

Bologna, 29 novembre 2003

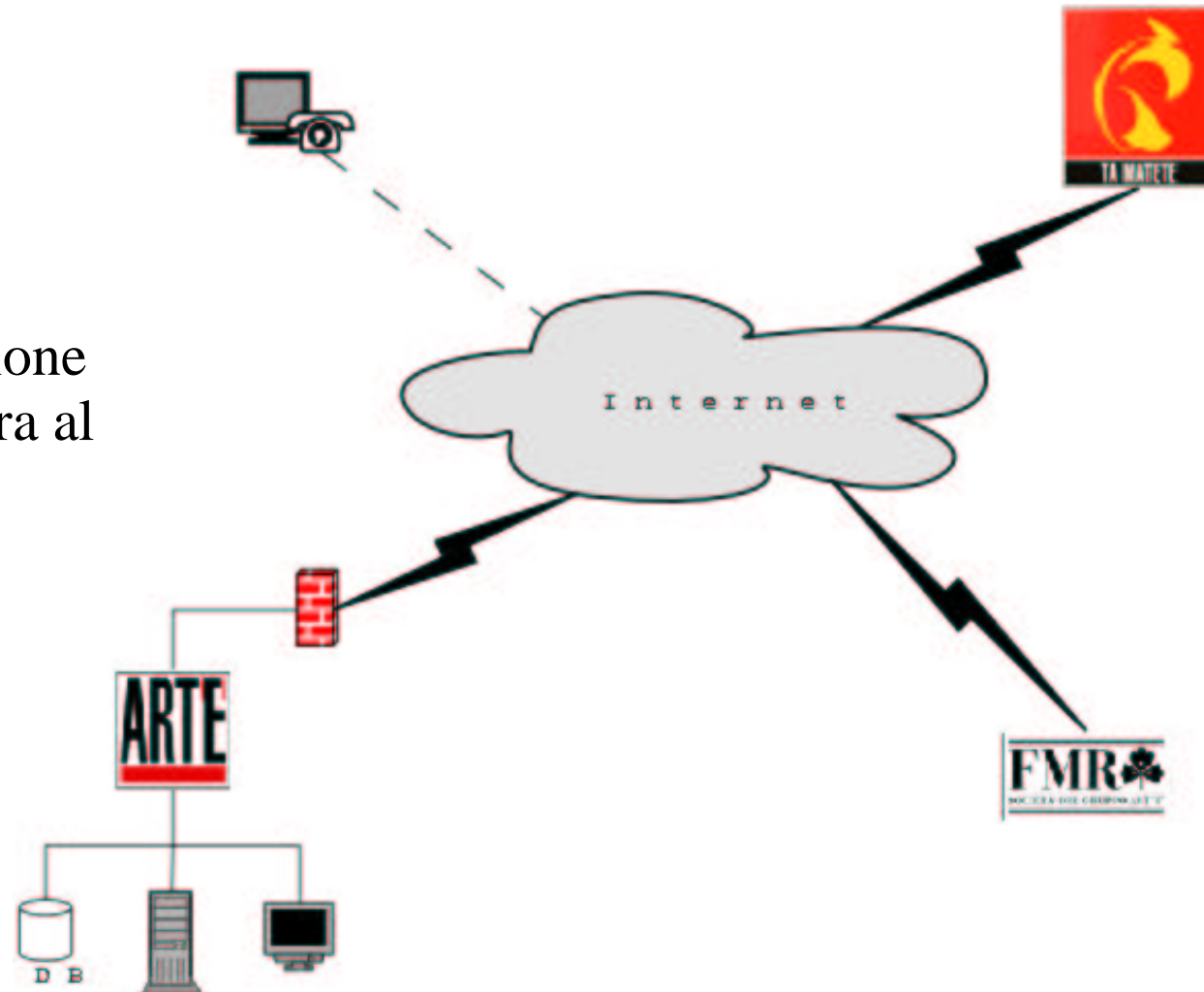
LinuxDay 2003

FreeS/WAN e Linux:
la risposta alla richiesta di flessibilità,
prestazioni e interoperabilità

Tommaso Di Donato
RHCE

Il Gruppo Art'è

- ✓Dinamicità
- ✓Estrema velocità di reazione
- ✓Forte necessità di apertura al mondo esterno



La security in outsourcing

Pro:

- Non necessita di skill interni
- Spesso l'hardware è in comodato

Contro:

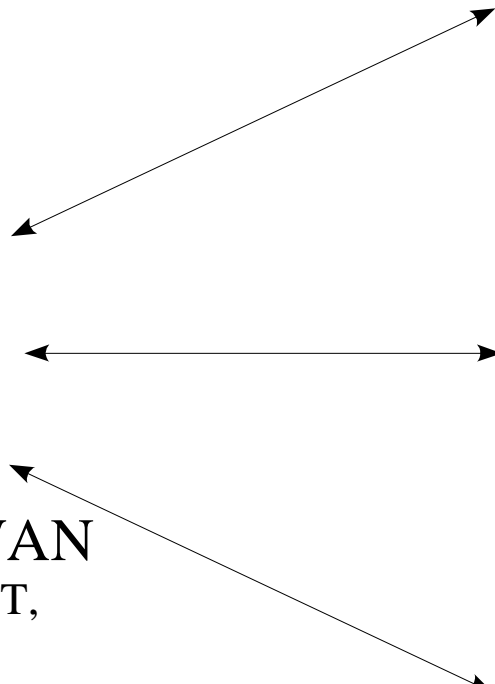
- E' più costoso
- Può essere poco flessibile
- I tempi di risposta possono essere troppo lunghi

In particolare, **per le VPN**, possono esistere problemi di interoperabilità, di tempi di intervento e di necessità di soluzioni “ad hoc”.

Attuali interconnessioni



Linux + FreeS/WAN
e varie patch: NAT-T,
X.509, Dead Peer
Detection, AES, ecc



I certificati X.509

METODI DI AUTENTICAZIONE

PSK

- Facilissima gestione per pochi tunnel
- Le usano tutti i dispositivi IPsec

Chiavi RSA

- Facile gestione
- Più sicure
- Largamente utilizzate

Certificati X.509

- Permettono di gestire tante chiavi per ogni tunnel
- Molto sicuri

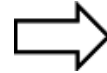
...ma le PSK non possono essere utilizzate per i Road Warrior, e le RSA, per tanti tunnel, diventano di difficilissima gestione...



I certificati X.509 diventano il modo più comodo per autenticare certi endpoint. Inoltre, tramite le *CRL*, ne ho una gestione molto “puntuale”

Il NAT-Traversal

Ogni *Address Translation* (NAT, PAT) altera gli header del pacchetto, quindi ogni connessione Isec viene rifiutata.



Bisogna incapsulare il pacchetto (UDP encapsulation)

I secure gateway si scambiano i payload NAT-D



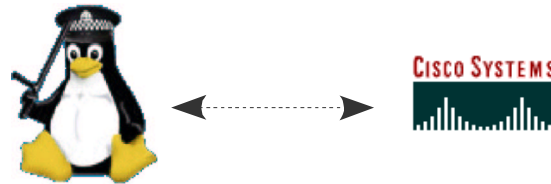
no

Uno dei due gw è NAT'ed. Incapsulamento

sì

Nessuna forma di NAT tra i gateway

FreeS/WAN – IOS Firewall



Recupero dell'investimento:
Router Cisco 2620+IOS Firewall+3DES

Pro

- Parziale recupero dell'investimento
- firewall/VPN in appliance

Contro

- Difficoltà di configurazione
- Limitato numero di tunnel (non il nostro caso)
- Certificati X.509 non supportati

FreeS/WAN – CheckPoint FW-1



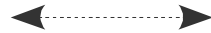
Checkpoint è molto usato negli ambienti “enterprise”, quindi è molto importante che FreeS/WAN possa interagire con esso!

FW-1 NG supporta PSK, chiavi RSA e certificati X.509

Uniche accortezze:

- disabilitare il *pfs* (perfect forward secrecy)
- utilizzare tempi di re-keying inferiori a 480 minuti
- se non viene utilizzata l'apposita patch, FreeS/WAN non supporta la modalità aggressiva

FreeS/WAN – SSH Sentinel

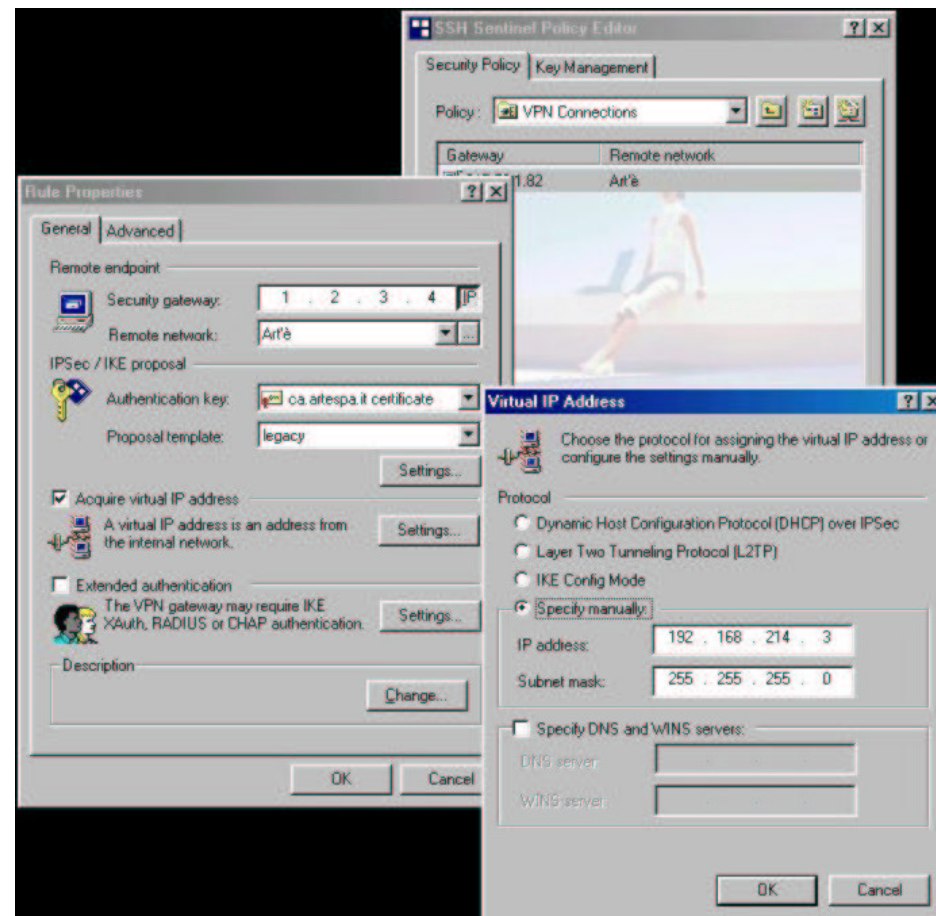


SSH Sentinel

Tramite un modem GPRS pcmcia, gli utenti si connettono ad internet dal portatile (connessione NAT-tata)

SSH Sentinel è un client per Win32 che supporta il NAT-T e i certificati X.509

Assegnando ad ogni portatile un certificato ed un IP virtuale, i road warrior accedono alle risorse della LAN in modo sicuro!



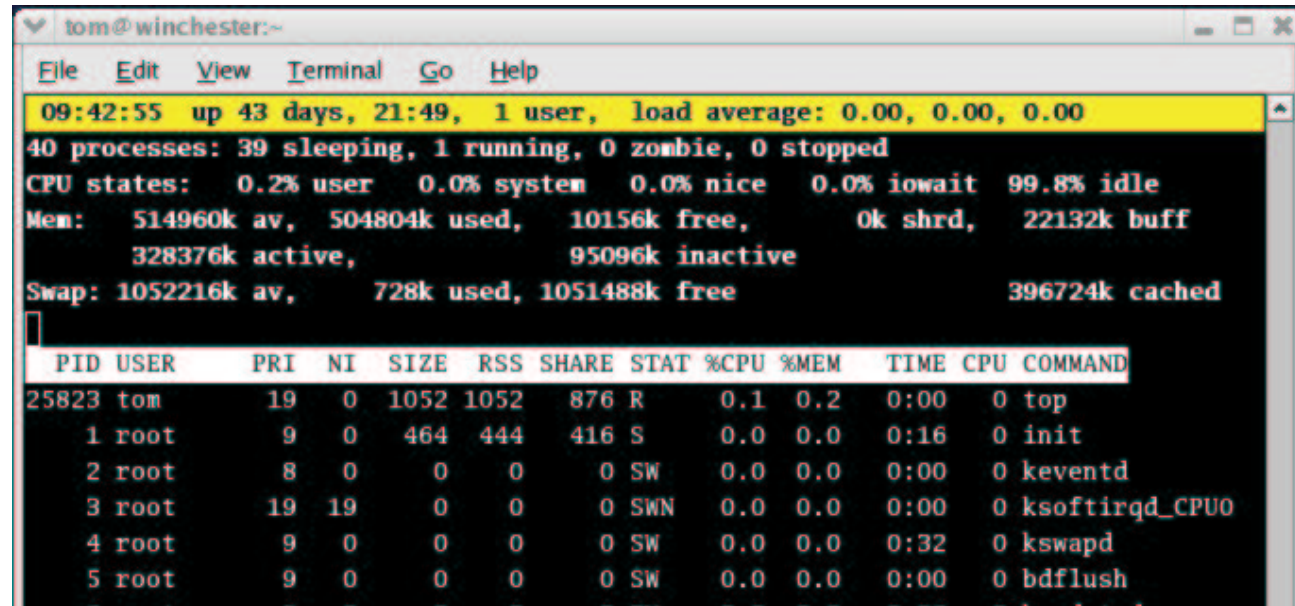
...ma con questo cosa voglio dire?

Linux e FreeS/WAN:

Una soluzione affidabile,
estremamente performante,
economica, molto scalabile.

E' trasparente a tutta la rete

E' la soluzione ideale per
security gateway che vanno
dall'entry level al mid-range.



```
tom@winchester:~  
File Edit View Terminal Go Help  
09:42:55 up 43 days, 21:49, 1 user, load average: 0.00, 0.00, 0.00  
40 processes: 39 sleeping, 1 running, 0 zombie, 0 stopped  
CPU states: 0.2% user 0.0% system 0.0% nice 0.0% iowait 99.8% idle  
Mem: 514960k av, 504804k used, 10156k free, 0k shrd, 22132k buff  
328376k active, 95096k inactive  
Swap: 1052216k av, 728k used, 1051488k free 396724k cached  


| PID   | USER | PRI | NI | SIZE | RSS  | SHARE | STAT | %CPU | %MEM | TIME | CPU | COMMAND        |
|-------|------|-----|----|------|------|-------|------|------|------|------|-----|----------------|
| 25823 | tom  | 19  | 0  | 1052 | 1052 | 876   | R    | 0.1  | 0.2  | 0:00 | 0   | top            |
| 1     | root | 9   | 0  | 464  | 444  | 416   | S    | 0.0  | 0.0  | 0:16 | 0   | init           |
| 2     | root | 8   | 0  | 0    | 0    | 0     | SW   | 0.0  | 0.0  | 0:00 | 0   | keventd        |
| 3     | root | 19  | 19 | 0    | 0    | 0     | SWN  | 0.0  | 0.0  | 0:00 | 0   | ksoftirqd_CPU0 |
| 4     | root | 9   | 0  | 0    | 0    | 0     | SW   | 0.0  | 0.0  | 0:32 | 0   | kswapd         |
| 5     | root | 9   | 0  | 0    | 0    | 0     | SW   | 0.0  | 0.0  | 0:00 | 0   | bdflush        |


```

...ma ci sono alcuni limiti:

- ✗ Non ci sono facili interfacce grafiche (escludendo distro commerciali)
- ✗ Manca una gestione "Enterprise" centralizzata

Ringraziamenti...

La ditta General Impianti (Jesi) per averci aiutato sulla parte Cisco

www.linuxsecurity.org per il logo utilizzato

Il software libero, con il quale lavorare è sempre un gioco divertentissimo

Tommaso Di Donato

tom@pluto.it

(dido@sicurweb.com)