

Da Internet all'Infranet: l'Evoluzione della Sicurezza

Creare una rete che combini la connettività onnipresente di Internet con le prestazioni e la sicurezza garantite dalle reti private. Questa è la "corporate vision" di Juniper Networks, di cui ci parla Giulio Barki, Corporate and Government Division.

Qual è la "mission" di Juniper Networks e come si pone sul mercato dell'Information Communication Technology?

Fin dalla sua costituzione, Juniper Networks ha sempre rivolto la propria attenzione verso le innovazioni nel settore del networking trasformandole in infrastrutture e servizi Ip (*Internet Protocol*) e MPLS (*Multiprotocol Label Switching*) redditizi per le grandi reti di tutto mondo. La famiglia dei prodotti JN utilizza processori di pacchetto avanzati, che consentono ai clienti di offrire servizi che spaziano dall'accesso Internet, fino al *delivery* garantito di traffico voce, video e multimediale, alle massime velocità consentite dai cablaggi. Ultimamente l'attenzione è stata focalizzata sul miglioramento del traffico all'interno della rete, cercando di ottimizzare tutte le problematiche di latenza applicativa.

Che cos'è l'Infranet?

L'Infranet è un contesto al quale JN si appoggia per fornire un controllo unificato e dinamico sugli accessi alle reti delle aziende. È un contesto che prevede una combinazione tra *policy* basate sull'identità e intelligenza degli "endpoint" per fornire alle aziende la visibilità in tempo reale e il pieno controllo delle *policy* sull'intera rete. Di conseguenza, le aziende possono controllare gli accessi, prevenire le minacce, assicurare la conformità normativa ed erogare servizi di rete protetti e garantiti.

A quale clientela è rivolta?

A tutte quelle aziende che hanno il proprio quartiere generale in un determinato sito, con periferie in tutto il resto del mondo e necessitano quindi di utilizzare una rete capillare, che garantisca la possibilità di utilizzare tutto un insieme di servizi, con una gestione integrata anche a livello di sicurezza. Infatti, la soluzione Juniper per il controllo unificato degli accessi è la prima a proporre controlli sugli "end-point" e sulle identità, e la prima a supportare l'applicazione di *policy* IPSec e firewall dinamicamente configurate in ambito sia client-host sia di rete.

Cosa vi ha spinto a lanciare questa iniziativa?

Abbiamo preso atto che, per il dipartimento It, è finito il tempo del 'bricolage' tra apparecchiature eterogenee, e inseguiamo la voglia di semplificazione e standardizzazione (*one-stop-shop*) nata nelle imprese, sulla spinta dei tagli ai costi di acquisto e di gestione. Da questa convinzione è nato il lancio del *framework architetturale* che va sotto il nome di "Infranet", proposto da poco anche sul mercato europeo.

Qual è il vantaggio tecnologico che Juniper offre alle imprese clienti?

Offriamo un vantaggio tecnologico sicuramente qualitativo, determinato dal fatto che siamo partiti per rispondere a delle necessità, espresse dai nostri clienti, di livello molto alto. Inizialmente, abbiamo offerto le nostre soluzioni quasi solo agli operatori che, a loro volta, dovevano offrire un servizio con un livello di continuità assai elevato. Il mondo “enterprise” ha, oggi, molto del suo business basato sul traffico della propria rete. Per cui, abbiamo trasportato il livello di affidabilità, che caratterizza la nostra esperienza di offerta al mercato, dai service provider al mondo “enterprise”, garantendo un livello di continuità unico.

E quello economico?

jn ha un approccio al mercato di tipo progettuale. Ciò comporta degli investimenti infrastrutturali che hanno un ritorno nel tempo più o meno lungo, a seconda delle soluzioni proposte. Sicuramente, dal punto di vista del costo, il nostro approccio non è di tipo quantitativo ma qualitativo. A monte esiste un progetto che richiede una infrastruttura di una certa natura, noi cerchiamo di capire quali sono le applicazioni che servono al cliente. Quando il cliente manifesta un’esigenza, noi gli curiamo tutto il progetto.

Quanto è importante la sicurezza della rete nel settore bancario?

Ha un’importanza enorme. Il mondo bancario ha vissuto pesantemente una migrazione da linee dedicate, a infrastrutture pubbliche. All’interno delle reti pubbliche le aziende bancarie proteggono il dato in vari modi. Crittografandolo, mettendo dei firewall in tutte le periferie, mettendo un doppio router in periferia, uno gestito dal service provider e uno gestito dall’azienda stessa, e via scorrendo. D’altronde, è sempre più evidente il fenomeno per cui gli attacchi e le intrusioni non provengono solo dall’esterno. Per questo, anche a livello centrale, le banche si stanno dotando di infrastrutture che proteggono a livello di regole d’accesso, e di flussi di traffico di un certo tipo.

Quali differenze si riscontrano nelle esigenze manifestate da piccole e grandi banche?

In termini di natura delle esigenze, non ci sono grosse differenze. Esistono delle banche che hanno la volontà o l’esigenza di un’alta affidabilità del sistema e di non dismissione del servizio, il che implica l’acquisto di soluzioni più sofisticate. Tutto dipende dal livello di riservatezza del dato e dal livello di affidabilità che la banca vuole garantirsi. Alcune banche non possono mai fermarsi, per cui devono essere necessariamente in grado di gestire le eventuali cadute di linea, in modo tale che l’utente non si accorga di nulla.

In termini di sensibilità al problema sicurezza, qual è la situazione italiana?

L’evoluzione normativa, probabilmente, ha dato una grossa spinta al mercato della *security*. Le banche si stanno attrezzando per la costruzione del sito di *disaster recovery*. Gli operatori stanno migrando tutte le linee dedicate verso il mondo MPLS e questo richiederà una maggiore sicurezza del dato. In base alla nostra esperienza, non ritengo che l’Italia sia indietro rispetto all’Europa, in termini di sensibilità al problema, né tanto meno in termini di adeguatezza delle strutture.

Intervista a cura di Titti Acone