



ICDL/ECDL
FULL STANDARD
IT – SECURITY
3 – SICUREZZA in RETE
3.1 – Reti e Connessioni



IT – SECURITY
Syllabus
Versione 2.0



IT – SECURITY

SEZIONE 1 - CONCETTI di SICUREZZA

- **1.1 Minacce ai Dati**
- **1.2 Valore delle Informazioni**
- **1.3 Sicurezza Personale**
- **1.4 Sicurezza dei File**



IT – SECURITY

SEZIONE 2 - MALWARE

- 2.1 Tipi di MalWare e Loro Funzionamento**
- 2.2 Protezione dal MalWare**
- 2.3 Risoluzione e Rimozione del MalWare**



IT – SECURITY

SEZIONE 3 - SICUREZZA IN RETE

- 3.1 Reti e Connessioni

- 3.2 Sicurezza su Reti Wireless



IT – SECURITY

SEZIONE 4 - CONTROLLO di ACCESSO

- 4.1 Metodi per Impedire Accessi Non Autorizzati**
- 4.2 Gestione delle Password**



IT – SECURITY

SEZIONE 5 - USO SICURO DEL WEB

- 5.1 Impostazioni del Browser**
- 5.2 Navigazione Sicura in Rete**



IT – SECURITY

SEZIONE 6 - COMUNICAZIONI

- 6.1 Posta Elettronica**
- 6.2 Reti Sociali**
- 6.3 VoIP e Messaggistica Istantanea**
- 6.4 Dispositivi Mobili**



IT – SECURITY

SEZIONE 7 - GESTIONE SICURA dei DATI

- 7.1 Messa in Sicurezza e Salvataggio dei Dati**
- 7.2 Cancellazione e Distruzione Sicura dei Dati**



IT – SECURITY
Syllabus Versione 2.0
SEZIONE 3
Sicurezza in Rete



Sicurezza in Rete

3.1 Reti e Connessioni



Sicurezza in Rete

3.1 Reti e Connessioni

**3.1.1 Comprendere il termine “rete”
e riconoscere i più comuni tipi di rete,
quali LAN (rete locale), WLAN (rete locale wireless),
WAN (rete geografica), VPN (rete privata virtuale).**

Sicurezza in Rete

3.1 Reti e Connessioni

3.1.1 Comprendere il termine “rete”
e riconoscere i più comuni tipi di rete,
quali LAN (rete locale), WLAN (rete locale wireless),
WAN (rete geografica), VPN (rete privata virtuale).

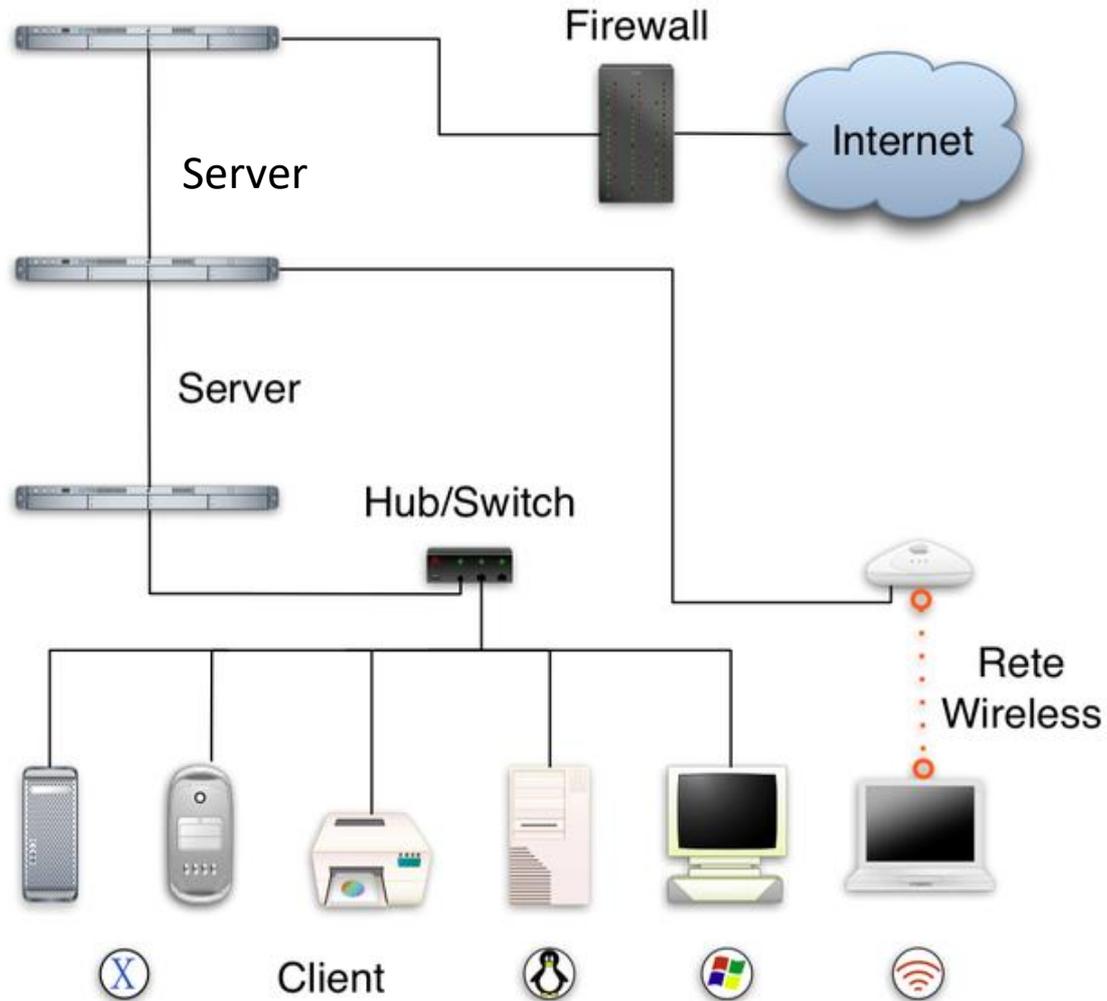
I più comuni tipi di rete:

- **LAN** (Rete Locale)
- **WLAN** (Rete Locale WireLess)
- **WAN** (Rete Geografica)
- **VPN** (Rete Privata Virtuale)

TIPI di RETI:

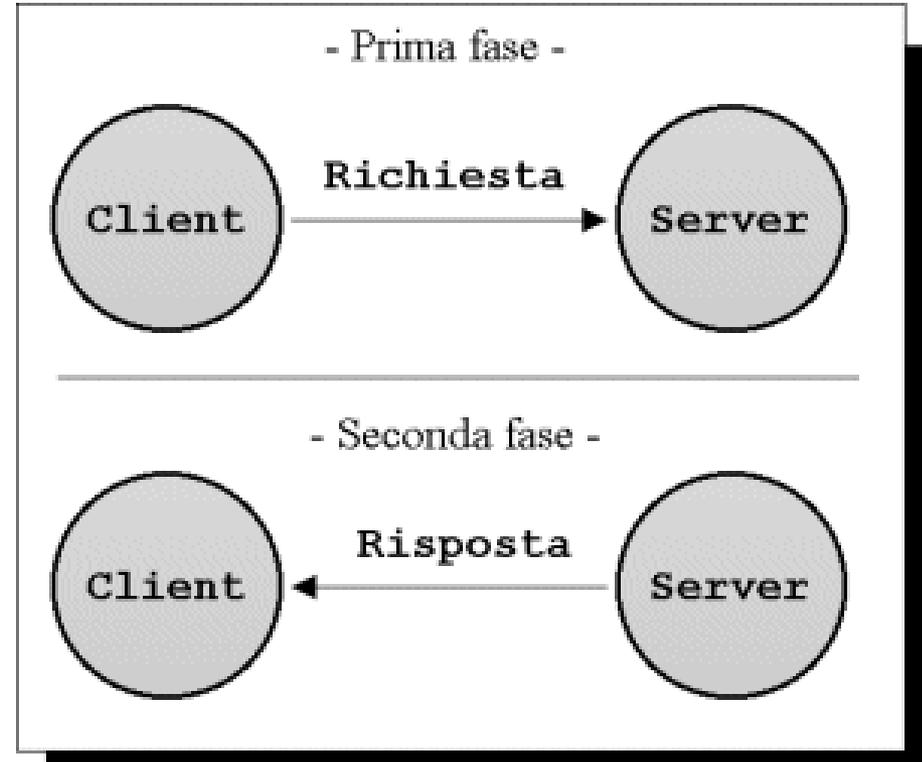
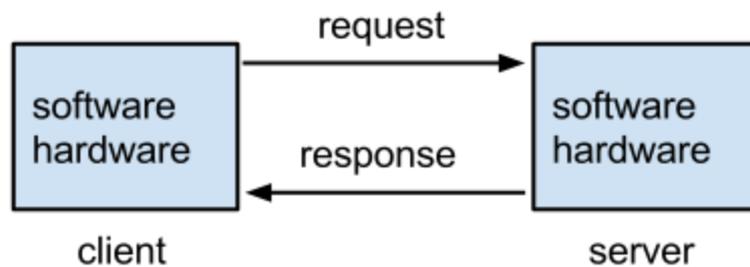
- PAN-Personal Area NetWork (Pochi Metri)
- LAN-Local Area NetWork (Edifici Adiacenti)
- WLAN-Wireless LAN (LAN Senza Cavi)
- MAN-Metropolitan Area NetWork (Perimetro Metropolitano)
- WAN-Wide Area NetWork (Una o più Regioni)

LAN-Local Area NetWork



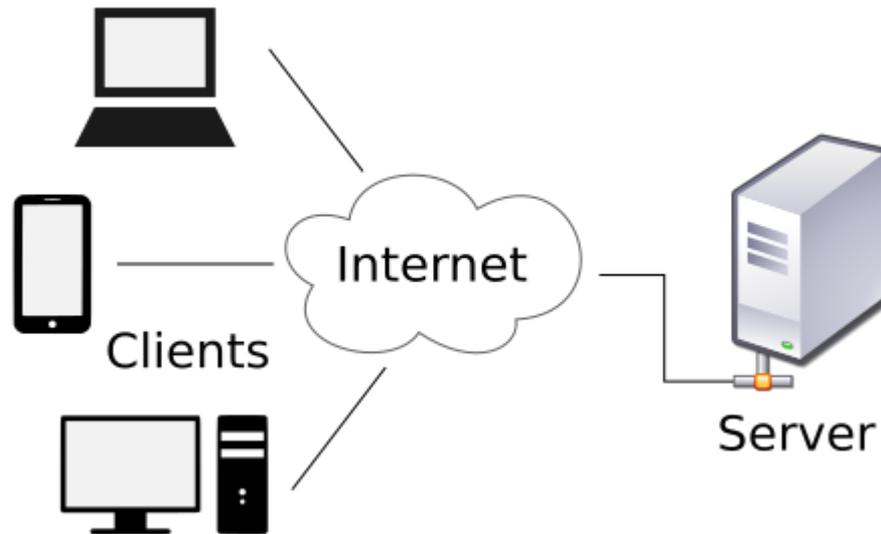
A Cura di Enzo Expsyto

Client - Server



Modalità Client-Server

Client - Server



Modalità Client-Server in Internet

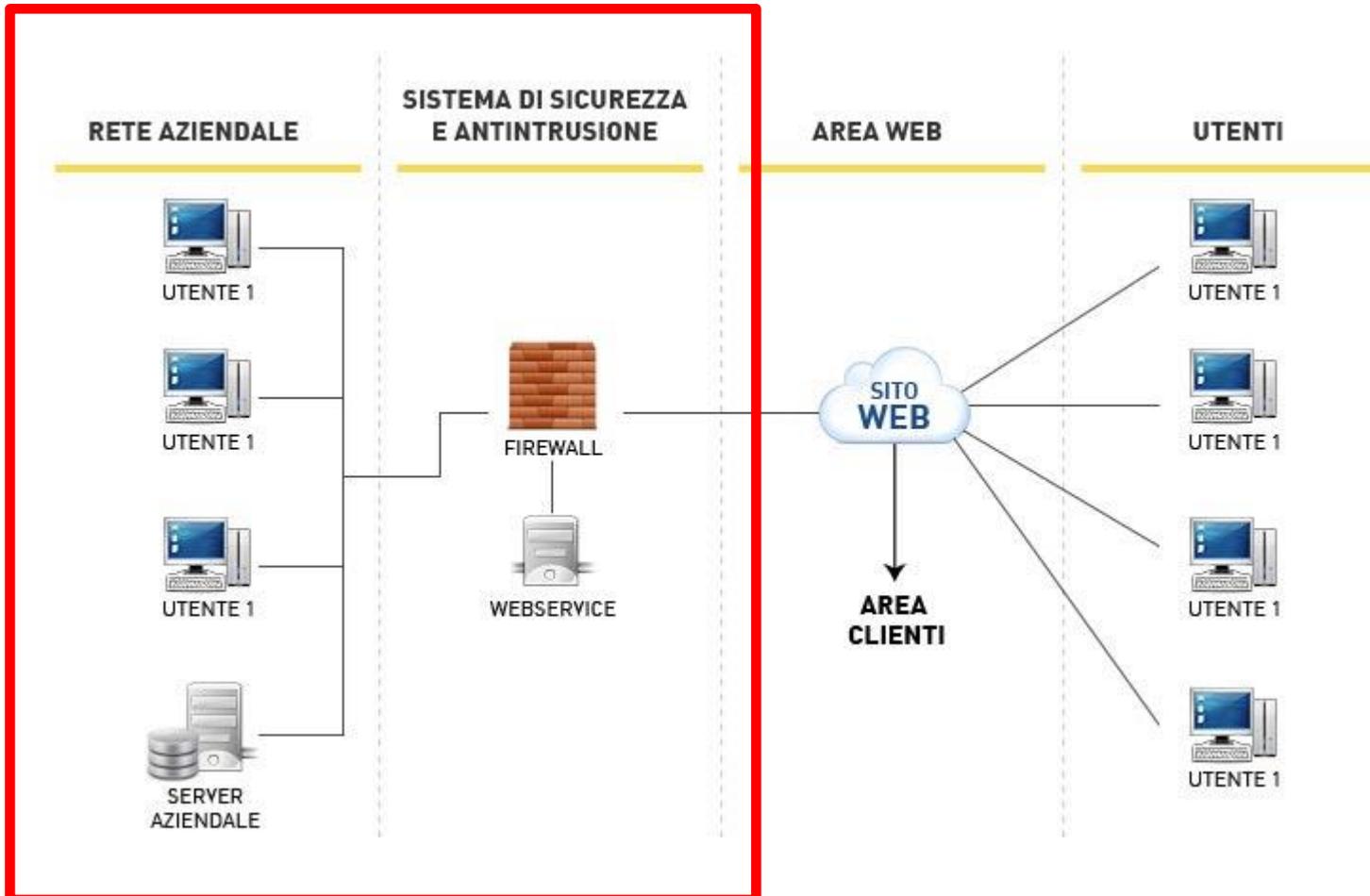
IntraNet, ExtraNet

IntraNet

**Rete aziendale privata,
con accesso a Internet,
protetta da firewall,
INACCESSIBILE DA INTERNET,
con uso di applicazioni
specifiche per l'azienda
e di tecnologie proprie
di Internet
(browser, server,
WebService, ...)**

IntraNet, ExtraNet

IntraNet



A Cura di Enzo Expsyto

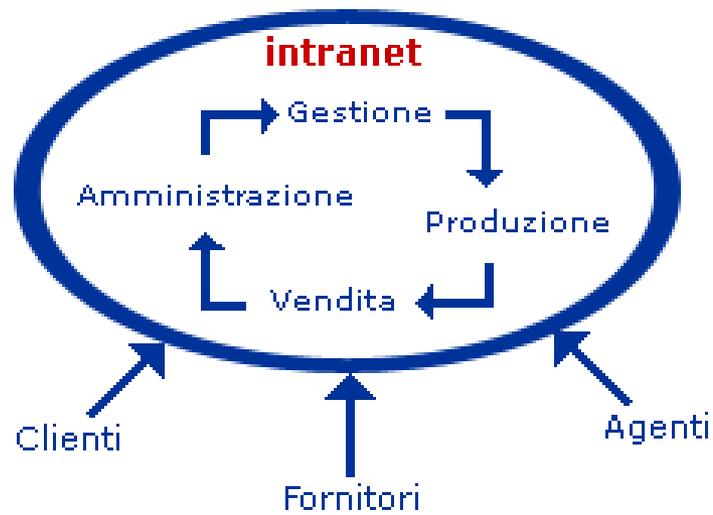
IntraNet, ExtraNet

ExtraNet

**A metà strada
tra Intranet e Internet,
rete aziendale aperta
a particolari pubblici esterni:
fornitori, clienti, altri partner**

IntraNet, ExtraNet

ExtraNet



1.1.1 Comprendere i termini: **Internet**, World Wide Web (WWW), Uniform Resource Locator (URL), collegamento ipertestuale (hyperlink)

- >Internet = Contenitore di Informazioni +
Strumento di Comunicazione tra Utenti
- >Internet = INTERconnected NETworks
- >Internet = **HardWare** + **SoftWare**
HW - Insieme di reti di computer sparse in tutto il mondo,
collegate tra loro con modi diversi (cavi, wireless, ...)
SW - Insieme di reti di computer comunicanti tra loro
con protocolli diversi
- >Internet = web (http) + posta (smtp) + voce (voip) +
newsgroup (nntp) + trasmissione file (ftp) + ...



Sicurezza in Rete

3.1 Reti e Connessioni

3.1.2 Comprendere che la connessione ad una rete ha implicazioni di sicurezza, quali malware, accessi non autorizzati ai dati, difesa della riservatezza.

Conoscere le minacce alla sicurezza provenienti da siti web, quali: virus, worm, cavalli di Troia, spyware.

Comprendere il termine “malware”.

Malware (Malicious Software)

Elenco

- Virus
- Worm
- Cavalli di Troia, Trojans
- Spyware
- BackDoor
- KeyLogger (HW o SW negativi e positivi)
- ...

Conoscere le minacce alla sicurezza provenienti da siti web, quali: virus, worm, cavalli di Troia, spyware.

Comprendere il termine “malware”.

Problemi derivanti da:

- **Scambio di File**
- **Collegamento in Rete con Altri Computer**
- **File Scaricati da Internet**
- **File Allegati di Posta Elettronica**
- **...**



Sicurezza in Rete

3.1 Reti e Connessioni

3.1.3 Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete; verifica e installazione di patch e aggiornamenti di sicurezza importanti; controllo del traffico di rete e trattamento del malware rilevato su una rete.



Sicurezza in Rete

3.1 Reti e Connessioni

3.1.4 Comprendere la funzione e i limiti di un firewall in ambiente domestico e di lavoro.

Comprendere che un firewall aiuta a proteggere il computer dalle intrusioni.

- **>Firewall = Dispositivo hardware o software che filtra tutti i pacchetti entranti ed uscenti, da e verso una rete o un computer, applicando regole che contribuiscono alla sicurezza della/o stessa/o**
- **>Hardware e Software**
- **>Tra Internet e una LAN**



Sicurezza in Rete

3.1 Reti e Connessioni

3.1.5 Attivare, disattivare un firewall personale.

**Consentire o bloccare l'accesso
attraverso un firewall personale
a un'applicazione, servizio/funzione.**