Programma di Sistemi e Reti svolto nella Classe VBI

Richiami sul modello ISO-OSI e l'architettura TCP-IP

Problemi di sicurezza nei sistemi informatici e nelle reti

- I principali pericoli per la sicurezza
  - danni accidentali e dolosi
  - rotture e guasti
  - attacchi informatici
  - virus, worm, troyan
  - attacchi informatici: hacking, sniffing, spoofing, phishing
- Misure di sicurezza
  - protezione fisica (gruppi di continuità, dischi raid, server fault tolerance, controllo degli accessi)
  - credenziali di autenticazione
  - protezione logica (aggiornamento del software, antivirus, antispam, crittografia, ecc)
  - backup e restore (disaster recovery)
  - buone pratiche

Tecniche di filtraggio del traffico di rete

- Protezione della rete con tecniche Nat/Pat
- Firewall
  - Packet Filter Firewall
  - Personal Firewall
  - DMZ
  - Content filtering
- Proxy Server

Tecniche crittografiche applicate alla protezione dei sistemi e delle reti

- Crittografia, chiave simmetrica e chiave asimmetrica
- Firma digitale
- Software e protocolli per la crittografia

Reti private virtuali

- Caratteristiche di una VPN
- La sicurezza di una VPN

Modello client/server e distribuito per i servizi di rete. Funzionalità e caratteristiche dei principali servizi di rete

- World Wide Web (Web)
- File Transfer Protocol (FTP)
- E-Mail (Posta elettronica)
- Posta elettronica certificata

Strumenti e protocolli per la gestione ed il monitoraggio delle reti

- I comandi Windows ipconfig, arp, netstat, ping, traceroute, nslookup

Macchine e servizi virtuali, reti per la loro implementazione

- Server dedicati e server virtuali
- Virtualizzazione dei server e del software
- Le soluzioni cloud

Esercitazioni di laboratorio

- Analisi e sintesi di reti informatiche utilizzando Packet Tracer
- Esercitazioni sui comandi di rete ipconfig, ping, netstat, traceroute
- Sviluppo di applicazioni Visual CSharp: numeri IP, trasmissione di pacchetti, servizi di posta elettronica, criptatura, generazione password
- Sviluppo applicazioni php: criptatura password, autenticazione, posta elettronica, download e upload con protocolli http e ftp

La sicurezza delle reti e dei sistemi

Che cos'è la sicurezza?

La "Sicurezza Informatica" è l'insieme delle misure di carattere organizzativo, tecnologico e procedurale idonee a garantire la protezione dei sistemi informatici e dei dati in essi contenuti.
I rischi e i pericoli, ovvero le azioni o gli eventi in grado di modificare o alterare le normali funzionalità di un sistema informatico o dei dati in esso contenuti, si possono distinguere in:

1. guasti dell'hardware
2. errori del software
3. errori umani
4. cause accidentali ed imprevedibili (allagamenti, incendi, terremoti)
5. malware (virus, worms, trojan ecc)
6. intrusioni e attacchi malevoli

E' chiaro che con l'avvento di Internet, le problematiche della sicurezza sono diventate importantissime e riguardano in larga parte la difesa nei riguardi del malware e delle intrusioni da parte di pirati informatici (hacker, cracker, troller), ovvero di persone che entrano in un sistema informatico senza l'autorizzazione per farlo. Le tecniche di attacco sono molteplici:

- Cavalli di Troia: programmi o documenti che contengono software dannoso nascosto da una normale applicazione (es. virus in file o email)
- Hacking: spezzare i meccanismi di autenticazione della password ("intuizione", furto, generazione automatica di password) per puro diletto, senza fare danni
- Sniffing: possibilità di "fiutare"le password attraverso software in grado di monitorare il flusso di pacchetti dati che attraversano la rete
- Spoofing: possibilità di modificare in maniera fraudolenta il contenuto dei pacchetti in circolazione (es. falsificando l'indirizzo IP di provenienza e assumendo indebitamente l'identità altrui)
- Phishing: possibilità di indurre ignari utenti a fornire in buona fede le proprie credenziali (es. indirizzandoli tramite link camuffati in email di invito su siti che riproducono siti istituzionali), utilizzate poi fraudolentemente

Misure di sicurezza

La sicurezza informatica si attua:

1. riducendo i rischi a cui sistemi e dati sono esposti
2. limitando gli effetti causati dall'eventuale verificarsi di un'azione nociva per la sicurezza (incidente informatico)

<u>Protezione fisica</u>

La protezione dei sistemi informatici viene ottenuta agendo a più livelli: innanzitutto a livello fisico e materiale, ponendo i server in luoghi il più possibile sicuri, dotati di sorveglianza e/o di controllo degli accessi. Si tratta di una misura di sicurezza passiva il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata. Il concetto di sicurezza passiva pertanto è molto generale: ad esempio, per l'accesso fisico a locali protetti, l'utilizzo di porte di accesso blindate, congiuntamente all'impiego di sistemi di identificazione personale, sono da considerarsi componenti di sicurezza passiva.

Gli eventi accidentali non riguardano attacchi malevoli, ma fanno riferimento a eventi causati accidentalmente dall'utente stesso, tipo: uso errato delle procedure, incompatibilità di parti hardware, guasti imprevisti, ecc … Tutti eventi che comunque compromettono la sicurezza del sistema soprattutto in termini di disponibilità.
Per far fronte a tali evenienze, specie se derivanti da possibili guasti o danni fisici, molte volte si opera in un contesto di ridondanza degli apparati (dischi raid, server fault tolerance) ovvero con sistemi che grazie alla tolleranza ai guasti, garantiscano affidabilità e disponibilità del sistema informatico.

Protezione logica-organizzativa

Il secondo livello è normalmente quello logico che prevede l'autenticazione e l'autorizzazione attraverso le credenziali username e password. Successivamente al processo di autenticazione, le operazioni effettuate dall'utente sono tracciate in un file di log, ovvero in un file in cui vengono registrate le operazioni compiute dall'utente che ha effettuato il login. Questo processo di monitoraggio delle attività è detto audit o accountability.
Per evitare invece gli eventi accidentali, non esistono soluzioni generali, ma un primo rimedio è il fare regolarmente una copia di backup del sistema, comprendente dati e applicazioni, com'è tipico delle procedure di disaster recovery, in modo da poter fronteggiare un danno imprevisto.
Antivirus: consente di proteggere il proprio personal computer da software dannosi conosciuti genericamente come **malware**. Un buon antivirus deve essere costantemente aggiornato ad avere in continua esecuzione le funzioni di scansione in tempo reale. Per un miglior utilizzo l'utente deve avviare con regolarità la scansione dei dispositivi del PC (dischi fissi, CD, DVD, memorie USB), per verificare la presenza di virus, worm e trojan. Per evitare la diffusione di malware è inoltre utile controllare tutti i file che si ricevono o che vengono spediti tramite posta elettronica facendoli verificare dall'antivirus correttamente configurato a tale scopo. I **virus** sono programmi che si replicano e infettano tutti i computer a cui si connettono, modificando e spesso distruggendo funzionalità vitali per l'esecuzione dei programmi applicativi e dei files del sistema operativo.
I **worm** sono tra i malware più dannosi soprattutto per i computer collegati in rete in cui possono penetrare sfruttando le falle di sicurezze del SO e che possono distruggere in pochi minuti. La principale differenza tra i virus e i worm è la seguente: i worm si replicano usando i protocolli di rete e le vulnerabilità del sistema, replicandosi ed infettando senza alcuna interazione degli utenti; i virus possono diffondersi solo se veicolati da mezzi fisici o virtuali, quali i supporti rimovibili o le email, e richiedono in ogni caso un minimo d'interazione da parte degli utenti.
I **trojan** sono codici nascosti all'interno di altro software apparentemente utile (cavallo di Troia per ingannare gli utenti) ma che di nascosto attivano la connessione a server maligni dai quali vengono scaricati altri malware per infettare il PC e utili per assumerne il controllo completo**.**

- Antispyware: software facilmente reperibile sul web in versione freeware, shareware o a pagamento. È diventato un utilissimo tool per la rimozione di "file spia", gli spyware appunto, in grado di carpire informazioni riguardanti le attività online dell'utente ed inviarle ad un'organizzazione che le utilizzerà per trarne profitto.
- Firewall: installato e ben configurato un firewall garantisce un sistema di controllo degli accessi verificando tutto il traffico che lo attraversa. Protegge contro aggressioni provenienti dall'esterno e blocca eventuali programmi presenti sul computer che tentano di accedere ad internet senza il controllo dell'utente.

- Firma digitale, Crittografia: è possibile proteggere documenti e dati sensibili da accessi non autorizzati utilizzando meccanismi di sicurezza specifici quali: la crittografia, la firma digitale, e l'utilizzo di certificati digitali e algoritmi crittografici per identificare l'autorità di certificazione, un sito, un soggetto o un software.
- Backup: più che un sistema di difesa si tratta di un utile metodo per recuperare dati eventualmente persi o danneggiati. Il backup consiste nell'esecuzione di una copia di sicurezza dei dati di un personal computer o comunque di dati considerati importanti onde evitare che vadano perduti o diventino illeggibili.

Tecniche di filtraggio del traffico di rete.

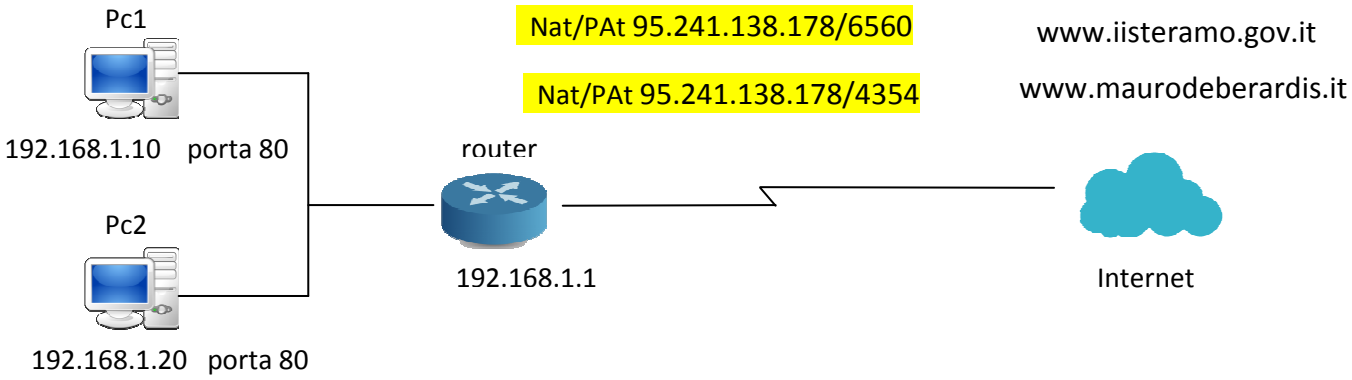
Protezione della rete con tecniche di NAT e PAT

Ciascun dispositivo (computer o periferica) connesso ad una rete, è contraddistinto da un indirizzo IP a 32 bit (versione IPv4). I 32 bit sono suddivisi in gruppi di 8; in decimale il formato è XXX.XXX.XXX.XXX dove XXX è un numero decimale compreso tra 0 e 255 essendo 2^8= 256 le combinazioni che si possono ottenere con 8 bit. Il numero di indirizzi IPv4 disponibili è di 2^32 ovvero circa 4 miliardi; sembrano tanti ma presto saranno insufficienti. Per questo motivo è nato lo standard IPv6, che in futuro sostituirà l'IPv4, in cui l'indirizzo IP è formato da 128 bit e il numero di indirizzi disponibili (2^128) è praticamente inesauribile.
In attesa che l'IPv6 diventi uno standard, per far fronte al problema degli indirizzi IP che cominciano a scarseggiare, sono stati definiti blocchi di indirizzi IP chiamati indirizzi privati utilizzabili soltanto all'interno di reti locali e replicabili quante volte si vuole su altre reti locali.
In genere le reti private usano indirizzi che fanno parte delle seguenti serie di indirizzi riservati (chiamati "non instradabili" perché non possono essere instradati su Internet):
10.0.0.0 – 10.255.255.255 172.16.0.0 – 172.31.255.255 192.168.0.0 – 192.168.255.255
Gli indirizzi pubblici sono invece non replicabili in quanto non ci possono essere due indirizzi IP pubblici uguali.

Prima di andare avanti è opportuno ricordare i principi di funzionamento sui quali si basa la suite di protocolli TCP/IP (Transport Control Protocol/Internet Protocol) che è alla base del funzionamento della stragrande maggioranza delle reti pubbliche e private.
In un network basato sul TCP/IP, ciascun sistema è identificato in modo univoco da un indirizzo IP, costituito da quattro byte del tipo 192.168.1.100 e da un numero di porta di comunicazione, e comunica con altri sistemi scambiando messaggi sotto forma di pacchetti. L'indirizzo IP, analogamente ad un numero di telefono, garantisce la possibilità di instaurare la comunicazione mentre la porta non è altro che un numero che serve a differenziare il servizio di rete, cioè l'applicazione usata per la comunicazione stessa (ad es. il servizio http ha tipicamente un numero di porta uguale ad 80, il servizio ftp ha la porta 21 ecc.).

Ogni dispositivo di una rete locale per connettersi ad Internet ha bisogno di un indirizzo Ip pubblico: ad esempio per collegare tutti i dispositivi dell'ITIS di Teramo occorrerebbero diverse decine di numeri IP pubblici, uno per ciascun dispositivo. Ma l'ITIS di Teramo dispone di un solo indirizzo IP pubblico. Ecco allora che entrano in azione i processi di NAT (Network Area Translation) e PAT (Port Address Translation) che permettono di connettere ad Internet decine e decine di indirizzi privati di altrettanti dispositivi di rete utilizzando un unico indirizzo pubblico. In pratica il gateway, cioè la via di uscita su Internet (il router ADSL) , tiene per sé l'indirizzo pubblico e si prende l'incarico di gestire le connessioni.

Facciamo un esempio concreto: rete di 2 pc collegati ad Internet che navigano sul web, indirizzo pubblico 95.242.138.178



Il Pc1 esegue una richiesta di accesso al sito www.iisteramo.gov.it. (IP 62.149.142.221 in ascolto sulla porta 80) Il Router "natta" l'indirizzo privato 192.168.1.10 e lo trasla all'indirizzo pubblico 95.242.138.178 che può essere instradato su Internet e transla anche il numero di porta assegnandogli un numero casuale (tra 0-65535) ad esempio 6560. Alla pagina www.iisteramo.gov.it arrivano le informazioni: IP 95.241.138.178 e Porta 6560
Su una tabella (Tabella di routing), il router memorizza le seguenti informazioni:

Ip sorgente	Porta sorgente	Ip traslato	Porta traslata	Ip destinatario	Porta destinatario
192.168.1.10	80	95.241.138.178	6560	62.149.142.221	80

Il Pc2 esegue una richiesta di accesso al sito www.maurodeberardis.it (IP 62.149.130.44 in ascolto sulla porta 80)
Il Router "natta" l'indirizzo privato 192.168.1.20 e lo trasla ancora all'indirizzo pubblico 95.242.138.178. Inopltre transla anche il numero di porta assegnandogli un numero casuale , questa volta ad esempio 4354. Alla pagina www.maurodeberardis.it arrivano le informazioni: IP 95.241.138.178 e Porta 4354

La tabella di routing viene aggiornata con le informazioni realtive al Pc2

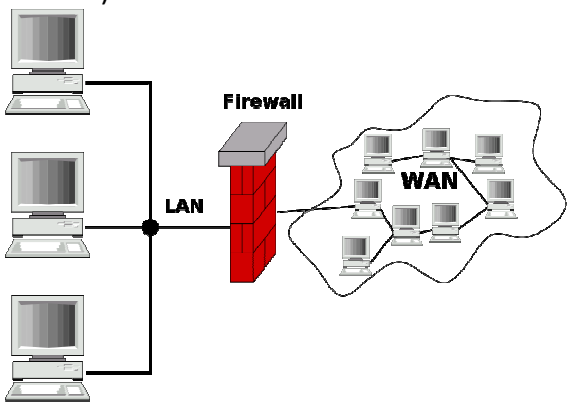
Ip sorgente	Porta sorgente	Ip traslato	Porta traslata	Ip destinatario	Porta destinatario
192.168.1.10	80	95.241.138.178	6560	62.149.142.221	80
192.168.1.20	80	95.241.138.178	4354	62.149.130.44	80

E cosi via per altre richieste …
Che cosa accade quando al router arrivano pacchetti da Internet?
Il router legge l'indirizzo IP del mittente e consulta la tabella di routing. Se l'indirizzo è presente nella colonna Ip destinatario, vuol dire che si tratta della risposta ad una richiesta fatta da un pc della rete locale e tramite il numero di porta traslata, individua il pc cui è destinato il pacchetto e glie lo inoltra.
Se l'indirizzo IP del mittente del pacchetto non si trova nella tabella di routing, vuol dire che non esiste una richiesta dalla rete locale e il pacchetto viene respinto.

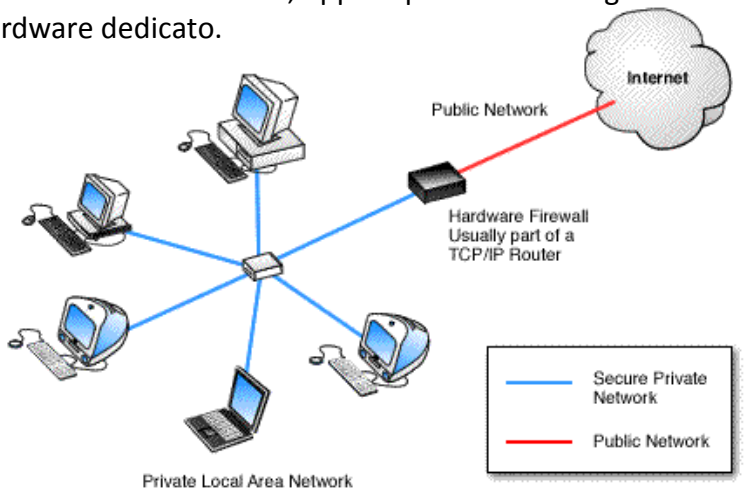
La tecnica di Nat/Pat protegge la rete locale perché gli indirizzi IP privati sono nascosti alla rete pubblica: inoltre un pacchetto con un indirizzo IP che non è presente nella tabella di routing, viene scartato.

Firewall

Il termine firewall significa "muro antincendio". Il suo scopo è quello di impedire che un incendio si propaghi da una parte all'altra del muro. Nel caso delle reti, il firewall è un dispositivo di sicurezza hardware o software che filtra tutti i pacchetti di dati entranti ed uscenti, da e verso una rete o un computer, secondo regole prestabilite. Di norma il firewall si pone tra la rete Internet esterna e la LAN (Local Area Network) interna.



Il firewall può essere realizzato con un pc dotato di un software, oppure può essere integrato in un router o implementato in un apparato hardware dedicato.



La funzionalità principale di un firewall è quella di creare un filtro sulle connessioni entranti ed uscenti e consentire agli utenti di operare nel massimo della sicurezza. Il firewall infatti agisce sui pacchetti in transito ed è in grado di eseguire su di essi operazioni di controllo, modifica o monitoraggio.

Packet filter firewall

Il firewall più semplice è il **packet filter firewall** che si limita a valutare gli header di ciascun pacchetto, ovvero l'indirizzo IP di origine e destinazione, il numero della porta TCP/UDP di origine e destinazione e il protocollo usato, decidendo quali pacchetti far passare e quali no sulla base esclusivamente delle regole configurate. Per questo motivo un firewall di questo tipo è detto stateless. Analizzando i flag dell'header TCP, sono in grado di discriminare se un pacchetto appartenente o non appartiene ad una "connessione TCP stabilita" e lo lasciano passare o la bloccano ma non sono in grado di riconoscere un pacchetto malevolo che finge di appartenere ad una connessione TCP già stabilita.

Il packet Filter Firewall è molto veloce (non deve fare un controllo approfondito del pacchetto, controlla solo alcuni parametri) e non rallenta la connessione di rete. Non è però un firewall performante riguardo alla sicurezza in quanto non controlla i dati in transito a livello di applicazioni. Per esempio, una e-mail contenente un virus può tranquillamente passare attraverso il firewall, se è consentito il traffico per i pacchetti POP/SMTP.

Personal firewall

Un altro **firewall** molto diffuso è quello **software** che si installa direttamente sui sistemi da proteggere. In tal caso, un buon firewall effettua anche un controllo di tutti i programmi che tentano di accedere ad Internet presenti sul computer nel quale è installato, consentendo all'utente di impostare delle regole che possano concedere o negare l'accesso ad Internet da parte dei programmi stessi, questo per prevenire la possibilità che un programma malevolo possa connettere il computer all'esterno pregiudicandone la sicurezza.

Il principio di funzionamento differisce rispetto a quello dei packet filter firewall in quanto, in quest'ultimi, le regole che definiscono i flussi di traffico permessi vengono impostate in base all'indirizzo IP sorgente, quello di destinazione e la porta attraverso la quale viene erogato il servizio, mentre nel personal firewall all'utente è sufficiente esprimere il consenso affinché una determinata applicazione possa interagire con il mondo esterno attraverso il protocollo IP.

Content Filtering

Una funzione che alcuni firewall prevedono è la possibilità di filtrare ciò che arriva da Internet sulla base di diversi tipi di criteri non relativi alla sicurezza informatica, ma volti a limitare gli utilizzi della rete sulla base di decisioni politiche, in particolare vietando la connessione su determinate porte o, per quanto riguarda il web, a determinate categorie di siti:

- contenuti non adatti ai minori (ad esempio in una rete domestica con postazioni libere non protette individualmente)
- contenuti ritenuti non pertinenti con l'attività lavorativa (in una rete aziendale)
- contenuti esclusi in base alle informazioni veicolate, su base politica, religiosa o per limitare la diffusione della conoscenza (in questi casi il firewall è uno strumento di censura)

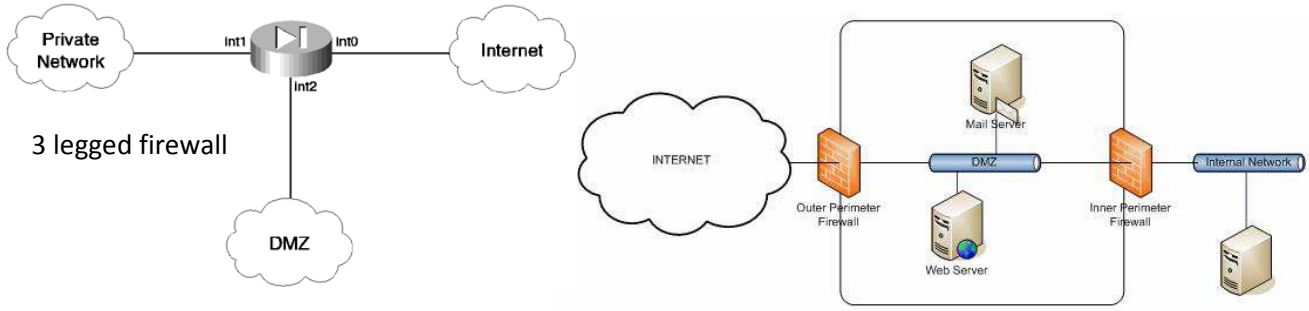
Alcune nazioni arrivano a filtrare tutto il traffico internet proveniente dal proprio territorio nazionale nel tentativo di controllare il flusso di informazioni.

Spesso l'attivazione di questa funzionalità è demandata a software e/o hardware aggiuntivi appartenenti alla categoria dell'URL filtering. Ai firewall viene però richiesto di impedire che gli utenti aggirino tali limitazioni.

DMZ

Per aumentare la sicurezza di una rete spesso si ricorre alla tecnica di dividere la rete in zone. Nei casi più semplici ci sono due uniche zone, la LAN e la WAN. La Lan è la parte di rete, protetta dal firewall, dove si trovano i dispositivi (server, pc, stampanti) i cui servizi sono riservati all'uso privato: la WAN è la parte esterna alla quale appartengono i dispositivi di routing che instradano il traffico rete locale-Internet o rete locale-altre reti remote.

Nei casi più complessi, in cui alcuni servizi devono essere pubblicati all'esterno (ad esempio vogliamo pubblicare una pagina web su un server della rete interna), è opportuno creare una terza zona: la DMZ (DeMilatarized Zone ovvero "zona demilitarizzata")
Essa è un'area in cui sia il traffico WAN che quello LAN sono fortemente limitati e controllati; in pratica, si tratta di una zona che è protetta dal firewall verso Internet ma allo stesso tempo è nascosta alla rete interna. Se il server esposto verso la rete Internet è soggetto ad un attacco esterno, questo attacco non si può propagarsi alla rete interna perché il firewall protegge la rete interna sia dalla DMZ che dalla rete esterna. La DMZ si può realizzare o con un firewall con tre interfaccie (3 legged firewall: una verso la rete esterna, una verso la rete interna e una verso la DMZ) oppure utilizzando due firewall.



Proxy Server

Un proxy (che significa intermediario) è un programma che viene eseguito su un pc che si interpone tra un client ed un server facendo da tramite tra i due, inoltrando le richieste e le risposte dall'uno all'altro. Il client si collega al proxy invece che al server, e gli invia delle richieste. Il proxy a sua volta si collega al server e inoltra la richiesta del client, riceve la risposta e la inoltra al client. Un caso in cui viene spesso usato un proxy è la navigazione web .
Per utilizzare un proxy è possibile configurare il client in modo che si colleghi al proxy invece che al
Un proxy può essere usato per una o più delle seguenti ragioni:

- connettività: per permettere ad una rete privata di accedere all'esterno è possibile configurare un computer in modo che faccia da proxy tra gli altri computer e Internet, in modo da mantenere un unico computer connesso all'esterno, ma permettere a tutti di accedere. In questa situazione, solitamente il proxy viene usato anche come firewall.
- caching: un proxy può immagazzinare per un certo tempo i risultati delle richieste di un utente, e se un altro utente effettua le stesse richieste può rispondere senza dover consultare il server originale. Collocando il proxy in una posizione "vicina" agli utenti, questo permette un miglioramento delle prestazioni ed una riduzione del consumo di ampiezza di banda.
- monitoraggio: un proxy può permettere di tenere traccia di tutte le operazioni effettuate (ad esempio, tutte le pagine web visitate), consentendo statistiche ed osservazioni dell'utilizzo della rete che possono anche violare la privacy degli utenti.
- controllo: un proxy può applicare regole definite dall'amministratore di sistema per determinare quali richieste inoltrare e quali rifiutare, oppure limitare l'Ampiezza di banda utilizzata dai client, oppure filtrare le pagine Web in transito, ad esempio bloccando quelle il cui contenuto è ritenuto offensivo in base a determinate regole o contrarie alle policy aziendali.
- privacy: un proxy può garantire un maggiore livello di privacy mascherando il vero indirizzo IP del client in modo che il server non venga a conoscenza di chi ha effettuato la richiesta

Tecniche crittografiche applicate alla protezione dei sistemi e delle reti.

Crittografia

La crittografia (cryptography) studia come trasformare un messaggio (o un testo o una stringa) in modo che esso non possa essere comprensibile a persone non autorizzate a leggerlo.

Il processo che trasforma l'informazione da comprensibile a incomprensibile è chiamato **cifratura** (encryption). Il processo che riconverte l'informazione da incomprensibile a comprensibile è detto **decifratura** (decryption).

Per cifrare un messaggio si applica un algoritmo. Facciamo un semplicissimo esempio di cifratura: ad ogni carattere del messaggio si sostituisce il carattere di posto +X nell'alfabeto. SE X=1 la stringa "Roma" verrebbe cifrata in "Spnb". Chi conosce come "Roma" è stata cifrata, ovvero chi conosce la **chiave** (key) di cifratura (in questo caso 1) , può decifrare la stringa "Spnb" e risalire a quella originale, "Roma" appunto. L'informazione nella sua forma comprensibile è chiamata **testo in chiaro** (plaintext), nella sua forma incomprensibile è chiamata **testo cifrato** (ciphertext). L'algoritmo usato per la cifratura e la decifratura è chiamato cipher o cypher.

Chiave simmetrica e chiave asimettrica

La **crittografia simmetrica** è quella tecnica di codifica nella quale i due interlocutori devono accordarsi precedentemente sulla chiave di lettura, in quanto una sola.

La robustezza degli algoritmi di cifratura dipende dalla lunghezza della chiave utilizzata, tanto è più lungo il testo della chiave, tanto più difficile sarà decifrare il messaggio. Una chiave di 40 bit ad esempio viene definita debole in quanto di facile decifratura, una di 128 invece è definita forte. Il problema nell'utilizzo della crittografia simmetrica comunque non è relativo all'algoritmo utilizzato, bensì alla difficoltà nella distribuzione della chiave, dovendo questa essere trasmessa in modo sicuro tra gli interlocutori. Oltre alla sicurezza si deve pensare che, se si gestisce un numero alto di utenti (pensiamo a un servizio bancario via internet) allora dovranno esistere N chiavi segrete, le quali comportano elevati costi e tempi di amministrazione.

Nella crittografia simmetrica

- Il ruolo del Mittente (chi invia il messaggio) e del Destinatario (chi lo riceve il messaggio) è completamente interscambiabile
- Mittente e Destinatario conoscono la stessa chiave *k* e possono cifrare e decifrare, si accordano sulla chiave e la segretezza della chiave dipende da entrambi. Cifratura e decifrazione sono molto efficienti in pratica.
- Occorre scambiarsi la chiave

Gli algoritmi di uso comune più difficili da decifrare utilizzano uno sei seguenti sistemi:

- DES (Data Encryption Standard);
- 3DES (Triple DES);
- RC-4 (Rivest Cipher 4);
- IDEA (International Data Encryption Algorithm).
- Nel novembre 2001 NIST ha annunciato il sostituto di DES: AES. AES processa i blocchi a 128 bit e opera con chiavi a 128, 192 e 256 bit. Si stima che un calcolatore può individuare una chiave DES a 56 bit in 1 sec.; invece per violare una chiave AES a 128 bit ci impiegherebbe 149 miliardi di anni.

La **crittografia asimmetrica** viene spesso definita come crittografia a chiave pubblica e può utilizzare lo stesso algoritmo, oppure algoritmi diversi ma complementari, per codificare e decodificare i dati. Nella crittografia asimmetrica, esiste una coppia di chiavi:

Chiave pubblica: attraverso questo algoritmo di cifratura, che è pubblico e deve essere distribuito, si potranno proteggere i documenti destinati al titolare della chiave privata.

Chiave privata: è l'unico algoritmo in grado di decifrare i documenti criptati con chiave pubblica.

Per questo motivo, la crittografia asimmetrica ha assunto anche la definizione di crittografia a coppia di chiavi o a chiave pubblica.

Per utilizzare questo tipo di crittografia, è necessario creare una coppia di chiavi. Quando vengono generate le due chiavi sono equivalenti (una delle due indifferentemente può essere resa pubblica). La proprietà fondamentale delle due chiavi è che un messaggio cifrato usando una delle due chiavi può essere decifrato soltanto usando l'altra chiave e viceversa. Ciò significa sostanzialmente che le due chiavi funzionano "insieme" pur non essendo possibile dall'una desumere l'altra.

Quando una delle due chiavi viene resa pubblica e l'altra privata, è possibile utilizzarle insieme fondamentalmente per due scopi:

1. Inviare un messaggio cifrato ad un destinatario. Per fare ciò il mittente cifra il messaggio con la chiave pubblica del destinatario. Per la proprietà delle due chiavi, l'unico a poter decifrare il messaggio è il destinatario, possessore della chiave privata.
2. Verificare l'autenticità di un messaggio. In questo caso il possessore della chiave privata cifra il messaggio con la sua chiave privata. Il destinatario verifica l'autenticità del messaggio decifrando con la chiave pubblica del mittente. Si noti che in questo caso tutti i possessori della chiave pubblica del mittente potranno leggere il messaggio, verificandone l'autenticità.

Quando l'utente genera la coppia di chiavi, deve conservarne gelosamente una (la chiave privata) e diffondere il più possibile l'altra (la chiave pubblica) in modo che chiunque voglia comunicare con lui/lei la conosca .

Firma digitale

Gli algoritmi di cifratura a chiave asimmetrica vengono impiegati, tra l'altro, nella firma digitale. La firma digitale, in informatica, rappresenta l'insieme dei dati in forma elettronica utilizzati come metodo di identificazione informatica. In questo ambito, le due chiavi servono a verificare l'autenticità del mittente, così come l'integrità del documento sottoscritto.

La prima operazione per generare una firma digitale è l'estrazione dal documento della cosiddetta "impronta digitale", cioè una stringa di dati, ottenuta grazie a un algoritmo di hash, irreversibile (non è possibile, a partire dall' impronta, risalire al documento originario). Tale funzione matematica sintetizza il testo in modo univoco.
L'impronta digitale o digest viene poi criptata con chiave privata ottenendo la firma digitale. Il digest potrà essere decodificato dai destinatari con la chiave pubblica e confrontato con il digest da essi prodotto sulla base del documento ricevuto, per la verifica di autenticità e integrità.
Volendo elencare i passi da compiere:

1. Il mittente crea una coppia chiave pubblica/chiave privata
2. Il mittente dà al destinatario la propria chiave pubblica
3. Il mittente scrive un messaggio che inserisce in una funzione hash; in uscita si ha un output di lunghezza fissa: il digest
4. Il mittente codifica il digest con la propria chiave privata ottenendo la propria firma digitale
5. Il mittente spedisce il documento e la firma digitale
6. Il ricevente separa il documento e la firma digitale
7. Il ricevente utilizza la chiave pubblica per decifrare la firma digitale e ottiene il digest
8. Il ricevente utilizza la stessa funzione hash del mittente sul messaggio e ottiene un nuovo digest
9. Verificando i due digest il ricevente si assicura che il messaggio non sia stato alterato e verifica l'autenticità del mittente

Software e protocolli per la crittografia

Tutti gli utenti che hanno a che fare con informazioni importanti si affidano ai computer per creare, archiviare, conservare e gestire i propri dati. Visto che la maggior parte dei PC si collega quotidianamente a Internet si può incorrere in accessi indesiderati a questi file preziosi.
Per questo motivo esistono i software di crittografia dei dati, in grado di rendere illeggibili i file a meno che non si usi la chiave virtuale in grado di decodificarli.
Il software più famoso è **Pretty Good Privacy (PGP)**: l'uso appropriato di PGP può portare ad un livello di protezione della riservatezza abbastanza elevato, tanto da rendere, quantomeno in linea teorica, praticamente impossibile la forzatura della cifratura. Tuttavia questa affermazione è vera solo in parte: la sicurezza di ogni algoritmo è subordinata alla sicurezza della passphrase con cui si protegge la propria chiave privata. Se si usa come passphrase "pippo" un attacco di forza bruta sul nostro computer impiegherà pochissimi istanti per fornire i dati cercati. Diversamente una passphrase più robusta consentirebbe di elevare la classe di complessità del problema, rendendo praticamente impossibile la ricerca di una soluzione in tempi accettabili.
PGP è più facile da usare di tanti altri crittosistemi ma, come sempre in crittografia, l'implementazione e il modo di utilizzo possono diminuire anche di molto l'effettiva sicurezza raggiunta. Gli errori nell'implementazione possono sempre essere presenti e un uso incauto può rendere vana la protezione di un qualsiasi dato. Ogni crittosistema può essere non sicuro per quanto pensato bene. Al contrario di protocolli di sicurezza come SSL, che proteggono i soli dati "in transito" (ovvero solo mentre gli stessi vengono trasmessi su una connessione di rete), PGP può essere utilizzato anche per proteggere dati su disco, o dati di backup.

Nessun crittosistema, PGP incluso, può proteggere informazioni che sono disponibili (o possono essere ottenute) in altro modo. PGP non può impedire che le informazioni che l'utilizzatore vuole proteggere possano essere ottenute tramite intercettazione o la semplice ricerca di documenti inavvertitamente eliminati nel cestino.
Anche se col PGP è possibile cifrare ogni tipo di dato o file, viene usato prevalentemente per proteggere le e-mail che non hanno un sistema di sicurezza nativo. Il PGP e l'S/MIME sono i due sistemi di sicurezza per le e-mail attualmente più utilizzati.
Sono disponibili plug-in che implementano le funzionalità del PGP per molte delle più popolari applicazioni e-mail (come Outlook, Outlook Express, Eudora, Evolution, Mutt, Mozilla Thunderbird).

Nell'ambito delle comunicazioni web, la crittografia assume un'importanza sempre maggiore. Lungo le varie dorsali viaggiano sempre più spesso dati rilevanti e informazioni riservate: da quelli personali alle informazioni bancarie, passando per le credenziali di accesso ai vari servizi web. Tra le modalità maggiormente utilizzate per criptare e quindi proteggere questi dati troviamo il **protocollo HTTPS** (HyperText Transfer Protocol over Secure Socket Layer) che è il risultato dell'applicazione di un protocollo di crittografia asimmetrica al protocollo di trasferimento di ipertesti HTTP. Viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti.
Nei browser web, la URI (Uniform Resource Identifier) che si riferisce a tale tecnologia ha nome di schema https ed è in tutto e per tutto analoga alle URI http. Tuttavia, la porta di default impiegata non è la 80 come in HTTP, ma la 443, mentre (trasparentemente all'utente) tra il protocollo TCP e HTTP si interpone un livello di crittografia/autenticazione come il Secure Sockets Layer (SSL) o il Transport Layer Security (TLS).

Per impostare un web server in modo che accetti connessioni di tipo HTTPS, l'amministratore di rete deve creare un certificato digitale ovvero un documento elettronico che associ l'identità di una persona ad una chiave pubblica. Questi certificati devono essere rilasciati da un certificate authority o comunque da un sistema che accerta la validità dello stesso in modo da definire la vera identità del possessore (i browser web sono creati in modo da poter verificare la loro validità tramite una lista preimpostata).
In particolari situazioni (come per esempio nel caso di aziende con una rete intranet privata) è possibile avere un proprio certificato digitale che si può rilasciare ai propri utenti.
Questa tecnologia quindi può essere usata anche per permettere un accesso limitato ad un web server.

Reti private virtuali (VPN)

Caratteristiche di una VPN (Virtual Private Network)

Le reti privati dedicate sono state progettate per risolvere il problema del collegamento tra sedi remote di una stessa società, o genericamente tra reti LAN remote, con la finalità di garantire un servizio sicuro, affidabile e riservato. Una soluzione a questo problema potrebbe consistere nel collegare fisicamente la rete LAN della sede centrale e la rete LAN della sede remota, ovvero realizzare una rete fisica dedicata tra due sedi. Questa soluzione è evidentemente molto costosa. La VPN è la soluzione ideale per risolvere tale problema in quanto

1. utilizza un'infrastruttura già esistente largamente diffusa ed economica come Internet, per realizzare i collegamenti fra gli utenti
2. adotta rigidi protocolli di sicurezza per far si che le comunicazioni rimangano private, sicure e soprattutto "logicamente separate" dal resto della rete mondiale come se si trattasse di una linea riservata

Una VPN è dunque un servizio di comunicazione sicuro e affidabile fra due o più dispositivi, realizzato sopra una infrastruttura di rete pubblica che rispetta i principi di riservatezza, integrità e autenticazione. Le VPN riducono in maniera profonda i costi di mantenimento di una rete sicura, migliorano le comunicazioni poiché gli utenti remoti si possono connettere alle risorse della rete aziendale o tra di loro, in completa sicurezza, da qualunque posto e 24 ore su 24. Sono infrastrutture flessibili e scalabili che possono adattarsi con facilità alle necessità di cambiamento delle reti.

Tipologie di VPN

Sostanzialmente ci sono due tipo di VPN: le VPN di accesso remoto e le VPN da sito a sito

Le connessioni VPN di accesso remoto consentono agli utenti che lavorano da casa o in movimento di accedere a un server su una rete privata utilizzando l'infrastruttura resa disponibile da una rete pubblica, ad esempio Internet. Dal punto di vista dell'utente, la VPN è una connessione point-to-point tra il computer (il client VPN) e il server di un'organizzazione. L'infrastruttura della rete condivisa è irrilevante, in quanto, dal punto di vista logico, è come se i dati venissero inviati su un collegamento privato dedicato.

Le connessioni VPN da sito a sito connettono due parti di una rete privata (sono dette anche connessioni VPN da router a router) consentendo alle organizzazioni di disporre di connessioni con routing tra uffici distanti o con altre organizzazioni su una rete pubblica e mantenendo al contempo la sicurezza delle comunicazioni. Quando le reti sono connesse su Internet un router inoltra i pacchetti a un altro router tramite la connessione VPN. Il server VPN rende disponibile una connessione con routing alla rete cui è connesso. Il router che esegue la chiamata (il client VPN) si autentica sul router che risponde (il server VPN) e, per autenticazione reciproca, quest'ultimo si autentica sul router chiamante. In una connessione VPN da sito a sito, ogni host condivide informazioni con sedi remote senza sapere dell'esistenza di un collegamento VPN; tutto il lavoro viene svolto in modo trasparente dai due router VPN che elaborano solamente i pacchetti IP diretti verso le reti remote esistenti ovvero le altri sedi dell'azienda.

Principio di funzionamento della VPN.

Il metodo di comunicazione di una VPN è molto elaborato perché i dati non si possono inviare direttamente al destinatario dato che i pacchetti transiteranno in chiaro su una rete pubblica non protetta. Per capire il meccanismo con cui una Virtual Private Network instaura una comunicazione sicura attraverso internet è necessario illustrare il concetto di **tunneling.**

Tunneling

Concettualmente, è come se un tunnel sicuro venisse costruito tra due apparecchiature finali. I dati possono essere spediti dall'origine verso la fine del tunnel, avendo la certezza che arriveranno a destinazione. Tecnicamente non esiste nessun tunnel e il Tunneling è un processo "logico" di collegamento punto-a-punto attraverso una rete IP. I due punti finali del tunnel anche se sono distanti e collegati da molti nodi, diventano per un processo logico adiacenti.

Il Tunneling compie un incapsulamento multiprotocollo dei dati. Significa che i pacchetti di dati, anche se sono di protocolli differenti, vengono imbustati nuovamente all'interno di un secondo pacchetto IP e vengono spediti sulla rete con un nuovo header IP e trasportati verso la fine del tunnel. Una volta giunti alla fine del tunnel vengono spogliati dell'imbustamento supplementare e instradati verso la destinazione. Essenzialmente, quindi, il tunneling è un processo che incapsula il pacchetto di dati all'interno di un altro pacchetto che viene spedito sulla rete. I dati vengono imbustati due volte per far si che essi siano trasmessi solamente ai destinatari finali autorizzati.

Sicurezza del tunneling

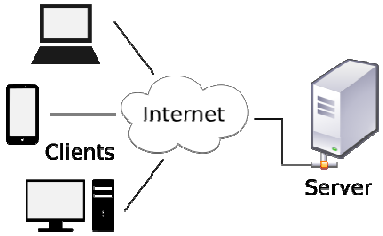
A maggiore tutela dei dati trasmessi, subentra un ulteriore processo, ossia la cifratura. Oltre a essere impacchettati a parte e spediti lungo una "corsia preferenziale" rispetto al normale traffico di rete, i dati all'interno di un VPN sono anche crittografati. In tal modo tutto il traffico che passa per un VPN è traffico riservato, al contrario del normale traffico internet che è invece "in chiaro". Il normale traffico di Rete, infatti, non è protetto in alcun modo: chiunque sia capace di intercettare una nostra comunicazione, si ritroverà in mano il suo contenuto pronto per la lettura. Chi invece dovesse riuscire a intercettare il traffico su una rete VPN si ritroverà per le mani un testo criptato difficile da decifrare.

Conclusioni

In sintesi, una rete VPN permette di collegare tra loro più computer come se fossero collegati in locale, ma sfruttando la normale connessione internet. La sicurezza di una rete VPN è variabile e dipende da come è stata costruita, ma è comunque molto più elevata rispetto alla connessione in chiaro garantita dalla normale Rete pubblica. Una rete VPN, inoltre, può essere costruita a basso costo: è sufficiente che su ogni computer connesso alla rete sia installato il programma client della rete VPN in questione.

Modello client/server e distribuito per i servizi di rete. Funzionalità e caratteristiche dei principali servizi di rete.

In informatica il termine sistema client-server indica un'architettura di rete nella quale un computer client si connette ad un server per la fruizione di un servizio, quale ad esempio la condivisione di una risorsa hardware o software con altri client.
Le reti locali aziendali (LAN), la rete Internet, i sistemi informatici e i sistemi operativi sono organizzati sotto forma di una tipica architettura client-server.



- Un server è solitamente in grado di gestire molti client
- Il client spesso deve autenticarsi, cioè eseguire il login, per poter accedere al server
- Il server si occupa di salvare in modo permanente le informazioni inviate dal client

L'architettura di un ambiente di elaborazione o di rete è distribuita quando tutte le risorse non sono nella stessa posizione o sulla stessa macchina. Internet è un esempio di una rete distribuita in quanto non esiste un centrale.

1. L'esempio più comune di questa architettura è il funzionamento di un comune browser. Il browser è un client HTTP, ovvero un'applicazione che sfrutta il protocollo HTTP per richiedere pagine web ad un server remoto.
2. Un client HTTPS è un'applicazione che utilizza il protocollo HTTPS per scambiare informazioni "sicure" tra client e server (mediante crittografia)
3. Un client FTP è un'applicazione che sfrutta il protocollo FTP per trasferire file tra il client ed un server remoto
4. Un client SQL è un'applicazione che si collega via TCP/IP (o in altro modo) ad un database server per consultare, modificare o inserire i dati memorizzati nel database
5. Un client DHCP è un computer che vuole collegarsi ad una sottorete, per cui avanza la richiesta di assegnazione di un indirizzo IP ad un server DHCP

Principali servizi disponibili su Internet

I servizi disponibili sono tantissimi, i principali sono i seguenti:

1. World Wide Web (Web)
2. File Transfer Protocol (FTP)
3. E-Mail (Posta elettronica)

<u>World Wide Web (Web)</u>

E' uno dei principali servizi di Internet che permette di navigare e usufruire di un insieme vastissimo di contenuti collegati tra loro attraverso link ipertestuali. I contenuti multimediali del Web sono organizzati in siti web a loro volta strutturati in pagine web le quali si presentano come composizioni di testo e/o grafica visualizzate sullo schermo del computer dal browser. Le pagine web, anche appartenenti a siti diversi, sono collegate fra loro in modo non sequenziale attraverso i link o collegamenti, parti di testo e/o grafica di una pagina web che permettono di accedere ad un'altra pagina web, di scaricare particolari contenuti, o di accedere a particolari funzionalità, cliccandoci sopra con il mouse, creando così un ipertesto.
Tutti i siti web, sono identificati dall'indirizzo web, una sequenza di caratteri univoca chiamata in termini tecnici URL che ne permette la rintracciabilità nel Web.

Non è previsto un indice aggiornato in tempo reale dei contenuti del Web, quindi nel corso degli anni sono nati ed hanno riscosso notevole successo i motori di ricerca, siti web da cui è possibile ricercare contenuti nel Web in modo automatico sulla base di parole chiave inserite dall'utente, e i portali web, siti da cui è possibile accedere ad ampie quantità di contenuti del Web selezionati dai redattori del portale web attraverso l'utilizzo di motori di ricerca o su segnalazione dei redattori dei siti stessi.
Oltre alla pubblicazione di contenuti multimediali il Web permette di offrire servizi particolari implementabili dagli stessi utenti del Web. I servizi implementabili sono innumerevoli, in pratica limitati solo dalla velocità della linea di telecomunicazioni con cui l'utente e chi fornisce il servizio sono collegati e dalla potenza di calcolo dei loro computer. Di seguito quindi sono elencati solo quelli contraddistinti da una denominazione generica:

- download: la distribuzione di software;
- web mail: la gestione della casella di posta elettronica attraverso il Web;
- streaming: la distribuzione di audio/video in tempo reale;
- web TV: la televisione fruita attraverso il Web;
- web radio: la radio fruita attraverso il Web;
- web chat: la comunicazione testuale in tempo reale tra più utenti di Internet, tramite pagine web;

Il Web è implementato attraverso un insieme di standard, i principali dei quali sono i seguenti:

- HTML , il linguaggio di markup con cui sono scritte e descritte le pagine web. Nel corso degli anni, per dare al web una maggiore interattività e dinamicità sono state perseguite due strade. Da un lato sono state aumentate le funzionalità dei browser attraverso un'evoluzione del linguaggio HTML e la possibilità d'interpretazione di linguaggi di scripting (come il JavaScript). Dall'altro, si è migliorata la qualità di elaborazione dei server attraverso una nuova generazione di linguaggi integrati con il web server (come JSP, PHP, ASP, etc.), trasformando pertanto i web server negli attuali application server.
- HTTP: il protocollo di rete appartenente al livello di applicazione del modello ISO/OSI su cui è basato il Web. La comunicazione tra server e client avviene tramite il protocollo HTTP, che utilizza la porta TCP 80 (o 8080), o eventualmente tramite il protocollo HTTPS, che utilizza invece la porta 443. I server http più utilizzati sono Apache HTTP Server e Apache Tomcat (sviluppati dalla Apache Software Foundation) e Internet Information Services (IIS, sviluppato da Microsoft)
- URL: lo schema di identificazione, e quindi di rintracciabilità, dei contenuti e dei servizi del Web.

I contenuti del Web sono distribuiti su più computer e non sono pertanto vincolati ad una particolare localizzazione fisica. Tale peculiarità è realizzata dal protocollo di rete HTTP il quale permette di vedere i contenuti del Web come un unico insieme anche se fisicamente risiedono su una moltitudine di computer di Internet sparsi per il pianeta.
La visualizzazione di una pagina web inizia digitandone l'URL nell'apposito campo del browser oppure cliccando su un collegamento ipertestuale presente in una pagina web precedentemente visualizzata. Per prima cosa la porzione di server-name dell'URL, cioè il nome della pagina richiesta, è risolta in un indirizzo IP usando il database globale e distribuito conosciuto come DNS (Domain Name System). Questo indirizzo IP è necessario per inviare e ricevere pacchetti dal server web. A questo punto il browser richiede le informazioni inviando una richiesta a quell'indirizzo. In caso di una tipica pagina web, il testo HTML di una pagina è richiesto per primo ed immediatamente interpretato dal browser web che, successivamente, richiede eventuali immagini o file che serviranno per formare la pagina definitiva.

Una volta ricevuti i file richiesti dal web server, il browser formatta la pagina sullo schermo seguendo le specifiche HTML, CSS, o di altri linguaggi web. Ogni immagine e le altre risorse sono incorporate per produrre la pagina web che l'utente vedrà.

File Transfer Protocol (FTP)

E' un protocollo per la trasmissione di dati basato su TCP, creato per

- promuovere la condivisione di file (programmi o dati)
- incoraggiare l'uso indiretto o implicito di computer remoti.
- risolvere in maniera trasparente l'incompatibilità tra differenti sistemi di memorizzazione di file
- trasferire dati in maniera affidabile ed efficiente.

FTP, a differenza di altri protocolli come per esempio HTTP, utilizza due connessioni separate per gestire comandi e dati. Un server FTP generalmente rimane in ascolto sulla porta 21 TCP a cui si connette il client. La connessione da parte del client determina l'inizializzazione del canale comandi attraverso il quale client e server si scambiano comandi e risposte. Lo scambio effettivo di dati (come per esempio un file) richiede l'apertura del canale dati.

Sia il canale comandi, sia il canale dati sono delle connessioni TCP; FTP crea un nuovo canale dati per ogni file trasferito all'interno della sessione utente, mentre il canale comandi rimane aperto per l'intera durata della sessione utente.

Un server FTP offre svariate funzioni che permettono al client di interagire con il suo file system e i file che lo popolano, tra cui:

- Download/upload di file.
- Riavvio (resume) di trasferimenti interrotti.
- Rimozione e rinomina di file.
- Creazione di directory.
- Navigazione tra directory.

FTP fornisce inoltre un sistema di autenticazione in chiaro (non criptato) degli accessi. Il client che si connette potrebbe dover fornire delle credenziali a seconda delle quali gli saranno assegnati determinati privilegi per poter operare sul file system. L'autenticazione cosiddetta "anonima" prevede che il client non specifichi nessuna password di accesso e che lo stesso abbia privilegi che sono generalmente di "sola lettura".

La specifica originale di FTP non prevede alcuna cifratura per i dati scambiati tra client e server. Questo comprende nomi utenti, password, comandi, codici di risposta e file trasferiti i quali possono essere "sniffati" o visionati da malintenzionati. Per ovviare al problema è stata definita una nuova specifica che aggiunge al protocollo FTP originale un layer di cifratura SSL/TLS più una nuova serie di comandi e codici di risposta. Il protocollo prende il nome di FTPS.

Tra le applicazioni che utilizzano FTP le più utilizzate sono FileZilla e JDownloader.

E-mail (posta elettronica)

La posta elettronica (e-mail o email, dall'inglese «electronic mail») è un servizio Internet grazie al quale ogni utente abilitato può inviare e ricevere dei messaggi utilizzando un computer o altro dispositivo elettronico (es. palmare, cellulare ecc.) connesso in rete attraverso un proprio account di posta registrato presso un provider del servizio. È una delle applicazioni Internet più conosciute e utilizzate assieme al web e rappresenta la controparte digitale ed elettronica della posta ordinaria e cartacea. A differenza di quest'ultima, il ritardo con cui arriva dal mittente al destinatario è normalmente di pochi secondi/minuti, anche se vi sono delle eccezioni che ritardano il servizio fino a qualche ora. Per questo l'email ha rappresentato una rivoluzione nel

modo di inviare e ricevere posta con la possibilità di allegare qualsiasi tipo di documento e di immagini digitali.
Scopo del servizio di posta elettronica è il trasferimento di messaggi da un utente ad un altro attraverso un sistema di comunicazione dati che coinvolge i client agli estremi e i server di posta, collocati presso i rispettivi provider del servizio, come nodi di raccolta/smistamento dei messaggi interni alla Rete.
Ciascun utente può possedere una o più caselle di posta elettronica, sulle quali riceve messaggi che vengono conservati. Quando lo desidera, l'utente può consultare il contenuto della sua casella, organizzarlo e inviare messaggi a uno o più utenti.
L'accesso alla casella di posta elettronica è normalmente controllato da una password o da altre forme di autenticazione.
La modalità di accesso al servizio è quindi asincrona, ovvero per la trasmissione di un messaggio non è assolutamente indispensabile che mittente e destinatario siano contemporaneamente attivi o collegati.
La consegna al destinatario dei messaggi inviati non è garantita. Nel caso un server SMTP non riesca a consegnare un messaggio ricevuto, tenta normalmente di inviare una notifica al mittente per avvisarlo della mancata consegna, ma anche questa notifica è a sua volta un messaggio di posta elettronica (generato automaticamente dal server), e quindi la sua consegna non è garantita (se il problema è relativo all'apparecchio usato dal mittente non sarà possibile effettuarla).
Il mittente può anche richiedere una conferma di consegna o di lettura dei messaggi inviati, però il destinatario è normalmente in grado di decidere se vuole inviare o meno tale conferma. Il significato della conferma di lettura può essere ambiguo, in quanto aver visualizzato un messaggio per pochi secondi in un client non significa averlo letto, compreso o averne condiviso il contenuto.
Indirizzi di posta elettronica

La chiocciola (la "a" commerciale) che separa il nome utente dal dominio.
A ciascuna casella sono associati uno o più indirizzi di posta elettronica necessari per identificare il destinatario. Questi hanno la forma nomeutente@dominio, dove nomeutente è un nome scelto dall'utente o dall'amministratore del server, che identifica in maniera univoca un utente (o un gruppo di utenti), e dominio è un nome DNS.
L'indirizzo di posta elettronica può contenere qualsiasi carattere alfabetico e numerico (escluse le vocali accentate) e alcuni simboli come il trattino basso (_) ed il punto (.). Molto spesso può tornare utile agli utenti usufruire dei servizi di reindirizzamento, utilizzati per inoltrare automaticamente tutti i messaggi che arrivano su una casella di posta elettronica verso un'altra di loro scelta, in modo che al momento della consultazione non si debba accedere a tutte le caselle di posta elettronica di cui si è in possesso ma sia sufficiente controllarne una.
Esempio di indirizzo mail: test@example.com

PEC (posta elettronica certificata)

La posta elettronica certificata (pec) è un tipo particolare di posta elettronica, disciplinata dalla legge italiana, che permette di dare a un messaggio di posta elettronica lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale garantendo così il non ripudio. Anche il contenuto può essere certificato e firmato elettronicamente oppure criptato garantendo quindi anche autenticazione, integrità dei dati e confidenzialità. oltre, il sistema di Posta Certificata, Grazie ai protocolli di sicurezza utilizzati, la PEC è in grado di garantire la certezza del contenuto non rendendo possibili modifiche al messaggio, sia per quanto riguarda i contenuti che gli eventuali allegati.

Il termine "Certificata" si riferisce al fatto che il gestore del servizio rilascia al mittente una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio ed eventuali allegati. Allo stesso modo, il gestore della casella PEC del destinatario invia al mittente la ricevuta di avvenuta consegna.
I gestori certificano quindi con le proprie "ricevute" che il messaggio:

1. E' stato spedito
2. E' stato consegnato
3. Non è stato alterato

In ogni avviso inviato dai gestori è apposto anche un riferimento temporale che certifica data ed ora di ognuna delle operazioni descritte. I gestori inviano ovviamente avvisi anche in caso di errore in una qualsiasi delle fasi del processo (accettazione, invio, consegna) in modo che non possano esserci dubbi sullo stato della spedizione di un messaggio. Nel caso in cui il mittente dovesse smarrire le ricevute, la traccia informatica delle operazioni svolte, conservata dal gestore per 30 mesi, consentirà la riproduzione, con lo stesso valore giuridico, delle ricevute stesse.

Macchine e servizi virtuali

Server dedicati e server virtuali

I server dedicati e virtuali riguardano prevalentemente i servizi di hosting. In informatica il termine **hosting** indica la locazione di uno spazio sul disco di un computer di un provider (Fornitore di Servizi Internet) da parte di un cliente, per memorizzare le pagine del suo sito e permetterne l'accesso da Internet. Le tipologie di hosting attualmente disponibili, che si differenziano per alcuni parametri quali lo spazio disponibile, la larghezza di banda, il SO Linux o Windows, si basano su :

1. **Server dedicati**: si tratta di un servizio che consente di utilizzare ad uso esclusivo un server, senza alcuna condivisione con altri utenti
2. **Server virtuali**: grazie alle tecnologie di virtualizzazione più sistemi operativi e, quindi, più server virtuali, sono in grado di girare su un'unica macchina, condividendo di fatto le risorse hardware
3. **Server condivisi**: si tratta della soluzione classica di hosting, scelta dalla maggior parte degli utenti. Una grande quantità di siti Internet girano su uno stesso server trovandosi a condividere capacità e risorse della stessa macchina. Di certo è la soluzione più economica dati gli svantaggi che comporta, ma è allo stesso tempo la soluzione ideale per siti dalle piccole pretese;
4. **Cloud**: si tratta di un servizio di hosting sempre condiviso, ma dalle garanzie maggiori in termini di spazio, larghezza di banda, CPU e RAM.

I **server dedicati** sono computer offerti in uso esclusivo ai clienti e sono pensati per lavorare 24 ore su 24, garantendo l'accesso costante a Internet. Questi computer risiedono nelle webfarm e vengono gestiti da remoto direttamente dai clienti. Il provider si occupa esclusivamente della manutenzione hardware e dei soli interventi hardware richiesti dagli stessi utenti. Il vantaggio principale per i clienti è, dunque, quello di poter operare sulle macchine come se queste fossero installate in sede, senza dover sostenere costi per il mantenimento e la gestione, dovuti ad esempio alla corrente elettrica necessaria per mantenere attivi 24 su 24 i computer, mantenere costante il raffreddamento del locale, garantire la connettiva su banda larga e via dicendo.
I server dedicati sono costituiti da una CPU, una RAM e uno spazio su disco. Ogni provider fornisce inoltre un servizio di Web server (che può essere Linux o Windows) con relativo software e una connessione permanente a Internet.

I server dedicati non sono la soluzione ottimale per tutti. Per prima cosa bisogna sottolineare che per gestirli è necessario avere le competenze adatte, pertanto, possono usufruirne solo le aziende che possiedono le competenze interne. Inoltre, i costi da sostenere, sono piuttosto elevati. Ne conviene che i server dedicati sono utili alle grandi aziende che non possono fare a meno di affidabilità, sicurezza e stabilità. Aziende, ad esempio, il cui sito riceve oltre 10 mila visite al giorno, hanno bisogno di una soluzione che sia veloce ed affidabile, onde evitare rallentamenti che possano "infastidire" gli utenti. Inoltre hanno bisogno di garanzia di continuità, in quanto, in caso di malfunzionamenti e irraggiungibilità del sito si troverebbero a dover perdere delle visite preziose per il proprio business. Capita spesso, infatti, che negli hosting condivisi, a causa del sovraccarico su un unico computer, i siti registrino rallentamenti, o a causa di script errati da parte di terzi i server sia down.

I server dedicati, inoltre, sono ideali per le aziende che hanno bisogno di notevoli quantità di memoria o hanno necessità di aggiornare continuamente le applicazioni lato server.

I server dedicati presentano importanti vantaggi:

1. garantiscono una migliore velocità di connessione rispetto ai server condivisi. Questo parametro comunque, dipende dalla larghezza di banda contrattualizzata con il provider e dal numero di connessioni. Quando si sceglie il servizio dedicato, infatti, è necessario valutare correttamente oltre ai parametri come spazio su disco, RAM e CPU, anche e soprattutto la larghezza di banda. Siti Internet che ricevono decine di migliaia di connessioni al giorno devono optare per larghezze di banda molto elevate.
2. è possibile gestire autonomamente il proprio server, senza dover dipendere in alcun modo dai provider, tranne che per piccoli interventi di tipo hardware. Questo fattore introduce vantaggi non soltanto dal punto di vista dei costi ma anche e soprattutto dal punto di vista del tempo, avendo la possibilità di intervenire per manutenzione in tempo reale e direttamente con le proprie risorse interneIl server dedicato, inoltre, non andrà mai down per colpa di terzi, come, invece, può avvenire nel caso dei server condivisi. Il lavoro altrui, infatti, non può in alcun modo influenzare il proprio server, ove nessuno ha accesso. Il server è a completa disposizione del cliente che potrà in ogni momento installare e disinstallare applicativi lato software, senza dover richiedere autorizzazioni e interventi al provider.
3. un ulteriore vantaggio da non sottovalutare è la sicurezza: i server dedicati sono di certo meno vulnerabili ad attacchi informatici rispetto ai server condivisi, proprio perché oltre a non condividere hardware con nessun altro utente, non condivide neppure nessun indirizzo IP.

Lo svantaggio principale degli hosting dedicati è sicuramente rappresentato dal costo mensile che può raggiungere cifre di migliaia di euro mensili.

I server virtuali VPS (Virtual Private Server), sono dei sistemi che vengono eseguiti all'interno di un ambiente virtuale, sfruttando la tecnica che va sotto il nome di virtualizzazione. Con questo termine si indicano i processi attraverso i quali è possibile astrarre i componenti hardware di un computer per renderli disponibili ai software sotto forma di risorse virtuali. Ciò significa che su una macchina virtuale, caratterizzata da una propria RAM, CPU e spazio su disco, può essere installato qualsiasi sistema operativo e di conseguenza qualsiasi software. Questa tecnica è molto sfruttata dagli ISP (*Internet Service Provider*) che offrono soluzioni di server virtuali a chiunque necessiti, per i propri servizi web, email, ftp, etc, di un server dedicato, ma ha a disposizione un budget limitato. La tecnica della virtualizzazione consente al Provider di offrire ai propri clienti servizi di server virtuali dedicati a cifre molto contenute. I server virtuali rappresentano delle singole istanze di sistema eseguite in ambienti virtuali. Un unico host (computer) può ospitare più istanze virtuali, che funzionano contemporaneamente sfruttando lo stesso hardware. A seconda della configurazione, ogni server può disporre di una quantità specifica della risorsa hardware condivisa (RAM, CPU, spazio su disco, …), che può essere impostata come fissa o variabile. I server virtuali, quindi, non dispongono di hardware proprio, ma si comportano come se l'hardware allocatogli dall'host sia di loro proprietà

Gli utenti che optano per i server virtuali si ritrovano, dunque, a poter sfruttare servizi dalle caratteristiche più o meno simili a quelle offerte dai server dedicati, a costi molti più convenienti. Ogni server virtuale, infatti, può disporre di un proprio indirizzo IP e di un proprio spazio di lavoro (accessibile tramite nome utente e password univoci), che sono completamente separati da quelli associati agli altri server ospitati sulla stessa macchina. Questa tecnica di condivisione, che consente di risparmiare sui costi delle infrastrutture, non inficia comunque sulla sicurezza dei dati:

i processi e il file system delle singole istanze non sono accessibili dagli altri utenti ed ognuno può contare su un proprio spazio con accesso esclusivo.

Dal punto di vista software, su ogni server è possibile scegliere autonomamente sia il sistema operativo, sia i programmi applicativi da installare. Così come per i server dedicati, anche sui server virtuali è possibile scegliere, tra il sistema operativo Windows e quello Linux. Certamente i sistemi operativi Windows si presentano con una interfaccia grafica molto più familiare e sono molto più semplici da utilizzare. I sistemi Linux, di contro, sono molto più convenienti dal punto di vista dei costi, che sono praticamente nulli essendo Linux un programma open-source. Inoltre molti dei software disponibili per piattaforma Linux sono gratuiti, al contrario di quelli per Windows.

Le soluzioni cloud

Il cloud computing indica l'insieme di tecnologie che permettono sotto forma di un servizio offerto da un provider IP, di memorizzare, archiviare ed elaborare dati grazie all'utilizzo di risorse hardware e software distribuite e virtualizzate in Rete. Non si tratta di una vera e propria nuova tecnologia ma di un approccio nuovo all'utilizzo di tecnologie già esistenti (Internet, virtualizzazione, Web) rimodellate allo scopo di creare una piattaforma di elaborazione che prescinde dalla localizzazione fisica e astrae le risorse hardware e software impiegate.

Internet, negli schemi e nei diagrammi, viene spesso rappresentato come una nuvola, appunto il cloud. È una metafora decisamente buona: al giorno d'oggi i dati e i programmi non devono necessariamente risiedere sul PC ma possono infatti essere "ospitati" su Internet o, come si dice in gergo tecnico, "in the cloud".

Le applicazioni aziendali tradizionali sono spesso complicate e costose e le risorse hardware e software necessarie per la loro esecuzione hanno elevati costi di manutenzione. È necessario un intero team di esperti per installarle, configurarle, testarle, eseguirle, proteggerle e aggiornarle. Se moltiplichiamo tutto questo per decine o centinaia di applicazioni è facile capire perché anche le più grandi aziende con i migliori reparti IT non riescono ad ottenere le applicazioni di cui hanno bisogno. Le piccole e medie sono letteralmente fuori gioco. Tempo addietro si è cercato di limare i costi dando l'infrastruttura IT in outsourcing a società esterne. Ma anche in questo caso i costi di gestione lievitano notevolmente.

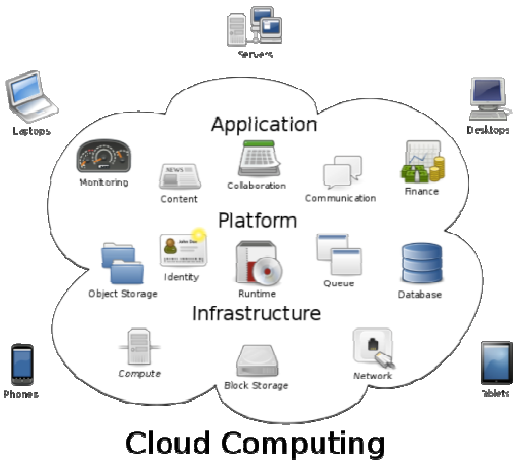
L'infrastruttura condivisa del cloud offre un funzionamento simile a quello dei servizi pubblici: l'utente paga solo le funzionalità necessarie, gli aggiornamenti sono automatici e la scalabilità verso l'alto o verso il basso è semplice. Le applicazioni basate su cloud possono essere operative in pochi giorni o settimane e sono meno costose. Con un'applicazione cloud, è sufficiente aprire un browser, accedere, personalizzare l'applicazione e iniziare a usarla. Le aziende eseguono tutti i tipi di applicazioni in the cloud, quali la gestione delle relazioni con i clienti (CRM), le risorse umane, la contabilità e molto altro ancora.

L'approccio Cloud all'acquisizione di risorse di elaborazione offre indubbi vantaggi. La fornitura come servizio evita all'azienda di fare investimenti hardware e software e di occuparsi della loro manutenzione ed evoluzione. L'azienda utilizza le risorse soltanto per il tempo che ritiene necessario; addirittura alcuni fornitori consentono un utilizzo ad ore delle risorse di calcolo.

Tra l'altro, la possibilità di poter aumentare o diminuire la richiesta di risorse di calcolo in base alla effettiva necessità del momento consente una elevata scalabilità di questo approccio all'elaborazione. L'accessibilità remota delle risorse di elaborazione offre la possibilità di poter lavorare da qualsiasi parte nel mondo, utilizzando in genere strumenti standard.

Il cloud computing è una tecnologia che utilizza Internet e server remoti centrali per mantenere i dati e le applicazioni permettendo quindi, ai consumatori di utilizzare le applicazioni senza installazione e accedere ai propri file personali da qualsiasi computer, smartphone, tablet ecc. basta avere un accesso internet.

Questa tecnologia consente il calcolo e il salvataggio dei dati in maniera molto più efficiente centralizzando lo storage, la memoria, l' elaborazione e la larghezza di banda. Un semplice esempio di cloud computing sono Yahoo mail, Gmail, Hotmail, Google Apps solo per citarne i più famosi e quelli più alla portata di tutti. c'è bisogno di un software o di un server per poterli usare per leggere l email, l'agenda o immagazzinare i dati, e per poter visionare i dati ed usarli basta che accediate ad internet da un qualsiasi pc o smartphone. Google+ inoltre ha sviluppato una serie di servizi che vanno dall'agenda giornaliera all'album photografico all'achiviazione video e tutto ciò che il consumatore avrebbe bisogno è solo una connessione a Internet La figura1 rende bene l'idea



Il cliente amministratore utilizza tali interfacce per selezionare il servizio richiesto (ad esempio un server virtuale completo oppure solo storage) e per amministrarlo (configurazione, attivazione, disattivazione). Il cliente finale utilizza il servizio configurato dal cliente amministratore. Le caratteristiche fisiche dell'implementazione, l'hardware del server, i software installati, la locazione del server remoto, divengono di fatto irrilevanti.

Immaginate di installare su un server online tutte le applicazioni utilizzate quotidianamente da milioni di persone per lavorare, giocare, trovare informazioni, ritoccare fotografie o montare il video delle vacanze. Immaginate anche di salvare tutti i file di milioni di persone nello stesso server: foto, video, documenti, elaborati vari. Tramite il collegamento Internet si potrebbe accedere al computer da qualsiasi parte del mondo e chiedergli di compiere per voi delle azioni sui vostri file e mandarvi i risultati.

Da questo è facile capire perchè oggi il cloud computing sia sulla bocca di tutti: cercando di rendere i nuovi dispositivi portatili (iPad, iPhone, smartphones ,tablet, netbook) sempre più potenti e performanti. Tanto è vero che Google con il sistema operativo per smartphones Android

e il browser Internet Chrome ha ricavato Chrome OS: un sistema operativo interamente basato su applicazioni online e sul cloud computing.

Niente più file d'installazione o salvataggi sull'hard disk, se vi servirà una nuova funzionalità, basterà cercare nel catalogo delle apps online. L'assenza di un hard disk sul vostro computer vi obbligherà ovviamente a salvare tutti i file direttamente sui server di Google. La funzionalità di memorizzazione in remoto fa si che abbiamo una copia di sicurezza (backup) in maniera automatica e l'operatività si trasferisce tutta online mentre i dati sono memorizzati in server farm generalmente localizzate nei Paesi di origine del service provider. Molto spesso i dati di backup ed i dati memorizzati vengono protetti dal cloud con una forma di crittografia con chiave digitale, in modo da preservarne la sicurezza.

Il cloud computing rende disponibili all'utilizzatore le risorse come se fossero implementate da sistemi (server o periferiche personali) "standard". L'implementazione effettiva delle risorse non è definita in modo dettagliato; anzi l'idea è proprio che l'implementazione sia un insieme eterogeneo e distribuito di risorse le cui caratteristiche non sono note all'utilizzatore ma i benefici per i suoi utenti sono molteplici:

Stoccaggio efficiente e servizi informatici a buon mercato, dal momento che tutte le risorse virtuali dall' hardware al software sono forniti dal fornitore di servizi.

Assicura l'utilizzo appropriato delle risorse, gli utenti sono tenuti a pagare solo per i servizi di cui hanno bisogno.

Altamente affidabile. Ampia disponibilità a prescindere dai distretti geografici. Lascia liberi gli utenti dalle preoccupazioni di acquisto, gestione e manutenzione di tutte le risorse, il Cloud fa tutto al posto dell'utente; in molti luoghi di lavoro oggi il cloud consente ai dipendenti di essere produttivi non solo all'interno del loro luogo di lavoro ma anche quando sono fuori dall'ufficio. Il modello SaaS (Software as a Service) assicura che le aziende risparmiano sulla spesa IT offrendo al contempo la flessibilità del software di produttività on the cloud.

Virtualizzazione dei server e del software

In informatica il termine virtualizzazione si riferisce alla possibilità di astrarre le componenti hardware, cioè fisiche, degli elaboratori al fine di renderle disponibili al software in forma di risorsa virtuale. Tramite questo processo è quindi possibile installare sistemi operativi su hardware virtuale; l'insieme delle componenti hardware virtuali (Hard Disk, RAM, CPU, NIC) prende il nome di macchina virtuale e su di esse può essere installato il software come, appunto, i sistemi operativi e relative applicazioni. Tale tecnica è applicabile sia su sistemi desktop che su sistemi server.

Uno dei principali vantaggi della virtualizzazione è la razionalizzazione e l'ottimizzazione delle risorse hardware grazie ai meccanismi di distribuzione delle risorse disponibili di una piattaforma fisica. Si ottiene che più macchine virtuali possono girare contemporaneamente su un sistema fisico condividendo le risorse della piattaforma. Le eventuali contese di risorse vengono gestite dai software di virtualizzazione che si occupano della gestione dell'ambiente (es: VirtualBox, VMware vSphere, Citrix XenServer).

Un server virtuale privato, o Virtual Private Server (VPS), è un server collegato alla rete internet che consente di installare qualsiasi tipo di software in maniera personalizzata senza richiedere alcun tipo di intervento operativo da parte del provider. Ogni utente del server virtuale è come se avesse un proprio server dedicato, quindi ha la sua RAM, la sua quota di CPU, il suo albero delle cartelle e tutto il resto. Il vantaggio principale è il costo ridotto rispetto a un analogo server fisico e il fatto di poter operare su un sistema altamente scalabile e configurabile, con la garanzia di backup automatici, continuità elettrica e di connessione alla rete.

Che differenza c'è tra server virtuale e un server fisico?
Un server virtuale ha tutte le potenzialità e le capacità di un server reale o fisico. L'unica differenza è che un server dedicato fisico mette a disposizione la totalità delle risorse hardware al solo utente. Nel caso di un server dedicato virtuale, le risorse hardware sono condivise con gli altri ospiti dell'infrastruttura, ma sono logicamente assegnate in maniera esclusiva agli utenti. Quindi, in un server fisico dedicato l'utente è "inquilino esclusivo" sia delle risorse hardware che software, mentre in un server virtuale dedicato (VPS), l'utente è inquilino esclusivo delle risorse software ma è un "condomino" delle risorse hardware.

Che differenza c'è tra server virtuale e un server cloud?
Un server cloud è sempre un server virtuale, in quanto deve poter essere scalabile, acceso o spento dall'utente in base alle proprie esigenze immediate. Un server virtuale non è necessariamente modificato in totale autonomia dall'utente, prerogativa che invece deve sempre avere un server cloud.
In generale un server cloud è definibile come:

- pagato a consumo (ore, minuti, secondi)
- scalabile, elastico on demand
- distribuito su infrastrutture ridondate geograficamente ma non replicate (scale out versus scale up)

In generale, il termine "virtuale" si riferisce alla tecnologia impiegata, mentre "cloud" è una vera e propria modalità operativa di fruizione di un servizio.
Tra i più diffusi software di virtualizzazione citiamo **VirtualBox,** gratuito per utilizzo personale, disponibile anche in versione open source, sul quale è possibile installare varie versioni di Windows e di Linux.
La velocità dei SO virtualizzati, installati facilmente a partire dall'immagine ISO del SO, sarà di sicuro più lenta rispetto al sistema operativo principale, tuttavia con un buon processore quasi non si sente la differenza. L'utilità della virtualizzazione è evidente: si possono provare programmi e tools, oppure navigare su internet in tutta tranquillità.

Tra i programmi di virtualizzazione commerciali, cioè a pagamento, citiamo **VMWare** con il quale è possibile virtualizzare qualunque versione di Windows, Linux e Solaris. In pratica, sul nostro desktop appare una finestra in cui si può installare il sistema operativo che vogliamo, come un altro computer dentro il computer. Dentro a questo nuovo sistema operativo possiamo installare i programmi che vogliamo e utilizzarli a nostro piacimento. La velocità è ottima: con certe versioni di Windows sembra addirittura di avere davanti il sistema operativo primario.