1. Dominio di rete Microsoft

Configurare una rete in **dominio** significa collegare un gruppo di computer aventi gli stessi parametri di sicurezza e di accesso e un medesimo database.

Le macchine del dominio hanno in comune diversi elementi, come: un nome univoco, un amministratore di sistema, uno o più server, credenziali di accesso, limitazioni di accesso alle impostazioni di un pc.

Vantaggi

- **Gestione centralizzata delle risorse del sistema** (Utenti, Computer, Stampanti, Share di Rete, Servizi distribuiti, documenti, ecc.).
- **Autenticazione** (criteri di scadenza e complessità password, credenziali nominali, ecc.).
- **Autorizzazione all'accesso alle risorse e logging degli accessi.**
- **Gestione e configurazione dei PC e installazione del Software** (Policy di sicurezza).

Requisiti

- Computer **Client** con sistema operativo Windows di tipo **Professional** (7/10).
- Connessione **LAN**.
- Computer **Server** con sistema operativo **Windows Server** (2008/2012/2016).

2. Antivirus

- La navigazione del nostro pc è sempre soggetta ad attacchi più o meno “violenti” da parte di malware. Con quest’ultimo termine si suole indicare un software creato per danneggiare un determinato sistema operativo.

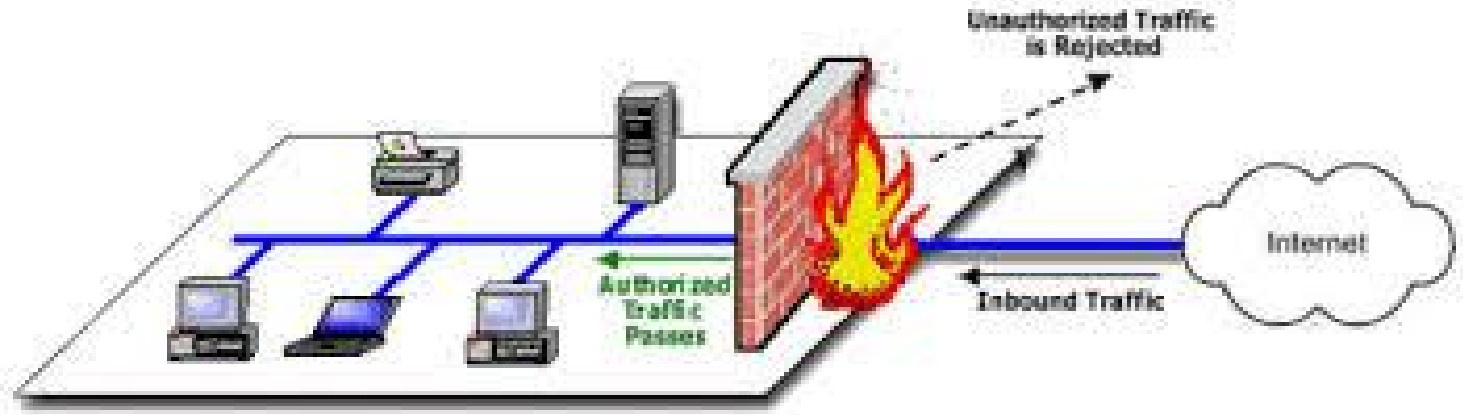
- **Esistono diversi tipi di virus informatici**: Warms, Keylogger, Trojan Horse, Backdoor, Dialer, Spyware, Rookit e tanti altri alcuni “mimetizzati” da programmi che dovrebbero aiutare le prestazioni del pc.

- Quando si riceve un attacco malware il pc rallenta progressivamente le sue funzione **ed espone a rischi i nostri dati in esso salvati**. Per ovviare a questi inconvenienti , alcuni dei quali così pericolosi da rovinare permanentemente il computer e i dati, esistono diversi programmi chiamati antivirus.

- E' consigliabile utilizzare **prodotti completi** che permettono di coprire tutte le piattaforme presenti, quali PC, **Server file**, portatili e dispositivi mobili, proteggendo il sistema da attacchi online, frodi finanziarie, ransomware e perdita di dati e offrendo la possibilità di monitorare qualsiasi dispositivo connesso.

3. Firewall perimetrale

- **Il firewall è un dispositivo installato sul perimetro della rete** , solitamente viene posizionato tra il router della connessione ad internet e la rete dei PC.
- **Ha il compito principale di filtrare le connessioni in entrata e in uscita, innalzando il livello di sicurezza della rete e permettendo agli utenti di operare nella massima sicurezza. Diventa particolarmente evidente a questo punto quale ruolo fondamentale abbia questa tecnologia rispetto alla sicurezza interna, esterna e di accesso di una rete rispetto all'uso che ne fanno i suoi utenti.**
- Il miglior modo per proteggere una rete o un singolo computer sta nel riconoscere e respingere in maniera preventiva gli attacchi, ancora prima che questi possano causare danni. Per tale ragione nei firewall di fascia alta, si fa sempre più uso di un sistema chiamato **IPS**.
- **L'Intrusion Prevention System (IPS)**, che può essere liberamente tradotto in italiano con sistema di prevenzione delle intrusioni, come suggerisce il nome, dopo aver appurato la possibilità di un attacco, questo tipo di sistema non si limita ad informare l'amministratore, ma attiva immediatamente delle misure di sicurezza adeguate. In questo modo si evita che passi un intervallo di tempo troppo lungo tra il rilevamento di un intrusione e l'attuazione di azioni volte a fermarlo.



4. Tipologie di backup

NAS

- **NAS È l'acronimo di Network Attached Storage**, in poche parole un dispositivo che contiene dei dischi fissi e che permette di accedere ai file memorizzati tramite una connessione di rete.

- I vantaggi di un **NAS**, rispetto ai metodi di archiviazione più classici, come gli HDD esterni, le pen drive o gli hard disk stessi dei computer, sono tanti.

- Un **NAS** è in grado di mettere al sicuro i dati con dei backup automatici.

Cloud Backup

I dispositivi fisici, gli hard disk, possono subire rotture o malfunzionamenti, sono facilmente accessibili e soprattutto possono essere rubati. Un'altra complicazione è rappresentata dallo spazio.

Nel momento in cui si è usufruito di tutto lo spazio disco disponibile e ne occorre dell'altro, l'unica soluzione che è possibile adottare è quella di acquistare un nuovo dispositivo.

Con la tecnologia Cloud e nello specifico, con il **Cloud Backup**, nulla di tutto ciò può accadere. I dati vengono salvati, tramite un backup online periodico, nel cloud, e sono conservati all'interno di web farm blindate, oltre ad essere crittografati.

5. Cifratura dei dati

- **Cifrare i dati** è un buon metodo per proteggere le informazioni sensibili dalla lettura di personale non autorizzato.

- Cosa è la cifratura? In termini molto semplici, la cifratura è una modalità di conversione del testo originale in una sequenza apparentemente casuale di lettere, numeri e segni speciali che solo la persona in possesso della corretta chiave di decifratura potrà riconvertire nel file di testo originale.