al fine di agevolare la comprensione anche per chi non ha una profonda cultura informatica.

## Contenuti

Contenuti .....	3
Contatti .....	4
Versione .....	4
Panoramica di una rete aziendale .....	5
Schema e servizi disponibili .....	5
I componenti principali di una rete .....	6
Modem/Router.....	6
Firewall.....	6
Server .....	6
Dispositivi di rete .....	7
L'utilità di una rete informatica .....	8
Server .....	8
Stampanti in rete .....	10
Connessioni VPN .....	10
Firewall.....	11
Connessioni WiFi .....	12
UPS.....	13
Conclusioni .....	14
Definizione della struttura di rete.....	14
Note.....	15

## **Contatti**

Per qualsiasi informazione:

### **PAOLO VALSECCHI**

Fax: 02.700532807

e-mail: [info@valsecchi.net](mailto:info@valsecchi.net)

web: [www.valsecchi.net](http://www.valsecchi.net)

## **Versione**

Versione manuale: 1.1

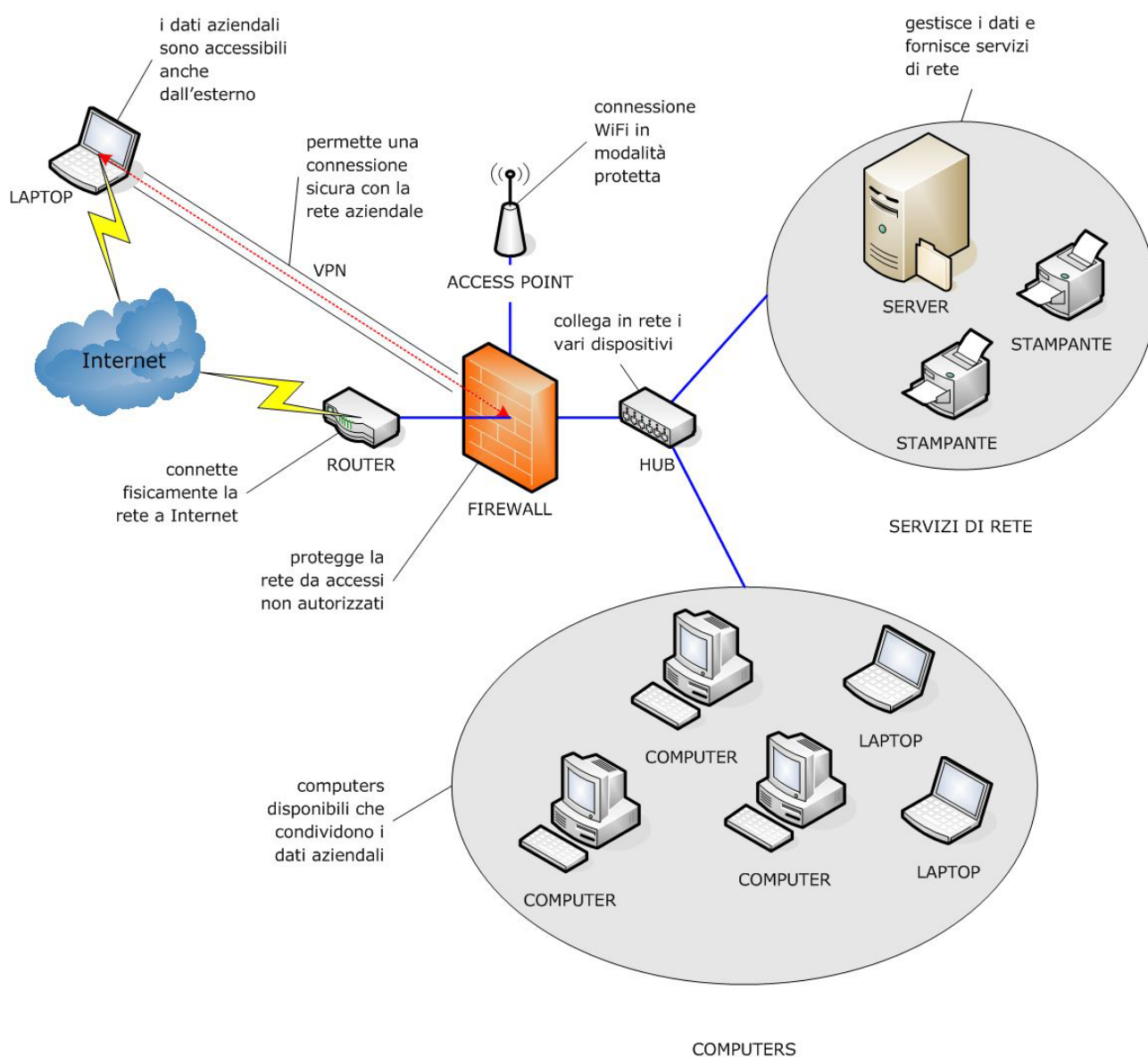
Aggiornato a: 20/12/2006

## Panoramica di una rete aziendale

### Schema e servizi disponibili

Per una più efficiente gestione e reperibilità dei dati aziendali, l'avvalersi di un sistema informatico è diventato ormai indispensabile.

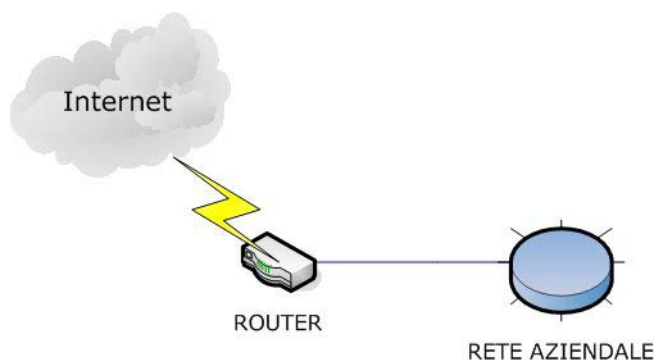
Viene qui illustrato un tipico scenario aziendale ed i servizi di rete disponibili.



## I componenti principali di una rete

### Modem/Router

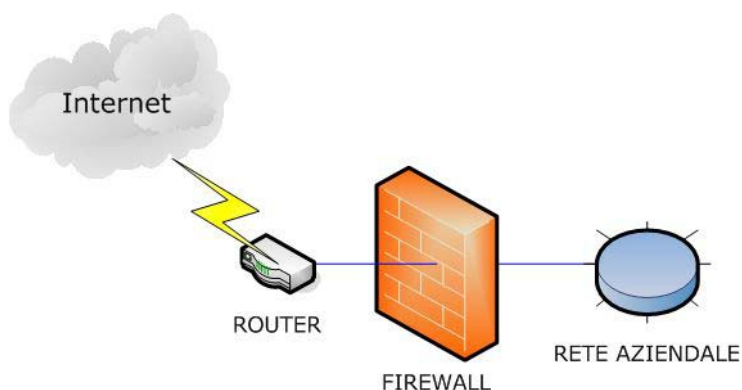
Collegare fisicamente la propria rete aziendale o un insieme di computers ad Internet richiede un modem/router che si connette al provider (detto ISP) con cui si è sottoscritto il contratto per l'accesso a Internet.



un tipo di modem/router

### Firewall

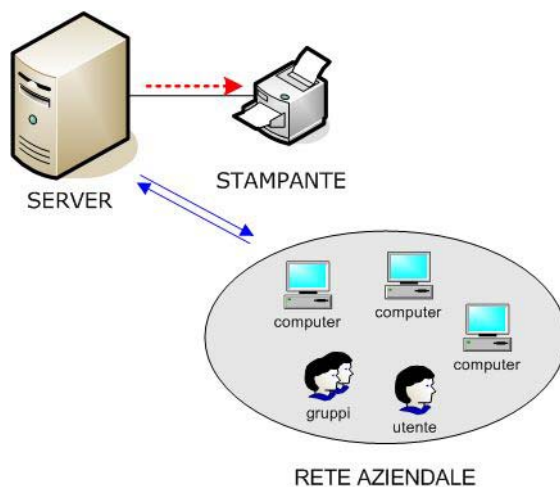
Il firewall è un dispositivo con il compito di regolare gli accessi esterni alla rete aziendale proteggendola da eventuali intrusioni non autorizzate.



un normale PC può avere il ruolo di firewall

### Server

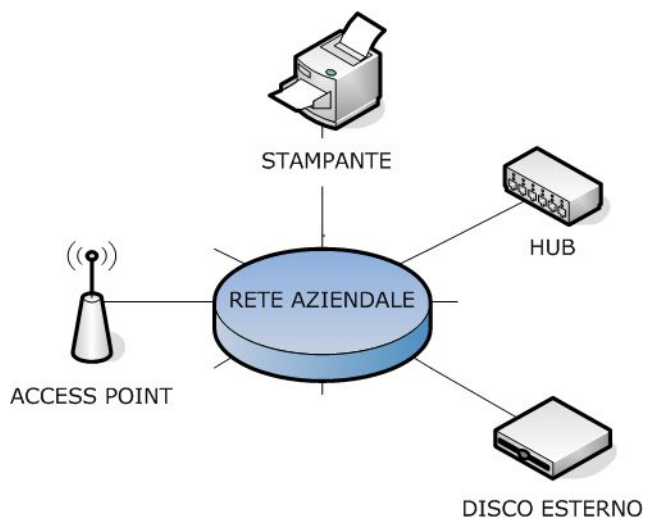
E' un computer dedicato a gestire il flusso centralizzato dei dati aziendali accessibili dai computers presenti nella rete. In base alla configurazione offre diversi servizi: gestione stampe, backup, autenticazione clients, etc.



un modello di server per la rete

## Dispositivi di rete

Permettono di interfacciare le periferiche (stampanti, dischi esterni, hubs, etc.) disponibili in azienda e renderle accessibili ai clients presenti nella rete.

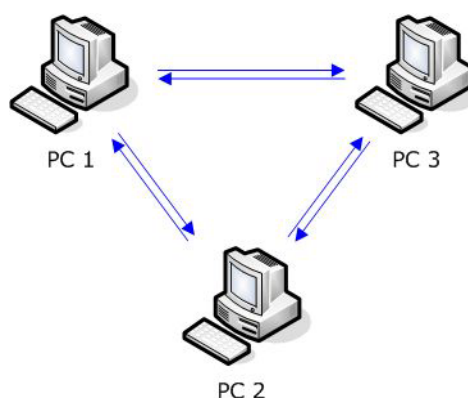


## L'utilità di una rete informatica

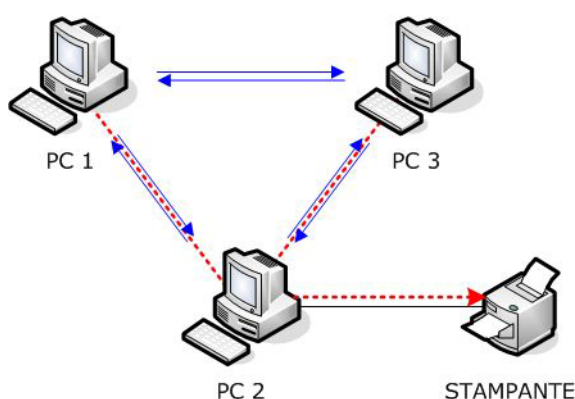
Per comprendere meglio i servizi che una rete può fornire e quali benefici può portare all'azienda, vengono analizzati alcuni aspetti di realtà lavorative.

### Server

In molte realtà aziendali la condivisione dei dati salvati nei computers avviene effettuando accessi diretti alle macchine (configurazione più comunemente chiamata peer-to-peer).



Spesso è presente anche una o più stampanti che vengono condivise in rete tramite una connessione diretta al computer alla quale sono collegate.

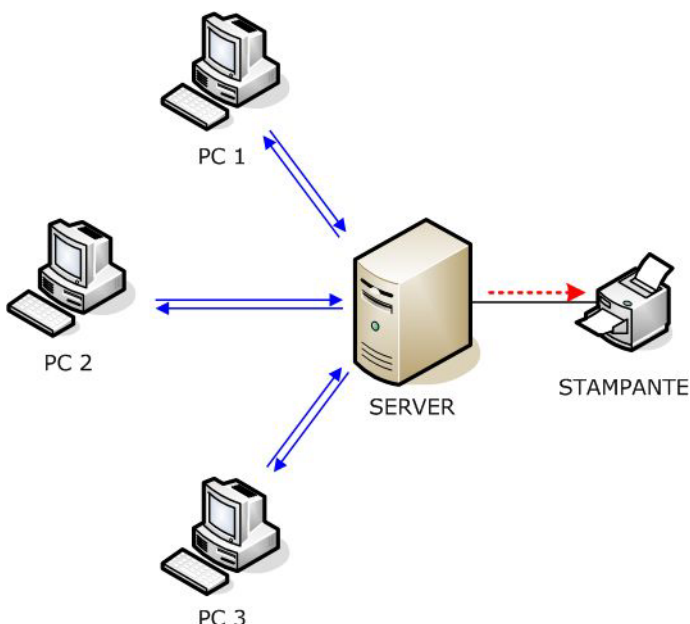


Uno scenario di questo tipo presenta diversi svantaggi:

- non è presente un singolo punto di raccolta dei dati, quindi il reperimento delle informazioni può essere laborioso.

- lavorando contemporaneamente con gli stessi dati, si devono affrontare problemi di sincronizzazione, cancellazioni accidentali, etc.
- i dati non sono protetti da backup (copie di sicurezza) che ne garantirebbe la salvaguardia anche in caso di danneggiamento (crash) dei computers.
- con i dati distribuiti su più computers, l'accesso richiede necessariamente che questi siano sempre accesi.
- nel caso di stampanti condivise, i computers a cui sono collegate devono rimanere accesi per fornire il servizio.
- durante la fase di stampa, il singolo computer elabora la coda da inviare alla stampante influenzando pesantemente le prestazioni globali della macchina durante tutto il processo.

Per evitare queste situazioni, l'installazione di un server nella rete porterebbe notevoli benefici alla propria attività in termini di accessibilità e disponibilità dei dati, prestazioni e sicurezza.



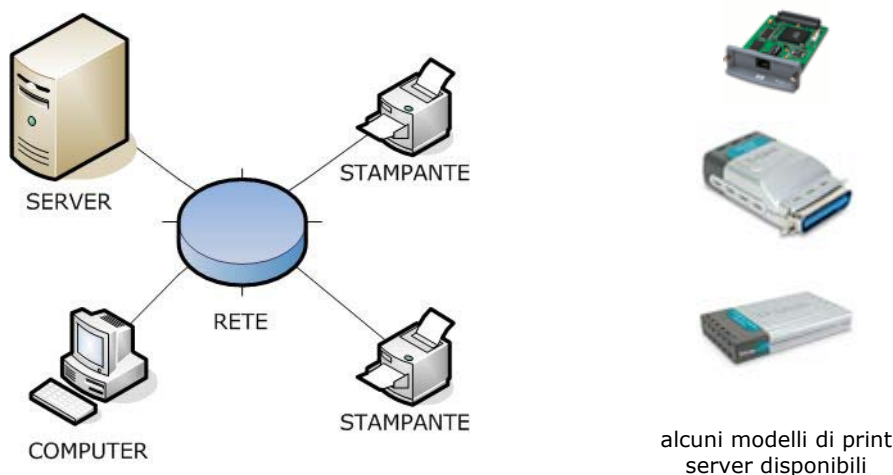
- il server essendo configurato con hardware e software specifici, assicura una gestione dei dati più efficiente e affidabile.
- essendo salvati in un'unica locazione, un'efficiente strategia di backup può essere implementata limitando notevolmente il rischio di perdita dati.
- la gestione delle stampe viene presa in carico dal server liberando i clients dalla fase di elaborazione.
- la disponibilità di un server permette l'implementazione di una procedura centralizzata per la gestione dei clients (aggiornamenti, correzioni, etc.) favorendo il mantenimento di un elevato standard di funzionalità e sicurezza.

La scelta del server deve essere attentamente valutata in base alla tipologia del lavoro svolto (utilizzo, ad esempio, di applicazioni client/server), al tipo di accesso richiesto (LAN/WAN), al numero di clients connessi (per determinare

il carico che il server deve sostenere), alla tipologia dei sistemi di protezione (fault tolerance) che si intendono adottare (sistemi RAID, UPS, etc.)...

## Stampanti in rete

Dotando le stampanti con dei dispositivi chiamati print server, è possibile conmetterle in rete senza la necessità di un collegamento diretto ad un computer o ad un server.

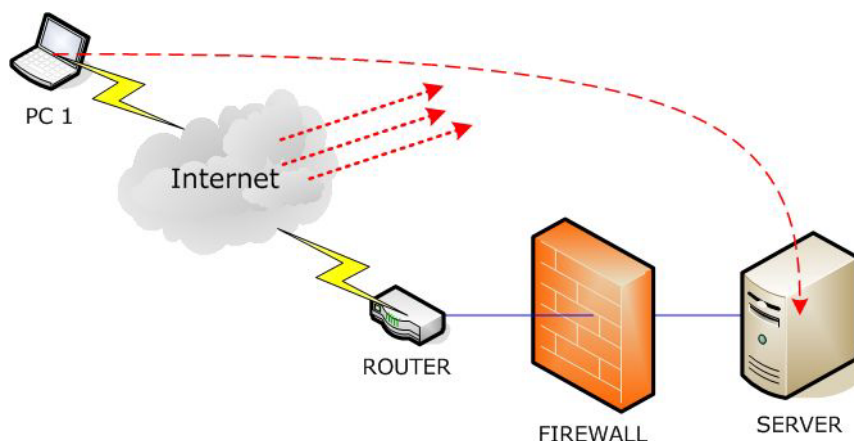


I vantaggi di questa soluzione sono molteplici:

- non è necessario tenere un computer sempre acceso per permettere l'utilizzo della stampante.
- è possibile collocare fisicamente la stampante nei posti più facilmente accessibili da parte degli utenti.
- se la rete è dotata di un server, è possibile gestire più stampanti da un singolo punto, il server appunto.

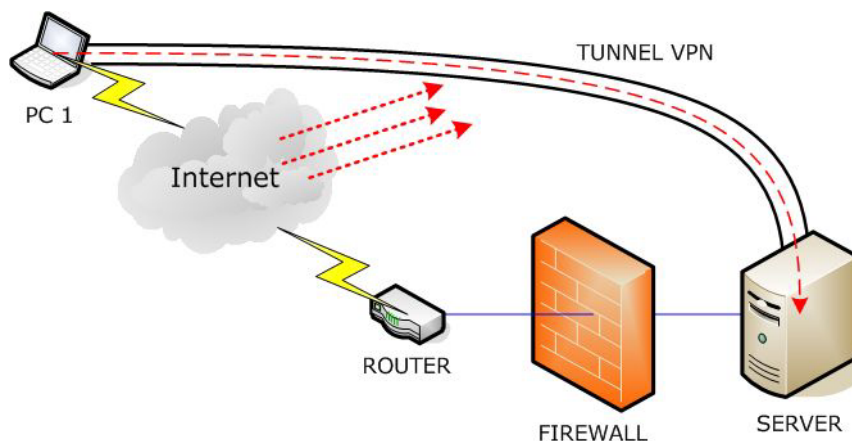
## Connessioni VPN

Se l'azienda dispone di un server, può essere utile avere la possibilità di accedere ai dati anche trovandosi fuori sede.



L'accesso alla rete deve essere comunque regolata rispettando i criteri di sicurezza per garantire l'integrità e la riservatezza dei dati durante la connessione.

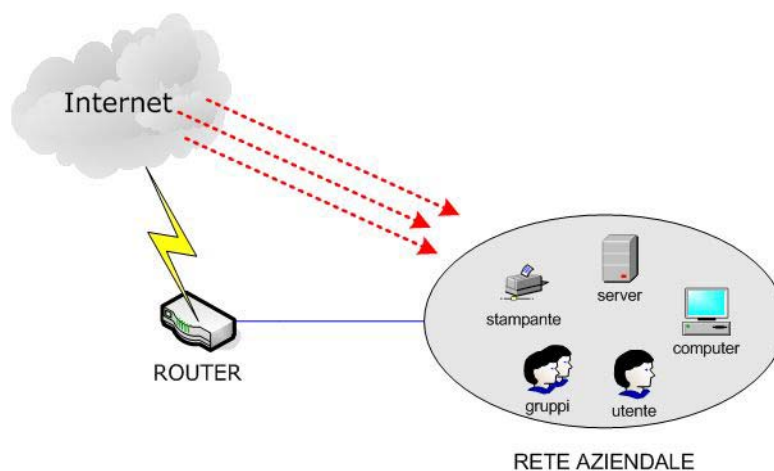
La protezione di una connessione tra un computer esterno alla rete e la rete stessa viene effettuata criptando la comunicazione tra client e server attraverso le normali connessioni Internet. Nei clients viene installato un software dedicato che permette il collegamento in modalità protetta e sicura (tunnel) al server che garantisce la riservatezza dei dati scambiati.



Queste connessioni possono essere effettuate sfruttando le normali linee analogiche PSTN, ISDN (quelle di casa per intenderci), tramite cellulare (GSM, GPRS, UMTS) o con le più veloci linee Internet ADSL.

## Firewall

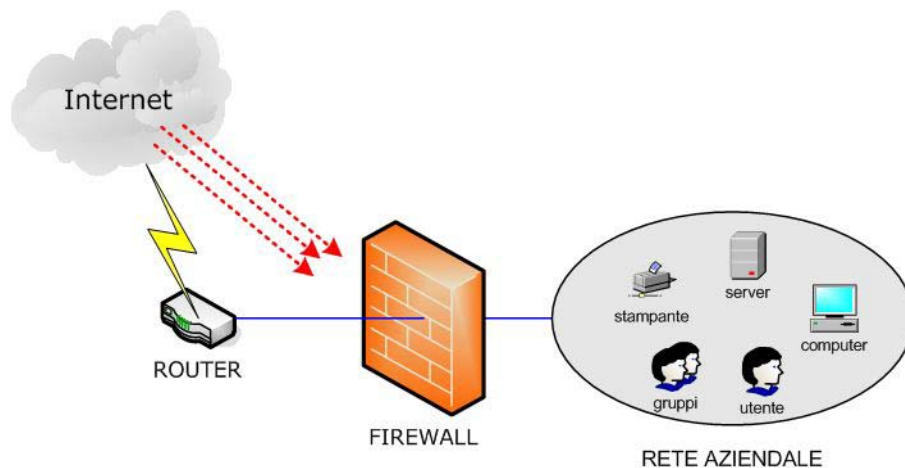
Connettendo la propria rete aziendale ad Internet senza un'adeguata protezione dall'esterno, l'integrità e la riservatezza dei dati sono esposti a possibili violazioni.



Un firewall permette la protezione della rete regolando gli accessi dall'esterno solo agli utenti autorizzati adottando le regole imposte dall'azienda. Il firewall è un computer dedicato collocato tra la rete e l'accesso a Internet.

Il risultato di queste intrusioni può portare a scenari imprevedibili che potrebbero compromettere l'attività svolta:

- cancellazione, alterazione o perdita di dati.
- manomissione dei sistemi informatici e/o dei servizi di rete con il rischio di blocco parziale o totale della propria attività.
- violazione della privacy.

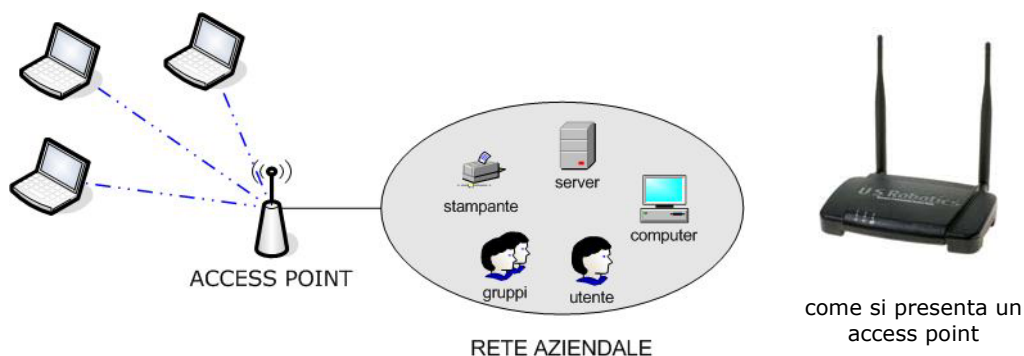


Grazie alla presenza di questo dispositivo è anche possibile implementare ulteriori servizi di rete quali:

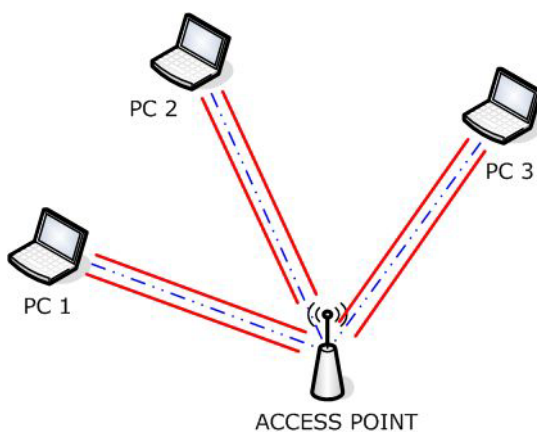
- accessi VPN dall'esterno.
- accessi Internet sicuri (proxy).
- sistemi di rilevamento anti-intrusione per monitorare eventuali tentativi di violazione della rete aziendale.

## Connessioni WiFi

In situazioni dove la stesura di una rete cablata risulta difficoltosa o troppo onerosa, dove si presenta la necessità di connettersi alla rete da punti non raggiunti o sprovvisti di attacchi di rete, le connessioni senza fili wireless (comunemente WiFi) vengono incontro a queste esigenze.



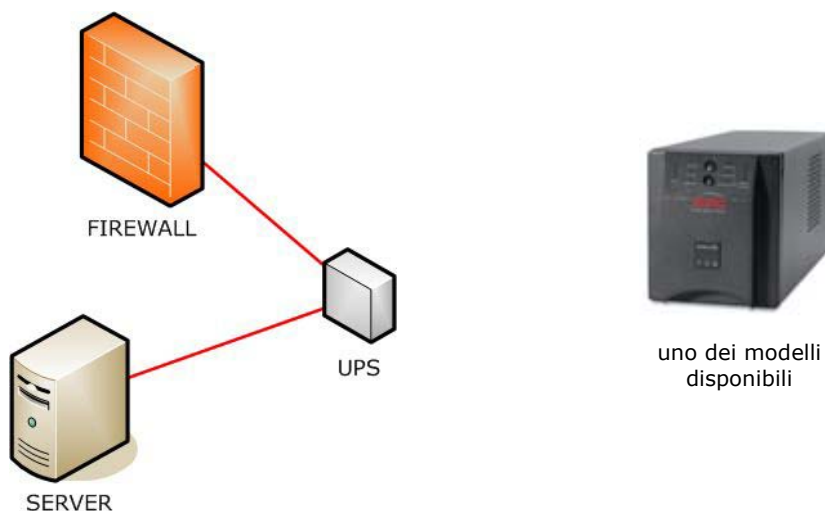
Data la natura del tipo di connessione, l'aspetto della sicurezza è un fattore da considerare attentamente e non deve essere sottovalutato. Proteggere questo tipo di connessioni è quindi fondamentale.



Per evitare intrusioni non autorizzate vengono implementate delle connessioni wireless crittate tra i clients e l'access point utilizzando la tecnologia VPN.

## UPS

L'UPS (gruppo di continuità) è un dispositivo che protegge gli apparati collegati da eventuali interruzioni di corrente che, per dispositivi come servers, routers, firewall, potrebbe causare dei problemi di funzionamento con il rischio di possibili interruzioni.



## Conclusioni

### Definizione della struttura di rete

Analizzate le esigenze che l'attività svolta richiede (detto piano informatico), vengono definite le configurazioni dei dispositivi che verranno installati nella rete. I componenti indispensabili sono così riassunti:



#### **MODEM/ROUTER**

Interfaccia che collega la rete a Internet.



#### **FIREWALL**

Protegge la rete contro le intrusioni e rende sicuri gli accessi a Internet.



#### **SERVER**

Gestisce i flussi dei dati aziendali.



#### **UPS**

Protegge i dispositivi collegati da eventuali blackout.



#### **HUB**

Collega gli apparati informatici alla rete.



#### **PRINT SERVER**

Connette le stampanti alla rete.



#### **ACCESSO WiFi** (facoltativo)

Fornisce l'accesso alla rete in modalità wireless.



#### **SOFTWARE**

Il software utilizzato in tutta la rete deve essere coperto da regolare licenza.

