ISTITUTO NAZIONALE DI FISICA NUCLEARE

Sezione di Bologna

INFN/TC-03/17
4 Dicembre 2003

STUDIO PRELIMINARE DI VPN PER L'INFN

Ombretta Pinazza[1], Alessandro Brunengo[2], Enrico M.V. Fasanelli[3], Enrico Mazzoni[4], Claudio Soprano[5], Riccardo Veraldi[6], Stefano Zani[7]

[1)]INFN-Sezione di Bologna
[2)]INFN-Sezione di Genova
[3)]INFN-Sezione di Lecce
[4)]INFN-Sezione di Pisa
[5)]INFN-Laboratori Nazionali di Frascati
[6)]INFN-Sezione di Firenze
[7)]INFN-CNAF

Abstract

Le Virtual Private Networks sono nate allo scopo di trasportare traffico privato su una rete pubblica in maniera sicura e autenticata.

L'introduzione delle VPN nel nostro Ente potrebbe rappresentare uno strumento per aumentare il livello di sicurezza nelle comunicazioni fra le unità operative decentrate e per agevolare i ricercatori che si spostano sempre più di frequente fra le sedi, i laboratori italiani o stranieri e coloro che lavorano da casa.

Il Netgroup ha promosso questo studio preliminare per fornire ai Servizi di Calcolo e Reti uno strumento di partenza per la scelta di tecnologie emergenti necessarie a una tipologia di lavoro sempre più mobile e dinamica.

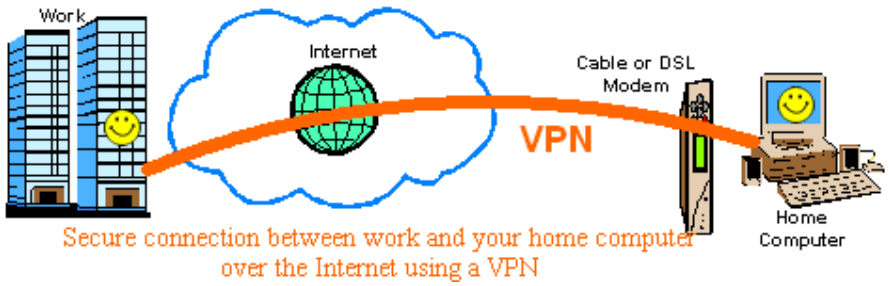
PACS.: **89.70.+c**

Published by ***SIS–Pubblicazioni***
Laboratori Nazionali di Frascati

1. Introduzione

Definizione di VPN

VPN (Virtual Private Networks) non è una tecnologia ma un concetto, che può essere implementato nella pratica con l'utilizzo di tecnologie diverse fra loro. Alla base vi è la necessità di avere una rete di calcolatori che possono fare parte fisicamente di reti diverse (distanti fra loro e topologicamente eterogenee) ma che virtualmente appartengano alla stessa rete logica.
Una VPN è un canale di comunicazione sicuro e privato tra due o più apparati attraverso una rete pubblica (Internet). Tali apparati possono essere indistintamente computer con software VPN o apparati proprietari dedicati alla funzione di VPN box.
L'utilizzo di questa tecnologia potrebbe rappresentare una soluzione valida per risolvere i problemi di sicurezza legati al tele-lavoro.



Le tecnologie che stanno alla base del mondo VPN sono in continua evoluzione, e si basano su soluzioni che consentono l'incapsulamento dei protocolli standard utilizzati nell'ambito di una LAN all'interno di tunnel veri e propri, fornendo servizi di autenticazione e cifratura.

Road Warriors e *Home Warriors*

La tipologia di lavoro, non solo nell'ambito delle attività di ricerca scientifica, è in corso di evoluzione, e negli ultimi anni ha evidenziato come la mobilità delle persone, sempre più importante per la collaborazione tra istituti diversi, comporta la necessità da parte del viaggiatore (comunemente definito col nome di Road Warrior) di accedere in remoto alle risorse del suo sito di appartenenza. Altrettanto spesso il ricercatore svolge parte del suo lavoro a casa, ed anche in queste circostanze si sente spesso l'esigenza di accedere alle risorse del sito di appartenenza.
In generale, la situazione in questi ultimi anni ha mostrato come sia crescente il conflitto tra l'esigenza del ricercatore fuori sede di accedere in remoto alle risorse locali, e

l’esigenza degli amministratori di rete di proteggere per motivi di sicurezza il proprio sito da un accesso indiscriminato alle risorse locali.

Una delle possibili soluzioni a questo problema è offerta dal concetto di VPN, che permettono di configurare un servizio attraverso il quale un calcolatore remoto (il laptop del Road Warrior, o il PC di casa) può entrare a far parte logicamente della rete del sito di appartenenza tramite meccanismi di tunneling, autenticazione e cifratura. La virtuale collocazione del calcolatore nella rete in questione, permette allo stesso l’accesso alle risorse del sito come se fosse direttamente connesso alla sua rete locale.

2. Obiettivo

Le VPN e l’INFN

La particolare struttura distribuita dell’INFN, costituita da una trentina di sedi tra sezioni, laboratori, gruppi collegati e sedi amministrative, e la tipologia delle attività di ricerca, che prevede frequenti contatti e collaborazioni con altri istituti di ricerca ed università in tutto il mondo, si presta in modo particolare all’utilizzo di una tecnologia come quella delle VPN.
La configurazione di nuovi servizi in una sezione o un laboratorio richiede spesso un notevole investimento di tempo, necessario all’acquisizione di nuove conoscenze e la formazione del personale, e di denaro, per reperire l’hardware necessario.
Lo scopo principale di questi test e della nota tecnica che ne segue è quello di raccogliere indicazioni utili a chi desideri implementare presso la propria unità un servizio di VPN.

Il gruppo ha svolto un lavoro di indagine relativa alle soluzioni disponibili al momento sul mercato, facendo riferimento sia a soluzioni software – gratuite o a pagamento – che a soluzioni proprietarie che comportano acquisto di materiale hardware specifico.
L’obiettivo del lavoro è la ricerca di una o più soluzioni per l’implementazione di un servizio di accesso in VPN nelle sezioni INFN. La ricerca tecnologica è stata accompagnata da attività di sperimentazione per testare le caratteristiche delle diverse soluzioni.

Non sono state imposte caratteristiche a priori per preselezionare i prodotti disponibili, anche se si sono tenuti in importante considerazione sia gli aspetti di sicurezza, quali i meccanismi di tunneling, algoritmi di cifratura, utilizzo di certificati, che gli aspetti di flessibilità ed interoperabilità delle soluzioni provate con le architetture principali in uso nel nostro ambiente (Windows, Linux, MacOS); infine, un parametro non trascurabile è stato quello della semplicità di installazione e configurazione del servizio.

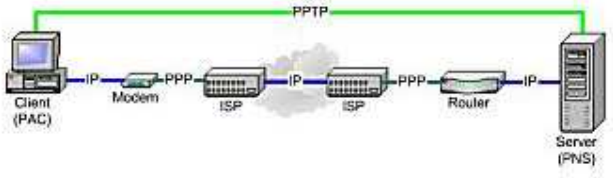
3. Tecnologie per VPN

L’implementazione di una VPN si può realizzare utilizzando diverse tecnologie.

Le componenti principali di una VPN sono il protocollo per la cifratura della connessione, il meccanismo di autenticazione per garantire l'accesso alla connessione, il meccanismo di tunneling per la comunicazione tra il server ed il client.
Alcune soluzioni si basano su protocolli standard a livello di data link layer (PPTP, L2TP) e network layer (IPSec), altre soluzioni sono a livello applicativo (CIPE, OpenVPN) e utilizzano soluzioni basate su SSL/TLS e algoritmi di cifratura standard (IDEA, Blowfish etc.). Dal momento che i protocolli di livello 2 e 3 sopra citati fanno parte di standard assodati e sono ormai supportati dalla maggior parte dei moderni sistemi operativi, i test preliminari di seguito descritti si sono rivolti principalmente a questi protocolli.

3.1.PPTP

Il PPTP (Point to Point Tunneling Protocol) è un protocollo che consente al PPP (Point to Point Protocol) di essere incapsulato all'interno di un tunnel IP. Il PPTP non apporta nessun cambiamento al PPP, ma introduce nuove specifiche di trasporto per il PPP all'interno di altri protocolli. Il PPTP risiede in un'architettura client-server per implementare il modello di VPN: il lato server è detto PNS (PPTP Network Server), mentre il lato client prende il nome di PAC (PPTP Access Concentrator).
L'utente in pratica si collega al PAC, il quale a sua volta stabilisce un tunnel con il PNS. La connessione tra utente, o PAC, e PNS è riferita come sessione PPTP.



PPTP può utilizzare il protocollo GRE (Generic Routing Encapsulation) per fornire un controllo di flusso e di congestione per il trasporto di pacchetti PPP.

Il PPTP è considerato come protocollo di default per l'implementazione di VPN ed è ben supportato da numerosi sistemi operativi. Il suo grande vantaggio è dato dal fatto che il PPTP è definito come protocollo a livello di data link layer, per cui può incapsulare al suo interno anche protocolli non IP, mentre ad esempio IPSec (tecnologia emergente applicata alle VPN, descritta di seguito) supporta soltanto il trasporto o il tunneling del protocollo IP. PPTP però fa parte di un tipo di tecnologia datata e ha lo svantaggio di fornire un flusso di dati non cifrato e non autenticato a livello di protocollo, pertanto è suscettibile a problemi di sicurezza come il *tampering*, *non-repudiation*, confidenzialità. Esistono comunque implementazioni che consentono di stabilire sessioni PPTP cifrate, basate sui protocolli MS-CHAPv2 e MPPE di Microsoft, anche se quest'ultimo tipo di soluzione non fornisce un livello di sicurezza accettabile a causa di noti bachi di sicurezza nel protocollo MS-CHAPv2 [1]. Inoltre, nonostante l'utilizzo della cifratura durante la sessione PPTP, la fase di autenticazione degli utenti avviene in modalità *cleartext*.

PPTP realizza l'autenticazione via password tramite i protocolli:

- § PAP (Password Authentication Protocol): è un protocollo per la verifica di password scambiate in chiaro sulla rete. Assolutamente insicuro: non è possibile cifrare le connessioni autenticate con questo meccanismo.
- § SPAP (Shiva PAP): rispetto al precedente utilizza una cifratura reversibile della password prima di trasmetterla via rete. Anche in questo caso però è assolutamente insicuro, poiché non è possibile cifrare le comunicazioni successive alla fase di autenticazione.
- § CHAP (Challenge Handshake Authentication Protocol): è un meccanismo che prevede la trasmissione da parte del server di una *hash string*, calcolata dalla password dell'utente tramite algoritmo di *hashing* MD5, che viene verificata dal client operando lo stesso algoritmo sulla password digitata dall'utente. Il livello di sicurezza di questo meccanismo di protezione della password è basso. Anche in questo caso la comunicazione successiva all'autenticazione non potrà essere criptata.
- § MS-CHAP (Microsoft CHAP): utilizza lo stesso meccanismo di CHAP, ma applica dapprima l'algoritmo di hashing MD4 sulla password e quindi l'algoritmo di cifratura DES (Data Encryption Standard) tramite lo scambio di chiavi (*shared keys*) secondo il protocollo MPPE (Microsoft Point to Point Encription). La fase di autenticazione sarà criptata secondo il protocollo MPPE. Presenta un livello di sicurezza migliore dei precedenti, ma con alcune documentate debolezze.
- § MS-CHAP v2: utilizza un meccanismo di cifratura più sicuro rispetto alla versione precedente, a chiavi asimmetriche per la mutua autenticazione delle due parti e chiavi più complesse. Livello di sicurezza più affidabile.

Il protocollo PPTP è nativo per la realizzazione di connessioni VPN in ambiente Windows, ma esistono implementazioni del client anche per Linux.

3.2.L2TP e L2TP/IPSec

L2TP (Layer 2 Transport Protocol) può essere considerato il successore di PPTP e L2F (Layer 2 Forwarding), protocollo proprietario di Cisco. Ha la stessa flessibilità di PPTP e quindi, essendo un protocollo di layer 2 (*data link layer*), può incapsulare diversi tipi di protocolli al suo interno. L2TP include gli stessi meccanismi di autenticazione utilizzati dal PPP: PAP, CHAP ed EAP (Extensible Authentication Protocol, come ad esempio RADIUS).
L2TP non esegue alcuna cifratura dei dati, operazione che demanda all'utilizzo di altri protocolli; in particolare, per la realizzazione di VPN, viene spesso utilizzato in unione ad IPSec (cfr. Par. 3.3), che si occupa della cifratura dei dati.

Il pacchetto dati, in figura rappresentato da un pacchetto PPP, incapsulato tramite L2TP e cifrato utilizzando IPSec, è il seguente:

L'utilizzo di IPSec fornisce un ottimo livello di sicurezza per la comunicazione.

3.3.IPSEC

IPSec (IP Security) è una suite di protocolli che implementano la cifratura a livello di *network layer* per fornire servizi di autenticazione (*non repudiation*) e confidenzialità (*encryption*). In più, IPSec è in grado di proteggere i protocolli che lavorano al livello superiore, quali TCP, UDP e ICMP.

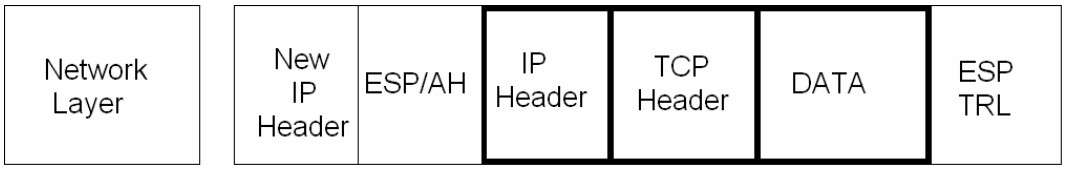
IPSec può essere implementato fra reti o fra singoli host che comunicano attraverso una *untrusted network* consentendo la creazione di VPN.

Gli elementi fondamentali di IPSec sono:

- **SA: Security Association**. Sta alla base di una VPN IPSec. È un set di proprietà relative alla connessione tra due host, è una sorta di tabella che descrive le proprietà specifiche di una VPN IPSec
  - **SPI**: numero che identifica il flusso di dati attraverso la VPN IPSec serve per discriminare tra le varie SA relative a una connessione IPSec
  - **AH** (Authentication Header, protocol number 51): data integrity, origin authentication, protezione anti-reply
  - **ESP** (Encapsulated Security Payload, protocol number 50): confidentiality, data origin authentication, data integrity, protezione anti-reply
- **IKE**: protocollo per la gestione automatica delle chiavi necessarie per tutte le operazioni di security fornite da IPSec.

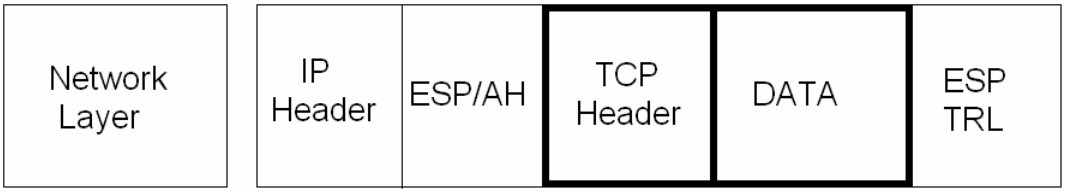
I protocolli AH e ESP possono essere usati per proteggere un pacchetto IP intero o solamente i protocolli di livello superiore del pacchetto IP. Il primo caso è detto **tunnel mode** e può essere utilizzato fra gateway per proteggere le comunicazioni fra macchine che non sono in grado di utilizzare IPSec. Il secondo caso è detto **transport mode** e viene generalmente attivato per la comunicazione diretta fra due host.

IPSec Tunnel mode



L'intero pacchetto originario viene incapsulato e cifrato e vengono aggiunti in testa un nuovo header IP e l'authentication protocol header (ESP/AH). A livello di network layer IPSec cifra l'intero pacchetto IP originario comprendente l'header TCP e il relativo payload, viene creato l'header ESP/AH aggiunto in testa al pacchetto cifrato, inoltre viene creato un nuovo header IP che consente al client di inviare il pacchetto originario al gateway VPN appropriato. Soluzione network-to-network VPN.

IPSec Transport Mode



Attraversando lo stack TCP/IP verso il basso a livello di network layer, IPSec rimuove l'header IP originale, cifra i dati relativi ai layer OSI più alti, aggiunge in testa il security header appropriato (ESP/AH) e riapplica l'header IP originale. Quindi il payload del pacchetto originario viene cifrato e viene calcolato l'opportuno authentication protocol header e inserito tra header IP originario e paylod cifrato. Questa è la tipica soluzione host-to-host VPN.

3.4.Porte utilizzate dai protocolli per VPN

Per poter utilizzare i protocolli sopra descritti deve essere garantita la comunicazione verso il server attraverso eventuali filtri (firewall o ACL).
Le porte e i protocolli utilizzati per la comunicazione sono i seguenti:

- PPTP: utilizza la porta 1723 TCP; se è configurato l'incapsulamento tramite GRE si deve garantire il passaggio al protocollo IP numero 47
- L2TP: il protocollo utilizza la porta 1701 UDP; per la funzionalità di L2TP/IPSec si deve garantire anche il passaggio dei protocolli coinvolti nella comunicazione IPSec (vedi oltre)
- IPSec: le caratteristiche della sessione cifrata vengono stabilite tramite il protocollo IKE, che utilizza la porta 500 UDP, mentre i protocolli AH ed ESP sono conosciuti come protocolli IP 51 e 50.

3.5.Alcuni esempi di VPN

Vi sono diverse implementazioni di VPN che utilizzano uno o più fra i protocolli descritti in precedenza; tuttavia, nonostante questi protocolli siano specificati da regole standard, non sempre si ha compatibilità tra server e client per architetture differenti.
Quello che segue è un elenco non esaustivo di diversi esempi di implementazione di VPN:

- PPTP/MPPE (Microsoft VPN) - Windows, UNIX/Linux, e Mac clients.
- PPTP/IPSec - Windows (2000 & NT) e UNIX/Linux clients
- L2TP/IPSec - Windows (2000 & NT) e UNIX/Linux clients
- CIPE - Linux clients e Windows (2000 & NT) clients
- OpenVPN - UNIX/Linux clients
- SSL-wrapped PPP - Linux clients
- GRE and IP/IP - Linux clients, Cisco routers
- IPSec, tunnel mode, transport mode - Windows (2000 & NT) e UNIX/Linux clients

4. Test su soluzioni software

Le soluzioni software qui descritte sono state provate per valutarne la facilità di installazione e di impiego, le funzionalità e l'interoperabilità fra diverse piattaforme. Non sono stati eseguiti test approfonditi sulle prestazioni in caso di utilizzo effettivo da parte di utenti.

4.1.Microsoft VPN/PPTP (Windows/Linux)

Configurazione del server
È stata testata la realizzazione di VPN utilizzando come server un W2000 server, configurato come *domain controller*. La configurazione del servizio è semplice, e consiste nella attivazione del *Routing and Remote Access*, e nella configurazione del sistema come *Router* e *Remote Access Server*.
Si possono configurare diversi parametri:

- i meccanismi di autenticazione (è possibile ad esempio utilizzare un server RADIUS esterno)
- l'utilizzo o meno di protocolli cifrati
- il meccanismo per assegnare i numeri IP ai client, utilizzando ad esempio un server esterno per con un pool di indirizzi staticamente configurato, o un DHCP server.

Installazione e configurazione del client Windows
Le più recenti piattaforme Windows hanno preinstallato il software necessario alla configurazione del client.

Il client disponibile è di semplice utilizzo, e può essere configurato tramite i menu per la creazione di una nuova connessione di rete.
Sono stati eseguiti con successo test di configurazione e attivazione della VPN fra client Windows XP e 2000 e il server Windows 2000.

Installazione e configurazione del client Linux
L'attivazione del client su Linux richiede l'installazione di un kernel opportuno ed un modulo PPP modificato. Dopo il reboot si può configurare il client attraverso uno script; i parametri da configurare sono pochi, ma non ovvi per l'utente non esperto.
L'attivazione della VPN non ha presentato alcun problema.
Il grave difetto di questa implementazione sta nel fatto che la password per la connessione – tipicamente la password di dominio sul sito che ospita il server – è salvata in chiaro sui file di configurazione del client.

4.2.CIPE (Linux/Windows)

Descrizione

CIPE (Crypto IP Encapsulation) è un software distribuito con licenza GPL per l'implementazione di una comunicazione cifrata tra due calcolatori, tramite l'incapsulamento dei pacchetti IP in forma cifrata in pacchetti UDP. La porta di ascolto è configurabile. La cifratura viene operata attraverso lo scambio di *shared secrets*. Non c'è compatibilità con altri protocolli, quali ad esempio IPSec.
Il prodotto è un applicativo che si installa e si configura senza problemi.
Ne esiste anche una versione per Windows.

Considerazioni

La funzionalità è stata testata con successo tra macchine linux.
Il client Windows ha manifestato grave instabilità.
Il software è dotato di script di startup delle interfacce virtuali che configurano opportunamente le route necessarie ad incanalare il traffico attraverso il tunnel, ma possono essere configurati a mano l'*IP forwarding* e le route statiche opportune per configurazioni diverse da quelle previste.
Il problema più evidente è che manca completamente un meccanismo di autenticazione per consentire o negare l'accesso al tunnel: se il client dispone dello *shared secret* corretto l'accesso viene fornito.

4.3.Test su IPSec: Windows, FreeS/Wan-Linux, KAME-FreeBSD

Realizzazione di una VPN fra due host Linux usando FreeS/WAN

In questo test IPSec è stato utilizzato per far comunicare due gateway fornendo autenticazione e cifratura a livello IP (ovvero in *tunnel mode*). Sono stati utilizzati due PC con RedHat Linux e il pacchetto FreeS/WAN che implementa lo stack IPSec in Linux.

La configurazione si basa su due file:

- **`/etc/ipsec.conf`**, contenente le configurazioni generali e le caratteristiche delle diverse connessioni
- **`/etc/ipsec.secrets`**, che contiene le chiavi pubblica e privata per l'autenticazione delle connessioni e per la cifratura dei dati.

IPSec supporta due tipi di connessioni:

- ***a chiavi manuali***, che utilizza le chiavi memorizzate in */etc/ipsec.conf*
- ***a chiavi automatiche***, che autentica tramite il protocollo IKE e le chiavi generate dinamicamente dal daemon **Pluto**, utilizzando le chiavi segrete memorizzate in */etc/ipsec.secrets*.
  Le connessioni a chiavi automatiche possono essere di tipo:
  - preshared secrets (PSK - default - utilizzate durante lo scambio delle chiavi)
  - RSA private keys:

Per utilizzare la modalità RSA è necessario generare le chiavi RSA su entrambi i gateway.

Se fra i gateway è presente un firewall bisogna permettere il seguente traffico
- porta 500/UDP per IKE
- ESP (protocollo 50)
- AH (protocollo 51)

Realizzazione di una VPN fra due host Windows 2000 usando IPSec

Usando l'implementazione IPSec di Windows è stato possibile instaurare un tunnel cifrato con autenticazione fra due PC Windows 2000 Professional. In particolare, è stata realizzata una VPN di tipo *transport* fra un PC all'interno della LAN e un PC connesso a un provider commerciale tramite modem.
Tutta la configurazione è stata effettuata tramite MMC (Microsoft Management Console).

Realizzazione di una VPN fra un host Windows 2000 (IPSec di Windows) e un host linux (FreeS/WAN)

E' stata inoltre realizzata una VPN fra un PC linux con FreeS/WAN e un PC Windows 2000 Professional, configurati come descritto nei test precedenti.
La modalità prescelta per lo scambio delle chiavi è stata quella a "*preshared keys*" e la VPN realizzata è stata di tipo *IPSec transport mode*.

IPSec standard e interoperabilità fra FreeBSD e Windows XP

E' stata infine realizzata una prova di interoperabilità fra Windows XP e FreeBSD (KAME). La VPN realizzata è stata di tipo *transport* e sono stati impiegati con successo i certificati X.509 per autenticare e inizializzare la connessione IPSec.

La configurazione di FreeBSD si basa sulle seguenti configurazioni:

- il file di configurazione del demone *racoon* **/usr/local/etc/racoon/racoon.conf,** che implementa il protocollo IKE per lo scambio automatico di chiavi tramite certificati
- i comandi **setkey** e **spdadd** che consentono di configurare le policy IPSec.

La parte Windows XP si configura tramite MMC come nei casi precedenti, includendo questa volta il management dei certificati X.509.

Test IPSec: conclusioni

Con i test svolti si è voluta provare l'interoperabilità fra diverse implementazioni della suite di protocolli IPSec realizzando VPN host-to-host senza trasportare servizi all'interno di queste.

I test realizzati hanno avuto come finalità pricipale l'analisi della tecnologia IPSec in sè, la sua compatibilità tra diversi stack e le modalità di configurazione, ma non il tunneling di servizi attraverso IPSec. I layout di test sopra descritti non sono quindi immediatamente portabili come soluzioni di casi reali di VPN end-user, ma rappresentano un primo test essenziale delle nuove tecnologie di base, al quale potrà seguire un'ulteriore analisi della VPN a più alto livello di astrazione, utilizzando in particolare sistemi OpenSource.

5. Test su soluzioni con hardware dedicato

I test successivi riguardano soluzioni proprietarie che forniscono un servizio di VPN "*chiavi in mano*" per gli operatori e gli utenti.

Sono stati analizzati e testati due tipi di apparati hardware dedicati alla funzione di VPN server.

5.1.Cisco VPN Concentrator 3000 series

Cisco VPN Concentrator 3000 series è una famiglia di apparati espressamente dedicati alla realizzazione di VPN LAN-to-LAN e LAN-to-Host.

Sono disponibili diversi modelli di questo apparato, che si differenziano per prestazioni e prezzo:

The Cisco VPN 3000 Series Concentrator Features

	Cisco VPN 3005	Cisco VPN 3015	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Simultaneous Users*	100	100	1500	5000	10,000
Maximum LAN-to-LAN Sessions	100	100	500	1000	1000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	100 Mbps	100 Mbps
Encryption Method	Software	Software	Hardware	Hardware	Hardware
Encryption (SEP) Module	0	0	1	2	4
Redundant SEP	N/A	N/A	Op	Option	Yes
Available Expansion Slots	0	4	3	2	N/A
Upgrade Capability	No	Yes	Yes	N/A	N/A
System Memory	32/64 MB	128 MB	128 MB	256 MB	256 MB
Hardware Configuration	1U, Fixed	2U, Scalable	2U, Scalable	2U, Scalable	2U
Dual Power Supply	Single	Option	Option	Option	Yes
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

* For planning purposes, a simultaneous user is considered to be a Remote Access VPN user connected in ALL tunneling mode—this includes 1 IKE Security Association and 2 unidirectional IPsec SA's. For environments with rekeying or split tunneling, we recommend using a VPN Remote Access load-balancing environment with spare capacity since these particular sessions will utilize additional system resources that otherwise would be used to support additional users.

Il concentratore ottenuto in prova è stato il modello base, il 3005. Le sue caratteristiche principali sono:

Configurazione hardware: è dotato di due interfacce di rete in rame 10/100 Mb/s, una delle quali viene configurata per l'utilizzo verso la rete esterna (*untrusted*) e l'altra verso la rete interna, ed una linea seriale per la configurazione iniziale.

Configurazione: la prima configurazione avviene tramite porta seriale. Il configuratore a linea di comando permette la configurazione completa della macchina, a cominciare dalle interfacce di rete e la default route; abilitando poi l'accesso al configuratore tramite protocollo http/https si potrà disporre di una interfaccia più semplice ed intuitiva.

Filtri: è possibile configurare filtri a livello di indirizzi IP e di porte TCP/UDP (di tipo equivalente alle ACL del Cisco IOS) indipendenti sulle due interfacce di rete.

Protocolli: il concentratore è capace di stabilire VPN secondo i protocolli PPTP, L2TP/IPSec e IPSec nativo; il protocollo IPSec nativo può essere utilizzato per stabilire VPN LAN-to-LAN o LAN-to-host, tramite IKE proposal, sia in modalità diretta che in

modalità tunnel su TCP e su UDP. La modalità in tunnel consente di attivare una connessione VPN anche quando il client si trovi in una rete connessa via NAT, che renderebbe impossibile l'utilizzo di IPSec nativo.

Assegnazione di indirizzi: il concentratore può assegnare ai client indirizzi utilizzando differenti meccanismi, quali indirizzo scelto dinamicamente in un range configurato sul concentratore, indirizzo staticamente assegnato al client, indirizzo assegnato da un DHCP server esterno.

Gestione del Box: oltre all'accesso tramite la porta seriale, è possibile configurare e gestire il Box tramite i più comuni protocolli di rete: http, https, telnet, ssh, SNMP, TFTP, FTP ...

Logging: il concentratore ha un sistema di logging basato su *syslogd* ed un sistema di notifica in grado di segnalare anche via mail eventi di particolare rilevanza.

Monitoraggio: il sistema di monitoraggio permette di seguire gli eventi in tempo reale e di visualizzare le statistiche relative al funzionamento dell'apparato (numero di connessioni, durata, livello di compressione e throughput). È ampiamente configurabile il tipo di evento sottoposto a monitoraggio per categoria e verbosità.

Load balancing: è possibile creare cluster di concentratori in modalità load balancing.

Autenticazione: il concentratore supporta la connessione senza autenticazione, o con diverse modalità di autenticazione:

- § MS-Windows server esterno, con o senza Active Directory
- § RADIUS server esterno
- § user database interno; il database gestisce gli utenti in gruppi, ed è possibile definire caratteristiche di gruppo o specifiche, quali orario di accesso, massimo numero di login simultanei, caratteristiche della password, massima durata delle connessione, protocolli di tunnel
- § certificati X.509.

Client software: il server è accessibile, nella modalità IPSec, tramite un apposito client, distribuito gratuitamente da Cisco e disponibile per le piattaforme:

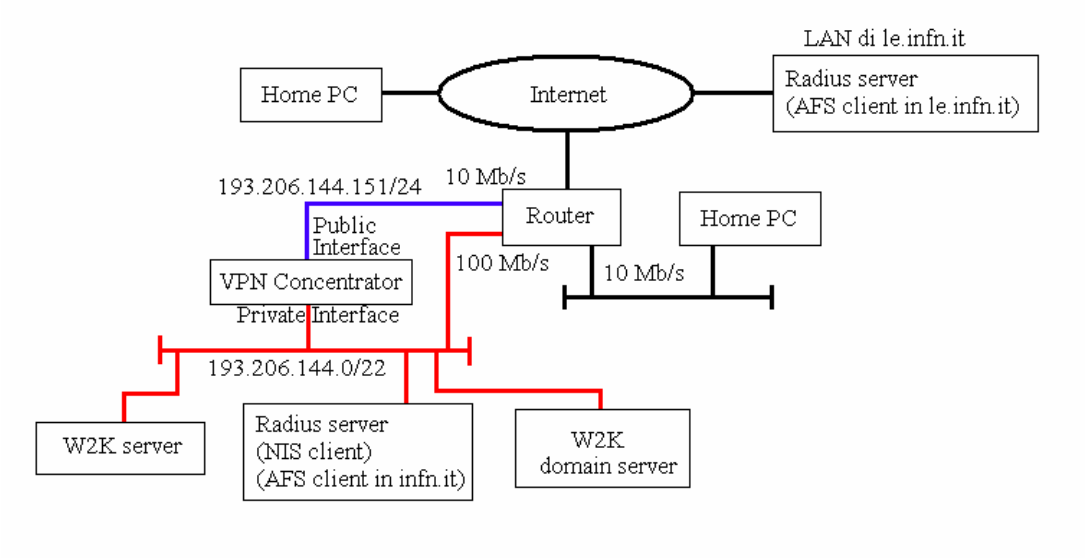
- Windows 2000, Windows XP, Windows 98
- Solaris fino alla versione 8
- Linux Kernel 2.2-2.4
- MacOS-X.

Nelle modalità L2TP/IPSec e PPTP, il concentratore è dichiarato compatibile con i client VPN di Windows 2000/XP/98.

5.2.Test sul Cisco VPN Concentrator 3005

È stata realizzata una piattaforma di test per effettuare prove sulle funzionalità del Cisco VPN Concentrator 3005, il modello meno performante e meno costoso della famiglia. I test effettuati hanno coinvolto le sezioni INFN di Bologna, Genova, Lecce ed il CNAF.

Layout di test: il layout di test è riportato in figura:



L'interfaccia pubblica è stata connessa ad una interfaccia Ethernet del router di accesso alla rete geografica, in modo da poter disporre di banda sufficiente a gestire i 4 Mb/s di throughput aggregato nominalmente supportati dal modello.
L'interfaccia privata è stata connessa alla rete locale.

Per testare i diversi meccanismi di autenticazione sono stati utilizzati, in aggiunta al database locale del concentratore, un server W2000 stand alone, un server W2000 domain controller con Active Directory, un radius server sulla rete locale, a sua volta client di un dominio NIS locale e client della cella AFS infn.it (autenticazione mediante kerberos4), ed un radius server remoto (situato sulla LAN di le.infn.it), client della cella AFS le.infn.it configurata con autenticazione mediante kerberos5.
L'accesso via VPN alla rete locale è stato testato utilizzando client linux, Windows 2000 e MacOsX connessi ad un'altra interfaccia Ethernet del router, il cui accesso normale è sottoposto ai filtri delle ACL configurate sul router in ingresso alla rete locale della sezione INFN di Genova.
Per testare la funzionalità dell'accesso via IPSec/TCP e IPSec/UDP è stato utilizzato un client posto a valle di una rete (presso il Dipartimento di Fisica dell'Università di Genova) protetta da firewall configurato per fare NAT.

Connessioni via PPTP: questa connessione è stata testata utilizzando un client W2000 ed un client linux. La configurazione del client Windows è risultata banale, e consiste nella configurazione di una nuova connessione di rete di tipo VPN tramite il configuratore standard di Windows per le connessioni di rete. La configurazione del client linux prevede la ricompilazione di un modulo del kernel e la configurazione della interfaccia virtuale per la connessione VPN, tramite uno script di installazione; tuttavia il significato dei parametri da configurare non è sempre ovvio da interpretare.
L'autenticazione è stata testata con i tre meccanismi di autenticazione che richiedono username e password. A questo scopo è stata definita una lista di server di autenticazione, uno per ogni tipo.

Il risultato delle prove effettuate è il seguente:

- Se non viene richiesta autenticazione, tutto funziona correttamente.
- Se viene richiesta autenticazione senza cifratura (PAP), la connessione funziona con i tre meccanismi di autenticazione.
- Se viene richiesta la cifratura (MSCHAP v1 e v2) l'autenticazione funziona solo sul database locale (ma la documentazione dice che dovrebbe funzionare anche con autentication server esterni).
- Pur disponendo di una lista di server per i tre tipi di autenticazione, la verifica delle credenziali viene eseguita solo sul primo server nella lista.

Connessioni via IPSec: sono stati effettuati con successo test con il software client Cisco su piattaforme W2K Professional, Linux RH 7.*, MacOsX (darwin kernel 5.5).
Sul server va creato un gruppo tra le cui proprietà si definisce il server di autenticazione da utilizzare; nel caso di autenticazione locale, vanno definiti gli utenti nel database locale.
Il client va configurato per accedere al gruppo desiderato.
I test hanno verificato il successo della connessione utilizzando i tre diversi meccanismi di autenticazione. Il server è capace di gestire connessioni contemporanee sui gruppi diversi.
Con questo meccanismo la comunicazione è sempre cifrata e sicura; sono ampiamente configurabili i protocolli e gli algoritmi di cifratura.

Connessioni via IPSec/TCP e IPSec/UDP: sono state effettuate anche prove di utilizzo di IPSec incapsulato su TCP ed UDP con client Cisco su piattaforma W2000 e Linux. Al fine di verificare la piena funzionalità è stata testata con successo l'attivazione di una connessione attraverso NAT.
Dal lato server è possibile configurare le porte da utilizzare per il tunnel, ed il client deve essere configurato conseguentemente.

Note sulla autenticazione via Radius: è stata utilizzata la possibilità di utilizzare il Radius server per rendere più flessibile la scelta dell'authentication server.
È stato a tale scopo installato il radius server *freeradius.0.8.1* su un calcolatore linux RedHat 7.3. Il server radius è stato configurato per utilizzare PAM quale meccanismo di autenticazione e, tramite PAM, è stata operata con successo l'autenticazione via NIS (quando il radius server è NIS client di un dominio NIS) e via AFS (quando il radius server è AFS client). L'autenticazione ha funzionato anche utilizzando come radius server

una macchina collocata fisicamente su una LAN remota (le.infn.it), cosa che ha permesso di verificare l'autenticazione anche su una cella AFS utilizzante kerberos5.

Test di throughput: è stato misurato il throughput massimo ottenibile attraverso una connessione con il concentratore in prova. È stato misurato un throughput aggregato pari a 3.4 Mb/s, sia con una singola connessione che con più connessioni contemporanee (durante i test sono state attivate al massimo 5 connessioni). Il limite alla capacità trasmissiva è dato dalla CPU del concentratore, che in entrambi i casi risulta occupata al 100%.

Cosa non è stato provato: non sono state provate connessioni con autenticazione tramite certificati per mancanza di tempo; non sono stati effettuati test di utilizzo del protocollo di tunneling L2TP/IPSec, essenzialmente in virtù del fatto che la complessità della configurazione del client in ambiente Windows non giustifica l'utilizzo di questo protocollo potendo disporre del client Cisco, molto più semplice da configurare, che fornisce una sicurezza equivalente e maggiore flessibilità.

Nota: è necessario configurare le interfacce del concentratore su due sottoreti diverse.

Considerazioni sulle prove con il Cisco VPN concentrator 3005: l'oggetto risulta estremamente flessibile e configurabile sotto diversi aspetti, quali protocolli di configurazione e monitoring, protocolli di cifratura, meccanismi di autenticazione, filtri sulle interfacce.

Caratteristica molto importante è quella di poter disporre di client per tutte le piattaforme più comuni nel nostro ambiente.

Particolarmente apprezzata, dal punto di vista della sicurezza, è la possibilità di configurare il server in modo da rendere impossibile la memorizzazione della password sul client (solo per connessioni IPSec native); altrettanto dicasi per la possibilità di configurare il server in modo da determinare quali network, sul client, debbano essere instradate attraverso il tunnel: in particolare si può facilmente configurare il server per imporre al client di passare attraverso il tunnel per qualsiasi comunicazione verso l'esterno, ivi compresa la comunicazione verso la rete locale fisicamente connessa al client. Questo trasforma il client in tutto e per tutto in una macchina connessa logicamente alla rete del VPN server. Anche questa configurazione non è modificabile dal lato client.

Le caratteristiche sopra citate, unitamente alle prove di throughput, ne fanno un oggetto molto interessante e di basso costo per un sito di non eccessive dimensioni, che non abbia necessità di avere alto numero di connessioni contemporanee e non abbia necessità di throughput elevati.
Bisogna ricordare infatti che il numero massimo di connessioni concorrenti dichiarato dal produttore è 100 (comprese le eventuali sessioni per il monitoraggio da parte dell'amministratore), che si suddividono in modo abbastanza uniforme le prestazioni del

server. Durante la fase di test non è stato però possibile raggiungere un numero significativo di sessioni contemporanee.

Qualora si rendesse necessario un servizio più solido e performante, si deve prendere in considerazione l'utilizzo di uno dei modelli superiori, valutando in questo caso l'aumento dei costi rispetto a soluzioni alternative.

5.3. Test sul Netscreen

I prodotti Netscreen utilizzabili come concentratori VPN si dividono in due grandi famiglie: "appliance" e "security systems", che si differenziano in termini di densità di porte, throughput e scalabilità. Entrambe le famiglie realizzano le loro funzionalità con ASIC dedicati garantendo così prestazioni superiori rispetto ad architetture di tipo CPU.
Per gli scopi del test è stata presa in considerazione la famiglia degli *Appliance* che si compone di 6 modelli differenti per prestazioni e prezzi.

Modello	***n. interfacce (Mb/s)***	***Throughput firewall***	***Throughput VPN***	***n. Sessioni simultanee***	***n. tunnel IPSec statici***
NS-5XP	2 (10)	10 Mb/s	10 Mb/s	2000	10
NS-5XT	4+1 (10/100)	70 Mb/s	20 Mb/s	2000	10
NS-25	4 (10/100)	100 Mb/s	20 Mb/s	4000	25
NS-50	4 (10/100)	170 Mb/s	50 Mb/s	8000	100
NS-204	4 (10/100)	400 Mb/s	200 Mb/s	128000	1000
NS-208	8 (10/100)	550 Mb/s	200 Mb/s	128000	1000

Le caratteristiche principali di questa famiglia sono:

Configurazione hardware: in tutti gli apparati è presente una linea seriale per la configurazione iniziale. Delle interfacce di rete disponibili almeno una deve essere utilizzata verso la rete esterna (*untrusted*) ed una verso la rete interna (*trusted*).

Configurazione: la prima configurazione avviene tramite porta seriale. Il configuratore a linea di comando permette la configurazione completa della macchina. Il configuratore via seriale deve essere utilizzato per configurare inizialmente almeno l'interfaccia *trusted* e la *default route*; quindi possono essere abilitati accessi al configuratore tramite protocollo *http/https* per poter disporre di una interfaccia più semplice ed intuitiva, da cui eventualmente configurare poi l'interfaccia *untrusted*.

Filtri: è indispensabile definire filtri (stile ACL) all'interno dei tunnel VPN definiti, questo comportamento è retaggio della natura intrinsecamente firewall di questo tipo di apparati.

Protocolli: il concentratore è capace di stabilire VPN utilizzando i protocolli L2TP, L2TP/IPSec e IPSec nativo; tramite il protocollo IPSec nativo possono essere stabilite VPN LAN-to-LAN o LAN-to-host (tramite IKE proposal) sia in modalità diretta che in modalità tunnel su TCP o su UDP. La modalità tunnel consente di attivare una connessione VPN anche quando il client si trovi in una rete connessa via NAT, che renderebbe impossibile l'utilizzo di IPSec nativo.

Assegnazione di indirizzi: il concentratore può assegnare ai client indirizzi utilizzando differenti meccanismi: l'indirizzo può essere scelto dinamicamente in un range configurato sul concentratore, può essere staticamente assegnato al client o assegnato da un DHCP server esterno.

Gestione del Box: oltre all'accesso via porta seriale, è possibile configurare e gestire il Box tramite i più comuni protocolli di rete: *http*, *https*, *telnet*, *ssh*, *SNMP*, *TFTP*, *FTP*.

Logging: il concentratore ha un sistema di logging basato su *syslogd* ed un sistema di notifica in grado di segnalare anche via e-mail eventi di particolare rilevanza.

Monitoraggio: il sistema di monitoraggio permette di seguire gli eventi in tempo reale e di visualizzare le statistiche relative al funzionamento dell'apparato.

Ridondanza: per i modelli superiori della famiglia (dal NS-50 in poi) è possibile realizzare configurazioni ridondate per sistemi ad alta affidabilità.

Autenticazione: il concentratore supporta la connessione con diverse modalità di autenticazione:

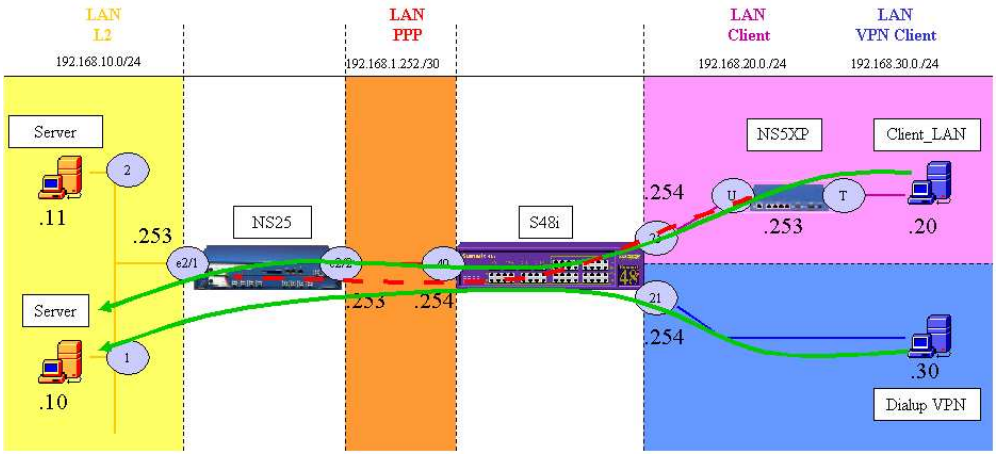
- Windows server esterno, con o senza Active Directory;
- RADIUS server esterno;
- user database interno; il database gestisce gli utenti in gruppi;
- certificati X.509.

Client software: il server è accessibile, nella modalità IPSec, tramite un apposito client, distribuito a pagamento da Netscreen per le sole piattaforme Windows. Nelle modalità L2TP/IPSec e L2TP, il concentratore è dichiarato compatibile con i client VPN di Windows 2000/XP/98 nonché tutti i client di altre piattaforme conformi con gli standard.

5.4. Test su Netscreen NS-5XP e NS-25

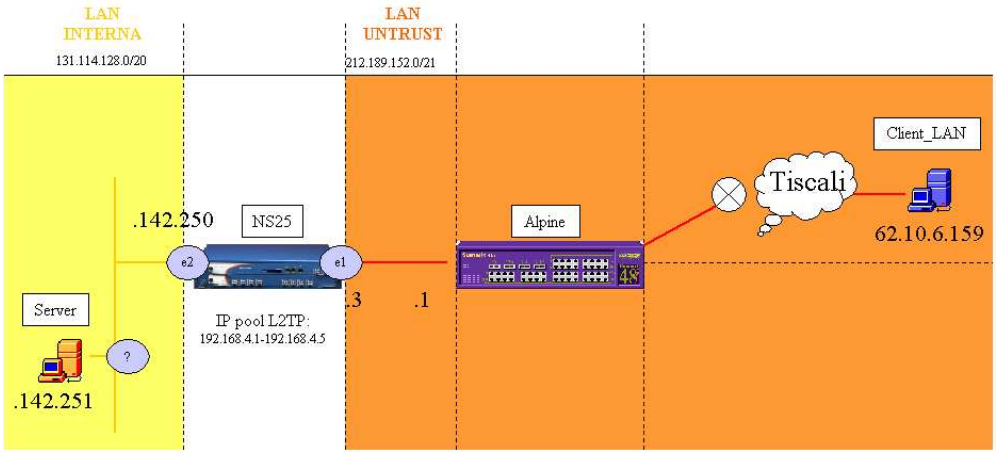
È stata realizzata una piattaforma di test per effettuare prove sulle funzionalità di due diversi apparati Netscreen sia in configurazione LAN-to-host che LAN-to-LAN. I test sono stati svolti nella sezione di Pisa simulando la situazione di due sedi distaccate della stessa struttura.

Test LAN-to-LAN: nella figura seguente è riportato il layout del test.



In questa configurazione è stato utilizzato l'appliance NS-5XP per la LAN remota e il NS-25 come concentratore per la LAN locale, intendendo con LAN remota quella della sede distaccata, e locale la LAN della sede principale in cui si assume siano ospitati i server di sezione e la maggioranza delle macchine degli utenti. I due apparati sono stati configurati in modo da realizzare staticamente un tunnel IPSec fra le loro interfacce untrusted; a questo tunnel vengono associate le opportune regole di firewall che in questo caso consistevano semplicemente nel fa passare tutto il traffico che veniva instradato all'interno del tunnel. I client della LAN remota utilizzano l'appliance come loro default gateway sul quale vengono definite le opportune regole di routing in modo da instradare il traffico diretto alla LAN locale all'interno del tunnel ed il resto direttamente verso internet. In questo modo il tunnel risulta del tutto trasparente ai client della LAN remota e non è necessaria la loro configurazione. Per far sì che tutto il traffico fra le due reti sia instradato attraverso il tunnel si deve configurare opportunamente il routing della LAN locale, oppure (come per la LAN remota) utilizzare il NS-25 come default gateway degli host.
È comunque possibile accedere al concentratore della LAN locale da un host dotato dell'opportuno client software.

Test Host-to-LAN: nella figura seguente è riportato il layout del test.



In questa configurazione è stato utilizzato il solo appliance NS-25 con le due interfacce collegate allo switch di centro stella della sezione ma configurate in modo da appartenere al dominio di broadcast del dipartimento di Fisica (interfaccia trusted) e a quello dell'INFN (interfaccia untrusted). Così come per il Cisco le due interfacce devono essere configurate in due diversi domini di broadcast; la configurazione adottata ha permesso di mettere alla prova il throughput aggregato dell'apparato.
Con questo layout sono possibili due configurazioni per quanto riguarda la modalità di accesso al servizio: tunnel di tipo IPSec e tunnel L2TP. Nel primo caso non è necessario nessun tipo di autenticazione con nome utente e password, ma semplicemente tramite certificati è possibile instaurare il tunnel utilizzando il client software specifico di Netscreen o altri software analoghi. Nel secondo caso, invece, si può autenticare l'utente che accede al servizio tramite username e password e si possono utilizzare la modalità VPN nativa di Windows e i client disponibili in rete per Linux. Dato che la connessione IPSec con il software Netscreen era già stata provata con il layout precedente, in questo caso si è deciso di concentrarsi sulla parte L2TP.
In questo tipo di configurazione (L2TP) il Netscreen si comporta come apparato di livello 3 e quindi per trasportare i pacchetti da una interfaccia all'altra viene utilizzato un indirizzo IP privato (192.168.4.0/24 nel test) che è poi l'indirizzo IP assegnato al client. Questo comportamento ha come effetto collaterale che tutto il traffico del client remoto entra nella LAN locale con un indirizzo IP diverso da quello degli host: è quindi necessario configurare opportunamente il routing locale per instradare il traffico dalla LAN all'*Appliance* oppure attivare l'opzione di NAT all'interfaccia trusted; per semplicità si è scelta quest'ultima configurazione.

Connessioni via IPSec: come detto in precedenza la connessione via IPSec è stata testata nel caso di LAN-to-LAN, nell'altro tipo di configurazione è stato provato solo il software Netscreen su un client Windows che è l'unica piattaforma supportata dal software. Per mancanza di tempo non è stato possibile provare altri software né altre piattaforme.

Connessioni via L2TP: come per i test con il Cisco questa connessione è stata testata utilizzando un client Windows 2000/XP ed un client Linux. La configurazione del client Windows è risultata banale consistendo semplicemente nella configurazione di una nuova connessione di rete di tipo VPN tramite il configuratore standard di Windows per le connessioni di rete. La configurazione del client linux prevede la ricompilazione di un modulo del kernel, e la configurazione della interfaccia virtuale per la connessione VPN, tramite uno script di installazione; tuttavia il significato dei parametri da configurare non è sempre ovvio da interpretare.
L'autenticazione è stata provata utilizzando il database locale dell'apparato e un radius server esterno, non è stata provata l'autenticazione verso un Domain Controller. Dalla documentazione emerge che è possibile suddividere gli utenti in gruppi e quindi per ciascun gruppo associare meccanismi di autenticazione differenti; per motivi di tempo e semplicità di configurazione i due sistemi di autenticazione non sono stati provati contemporaneamente ma singolarmente, legando quindi il meccanismo al tunnel stesso.
Entrambi i metodi di autenticazione hanno funzionato perfettamente sia con client Windows che Linux.

Note sulla autenticazione via Radius: si è utilizzato il server radius *freeradius 0.8.1* installato su Linux RedHat 9.0 con OpenAFS 1.2.9. Il server è stato configurato per autenticare atraverso PAM sulla cella AFS pi.infn.it di tipo kerberos 4; non è stato provata l'autenticazione NIS non essendo più utilizzata in sezione.

Test di throughput: è stato fatto un test semi-quantitativo ma comunque in grado di dare indicazioni attendibili circa il *feeling* che avrebbe avuto un utente rispetto alle prestazioni dell'eventuale servizio. Per questo si è deciso di metterci in condizioni di configurazione tali da poter utilizzare il massimo del throughput disponibile e quindi sono state fatte prove di installazione di software, copia di file o apertura di documenti attraverso la VPN; confrontando i tempi di attesa con le analoghe operazioni fatte sulla LAN. In tutti i casi i risultati VPN sono stati paragonabili con quelli della LAN.

Cosa non è stato provato: durante la fase di test non c'è stata la possibilità di provare le prestazioni dell'apparato in caso di un numero elevato di connessioni simultanee. Non è stato possibile provare in maniera più estesa i client software per diverse piattaforme (Linux, Mac), non disponibili direttamente da Netscreen e quindi da ricercarsi presso terze parti. Non è stata provata la configurazione con meccanismi di autenticazione differenti per lo stesso tunnel. Non è stato possibile provare le altre funzionalità avanzate che l'apparato offre.

Considerazioni finali sulle prove: così come il Cisco, l'apparato Netscreen risulta molto flessibile e ben configurabile.
Soffre della mancanza di client per le piattaforme utilizzate all'interno dell'ente; il software per Windows è disponibile solo a pagamento, ma questo non costituirebbe un grosso handicap data l'esiguità della cifra (3400 € per un numero illimitato di licenze).
Le elevate prestazioni sia in termini di throughput che di numero di connessioni ad un costo paragonabile, se non inferiore, a quello del Cisco lo rendono un apparato

interessante per tutte quelle situazioni in cui si prevede un utilizzo massiccio di un eventuale servizio di VPN. Inoltre il maggior numero di interfacce della versione NS-25 e il discreto numero di servizi disponibili nella macchina (VPN, firewall, traffic shaping) lo rendono molto interessante per l'implementazione di altri servizi di sicurezza oltre alla semplice applicazione VPN.

6. Analisi e confronto dei test effettuati

Nella formulazione di una analisi sul lavoro svolto, finalizzato a proporre una o più possibili soluzioni implementabili ad oggi nelle strutture INFN per fornire un servizio di connessione in VPN, sono stati tenuti in considerazione i seguenti fattori:

- semplicità di installazione e configurazione, sia per il servizio calcolo che per l'utente
- sicurezza del servizio e protezione dei dati trasmessi, cioè autenticazione e cifratura
- compatibilità ed interoperabilità tra i diversi sistemi operativi in uso (Windows*, Linux, MacOs)
- prestazioni (throughput e numero massimo di connessioni concomitanti)
- protocolli e meccanismi utilizzati, facendo particolare riferimento all'utilizzo di protocolli standard.

Le prove effettuate possono essere riassunte in una tabella che riporta, per le diverse soluzioni disponibili, informazioni sui protocolli, meccanismi di autenticazione, semplicità di setup del servizio, piattaforme client compatibili, performance e costi.

	Windows 2000 Server	**FreeS/WAN (Linux RH)**	**KAME (FreeBSD)**	**Cisco 3005**	**Netscreen**
Protocolli supportati	PPTP L2TP IPSec	IPSec	IPSec	PPTP, IPSec, L2TP/IPSec, IPSec/TCP, IPSec/UDP	L2TP, IPSec, L2TP/IPSec
Autenticazione	Certificati, presh. key, AD e domain	Certificati Preshar. key	Certificati Preshar. key	DB locale, Radius, AD o domain, NIS, AFS, certs…	DB locale, Radius, AD o domain, NIS, AFS, certs…
Complessità di configurazione	semplice	complesso	complesso	semplice	semplice
Client o sistemi compatibili	Windows*	tutti i sistemi IPSec	tutti i sistemi IPSec	client Win*, linux, MacOsX, SunOS	Client Windows*
Performance (dichiarate)	5000 conn a 15 Kbs, aggr. 60-70 Mbs	non testate	non testate	4 Mbs, 100 conn. simult	13 Mbs, 2000 conn. simult
Costo (listini primav. 2003)	Licenza W2000 Server	free	free	3000 €	1700 €

Tra i **sistemi software** testati, l'unico attualmente implementabile con semplicità e dotato di caratteristiche minime di sicurezza è il Remote Access Server di Windows 2000 Server. Il suo principale problema risiede nella difficoltà di installazione e configurazione di un client per Linux (mancano client per altre piattaforme). Garantisce ottime prestazioni per quanto riguarda il throughput. Varrebbe la pena di testare più a fondo la soluzione L2TP/IPSec per poter disporre di un meccanismo di comunicazione più sicuro e soddisfacente.
Le alternative software non hanno fornito risposte soddisfacenti, alcune per la difficoltà di configurazione (FreeS/Wan, KAME), altre per mancanza di funzionalità (CIPE).
Sembra comunque opportuno mantenere una certa attenzione alle soluzioni software *free* in attesa di prodotti più maturi e flessibili.

Entrambe le **soluzioni hardware** testate hanno mostrato notevoli pregi, in quanto a flessibilità di configurazione e supporto di protocolli che forniscono funzionalità anche in presenza di reti in configurazione NAT o dietro firewall.

La soluzione NetScreen offre un oggetto flessibile ad un ottimo prezzo, capace di notevoli prestazioni, e capace di effettuare anche operazioni di firewalling. Il suo difetto è la disponibilità di client per un numero limitato di piattaforme.

La soluzione Cisco rappresenta un prodotto notevolmente flessibile nella configurazione, offre caratteristiche di sicurezza che mancano in altre soluzioni, quale ad esempio la possibilità di impedire al client la memorizzazione della password, e la ridefinizione delle route interne. Altrettanto interessante la disponibilità del client per tutte le piattaforme di interesse (Windows*, Linux, MacOsX).
Di contro, la limitazione nelle performance del modello più economico può essere determinante; sono disponibili modelli più performanti, dotati di moduli ASIC per velocizzare le operazioni di cifratura alleggerendo la CPU, ma i costi di queste soluzioni sono decisamente superiori.

7. Problemi aperti

L'accesso alla rete locale tramite VPN fornisce un prezioso meccanismo per poter dare accesso alle risorse della rete locale del sito di appartenenza all'utente da remoto. Di fatto offre la possibilità di effettuare un *bypass* delle regole di firewalling che governano le politiche di accesso alla rete locale, proteggendo questo bypass con una verifica di autenticazione locale e con meccanismi di cifratura che garantiscono la sicurezza.

Esiste però un grosso problema di fondo: di fatto si permette ad una macchina remota, il PC portatile della persona in trasferta o il PC di casa del ricercatore, la cui configurazione non è nota o controllata dai meccanismi di controllo attivi all'interno della rete locale, di accedere alla LAN senza filtri. Questo può portare a ritrovarsi sulla rete locale calcolatori con sistemi operativi bacati o antivirus non aggiornati, e potenzialmente infettati da virus pronti a propagarsi all'interno della rete locale.

Si ritiene che un tale servizio debba essere affiancato da un meccanismo che permetta di ricollocare fuori dalla rete locale un PC potenzialmente pericoloso.
Questo aspetto non è stato trattato dalla analisi riportata in questo documento e si ritiene che un lavoro di ricerca in tale senso vada portato avanti in modo da arginare o eliminare il verificarsi di tali eventi, non solo per quanto riguarda un servizio di VPN ma, più in generale, per quanto riguarda la connessione diretta di calcolatori alla rete locale.

8. Riferimenti e Bibliografia

[1] “Exploiting known security holes in Microsoft's PPTP Authentication Extensions (MS-CHAPv2)” http://mopo.informatik.uni-freiburg.de/pptp_mschapv2/
[2] “Building and Managing Virtual Private Networks”, Dave Kosiur Wiley Computer Publishing, John Wiley & Sons, Inc. 1998
[3] “A Technical Guide to IPSec Virtual Private Networks”, James S. Tiller, Jim S. Tiller, Auerbach Publ. 2000
[4] CISCO http://www.cisco.com/univercd/cc/td/doc/product/vpn/
[5] NETSCREEN http://www.netscreen.com/products/vpn/

Ulteriori referenze, aggiornamenti e dettagli relativi ai test qui descritti sono disponibili nel sito web di NETGROUP:http://www.infn.it/netgroup

Abbreviazioni

```
AD      = Active Directory
AFS     = Andrew File System
AH      = Authentication Header
CCP     = Compression Control Protocol
CHAP    = Challenge-Handshake Authentication Protocol
DES     = Data Encryption Standard
ESP     = Encapsulated Security Payload
GRE     = General Routing Encapsulation
IDEA    = International Data Encryption Algorithm
IKE     = Internet Key Exchange
IPSec   = Internet Protocol Security
L2TP    = Layer 2 Tunneling Protocol
LAN     = Local Area Network
KLIPS   = KerneL IP Security
MSCHAP  = MicroSoft Challenge-Handshake Authentication Protocol
NIS     = Network Information Service
PAC     = PPTP Access Concentrator
PAP     = Password Authentication Protocol
PNS     = PPTP Network Server
PPP     = Point to Point Protocol
PPTP    = Point to Point Tunneling Protocol
PSK     = PreShared Keys
RSA     = Rivest Shamir Adleman public key encryption method
SSL     = Secure Socket Layer
SPAP    = Shiva Password Authentication Protocol
SPI     = Security Parameter Index
TLS     = Transport Layer Security
VPN     = Virtual Private Network
```