

Metti a norma la tua rete

SISTEMA SICUREZZA INFORMATICA FIREWALL NORMA PRIVACY



Le esigenze

Con la diffusione crescente delle reti e della necessita di condividere informazioni verso l'esterno, oggi la scuola ha esigenze di sicurezza sempre più pressanti. E' necessario quindi definire e proteggere la propria rete da intrusioni di applicazioni potenzialmente dannose.

Atswall è un dispositivo hardware, dotato di sistema operativo linux, garanzia di sicurezza e inattaccabilità, su cui è stato sviluppato tutto il software necessario per la messa a norma degli accessi anche wifi pubblici, nel rispetto della recente normativa (art6 e 7 del D.L. 144/2005 G.U. 27.07.2005)

Ats wall si amministra utilizzando il browser di un qualsiasi pc della rete.

Il sistema gestisce autonomamente l'anagrafica degli utenti, ai quali vengono associati codici di utilizzo a tempo o a scadenza, eventualmente ricaricabili.

Accedere alla rete wifi è un operazione molto semplice per l'utente: scegliere la rete e immettere il proprio codice nella pagina che compare sul browser;

il sistema tiene traccia della navigazione degli utenti se ne può fare un cd

L'obiettivo

La scuola deve poter disporre di livelli di sicurezza adeguati nella propria rete e soprattutto definire regole che diventino parte integrante dalla propria infrastruttura. Il firewall è sicuramente un elemento essenziale per raggiungere un elevato livello di sicurezza su una rete locale.

Spesso, cliccando su un semplice link che dovrebbe teoricamente mostrare un innocuo calendario, i ragazzi si immergono a scuola in una mare di pornografia internet o filmati non adatti alla loro età. I contenuti che normalmente sono ritenuti offensivi vengono classificati generalmente in:

- legali, ma pericolosi per i minori (scene di nudità e pornografia softcore)
- legali, ma indecenti (pornografia hardcore)
- illegali e osceni (generalmente violenza sessuale).

Per evitare la visualizzazione di questi contenuti di pessimo gusto è necessario proteggere la scuola e proteggere la rete , adottando delle precauzioni.

Funzioni base

- Funzioni specifiche per proteggere la rete da attacchi di varia natura (spoofing, flooding, smurf ...) in particolare filtri anti IP-Spoofing e anti DoS.
- Preconfigurazione per una protezione ottimale.
- Filtraggio attivo degli URL, controllando i siti visitabili dagli utenti, in base ad alcune black-list automatiche, a black-list personalizzabili, a criteri di orario, a criteri specifici per ogni utente.

infoline

091 6516150

