Captive-Portal e Laboratori Didattici: l'esperienza di UNICH

Autori: D. Verzulli - Università "G. D'Annunzio"

Abstract
Il bilanciamento delle esigenze degli studenti da un lato e quelle degli amministratori di Rete dall'altro ha sempre costituito un problema.
Gli studenti vogliono connettivita' (full-nat) e banda (la maggiore possibile). L'amministratore deve garantire banda per tutti (limitarla/prioritizzarla) e, soprattutto, deve poter associare i flussi di traffico all'utenza che li ha generati (PolPost). Gli ambienti wireless amplificano tali problemi.
Negli anni, il nostro approccio ha registrato l'implementazione di diverse soluzioni, tutte rigorosamente open-source e svincolate dall'impiego di access-point high-end a causa della necessità di minimizzare i costi.

NOCAT
La prima esperienza risale al 2006 ed è incentrata su NOCAT, progetto già allora in via di abbandono. Il suo nucleo è costituito da un demone PERL opportunamente interfacciato ad iptables che, sfruttando il MARKing di NETfilter gestisce la "cattura" del client anonimo ed il "forwarding" del client autenticato. Un CGI in azione su un server web esterno gestisce il login ed istruisce opportunamente iptables affinché marchi correttamente l'host il cui utente si è appena autenticato.
Vantaggi: la soluzione è leggerissima e sfrutta brillantemente netfilter (MARK)
Svantaggi: Progetto non più supportato; necessitàdi ricorrere al transparent-proxying per il LOGGING delle URL; difficolta' di impiego in ambienti multi-VLAN; difficoltà nel "tuning" delle politiche di filtraggio

CHILLISPOT
All'inizio del 2008, per un nuovo laboratorio didattico, si è scelto di "proteggere" la rete (dal laboratorio) attraverso un gateway con ChilliSpot. Rispetto a NOCAT è risultato banale interfacciarsi ad authentication-server esterni (Radius via FreeRadius) ma non si sono risolti alcuni problemi preesistenti (Squid/Transparent proxying) e ne sono insorti di nuovi (difficoltà maggiori nella personalizzazione di iptables e difficoltà con il DHCP). Inoltre resta complesso utilizzare chillispot in modalita multi-VLAN

BCROUTER -www.bcrouter.net-
Sviluppato ed in produzione in una rete particolarmente ampia (20K user, 700Mbps), BCROUTER approccia il problema in modo diverso:

- un modulo ad-hoc di NetFilter attraverso il quale far transitare il traffico da gestire;

- gestione attraverso un telnet-server che dialoga con il modulo via un character-device.
- una logica che permette, da subito, l'associazione del traffico all'utente (e non solo all'host) che lo genera.

Oltre al supporto ottimale di VLAN, BCROUTER aggiunge la "quota" di traffico IP (per user e per host) ed un sofisticato sistema di logging (kernel-based). Attualmente si stanno integrando il supporto NetFlowV9 (probe) e l'accounting radius-compliant. Il NOC della "d'Annunzio" è in contatto con gli sviluppatori e, di fatto, sta testando (con ottimi risultati) l'intero ambiente. La collaborazione con altri atenei è più che bene accetta.