Bruno Borgia – Università di Roma “La Sapienza”

## Il NAC della Sapienza

La rete SAPIENZANET dell’Università di Roma La Sapienza ha tra le sue caratteristiche quella di essere non dipendente da un unico vendor. La struttura centrale, il *core* della rete, è costituito da apparati CISCO, mentre i punti di presenza nei centri stella di zona e di edificio cono costituiti da apparati HP.
La rete di distribuzione ed i nodi cliente e server della rete sono sotto la gestione diretta dei diversi dipartimenti universitari e dei responsabili dei vari server. Di conseguenza gli apparati di distribuzione locale sono i più diversificati e frequentemente non gestibili.

Questa natura della rete SAPIENZANET, se da una parte costituisce una debolezza dal punto di vista gestionale, in quanto occorre far fronte a molteplici caratteristiche tecniche, dall’altra è una ricchezza per gli stessi utilizzatori che possono sviluppare tecniche e tecnologie indipendenti dai vendor più diffusi, vedi Microsoft o Linux.
La scelta e l’adozione di un sistema NAC in queste condizioni ha posto una notevole difficoltà di selezione del sistema che fosse in grado di intercettare gli ingressi in rete indipendentemente dal tipo o dal costruttore degli switch intermediari e di controllare la rispondenza alle politiche di accesso dei nodi di rete senza l’adozione di agenti installati nei nodi stessi.

Insightix nasce per dare una risposta a quanti hanno bisogno di controllare i dispositivi e gli utenti che accedono ed utilizzano la rete, in modo flessibile, semplice e poco invasivo.
Dopo uno studio durato circa due anni ed una gara, è stato scelto il NAC Insightix.
Insightix basa la sua efficacia su: discovery e controllo stateful real time di tutti elementi in rete, collezione delle informazioni di contesto dei disposiviti e degli utenti, sistema brevettato di isolamento dei dispositivi non conformi alle regole. Attraverso l'integrazione di tali elementi è possibile controllare che l'accesso in rete sia effettuato solo da dispositivi ed utenti conformi alle politiche definite senza utilizzare agenti o generare traffico in rete in modo invasivo ed indipendentemente dall'infrastruttura di rete

esistente. Infatti, il sistema consente di verificare l'identità del dispositivo e dell'utente, le caratteristiche hw/sw del dispositivo; nel caso alcune combinazioni non fossero conformi alle politiche definite, E' possibile isolare il dispositivo in questione, garantendo l'eventuale remediation senza utilizzare architetture VLAN Based. Attraverso quest'architettura si riesce a risolvere problemi molto diffusi, come il controllo dell'assegnazione dell'indirizzo IP ai dispositivi, o come il controllo dell'aggiornamento degli antivirus o dei SO fino ad arrivare all'inventario dei sistemi hardware e software. Inoltre è possibile localizzare topologicamente tutti i dispositivi presenti in rete e quindi anche quelli che vengono identificati come non conformi fino a determinare la porta dello switch ai quali sono connessi.