Servizio Informatico della Conferenza Episcopale Italiana
Via Aurelia, 468 - 00165 Roma
tel. 06 66398333 - fax 06 66398274 - sicei@chiesacattolica.it

Servizi di Sicurezza Informatica

Antivirus Centralizzato per Intranet CEI-Diocesi

Messina, Settembre 2005

Indice degli argomenti

1 Antivirus Centralizzato

1.1 Descrizione del servizio

Il servizio prevede l'adozione di una soluzione antivirus semplice ed efficiente che viene centralmente monitorata e mantenuta aggiornata dal SICEI con il minimo impatto di performance e con l'eliminazione dei problemi di configurazione/aggiornamento per le workstation, i portatili, i file server ed i Server della Diocesi

Il Servizio prevede:

- **Supporto nella fase di installazione dell'antivirus (con diverse modalità)**
  - Installazione da remoto (se è possibile accedere alla macchina come amministratore di sistema)
  - Indicazione di un link all'utente da dove scaricare l'antivirus
  - Invio del kit di installazione
- **Controllo centralizzato**
  - Della versione dell'antivirus
  - Dello stato di aggiornamento
  - Dei virus riscontrati
- **Aggiornamento repentino ed in modalità "push"**
  - Gli aggiornamenti dell'antivirus saranno inviati ai computer nel momento in cui si connettono alla rete con il vantaggio di essere subito aggiornati
- **Reportistica periodica**
  - Report periodici sullo stato dell'antivirus (virus rilevati, spyware rilevati, ultimo aggiornamento)

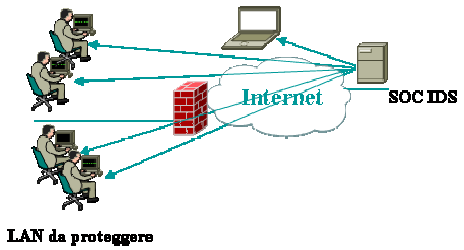
1.2 Architettura

Di seguito l'architettura della soluzione antivirus.
L'architettura prevede:

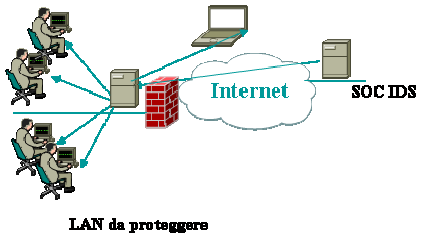
- 1 server centrale gestito dal SOC di IDS
- N client installati sulle workstation della Diocesi

Il software antivirus oltre a svolgere le operazioni di un software antivirus tradizionale, dialoga con il server centrale per:

- Download aggiornamenti
- Invio alert su virus rilevati



In reti protette da Firewall o dietro NAT la soluzione è applicabile mediante l'installazione di una componente software su un server o una workstation locale che dialoga con il server centrale



1.3 Tecnologie di riferimento

La Tecnologia di riferimento selezionata è Panda Software BusinesSecure : soluzione antivirus disegnata ad hoc per le reti delle piccole e medie imprese.
Panda **BusinesSecure** protegge sia le workstation che i server di file. **ClientShield** è la protezione antivirus di Panda Software realizzata appositamente per i PC connessi alla rete. Questo prodotto è stato sviluppato con l'obiettivo di minimizzare lo spazio occupato nei computer degli utenti e di ridurre la larghezza di banda utilizzata nella distribuzione. ClientShield incorpora anche un sistema completo di sicurezza, incrementando le funzioni del software antivirus con un sistema di bloccaggio dello spam, la protezione contro gli hacker e scoperta delle vulnerabilità, rendendolo così uno strumento di protezione semplice ma efficace per i client. Con ClientShield si possono scoprire e eliminare i virus senza pregiudicare le performance dei computer e senza che sia necessario l'intervento né dell'utente né dell'amministratore di rete.

Per assicurare la difesa dei file contenuti nei server della piccola e media impresa, fa parte di BusinesSecure anche **FileSecure** che protegge sia i server Windows incluse le installazioni in cluster, sia il sistema operativo Novell Netware (versione 4, 5 e 6).

Grazie ad **AdmineSecure**, tanto l'installazione quanto la distribuzione e l'aggiornamento di qualsiasi modulo antivirus può essere fatta in modo veloce ed intuitivo, sia per le reti locali che le reti WAN. Inoltre AdmineSecure, grazie al sistema attivo di avvisi, fornisce informazioni circa i nuovi virus in circolazione, così come i nuovi sviluppi dei prodotti offerti da Panda Software.

BusinesSecure comprende :
- ClientShield
- FileSecure
- AdminSecure

1.4 Documentazione prodotta

Su richiesta della Diocesi saranno prodotti report relativi allo stato di aggiornamento delle postazioni di lavoro della Diocesi.
Sarà dato un report che indica:

- postazioni protette
- postazioni con versioni aggiornate
- postazioni con versioni da aggiornare
- numero di virus bloccati
- numero di virus che non sono stati bloccati

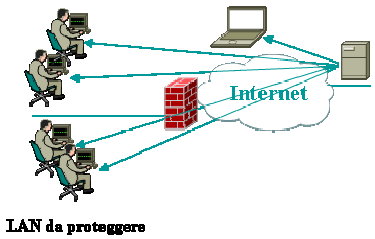
1.5 Benefici

- Semplicità di gestione
  - Mediante la gestione centralizzata è possibile tenere sotto controllo lo stato di aggiornamento dei client e dei file server della Diocesi, individuare eventuali virus che si stanno diffondendo per la rete
- Aggiornamenti tempestivi
  - L'adesione ad un network centralizzato consente di avere a disposizione gli aggiornamenti in tempi decisamente minori e di beneficiare dei problemi identificati e risolti su un nodo per riportarli in anticipo sugli altri nodi
  - Il controllo centralizzato consente di individuare utenti che non hanno effettuato l'aggiornamento in modo da contattarli in maniera proattiva.
- Aggiornamenti Automatici
  - Aggiornamenti automatici e rilasciati con cadenza almeno quotidiana.
- Costi Contenuti

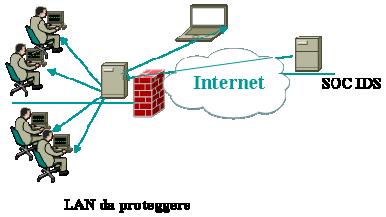
1.6 Modalità di erogazione del servizio

Per l'erogazione del servizio e' necessario che le postazioni client siano direttamente raggiungibili (via IP) dal server.
Il servizio può essere erogato:

- **Direttamente (Senza server intermedio sulla rete locale)**
  - a macchine collegate in VPN software (PC to LAN)
  - alle macchine connesse in VPN LAN to LAN alla Intranet
  - a macchine sulla rete Intrnet CEI-MPLS



- **Indirettamente (con software server intermedio da installare su un server/workstation sulla rete LAN della Diocesi)**
  - A tutte le macchine sulla rete LAN della Diocesi



1.7 Partner Tecnologico

Il servizio à offerto in collaborazione con il Security Operation Center (SOC) di IDS Informatica

Il SOC di IDS è una struttura integrata realizzata per gestire in outsourcing le informazioni di sicurezza in maniera continuativa durante l'intera giornata. Questo servizio si avvale per il suo espletamento di personale con esperienza, processi collaudati e sofisticate tecnologie per fornire un servizio completo e scalabile

Le opzioni dei Servizi di Sicurezza gestiti da IDS includono:

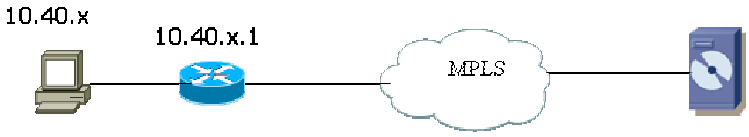
- **Gestione dei Firewall** – Installazione, configurazione e gestione centralizzata dei Firewall per la protezione della rete dei clienti.
- **Web Filtering –** Protezione dall'accesso a siti web pericolosi o indesiderati. Protezione da Spyware
- **Gestione di VPN** – Installazione, configurazione e gestione del sistema VPN per consentire l'accesso remoto alla rete della Diocesi o per collegare le parrocchie alla sede Diocesi
- **Servizi di Analisi delle vulnerabilità** – Analisi da remoto per identificare potenziali venerabilità di rete e mantiene sicure le vostre risorse on line
- **Sicurezza WIFI** – Realizzazione di una soluzione di accesso WIFI sicura

2 Appendice Tecnica

2.1 Requisiti per l'utilizzo del servizio (Senza server remoto)

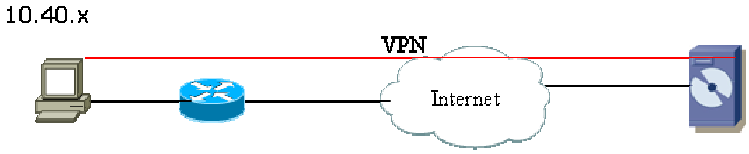
2.1.1 MPLS-IDS

I nodi che vogliono usufruire del servizio antivirus devono essere direttamente raggiungibili dall'MPLS-IDS tramite indirizzo 10.40.x.x o Nat 1 a 1. È inoltre necessario che la porta TCP 19226 e l'icmp non siano bloccati dal firewall. In alternativa è possibile installare un Server AV locale.



2.1.2 VPN Software

È necessario che il nodo interessato al servizio Antivirus abbia la porta TCP 19226 e l'icmp non bloccati dal firewall.



2.1.3 VPN LAN to LAN

I nodi che vogliono usufruire del servizio antivirus devono essere direttamente raggiungibili dall'Intranet tramite indirizzo 10.8.x.x o Nat 1 a 1 sul VPN gateway. È inoltre necessario che la porta TCP 19226 e l'icmp non siano bloccati dal firewall. In alternativa è possibile installare un Server AV locale.

2.1.4 702

È necessario che il nodo interessato al servizio Antivirus abbia la porta TCP 19226 e l'icmp non bloccati dal firewall.

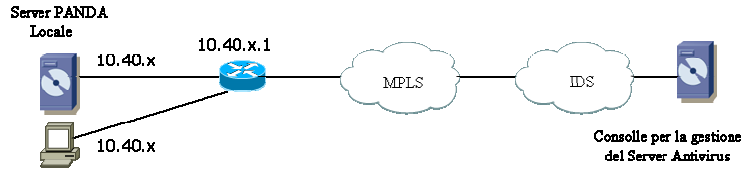
2.1.5 Collegamento Internet generico

È necessaria una connessione VPN o Per reti ampie è possibile pensare una soluzione basata su Server AV locale

2.2 Requisiti per l'utilizzo del servizio (Con server remoto)

2.2.1 MPLS-IDS

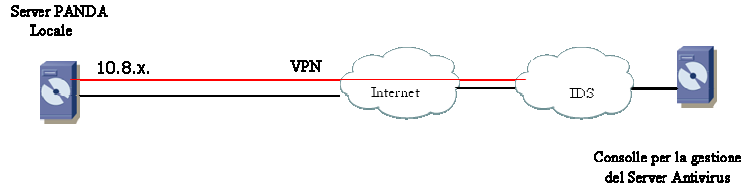
È necessario che il Server AV sia visibile sull'MPLS-IDS o utilizzi Nat statico 1 ad 1. è richiesto inoltre che il firewall non blocchi le comunicazioni tra il Server AV locale e il Server AV di IDS



2.2.2 VPN Software

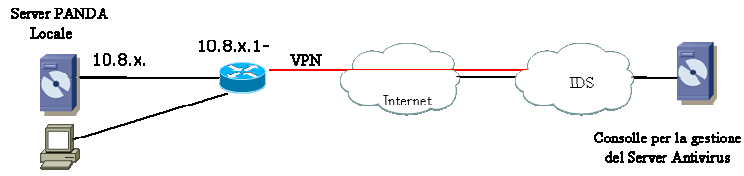
.

È necessario che il server AV locale sia anche la macchina dotata di VPN software. In tal caso il firewall non deve bloccare le comunicazioni tra il Server AV locale e il Server AV di IDS



2.2.3 VPN LAN to LAN

È necessario che il Server AV sia visibile sulla VPN. è richiesto inoltre che il firewall non blocchi le comunicazioni tra il Server AV locale e il Server AV di IDS.



2.2.4 702

Non applicabile

2.2.5 Collegamento Internet generico

È necessario che il Server AV sia visibile dal server IDS o utilizzi Nat statico 1 ad 1; consigliato l'uso di una VPN software. Il firewall non deve bloccare il traffico tra il server AV locale e il server AV IDS e viceversa.