La virtualizzazione delle risorse di rete e dei sistemi di sicurezza: l'implementazione di router e firewall virtuali sul bordo di una rete dati di accesso al GARR

Autori: A.Campa, A. Tommasi, G. Marullo, M. Ferri - Università del Salento

Abstract
Con la prospettiva di dover continuamente potenziare i propri collegamenti ad Internet, le organizzazioni della ricerca e della didattica si trovano costrette ad effettuare continui investimenti per dotarsi di sistemi di controllo passivo, attivo o proattivo sul traffico da esse veicolato. Concentrando l'attenzione su di un apparato di sicurezza quale un firewall di bordo, avente funzioni minime di ispezione ed analisi del traffico, questo deve essere dimensionato in maniera tale da garantire un throughput comparabile con la velocità di trasferimento dati che l'organizzazione possiede per l'accesso alla rete GARR e/o al suo ISP.

L'esperienza dell'Università del Salento è stata quella di dotarsi di un apparato in grado di concentrare al proprio interno le funzionalità di sicurezza e di routing. Nello specifico un router CISCO Systems Modello 7609 [1] con un modulo Route Switch Processor (RSP) [2] e con un modulo Firewall Service (FWSM) [3] hanno permesso di realizzare un'architettura integrata di firewalling e routing a difesa e controllo/logging del traffico scambiato dall'Università con il GARR.
Tale architettura ha permesso di evitare di approvvigionarsi di apparati fisicamente separati e di mantenere un unico apparato contenente al proprio interno un numero variabile di router virtuali ed un numero finito di istanze di firewall.
Attraverso il meccanismo di Virtual Routing and Forwarding (VRF) è possibile dividere un router o uno switch Layer 3 in diversi dispositivi virtuali indipendenti. Ogni router virtuale supporta una singola routing table virtuale completamente indipendente dalle altre. Il Firewall Service Module è un modulo (blade) che può essere inserito all'interno dello chassis 7609 e che riesce a garantire un throughput di altissimo livello (5Gbps).
Una delle più interessanti feature offerta dal FWSM è la "Virtualizzazione", anche conosciuta come "multiple context mode". Questa modalità operativa permette al FWSM di virtualizzare internamente le sue risorse e quindi di scindere il suo funzionamento in vari ambienti firewall virtualizzati (contesti).
Questa caratteristica, molto apprezzata in ambito Enterprise, permette di adottare la soluzione FWSM in scenari molto variegati i quali adottano soluzioni di connettività come MPLS-VPN, VRF- lite e GRE.
La flessibilità e la modularità della soluzione acquisita ha permesso di realizzare una cascata di una VRF di bordo che si interfaccia al collegamento al GARR, seguita da un contesto virtuale di firewalling (a cui è stata collegata la DMZ dei servizi di base), per finire ad una VRF interna che a sua volta si interfaccia agli apparati di dorsale.

La modularità del sistema in questione permette anche di procedere ad includere nell'apparato 7609 soluzioni di VPN, IPS ed IDS senza la necessità di dover fisicamente
installare nuovi apparati e nuovi cablaggi fisici ma con la sola necessità di installare dei moduli aggiuntivi all'interno del sistema.
L'impiego di protocolli standard in uscita al sistema acquisito, inoltre, permetterà a breve di implementare l'interfacciamento della VRF interna con la MAN/MPLS dell'Università del Salento realizzata con apparati di rete Juniper Networks.

Riferimenti bibliografici:
[1]http://www.cisco.com/en/US/prod/collateral/routers/ps368/ps367/product_data_sheet0900aecd8057f3d2.html
[2]http://www.cisco.com/en/US/prod/collateral/routers/ps368/product_data_sheet0900aecd8057f3b6.html
[3]http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/