NUOVE **TECNOLOGIE**,
risorsa per la **comunità ecclesiale**

Montesilvano 25-27 gennaio 2005

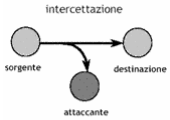
Sicurezza Informatica
- La Intranet CEI/Diocesi -

A cura di Carmelo Floridia,
c.floridia@glauco.it

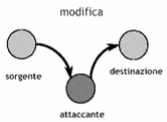
In..Sicurezza nello scambio delle informazioni

- **Considerato lo scambio di dati tra due fonti:**

- può essere violata la **segretezza della comunicazione**

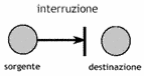


- possono essere **modificate le informazioni** in transito



- può essere falsificato **il mittente o la fonte di provenienza** dei dati

- può essere bloccata **l'operatività di un servizio** e la sua accessibilità e la fruibilità



Gli Obiettivi della Sicurezza

- Gli obiettivi della sicurezza delle informazioni, possono essere sintetizzati in:

- **Confidenzialità**
  - Tutelare la riservatezza delle informazioni affinché queste siano visibili solo da chi è autorizzato
- **Integrità**
  - Garantire l'integrità delle informazioni affinché queste non vengano modificate da chi non è autorizzato
- **Disponibilità**
  - Garantire la disponibilità e la raggiungibilità delle informazioni

- Si aggiungono come "corollario" le funzionalità di
  - **Autenticazione**
    - Chi sei?
  - **Autorizzazione**
    - Cosa puoi fare?

Sicurezza come fattore abilitante

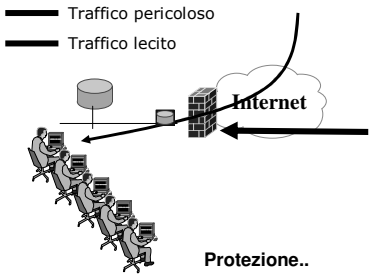
- Ciò che caratterizza i sistemi è **la frequenza e l'importanza degli scambi informativi** ⇨ **Comunicare con l'esterno e' necessario**

- I sistemi informativi **non possono più essere gestiti con logica feudale** ⇨ **Sicurezza non solo come misura preventiva ma anche come abilitatore**

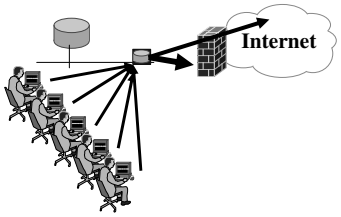
- **coinvolgimento di tutti coloro che partecipano a processi informatici** ⇨ **Ciascun utilizzatore delle postazioni deve aver presente il problema della sicurezza**

Come la Intranet e' protetta

- **Dal punto di vista Tecnologico**
  - Mediante l'adozione di strumenti di sicurezza quali
    - Realizzazione della VPN
    - Utilizzo di Firewall
    - Filtri per i siti web pericolosi
    - Autenticazione Forte



- **Iniziative anche dal punto di vista formativo**
  - Formazione ed Informazione agli utilizzatori delle postazioni che si collegano ad Internet
  - Responsabilizzazione
  - Istruzioni per la navigazione sicura su Internet



Intranet: Modalità di accesso

Modalità di accesso tradizionale

- Intervento presso la rete della diocesi per ottenere il collegamento ad Internet ed alla Intranet VPN

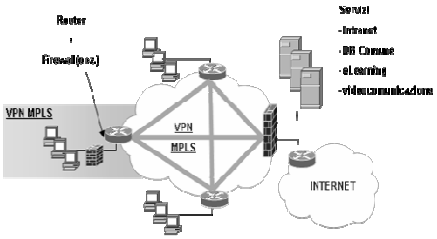
Nuove modalità di accesso

- Sono state introdotte altre due modalità semplificate di connessione alla VPN che **utilizzano il collegamento Internet già disponibile** presso le Diocesi
  - VPN Site2Site
    - Installazione di un VPN Gateway
  - VPN Software
    - Un semplice software da installare sulla propria postazione per connetterla direttamente alla Intranet VPN
    - Il software può essere ritirato oggi stesso presso lo stand dedicato rilasciando i proprio dati

Intranet : Modalità di accesso (1)
VPN-MPLS

La soluzione prevede

- Installazione router configurato per aggiungere il nodo al circuito della VPN
- Possibilità di scegliere la velocità di connessione
  - 640Kbps, 1,2Mbps, 2Mbps
- Collegamento Internet
- Servizio di sicurezza
  - Firewall centralizzato
  - Web filter
  - Firewall dedicato (opzionale)



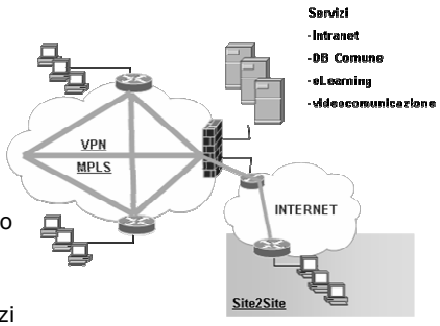
Soluzione indicata per:

- Sedi che non dispongono di collegamento ad INTERNET
- Esigenze di collegamento alla Intranet a velocità medio/alta
- Esigenze di protezione nel collegamento ad INTERNET
- Esigenze di protezione anche dall'interno

Intranet : Modalità di accesso (2)
VPN Site2Site

La soluzione prevede:

- L'installazione di un Gateway VPN per instaurare un canale di comunicazione sicuro su INTERNET (IPSEC) tra la sede e il nodo centrale della VPN
- Controllo degli accessi alla VPN e' regolamentato da Firewall
- La possibilità di far connettere tutte le postazioni della sede
- Banda limitata dalla tipologia di collegamento ad INTERNET



Soluzione indicata per:

- Sedi che dispongono di un collegamento ad INTERNET
- Esigenze di velocità di connessione alla Intranet medio/basse
- Sedi che intendono far utilizzare i servizi Intranet ad un numero di postazioni maggiori a 5

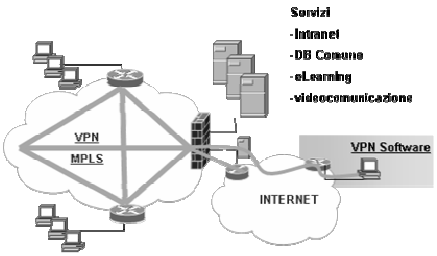
Intranet : Modalità di accesso (3)
VPN Software

La soluzione prevede:

- l'installazione di specifico software sulle postazioni che devono accedere alla Intranet (1 CD per postazione)
- l'istaurazione di un canale sicuro su INTERNET tra la postazione ed un server presso il nodo centrale della VPN
- banda limitata in base alla banda disponibile sulla connessione INTERNET

Soluzione Indicata per:

- poche postazioni che intendono accedere alla Intranet
- postazioni mobili che desiderano accedere alla Intranet quando si trovano fuori sede e dispongono di un collegamento INTERNET (in questi casi è **consigliata l'installazione di un personal firewall** per la protezione del notebook).



Riepilogando…

	VPN Standard MPLS	Site2Site	VPN Software
Velocità di connessione	In base al contratto (640 Kb,1.2Mb, 2 Mb)	Dipendente dal collegamento INTERNET	Dipendente dal collegamento INTERNET
Banda minima Garantita	Si	No	No
Installazione Client	No	No	Si
Installazione router/gateway	SI	SI	No
Tipologia di utilizzo	Sedi che non dispongono di collegamento ad INTERNET Esigenze di collegamento alla Intranet a velocità medio/alta Esigenze di protezione nel collegamento ad INTERNET	Sedi che dispongono di un collegamento ad INTERNET Esigenze di velocità di connessione alla Intranet medio/basse Sedi che intendono far utilizzare i servizi ad un numero elevato di postazioni.	Poche postazioni fisse che intendono accedere alla Intranet Postazioni mobili che desiderano accedere alla Intranet quando si trovano fuori sede e dispongono di un collegamento INTERNET (in questi casi è consigliato un personal firewall).
Servizi Centralizzati Firewall e Filtri Web	Si	No	No
Meccanismi di autenticazione	Password Token/Smart Card	Password Token/Smart Card	Password Token/Smart Card

Intranet : Modalità di accesso
Una nota sull'Autenticazione

- **Sulla Intranet e' possibili accedere mediante diversi fattori di autenticazione**
  - **Per i servizi piu' delicati sono previsti più fattori di autenticazione (token+PIN)**

Fattori di autenticazione

- **Un suggerimento sulle password**
  - **La password è composta da almeno otto caratteri;**
  - **non contiene riferimenti agevolmente riconducibili all'utente**
  - **modificata periodicamente.**

Intranet:
l'aumento di sicurezza

- **Obiettivi**
  - Adeguare il livello di sicurezza al passo con l'evolversi delle minacce
  - Tutelare la privacy della comunità
  - Evitare spiacevoli incidenti informatici
- **Il percorso di adeguamento avverrà su diversi fronti con l'obiettivo di innalzare il livello di sicurezza:**
  - **Organizzativo**
    - Formazione: Seminari di sensibilizzazione
  - **Tecnologico**
    - Rilevazione delle Intrusioni
    - Sistema di gestione e monitoraggio integrato