PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 438 di venerdì 09 novembre 2001

I termini da sapere - Un breve glossario sulla sicurezza in rete 1/2

Articolo a cura di Luca Garbato. Paura di perdersi tra le parole della sicurezza? Ecco un prontuario con quello che c'è da sapere sulla protezione delle reti.

Paura di perdersi tra le parole della sicurezza? Ecco un prontuario con quello che c'è da sapere sulla protezione delle reti

Firewall
Questa macchina collega la rete locale a reti non sicure, come, per esempio, Internet. Per mezzo di più schede di rete (una collegata alla rete 'remota', una alla propria LAN) filtra il traffico proveniente e quello diretto alla rete privata. In pratica, il Firewall confronta il traffico di rete in ingresso sulla propria scheda esterna con le regole definte dall'amministratore: in base all'esito lascia transitare o meno i pacchetti. Si possono creare regole molto articolate basate sugli indirizzi IP e sulle porte di origine e destinazione del traffico. Un'altra funzione svolta dal Firewall è il NAT (Network Address Translation), che permette di nascondere al mondo esterno lo schema di indirizzamento usato sulla LAN: il miglior modo di proteggere la propria rete è quello di non farne conoscere la struttura all'esterno. Ogni pacchetto generato sulla rete locale e diretto alla WAN viene manipolato dal Firewall, che sostituisce l'indirizzo sorgente nel pacchetto originale con l'indirizzo della propria scheda di rete esterna.

Proxy Server
Il Proxy è un server della rete che ha il compito di memorizzare (caching) i siti Web maggiormente frequentati dagli utenti della LAN. In questo modo, quando viene richiesta la visualizzazione di un sito già visitato, non è necessario aprire una connessione verso Internet, dal momento che la pagina richiesta (e tutti I suoi elementi) viene 'servita' dal server Proxy. Questo porta a un immediato vantaggio dal punto di vista della velocità di navigazione e, a volte ben più importante, a un notevole risparmio in termini di ampiezza di banda a disposizione per ulteriori collegamenti verso l'esterno. Molto spesso I Proxy Server vengono impiegati anche per realizzare un maggior grado di sicurezza per la propria rete, anche se non possono sostituire il Firewall. La differenza fondamentale tra i due server (il Proxy e il Firewall) sta nel funzionamento. Il Firewall controlla il traffico in uscita e, se una delle regole definite ne consente il transito, viene aperto un canale tra il client di rete e il server remoto. Il Proxy, invece, raccoglie le richieste dei client di rete e recupera personalmente le informazioni richieste. In un secondo tempo il Proxy trasferisce le informazioni al client che ne ha fatto richiesta. In realtà, recentemente I due tipi di prodotto stanno convergendo in una piattaforma unica, dal momento che sempre più Proxy offrono funzioni tipiche dei Firewall e viceversa.

Rete DMZ e SSN
Questa è la rete in cui vengono collocati i server di ogni azienda che vuole offrire servizi su Internet (per i propri dipendenti o per il pubblico). Si tratta di una 'zona di mezzo': non è una rete aziendale privata, ma non è neppure una rete pubblica. Questa zona viene individuata con due nomi diversi a seconda della tecnologia impiegata dal firewall per farla comunicare con la propria LAN o con Internet. Nel caso vengano impiegati indirizzi IP pubblici per gli host collocati in questa zona la rete prende il nome di DMZ (Demilitarized Zone); nel caso si usino indirizzi IP privati, la zona prende il nome di SSN (Secure Sorvices Network). Naturalmente, l'impiego di una SSN permette di acquistare da un service provider un insieme di indirizzi IP pubblici limitato, mentre nel caso delle DMZ bisogna assicurare un indirizzo IP pubblico per ogni macchina che si intende collocare in questa zona. Inoltre, per poter adottare la soluzione SSN è necessario assicurarsi che la propria soluzione firewall supporti le operazioni di riscrittura degli indirizzi e delle porte di applicazione.

VPN
La VPN (Virtual Private Network) è un canale di comunicazione stabilito tra due host appartenenti a reti diverse in cui tutto il traffico viene criptato. L'operazione di cifratura è necessaria per garantire la sicurezza delle transazioni, dal momento che il

mezzo di collegamento tra i due host è Internet. Queste soluzioni, sempre più diffuse ormai, vengono generalmente impiegate per mettere in comunicazione due macchine (o due reti) senza la necessità di stabilire un collegamento fisico (una linea dedicata, per esempio) tra di loro. Un esempio frequente di impiego della VPN consiste nella possibilità di collegare in modo sicuro il proprio PC alla LAN aziendale, da casa propria o in viaggio, usando Internet come trasporto.

La seconda parte del glossario sara' pubblicata prossimamente sul nostro quotidiano.

Articolo a cura di Luca Garbato - Siosistemi.
Articolo pubblicato su Networking Italia.

---

www.puntosicuro.it