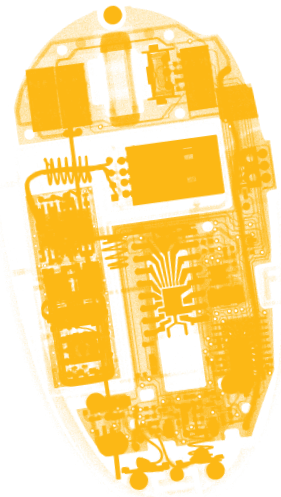
TECNOLOGIA TRASPARENTE

SISTEMI DI CONTROLLO E MONITORAGGIO DEL TRAFFICO INTERNET E DATI

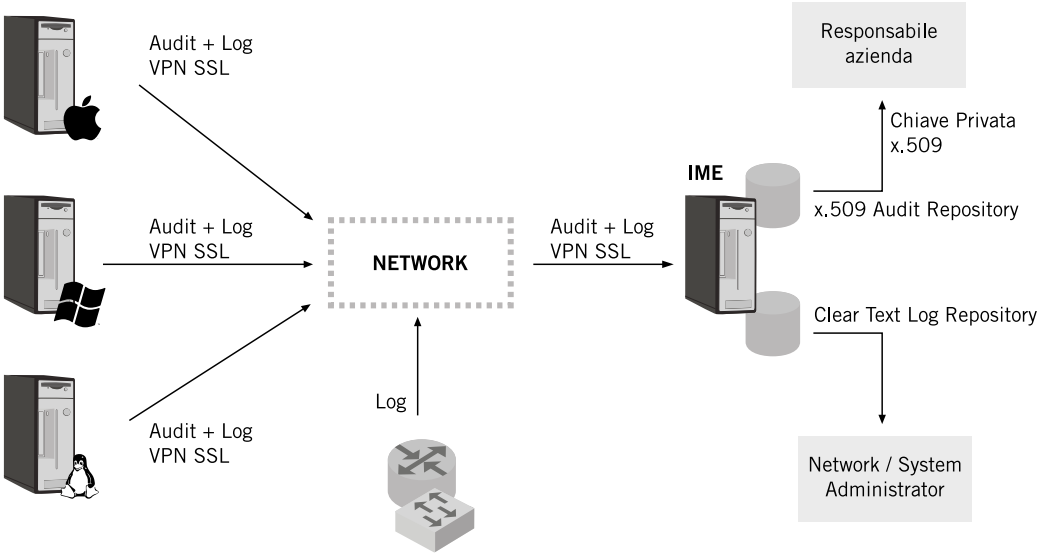


La diffusione dell'uso della rete internet come fondamentale strumento di lavoro, ha aperto problemi gestionali con declinazioni organizzative e legali. Che si tratti di ISP – internet service provider – aziende dedicate alla fornitura di servizi di rete, o imprese che della rete fanno un uso funzionale ai propri obiettivi di business, le recenti normative sulla sicurezza impongono di dotarsi di strumenti di gestione e controllo del traffico. Dalla ricerca applicata di CSP nascono CIA – Central Intranet Auditor – e SpyNetLog, soluzioni per il monitoraggio e controllo del traffico internet e dati, sviluppate nel rispetto delle vigente normativa in materia al servizio di ISP e imprese che gestiscono dati sensibili.

CIA - CENTRAL INTRANET AUDITOR

È una soluzione software pensata per ottemperare al Provvedimento del Garante Privacy sui log degli amministratori di sistema. Il provvedimento del 27 novembre 2008 a tema "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema" –, introduce, infatti, l'obbligo per le aziende di conservare gli access log (audit) per almeno sei mesi in archivi immodificabili e inalterabili. Basato sul protocollo Syslog ed essendo compatibile con qualunque sistema operativo, CIA permette di archiviare tutti gli access log e gestirli in appositi archivi cifrati con certificati digitali, garantendo e tutelando i requisiti di inalterabilità richiesti dalla normativa.

L'architettura di funzionamento



LE FUNZIONALITÀ PRINCIPALI

CIA è strutturato in due componenti software, una lato client, cioè per tutti i server all'interno di una rete aziendale che gestiscono dati sensibili, l'altra lato server.
Il sistema si basa sul protocollo Syslog che non è nativo nei server Microsoft; un problema che ha imposto, per tali architetture, l'integrazione di un apposito client, denominato Syslog Agent. CIA è quindi compatibile con qualunque tipo di server – linux, windows, mac – e interviene nella fase di invio al sistema centrale di tutti gli access log attraverso una connessione cifrata.
I messaggi vanno poi a costruire due archivi:

- uno visibile in sola lettura a fini di debug e controllo, attraverso una semplice interfaccia web a tutti gli amministratori di rete autorizzati;
- uno cifrato attraverso un certificato digitale, che permette la visualizzazione dei dati al responsabile della privacy aziendale, garantendo così i requisiti di inalterabilità dei log.

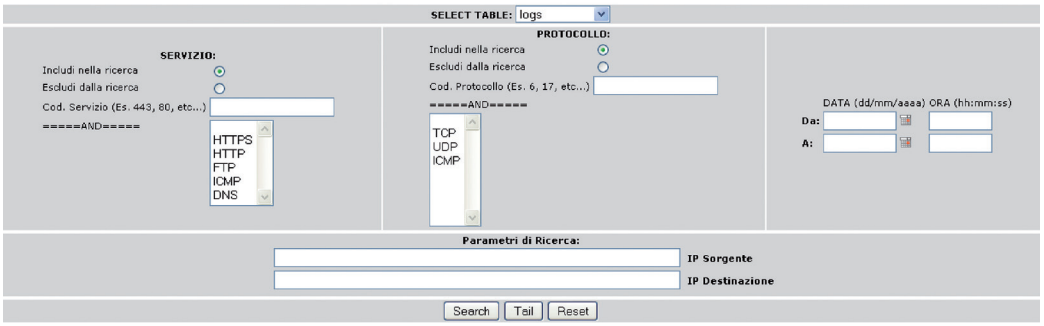
SPYNETLOG

È una soluzione software che permette di monitorare la tipologia di traffico che viene generata da una rete aziendale verso Internet, archiviando i dati riferiti a ogni singola connessione.
SpyNetLog permette dunque di effettuare ricerche da un IP sorgente a un IP destinatario, attraverso un'interfaccia utente pensata per facilitare il lavoro degli amministratori di rete.
L'applicativo è progettato in particolare per ISP e WISP, soggetti agli obblighi di legge nello sviluppo della propria attività, e per le aziende che non utilizzano server proxy, ma sono interessate a monitorare le connessioni per fini statistici, controlli di debug, ecc.

LE FUNZIONALITÀ PRINCIPALI

Il sistema si basa sul protocollo Netflow che trasporta i dati relativi alle connessioni IP transitate attraverso il border router dell'infrastruttura di rete.
L'integrazione di SpyNetLog non impone, quindi, modifiche all'architettura.
I messaggi NetFlow sono quindi analizzati dal software che, previo opportuno parsing, li inoltra ad un syslog server locale rendendoli fruibili attraverso una semplice interfaccia web.
L'amministratore di rete può effettuare query di ricerca a fini di statistica o debug, visualizzando i dati relativi a ogni singola connessione come segue: Protocollo: ip_sorgente:porta -> ip_destinazione:porta.

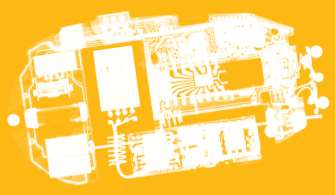
L'interfaccia per ricerca SpyNetLog



COMPATIBILITÀ CON ALTRI ASSET

I software possono essere integrati tra loro, con I.M.E. - Integrated Monitoring Environment – con un qualsiasi altro sistema per il monitoraggio, o utilizzati come sistemi stand alone.

CSP_CIA_PROD_ITA_07.12



CSP - Innovazione nelle ICT
Via Nizza 150, 10126 Torino (Ingresso da Via Alassio, 11/c)
Tel. +39 011 48.15.111 Fax +39 011 48.15.001
www.csp.it - innovazione@csp.it