Linux FreeS/WAN e Win2k

In un precedente numero di questa rubrica (*IPSEC−VPN con Linux FreeS/WAN*, Ottobre 2002) avevamo già parlato di FreeSWAN, la soluzione IPSEC più diffusa per Linux. In tale articolo ci eravamo limitati a considerare esplicitamente il caso di un tunnel tra due macchine Linux e citato la compatibilità con le implementazioni di vari vendor. Avevamo anche notato che vi erano molti aspetti del progetto in pieno sviluppo. A distanza di pochi mesi già alcuni nuovi risultati sono stati presentati.

NAT−Traversal Anche se il protocollo per incapsulare i tunnel IPSEC in pacchetti UDP è ancora allo stato di DRAFT [1], un patch (ancora in fase di test per dir la verità, ma già alla versione 0.5a) per FreeS/WAN è stato realizzato da Arkoon Network Security [2]. La tipica situazione in cui questo patch è utile quella in cui un client IPSEC che si trova dietro un router che fa NAT, e quindi trasforma il numero IP privato della macchina in un numero IP pubblico, si deve collegare ad un server IPSEC con un numero IP pubblico. Poiché il traffico IPSEC diretto su protocollo IP non riesce a passare il router che fa NAT, la soluzione è di incapsulare il tunnel in pacchetti UDP. Il client stabilisce una connessione UDP su di una fissata porta verso il server, ed il tunnel viene così stabilito. Una volta applicato il patch, la configurazione è molto semplice, basta aggiungere `nat_traversal=yes` al file di configurazione `/etc/ipsec.conf` e FreeS/WAN utilizzerà l'incapsulamento in UDP per stabilire il tunnel IPSEC.

Una domanda che spesso compare nelle varie mailing−list, è se sia possibile effettuare tunnel IPSEC tra macchine connesse ad internet in dialup e senza un numero IP fisso. Il problema è ovviamente rilevante non solo per IPSEC ma per qualunque servizio IP offerto da tali macchine. Poiché ogni volta che le macchine si connettono ad internet hanno indirizzi IP diversi (anche se ogni indirizzo fa parte sempre dello stesso pool), il problema principale è come far scoprire ad una macchina il numero IP dell'altra. A parte fare ogni volta una telefonata per scambiarsi i numeri IP e poi riconfigurare FreeS/WAN od il servizio in questione, è possibile utilizzare i servizi di *Dynamic DNS* [3]. Questi operatori permettono di registrare un nome a dominio, ad esempio *miamacchina.operatore.com*, ed una volta installato un particolare programmino cliente sulla propria macchina, ogni volta che ci si connette ad internet questo programmino si collega all'operatore e gli comunica il numero IP che ci è stato assegnato per la sessione ed immediatamente il record DNS di *miamacchina.operatore.com* viene aggiornato con il nuovo numero IP. A questo punto, con una banale aggiunta agli script di startup di FreeS/WAN possiamo

procedere come segue. Tutte le volte che ci si connette ad internet, appena partita la connessione e subito dopo che abbiamo registrato il nostro numero con l'operatore, possiamo ottenere dal DNS il numero IP del peer e se necessario inserirlo nella configurazione di FreeS/WAN.

Nuova Distribuzione Combo Per rispondere alle richieste di tutti coloro che hanno bisogno di una versione già con i vari patch ed estensioni di FreeS/WAN, è stata creata da Ken Bantoft una distribuzione di FreeS/WAN denominata Super−FreeS/WAN [3]. Questa distribuzione è disponibile in formato sorgente ed anche RPM, ed include tra gli altri i seguenti patch:

- X.509 (Now includes RFC 2401 IKE Port Selectors)
- ALG (All ciphers/hashes enabled)
- Notify/Delete SA
- NAT Traversal
- MODP 768bit Phase 1 Support
- RFC 2409 port selectors

quindi la possibilità di utilizzare i certificati digitali, DES (che non è consigliato visto che non è sicuro ma che può essere necessario per compatibilità con altri vendor) ed altri algoritmi crittografici, di selezionare le porte ad esempio per IKE, ecc.

Win2k In Windows2000 e WindowsXP Microsoft ha introdotto il supporto per IPSEC e l2tp. L'esperienza sul campo di molti tecnici indica che i prodotti Microsoft interagiscono bene tra loro, ma non è semplicissimo farli interagire con gli altri. Nelle mailing−list vi sono molte discussioni su come è meglio, più facile ecc. far interagire questi prodotti con FreeS/WAN ed altre implementazioni di IPSEC. Bisogna sottolineare che l'implementazione di default di Microsoft di IPSEC utilizza il Transport Mode, non il Tunnel Mode che è la modalità usuale di IPSEC. Il Transport Mode permette di collegare con una VPN direttamente due macchine, ma non le reti dietro di esse. Nell'implementazione di default di Microsoft il tunnelling è fatto da l2tp.
Cercheremo qui di fare un riassunto di quelle che a giudizio dei più sono le soluzioni migliori.[1]

1. La soluzione che è più apprezzata è l'utilizzo di SSH_Sentinel di SSH.COM (http://www.ssh.com/). Ovviamente non è un prodotto Microsoft, ne è un prodotto gratuito o open source. SSH_Sentinel è un client IPSEC con anche alcune funzionalità di personal firewall, che supporta la maggior parte degli standard, incluso NAT−Traversal ad esempio, ed è completamente compatibile con FreeS/WAN. Ovviamente molte altre soluzioni di terze parti esistono e sono compatibili con FreeS/WAN, ma questa è quella che al momento riscuote il

1 Nessuna indagine statistica è stata svolta, queste sono le soluzioni che più spesso sono state descritte o proposte all'autore di questo articolo.

maggior successo.

2. Una seconda soluzione possibile è quella di utilizzare sul lato Linux lo stesso setup dato da Microsoft al suo prodotto, ovvero di usare IPSEC+l2tp (in ogni caso su Windows bisogna installare l'High Encryption Package con supporto per 3DES e tutti i service pack necessari; inoltre se si è installato un prodotto IPSEC non Microsoft, bisogna almeno disabilitarlo e riabilitare il servizio IPSEC originale). Quindi oltre a FreeS/WAN bisogna installare su Linux anche l2tpd [5], mentre per FreeS/WAN è consigliato utilizzare i certificati digitali ed il patch per selezionare le porte di connessione. Una configurazione per il lato Linux è recentemente apparsa sulla mailing−list sikurezza.org (http://www.sikurezza.org/).
3. Un'altra soluzione è di utilizzare il programma di Marcus Müller `ipsec.exe` [6] su Windows. Questo programma, integrandolo, permette di utilizzare direttamente il prodotto Windows in modalità solo IPSEC con un file di configurazione alla FreeS/WAN. La configurazione per Linux FreeS/WAN è l'usuale utilizzando ad esempio i certificati digitali ed una guida dettagliata per l'installazione e configurazione su entrambe le piattaforme è in [7].
4. L'ultima soluzione è quella di usare direttamente il prodotto Microsoft da una parte e FreeS/WAN dall'altra. Come abbiamo già detto, l'implementazione IPSEC di default di Microsoft utilizza il Transport Mode, ed il tunnelling è fatto da l2tp. Pertanto se si vuole fare solo una VPN tra due macchine, senza tunnel per le reti che vi sono eventualmente dietro, la soluzione è semplice e non necessita di l2tpd od altro su Linux. La configurazione di FreeS/WAN è praticamente la solita, con la differenza che ora bisogna specificare `Type=transport`. In ogni caso, qualunque configurazione di rete si scelga, sempre senza l2tpd su Linux, su Microsoft bisogna creare una nuova *Security Policy*. Questo è purtroppo un processo relativamente complicato ed è descritto in dettaglio per alcuni esempi in [8].

Andrea Pasquinucci
Consulente di Sicurezza Informatica
pasquinucci@ucci.it

Riferimenti Bibliografici:

[1]In questo momento i draft IETF per NAT−Traversal sono: draft−ietf−ipsec−nat−t−ike−04.txt, draft−ietf−ipsec−udp−encaps−04.txt, http://www.ietf.org/

[2]Arkoon Network Security, http://open−source.arkoon.net/

[3]Super−FreeS/WAN, http://www.freeswan.ca/

[4]Alcuni operatori che offrono il servizio di Dynamic DNS sono: Dynamic DNS Network Services, LLC, http://www.dyndns.org/; Dynamic DNS, Static DNS for Your Dynamic IP, http://www.no−ip.com/; MyServer.org Dynamic DNS Services, http://www.myserver.org/

[5]http://www.l2tpd.org/ (precendentemente su http://www.marko.net/)

[6]Questo programma è disponibile su http://vpn.ebootis.de/

[7]http://www.natecarlson.com/linux/ipsec−x509.php

[8]http://security.nta.no/freeswan−w2k.html, http://www.freeswan.ca/docs/WindowsInterop/ FS−W2K%20Interop.pdf