

# **Gestione della sicurezza nella Intranet Aziendale: garantire la continuità dei processi**

**gennaio 2003**

**Dr. Michele Ciotti**

**Direttore Sistemi**

**IDI - Istituto Dermopatico dell'Immacolata**

**Via Monti di Creta 104 - Roma**

**mail: [m.ciotti@idi.i](mailto:m.ciotti@idi.i)**

**[www.idi.it](http://www.idi.it)**



# Cos'è un Sistema ?

**Il "Sistema" è un insieme di elementi diversi, in relazione tra loro, in cui "l'equilibrio" di ogni elemento e dell'intero sistema è condizionato in varia misura dagli altri elementi e dai legami tra loro esistenti.**



I dati

Mezzi e strumenti

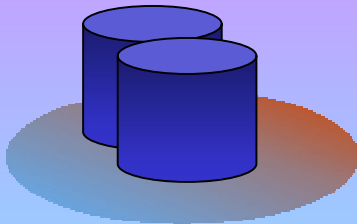
Le Procedure

Le Persone

# I DATI

I dati rappresentano il patrimonio aziendale, nonché la materia prima per costruire informazioni;

I dati si generano come risultato delle procedure operative elementari a supporto delle attività tipiche dell'impresa.



I dati sono solitamente organizzati con la tecnologia dei "database" così da poter essere leggibili per aree di interesse da parte delle diverse funzioni aziendali.

# Qual è la differenza tra “Dato” e “Informazione” ?

I "**dati**" sono numeri, lettere, caratteri, messaggi che possono essere disponibili ad un determinato individuo il quale **non li valuta dal punto di vista della loro utilità** in una specifica situazione.



Il termine "**informazione**" deve essere inteso invece come "**dato valutato**" in riferimento ad una specifica situazione.

L'informazione è **la misura del valore che un messaggio riveste** per un responsabile decisionale in una specifica situazione.

# LE PROCEDURE

Sono le **norme**, le **regole** che permettono il **trattamento dei dati**, dei messaggi, dei servizi e dei prodotti in una organizzazione.



Le procedure possono essere *formali* o *informali* e descrivere attività manuali o supportate da elaboratore.

# Le Persone

Sono elemento fondamentale del sistema informativo, hanno la responsabilità della gestione, sono incaricate di far funzionare l'intero sistema.



In funzione delle dimensioni aziendali, del tipo di attività, della collocazione geografica e di molte altre variabili, gli uomini vengono collocati all'interno del sistema azienda in una matrice gerarchica e gli vengono assegnati ruoli e mansioni secondo criteri diversi.

**L'uomo è la variabile del successo aziendale; l'uomo può con i suoi comportamenti portare il sistema all'eccellenza o alla mediocrità.**

# Mezzi e strumenti

I messaggi, i dati, i prodotti e i servizi, per poter essere trattati, veicolati, archiviati, prodotti, hanno bisogno di mezzi e strumenti.

Dai telefoni alle calcolatrici, dagli archivi cartacei ai dischi del computer, dalla voce alle linee di trasmissione telematica e per finire alla memoria e alla capacità elaborativa del nostro cervello, ognuno di queste "entità oggetto" può costituire un "mezzo" del sistema informativo aziendale.



# il sistema informativo

il sistema informativo è una variabile organizzativa che regola ed influenza i comportamenti organizzativi dell'impresa

Le variabili organizzative devono essere adeguate secondo il principio della coerenza.

# Il Sistema Informatico

Un sistema informatico deve prevedere:

- un'ampia possibilità di crescita
- criteri di sicurezza e servizi di manutenzione
- un alto livello di servizio
- facilità nell'utilizzo
- completabilità a stadi successivi
- economicità, anche nel tempo



**Ma ricordiamo sempre che...**

**L'informatica è uno STRUMENTO al servizio del Paziente  
e dell'Ospedale**

**Ogni lira spesa, ogni nuova funzionalità progettata, deve  
essere competitiva con altri investimenti di carattere  
sanitario (es. apparecchiature, letti, ecc.)**

## Normativa

DECRETO DEL PRESIDENTE DELLA REPUBBLICA 28 luglio 1999, n.318

Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675.

(GU n. 216 del 14-9-1999)

**Esigenze Utente:** I dati debbono essere sempre accessibili e sicuri

**Tecnologie:** .... Quelle sul mercato

**Infrastruttura:** ... in genere complessa

**Disponibilità finanziarie:** ... in genere basse

**Come Garantire la Continuità dei processi ??**

# Lo “SLA” (Service Level Agreement) in IDI :

- ★ **ZERO interruzioni di servizio: orario 6 am - 19 pm 6/7)  
(Pronto soccorso 24/24, 7/7)**
- ★ **Servizi internet 24/24, 7/7 (posta, web)**
- ★ **Ricostruibilità di documenti (versioni) fino a 60 gg**
- ★ **In caso di “disastro” (incendio, allagamento, ecc.)  
ripristino totale delle informazioni entro 48h (..hardware  
permettendo)**
- ★ **Tracciabilità di modifiche/utenti e tentativi di intrusione**

## Normativa

DECRETO DEL PRESIDENTE DELLA REPUBBLICA 28 luglio 1999, n.318

Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675.

(GU n. 216 del 14-9-1999)

a ciascun utente o incaricato del trattamento deve essere attribuito un codice identificativo personale per l'utilizzazione dell'elaboratore

i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi

gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale

### Adottare:

i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;

i criteri e le procedure per assicurare l'integrità dei dati;

i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;

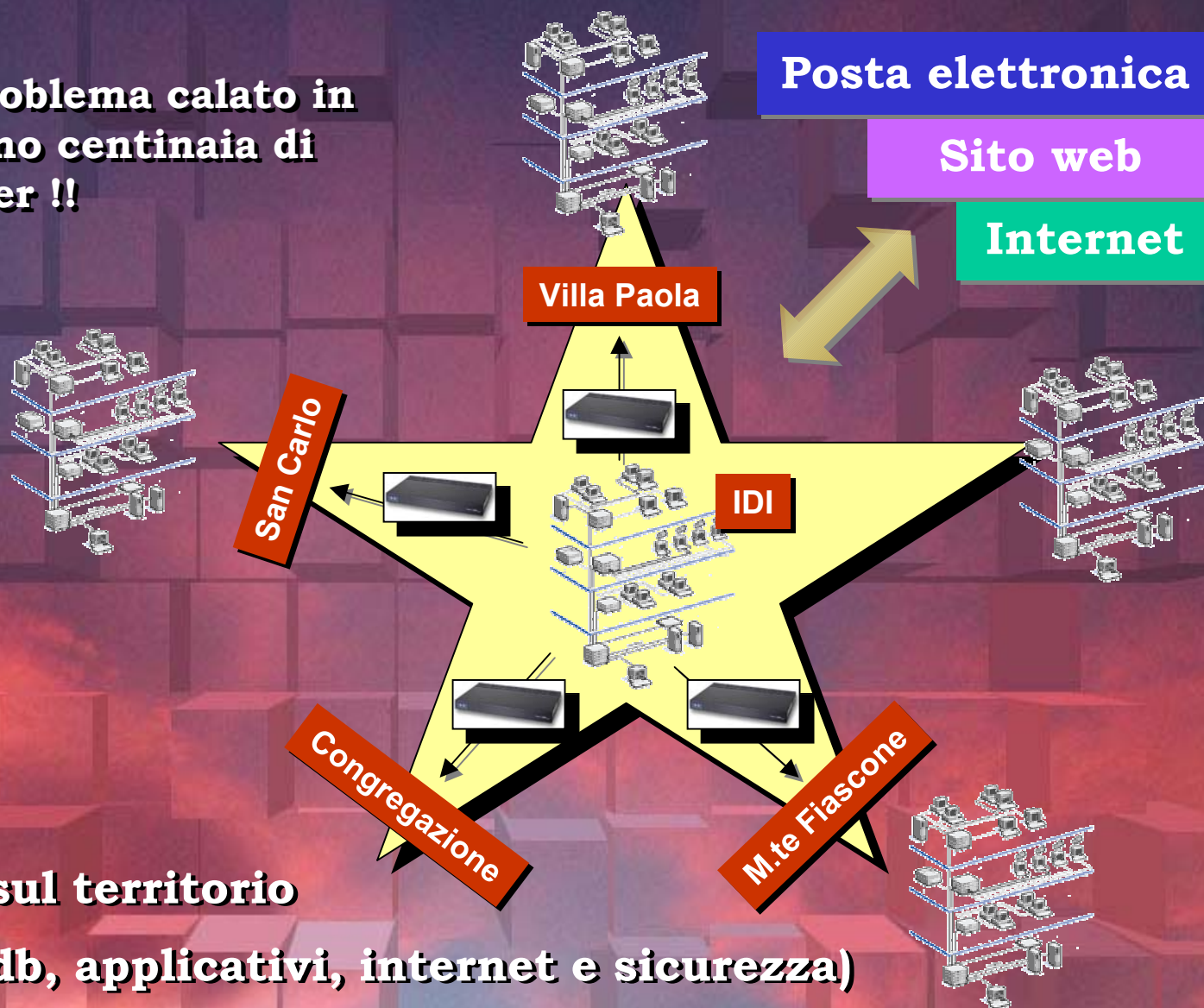


## ... anzitutto: il Personal Computer...

**... un PC “stand alone” (non collegato ad altri PC o Elaboratori) ha in se una logica applicativa, può contenere dati sensibili e riservati, ecc.**

- **Si può rompere !! -> perdita di dati**
- **Può essere acceduto da altri !! -> violazione di privacy**
- **I dati possono essere “corrotti” da virus !! -> perdita o cambiamento di informazioni**

**... immaginiamo il problema calato in realtà ove coesistono centinaia di Computer !!**



### **Qualche numero:**

- **5 sedi collegate sul territorio**
- **circa 22 server (db, applicativi, internet e sicurezza)**
- **circa 650 PC collegati sul territorio**
- **circa 1500 utenti configurati nei servizi di rete**

# Le risposte...

**Password di accesso ai PC**  
**Password di accesso ai programmi applicativi**

**policy per utenti e gruppi**

**file server**  
**application server**  
**data base server**  
**backup dei dati**

**separazione internet - intranet**

**firewall**

**antivirus**

**crittografia**

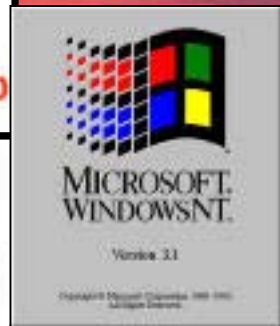
**Navigazione internet controllata**

**sistemi fault-tolerant**  
**gruppi di continuità ed elettrogeni**  
**sistemi anti-intrusione**



~~Chi accede “vede tutto”,  
l’unica è mettere un  
password in fase di avvio~~

## STANDARD SISTEMA OPERATIVO IDI Windows NT (nelle versioni NT4 e 2000)

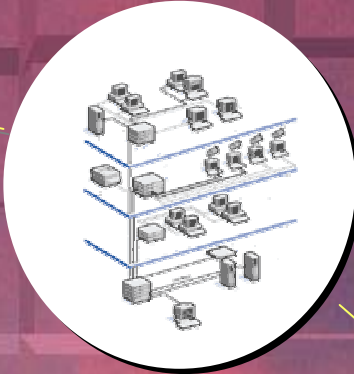


Chi accede si dichiara con il proprio nome/password ed accede ad un “computer virtuale” cui solo lui ha accesso (con i propri dati, documenti, posta elettronica, applicazioni gestionali, ecc).



I computer "personali" in rete possono condividere dati e risorse. Alcuni computer possono essere DEDICATI per dare "servizi" alla rete ed agli utenti collegati... questi computer vengono chiamati **SERVER** e si distinguono in funzione del tipo di servizio/risorsa messo a disposizione.

**File server**



**Print server**



**Data base server**



**Application server**



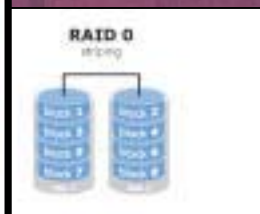
IL MELOGRANO  
DATA SERVICES





## File server

**I File server sono computer muniti di dischi di grandi dimensioni.**



**In alcuni casi si utilizzano “rack” di dischi ridondati per aumentare la sicurezza dei dati immagazzinati (**RAID**)**

Permission Entry for Boston Branch Office

Object Properties

Name: Boston Administrators (WILDWOODA\B)

Apply onto: Group objects

Permissions:	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
List Contents	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read All Properties	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write All Properties	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete Subtree	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read Permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modify Permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modify Owner	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All Validated Writes	<input checked="" type="checkbox"/>	<input type="checkbox"/>
All Extended Rights	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Create All Child Objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete All Child Objects	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Apply these permissions to objects and/or containers within this container only

Clear All

OK Cancel

**L'accesso alle informazioni viene limitato ad utenti e gruppi di utenti tramite politiche di accesso (**Policy**) e specifici permessi (**Permission**)**



## File server e Data base server

Accessi & backup



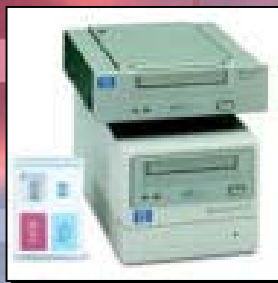
I File Server garantiscono:

- **sicurezza** (accessi registrati e controllati da policy)
- **ridondanza** (dischi RAID)
- **condivisione** (accesso consentito da più computer, in base al proprio profilo ed alle proprie “permissions”)
- **back-up** (copia periodica “incrementale” dei dati)

**In IDI il Data base server è una doppia macchina con doppi dischi... un qualsiasi componente che si rompesse viene “sostituito” in tempo reale**

**Il back-up viene generalmente garantito da sistemi di registrazione su cassette (tape), ad alta capacità (almeno 40/80Gb) montate su “rack”.**

**La tecnologia “incrementale” registra su cassetta solo i documenti modificati, permettendo di mantenerne una “storia” delle versioni precedenti.**



**Presso l'IDI vengono mantenuti in backup circa 2 mesi di “storico” dei documenti e degli archivi dei file server**

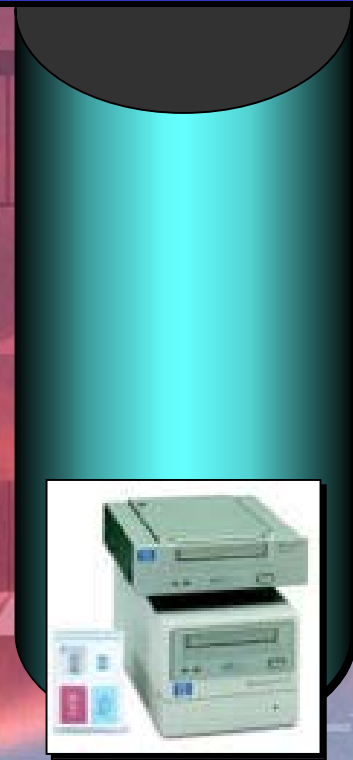
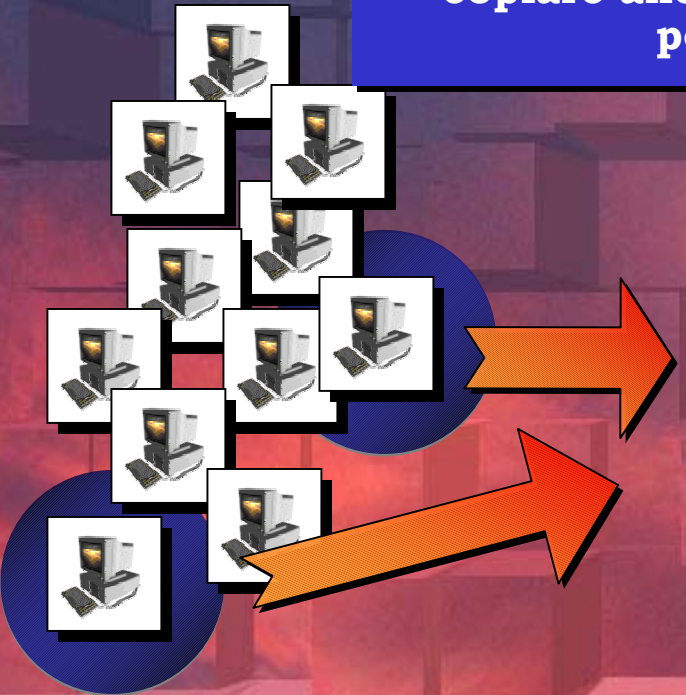




## Backup



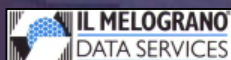
**Il servizio di backup dell'IDI permette di copiare anche dati da personal computer personali (non server)**



## Application server

Sono computer che forniscono le "applicazioni", "programmi" e "procedure".

**Sistemi di Accettazione CUP  
e Ricoveri Ord. E DH**



**Programmi amministrativi  
e contabili**



**Sistema integrato**

**Istologia**



**Gestione Clinica  
Laboratorio Analisi**



**Radiologia**



Presso l'IDI gli application server "critici" sono ridondati (doppio alimentatore, dischi di "pronto ripristino", ecc. ed, in alcuni casi, duplicati (vi è una macchina "copia" dell' application server spenta ma pronta ad essere attivata)

## Application server

Sono computer che forniscono le "applicazioni", "programmi" e "procedure".



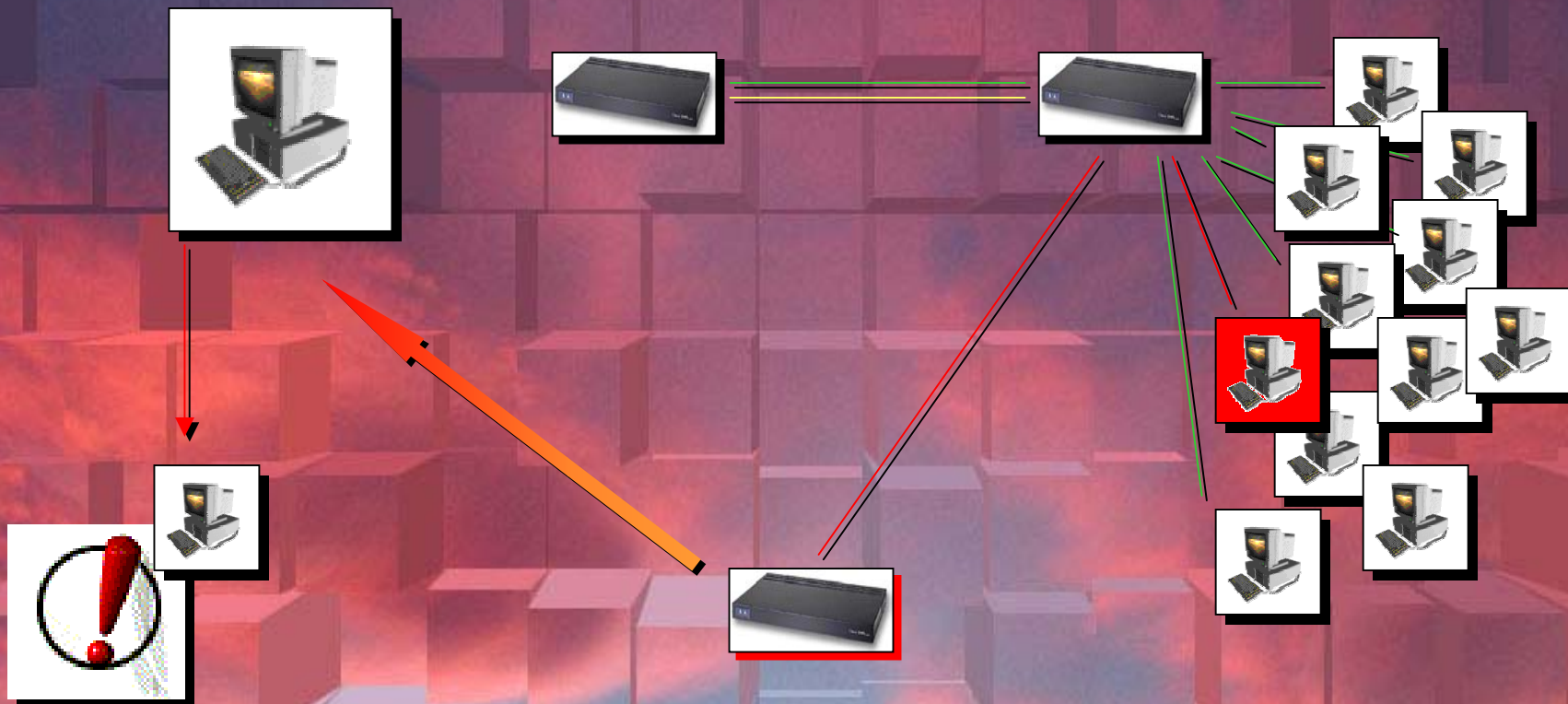
Quando un utente "chiede" dal PC un programma che risiede su un application server, immette una nuova e diversa password che lo identifica



Presso l'IDI il sistema operativo degli application server (linux, win2000, NT, unix) registrano una serie di dati relativi all'accesso, costringono un cambio periodico delle password, ecc.

## Sistema per il Monitoraggio della rete

Segnala e registra in maniera "intelligente" eventuali problemi sulla rete, carichi eccessivi o interruzioni.



## Sistemi per la manutenzione remota

**Server SMS**



**Computer che ha richiesto un intervento.**



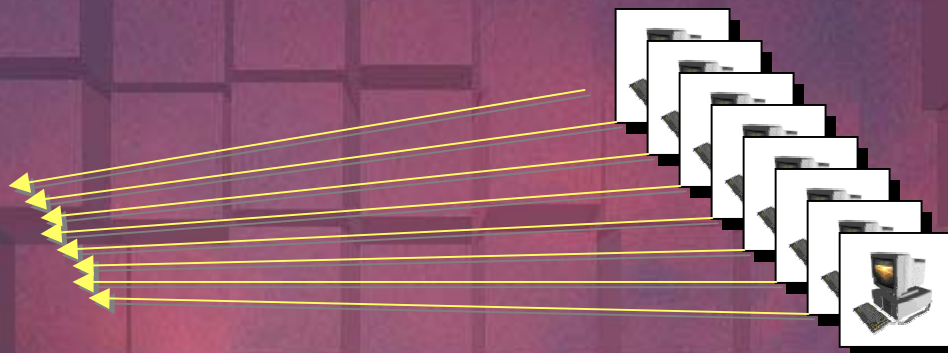
**Computer adibito all'assistenza tecnica.**

**Permettono di prendere il pieno possesso di un computer e di utilizzarlo come se fosse il proprio.**

**Sistema usato per effettuare interventi o comunque controllare il funzionamento di PC anche a notevole distanza, con forti risparmi ed efficienza negli interventi.**

## Sistemi per la manutenzione remota

Server SMS

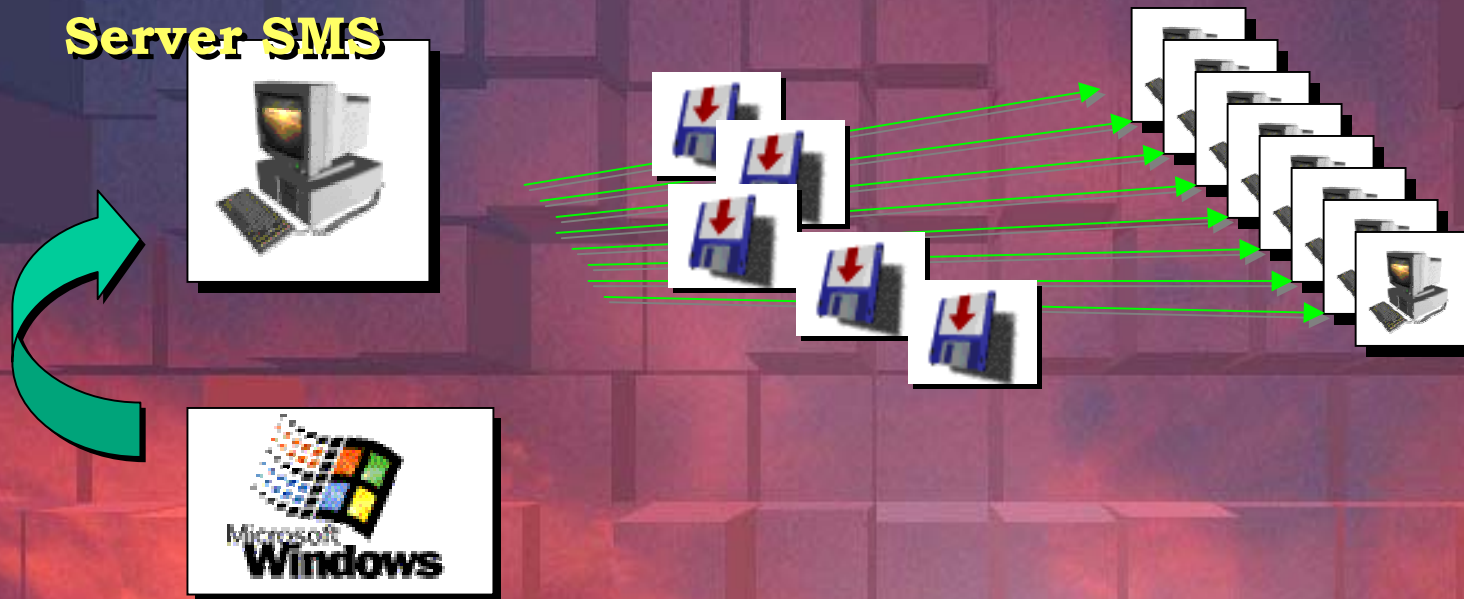


**Archivio  
hw e sw  
computer  
in rete**

**Il sistema effettua inoltre un "inventory" delle caratteristiche dei computer, mantenendo traccia di eventuali anomalie o modifiche apportate, sia a livello hardware (sostituzione di parti) che software (installazione di programmi non autorizzati).**



## Sistemi per la manutenzione remota



**Al contrario, permette anche la distribuzione, in maniera automatica, di programmi, procedure o configurazioni sui singoli "client" collegati (upload).**

**I Router, opportunamente configurati, permettono di far “dialogare” tra loro anche computer di reti private.**

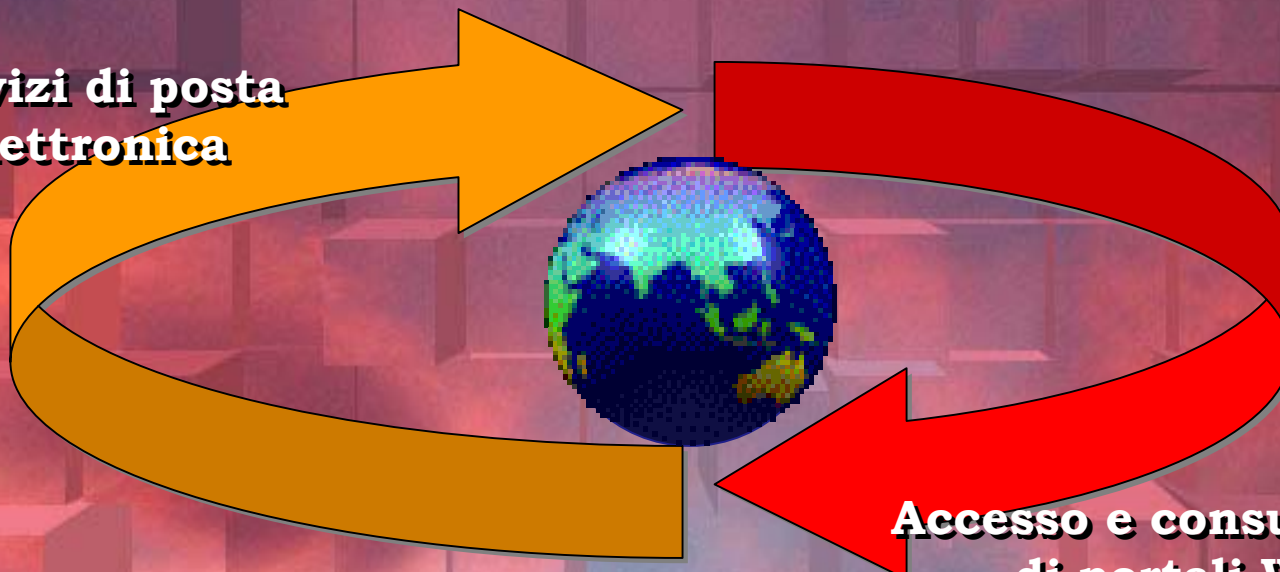
**I computer di reti Intranet connessi tra loro costituiscono una rete **INTERNET**.**



**In IDI il colloqui tra i router (su cavi esterni agli edifici, in pratica) avviene in forma crittografata.**

**La parola Internet viene ormai utilizzata, in senso “lato”, per definire un insieme di “servizi” informatici, i più comuni dei quali sono:**

**Servizi di posta elettronica**



**Accesso e consultazione di portali WEB**

**La cronaca più o meno recente ha portato all'attenzione di tutti i problemi legati all'uso improprio della rete:**

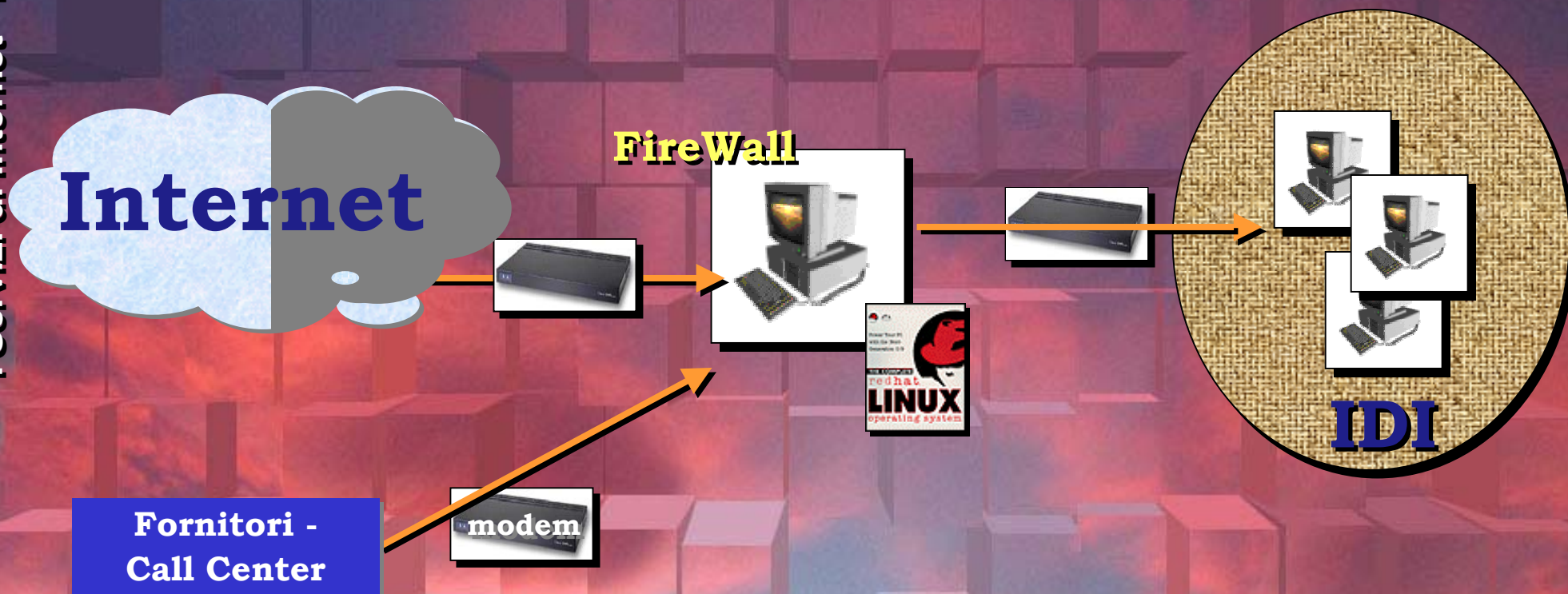
- **infezione di virus informatici in grado di distruggere informazioni ed archivi**
- **intrusione in sistemi informativi bancari nel tentativo di furti informatici**
- **spionaggio industriale**
- **intrusione in sistemi di controllo o di gestione**
- **terrorismo informatico**
- **....**

**Queste ed altre azioni sono possibili utilizzando “porte rimaste aperte” nei sistemi informativi e nelle reti intranet connesse al mondo internet... i malintenzionati “bussano” elettronicamente a queste porte e, sistemi informativi “non protetti”, aprono ingenuamente...**

# FireWall

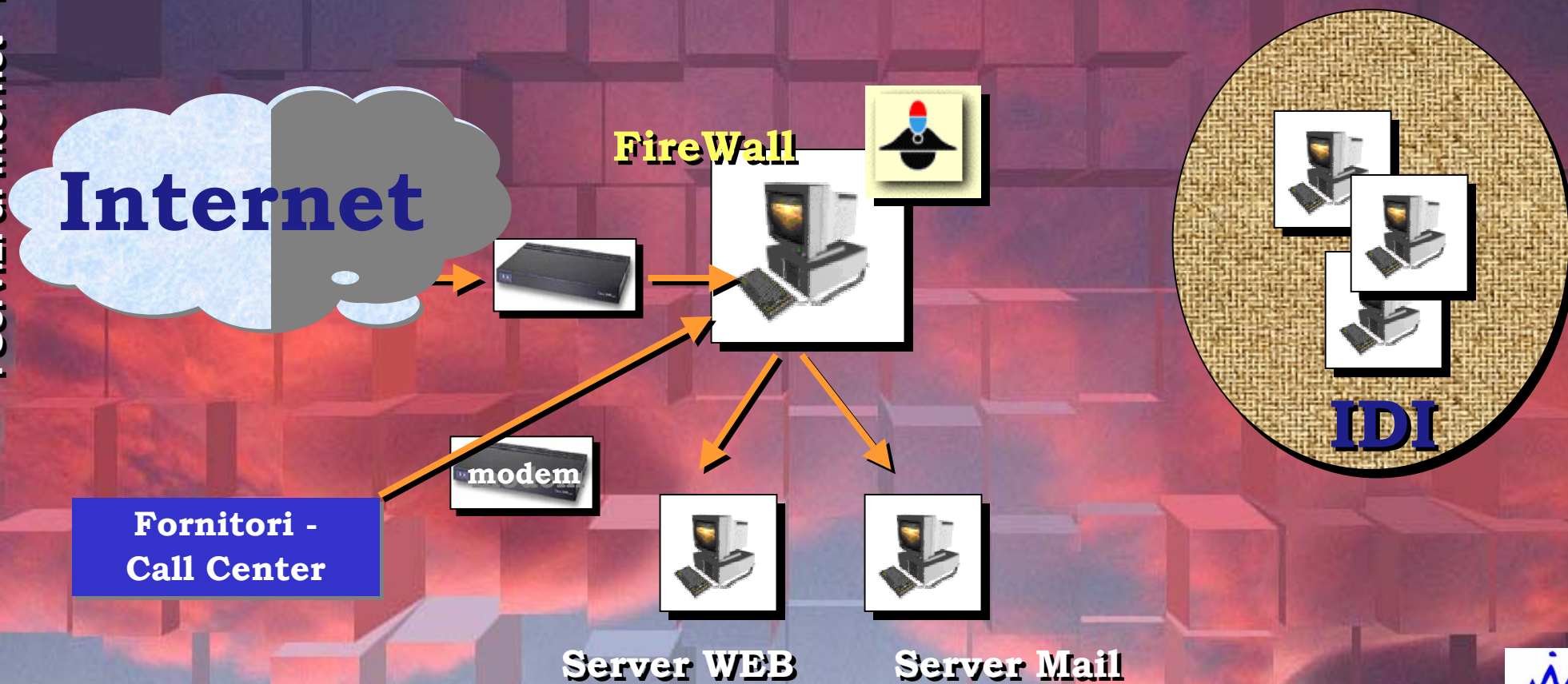
Il FireWall (porta “taglia fuoco”) ha funzioni di controllo del traffico entrante e uscente .

In IDI è un Server che regola e filtra i flussi di informazioni, secondo rigide regole, al fine di mantenere ben separate la rete Internet dalla rete Intranet dell'IDI



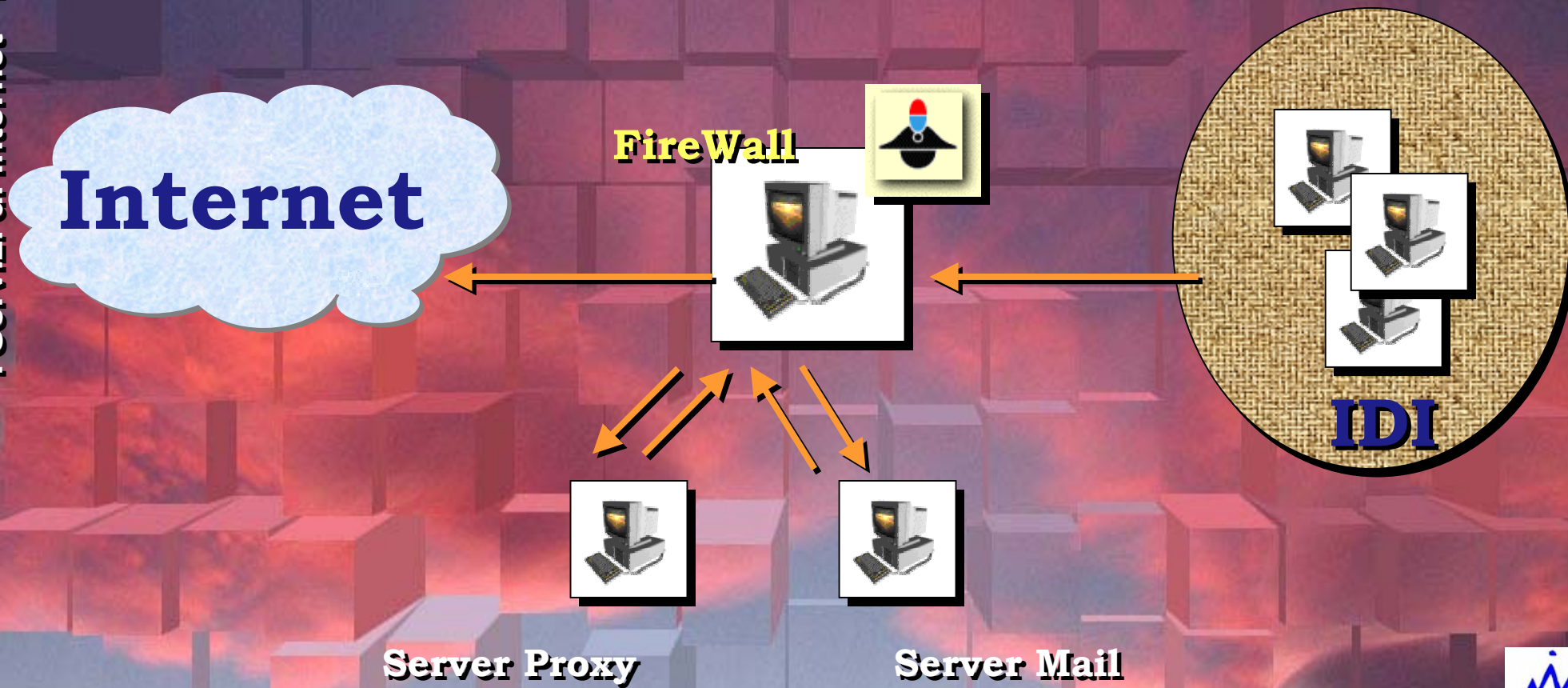
# FireWall

Un tentativo di accesso al WEB IDI o l'invio di Posta Elettronica sul server o l'accesso diretto (RAS) vengono instradati direttamente (l'utente esterno NON vede nessun PC della rete interna)...



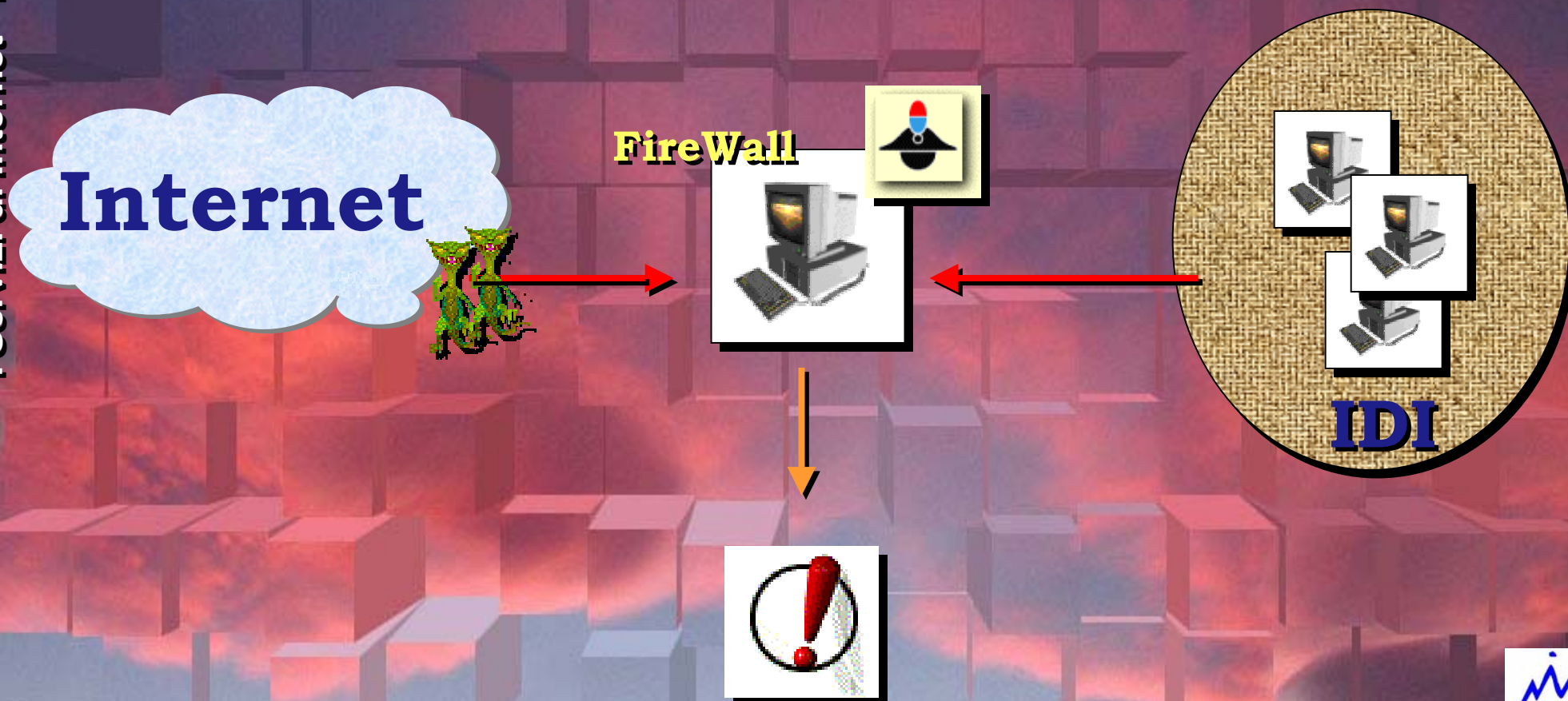
# FireWall

...l'accesso verso l'esterno da parte dei computer dell'IDI viene garantito nel senso inverso...



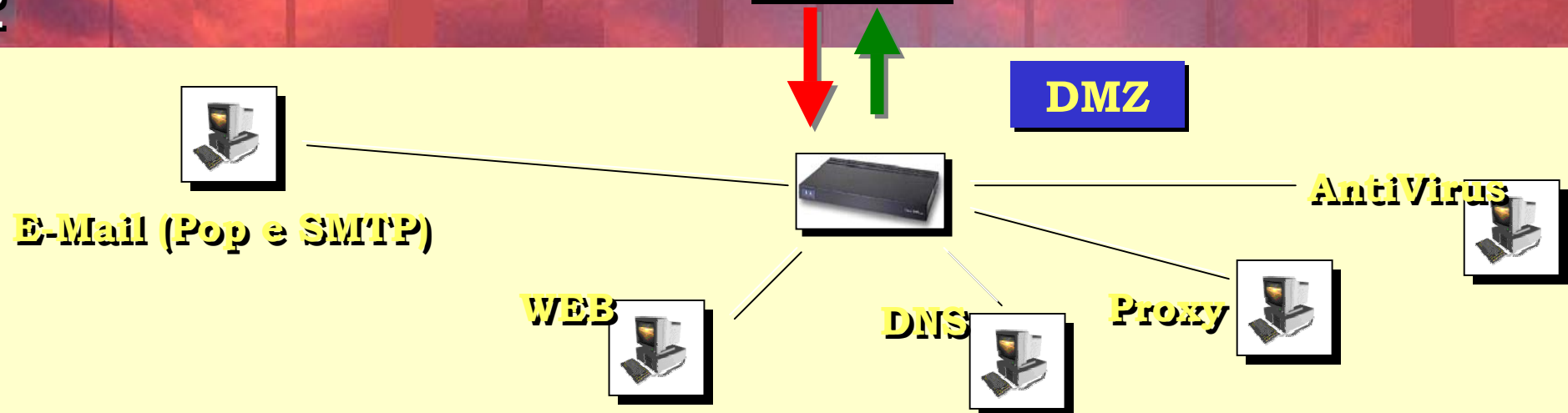
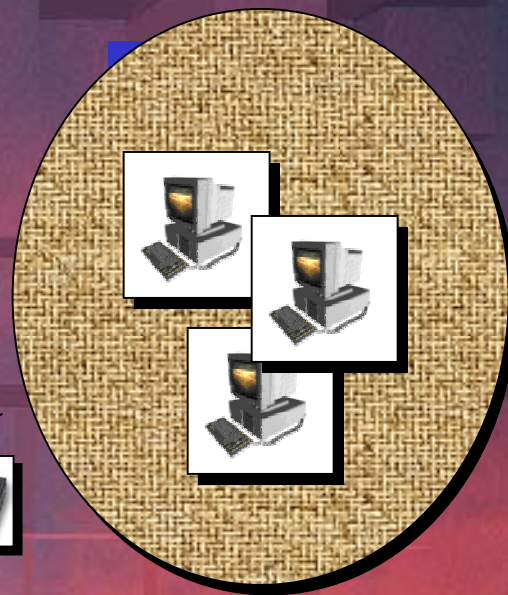
# FireWall

...tentativi di accesso illeciti vengono registrati e filtrati!



# FireWall

...i server Internet vengono solitamente "isolati", tramite il FW, in un'area detta "militarizzata" (DMZ)



## Sistemi Antivirus



**Consiste in un application server che verifica la presenza di virus:**

- **all'interno di allegati di posta elettronica (in/out)**
- **all'interno di siti WEB, tipicamente sotto forma di programmi scaricabili dal sito**
- **all'interno dei server della propria rete (per eventuali infezioni tramite dischi)**
- **all'interno di altri computer della propria rete (per eventuali infezioni da computer già infetti)**

**La presenza di virus viene segnalata ad un supervisore, al computer che ha subito l'attacco virale ed all'utente che utilizza il computer o ha ricevuto la mail.**

**Il virus viene eliminato o, in caso contrario, il documento interessato viene cancellato**

## Sistemi Antivirus



### Il virus può “infettare”:

- utilizzando files “infetti”, quindi scambiando programmi e documenti con dischetti (Office Scan Corporate) o tramite rete (**Server Scan**)
- scaricando programmi da Internet (**WEB Scan**)
- tramite “allegati” di posta elettronica (**Scan Mail**)

### Messaggi “terroristici”:

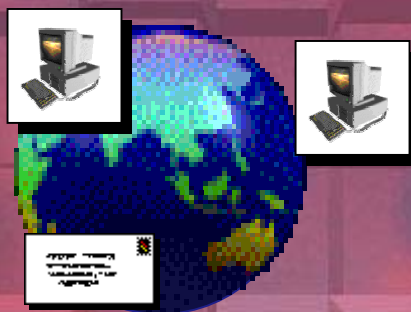
**ATTENZIONE, SE TROVI IL FILE XYZ NEL TUO COMPUTER CANCELLALO... SI TRATTA DI UN VIRUS PERICOLOSISSIMO.... Il più delle volte, dopo aver cancellato quel file, capirete di avere cancellato un programma essenziale del vostro PC!**

### Virus “Indotti”

Le “catene di S.Antonio”, pur non essendo dei “programmi virus”, inducono gli utenti ad “intasare” reti informatiche.

## Sistemi di posta

**I servizi di posta elettronica permettono di inviare e ricevere documenti con allegati di qualunque formato elettronico, in tempo reale, tra computer “riconoscibili” grazie all’attribuzione di specifici “indirizzi di rete”**

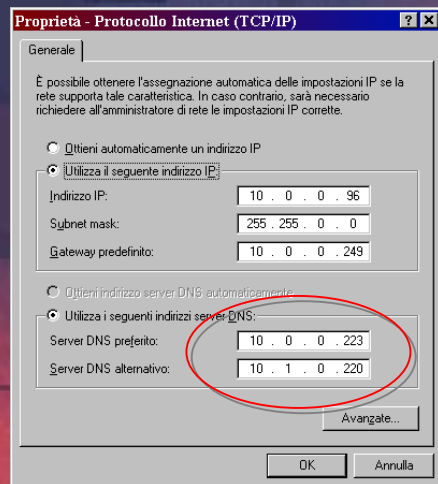


**E' però possibile che si riceva posta indesiderata..**

**O anche che si si “bombardati” (c.d. spamming) da messaggi al solo scopo di far collassare il sistema**

**In IDI vi sono specifici software che escludono mittenti indesiderati e “riconoscono” automaticamente attacchi di spamming**

I **WEB server** sono dedicati alla “pubblicazione” di pagine Internet... anche questi sono caratterizzati da un nome (URL) che viene “tradotto” in indirizzo numerico dal DNS.



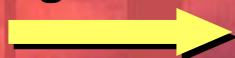
I DNS sono server essenziali per il funzionamento di Internet: ogni rete connessa ad Internet possiede un **DNS locale** che esegue una replica del DNS più vicino... Occorre definire il DNS più vicino nella configurazione di rete del proprio PC!



I **Proxy** server sono nati per “prossimizzare” le pagine internet più utilizzate (mantenendole in una memoria locale e rendendone più facile gli accessi da parte di più utenti)

1 - Quando un utente richiede una pagina, il proxy verifica se è stata già richiesta da qualcun altro...

www.tgcom.it ?



**Proxy**



2 - ... se la trova, la invia al richiedente senza “uscire” nella rete Internet...



www.pippo.com?



3 - ... altrimenti la cerca, la memorizza (per prossime richieste) e la invia al richiedente.

In IDI i **Proxy** server sono anche utilizzati per la sicurezza:

- forzare accessi a determinati siti
- limitare accessi a siti non professionali
- fare le cose di cui sopra agendo sulla base dei profili utente e delle policy

1 - La richiesta viene elaborata e confrontata con una "lista" di siti registrati in black list... oppure con le autorizzazioni dell'utente

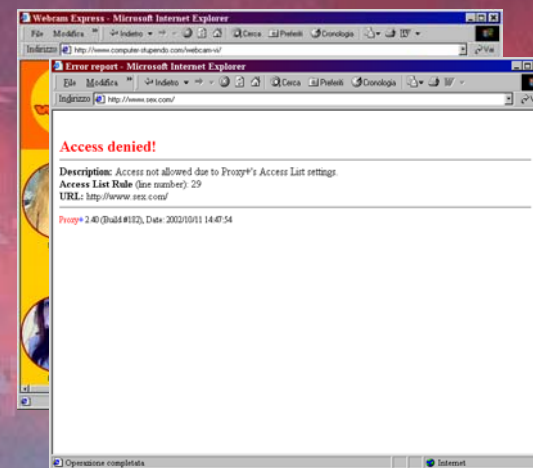
2 - ... se lo trova non da accesso al sito (**Access Denied**)

Utente



www.sexxx.org ?

Proxy



# ALTRI ASPETTI: LA "SICUREZZA FISICA"

## Centrale Informatica



✦ **Porta chiusa**

✦ **Aria ed Umidità controllata**

✦ **Gruppo di continuità da 1 ora  
con messaggio a tutti i PC 15  
min. prima dello spegnimento**

✦ **Gruppo elettrogeno automatico**

✦ **Rilevatore incendio/allagamento**

✦ **Armadio esterno ignifugo per  
copie di salvataggio**

**FINE**



**Dr. Michele Ciotti**

**Direttore Sistemi**

**IDI - Istituto Dermopatico dell'Immacolata**

**Via Monti di Creta 104 - Roma**

**mail: [m.ciotti@idi.i](mailto:m.ciotti@idi.i)**

**[www.idi.it](http://www.idi.it)**

