ISTITUTO NAZIONALE DI FISICA NUCLEARE

Sezione di Firenze

INFN/TC-04/17
26 Ottobre 2004

IMPLEMENTAZIONE DI UN VPN SERVER UTILIZZANDO IL CISCO VPN CONCENTRATOR 3005

Riccardo Veraldi, Francesca Del Corso

INFN, Sezione di Firenze

Abstract

Le VPN rappresentano una soluzione valida per il transito di traffico di tipo privato su rete pubblica, offrendo un servizio importante agli utenti che al di fuori delle sezioni INFN abbiano l'esigenza di potere accedere alle risorse e all'ambiente della LAN in modo trasparente, sicuro ed economico.
Di seguito è presentato uno studio di implementazione del servizio VPN attraverso l'utilizzo del Cisco VPN Concentrator 3005. Sono delineate le procedure per la configurazione del servizio con soluzioni che vogliono privilegiare l'aspetto della sicurezza attraverso l'uso dei certificati digitali.
Il seguente documento vuole essere una guida operativa per il LAN Manager che intende adottare questa soluzione.

PACS.: 89.70.+c

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

INDICE

Introduzione

Questo lavoro vuole essere una linea guida operativa relativamente alla configurazione del Cisco VPN Concentrator serie 3000, in uso attualmente nella Sezione INFN di Firenze. Questo appliance è stato scelto rispetto ad altre soluzioni proprietarie perché propone soluzioni VPN di nostro interesse per le caratteristiche di sicurezza offerte (utilizzo di IPSEC e certificati) e per l'economicità del prodotto.
Il lavoro si inserisce come approfondimento di argomenti presi in esame dal *Netgroup* INFN lo scorso dicembre 2003. In quella sede erano state testate varie funzionalità dell'oggetto in esame e confrontato con appliance di altri vendor e soluzioni freeware in modo da poter fornire una panoramica generale sulle soluzioni VPN disponibili al momento. In questa sede si è voluto approfondire l'aspetto della sicurezza di questa soluzione, in particolare attraverso l'utilizzo dei certificati digitali rilasciati dalla INFN Certification Authority, attualmente utilizzati in modo esteso all'interno dell'INFN per necessità diverse.

Virtual Private Network ed IPSec

VPN

Il termine VPN di per sè non identifica una particolare tecnologia, ma indica diversi tipi di implementazioni di varie tecnologie che come risultato hanno la creazione di una rete privata di calcolatori che fisicamente possono fare parte di reti diverse, distanti fra loro e topologicamente eterogenee. Una VPN è quindi una sorta di rete logica privata, un canale di comunicazione tra due o più nodi di rete che possono condividere fra loro l'utilizzo di un mezzo *untrusted* (rete Internet), ed utilizzarlo per una comunicazione privata.
Spesso le VPN vengono utilizzate per consentire ad un nodo esterno ad una LAN di potersi connettere all'interno della stessa e condividerne tutte le risorse anche confidenziali e private come se fosse direttamente collegato al suo interno.
È pertanto estremamente importante utilizzare tecnologie opportune che consentano ad una VPN di fornire un elevato grado di sicurezza in modo da proteggere l'integrità dei dati che vi transitano, ed è per questo motivo che abbiamo scelto di utilizzare il protocollo IPSec nella configurazione della VPN.

IPSec

IPSec rappresenta un insieme di protocolli che implementano la crittografia a livello di *network layer* per fornire un servizio di autenticazione (*non repudiation*) e confidenzialità (*encryption*). IPSec è in grado di proteggere i protocolli di livello superiore (TCP, UDP) autenticando il pacchetto IP che li contiene ed il relativo payload.
IPSec fornisce tre tipologie principali di comunicazione:

- Client to network
- Network to network
- Client to client

La tipologia *client to network* è tipicamente associata con soluzioni di VPN ad accesso remoto. Ad un determinato client viene fornito un software che consente di stabilire una connessione IPSec ad un *vpn concentrator* o *vpn gateway* connesso ad una data LAN privata. Tipicamente un client può quindi stabilire un connessione a internet tramite un ISP (Internet Service Provider) locale e stabilire successivamente una VPN IPSec protetta con la LAN remota sulla quale intende lavorare, avendo così virtualmente a disposizione tutte le risorse. Questo è il caso di nostro interesse.

Gli elementi che stanno alla base di IPSec sono:

- **SA (Security Association):** è il fondamento vero e proprio di una VPN IPSec. Rappresenta un insieme di proprietà di comunicazione che forniscono un relazione tra due o più sistemi in modo da costruire un'unica connessione (VPN). Sono richieste due SA per ogni connessione per una comunicazione di tipo bi-direzionale. A sua vola una SA è definita da:
    - **SPI (Security Parameter Index):** è un numero che identifica il flusso di dati attraverso la VPN IPSec, e serve per discriminare le varie SA relative ad una connessione IPSec.
    - **AH (Authentication Header, proto 51):** è un protocollo utilizzato per fornire integrità dei dati e autenticazione dell'origine per i pacchetti IP.
    - **ESP (Encapsulated Security Payload, proto 50):** è un protocollo che fornisce analoghi servizi di sicurezza di AH ma in più fornisce confidenzialità nella comunicazione utilizzando l'encryption (HMAC-MD5, HMAC-SHA).
- **IKE (Internet Key Exchange):** è il protocollo di gestione automatica per lo scambio delle chiavi necessario per tutte le operazione di security fornite da IPSec.

I protocolli AH e ESP possono essere utilizzati per proteggere l'intero pacchetto IP o solamente il suo contenuto. 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.

Modalità Tunnel e Trasporto

Nella modalità tunnel l'intero pacchetto originario viene incapsulato, cifrato e vengono aggiunti in testa un nuovo header IP e l'Authentication Protocol header (ESP/AH), come mostrato in Fig. 1

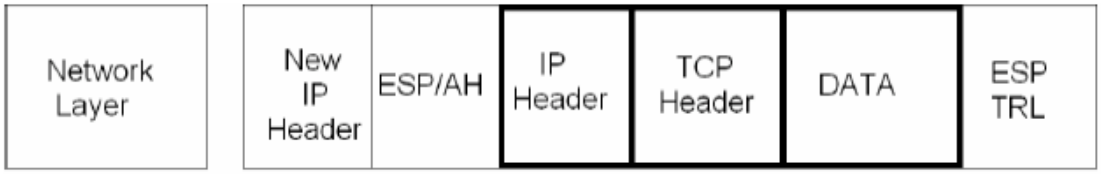


Fig. 1. IPSec in modalità Tunnel.

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 e 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.
Si tratta dunque di una soluzione host-to network o network-to-network VPN.

Nella modalità trasporto 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 (Fig.2).

Fig. 2. IPSec in modalità Tunnel.

Cisco VPN Concentrator 3005: configurazione

Sul CISCO VPN Concentrator serie 3005, vpnbox.fi.infn.it, è attualmente installata la versione 4.1.7 Rel-K9. La configurazione iniziale delle interfacce di rete pubblica e privata è stata impostata attraverso la console seriale, il resto della configurazione è stata eseguita utilizzando il *VPN Concentrator Manager*, l'interfaccia di gestione tramite web.
L'architettura di rete utilizzata è mostrata in Fig. 3.

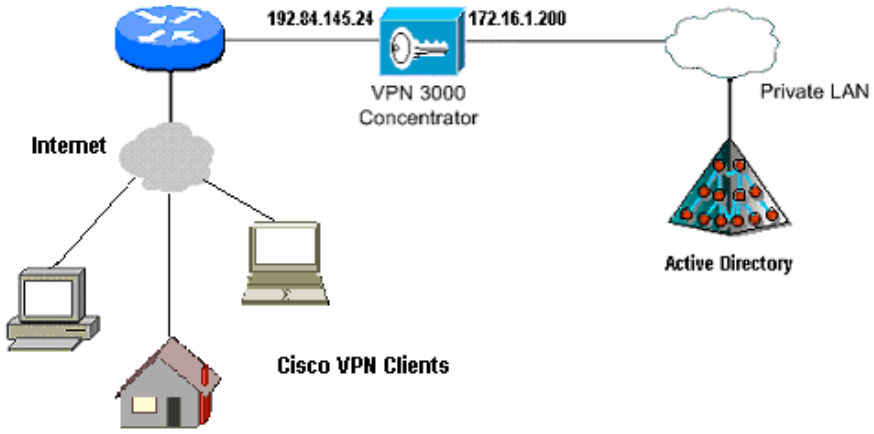


Fig. 3. Architettura di rete.

Nella parte iniziale di configurazione del vpnbox vanno impostate le due interfacce di rete, una pubblica ed una privata, il DNS ed il nome di dominio, come mostrato in Fig. 4. Nella nostra configurazione è stata impostata la gestione del VPN box solo attraverso l'interfaccia di rete privata.

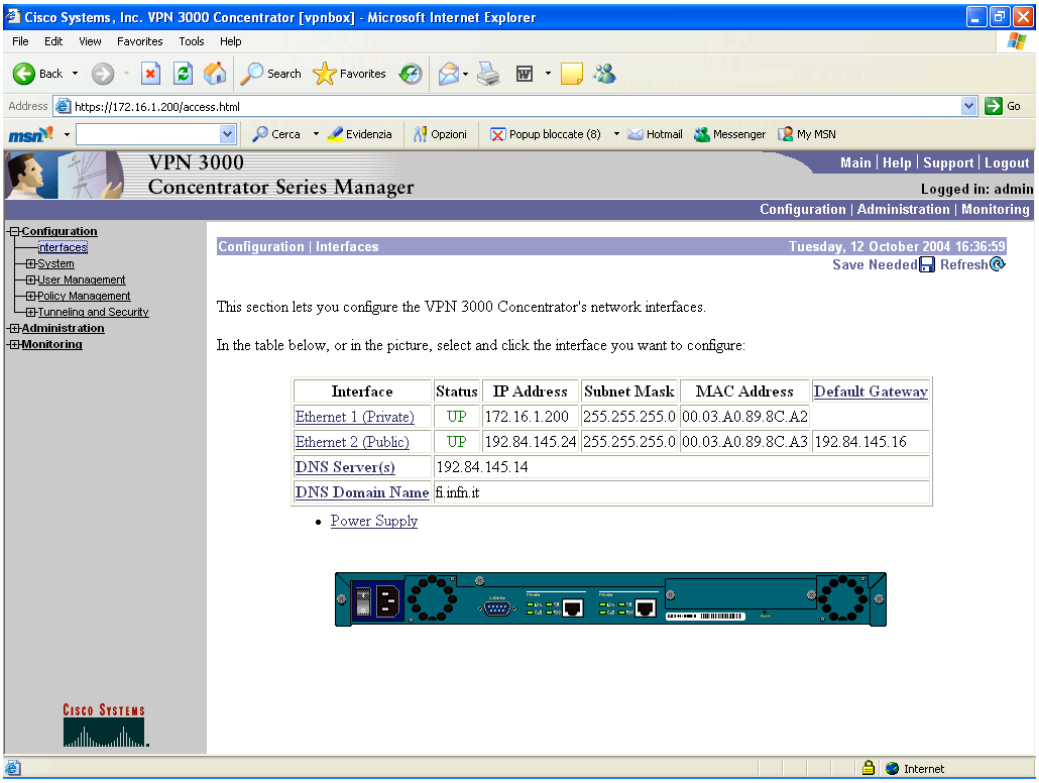


Fig. 4: configurazione delle interfacce di rete.

Le proprietà in dettaglio delle due interfacce sono mostrate in Fig. 5 e 6.

Configuring Ethernet Interface 1 (Private).

General | RIP | OSPF | Bandwidth | WebVPN

General Parameters			
Sel	**Attribute**	**Value**	**Description**
○	**Disabled**		Select to disable this interface.
○	**DHCP Client**		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.
◉	**Static IP Addressing**		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address	172.16.1.200	
	Subnet Mask	255.255.255.0	
	Public Interface	☐	Check to make this interface a "public" interface.
	MAC Address	00.03.A0.89.8C.A2	The MAC address for this interface.
	Filter	1. Private	Select the filter for this interface.
	Speed	100 Mbps	Select the speed for this interface.
	Duplex	Auto	Select the duplex mode for this interface.
	MTU	1200	Enter the Maximum Transmit Unit for this interface (68 - 1500).
	Public Interface IPSec Fragmentation Policy	○ Do not fragment prior to IPSec encapsulation; fragment prior to interface transmission ◉ Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP) ○ Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF bit)	

Apply Cancel

Fig. 5. Configurazione Ethernet Interface 1 (private).

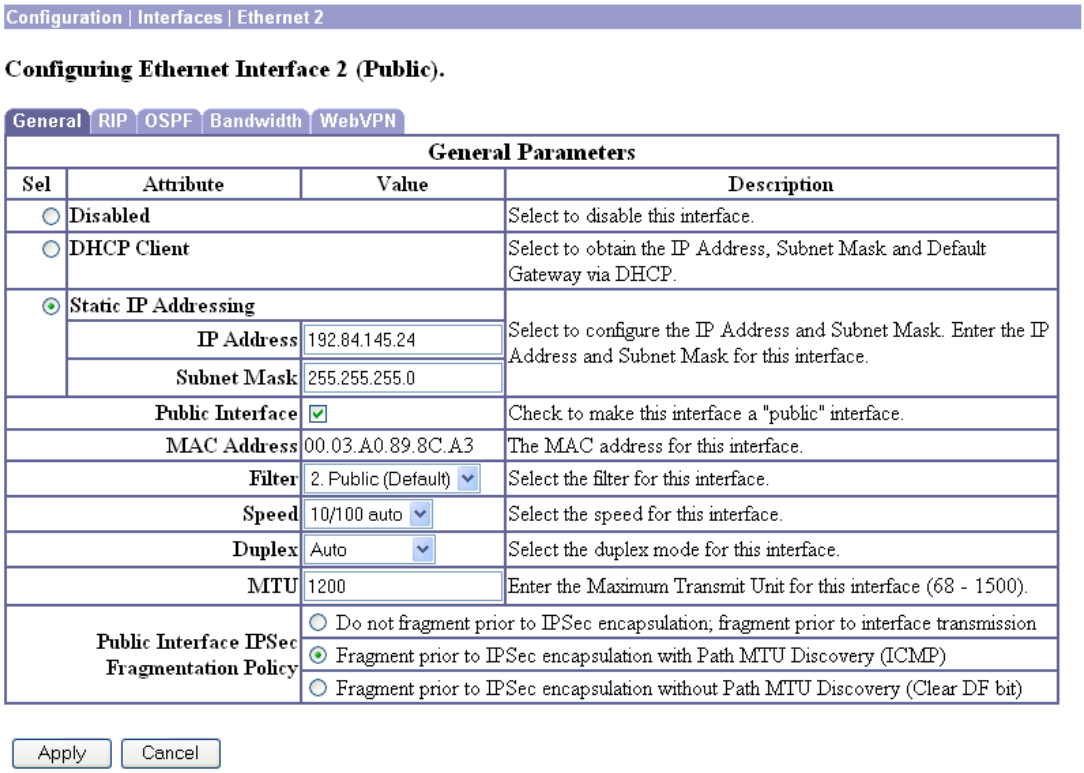


Fig. 6. Configurazione Ethernet Interface 2 (public).

Nella sezione **Configuration** > **Policy Management** > **Traffic Management** >**Filters** è infatti possibile creare regole e filtri per ogni interfaccia di rete. Ogni filtro può bloccare oppure consentire il traffico attraverso le interfacce in base a determinate regole.

Nella sezione **IP Routing** > **Default Gateways** vengono definiti il *Default Gateway,* che generalmente coincide con l'ip address del default router *dell'interfaccia pubblica*, ed il *Tunnel Default Gateway*, l'ip address del default router *dell'interfaccia privata*, ossia il default gateway per i client che si collegano con la VPN. L'impostazione è mostrata in Fig. 7:

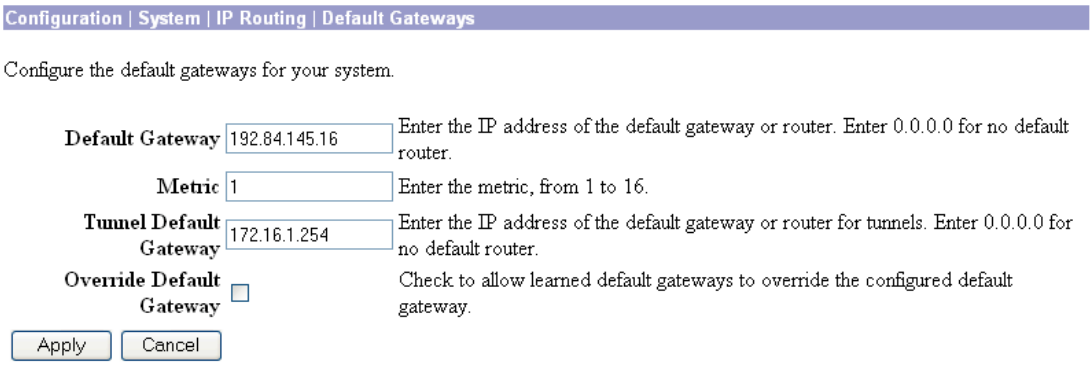


Fig. 7. Configurazione del Default Gateway.

Nella sezione **IP Routing** > **Static Routes** viene definita automaticamente una route statica di default che coincide con le impostazioni dei Default Gateway dell'interfaccia pubblica e privata.

Nella sezione **Configuration** > **System** > **Address Management > Assignment** è stato impostato l'utilizzo di un range di indirizzi da assegnare ai client che si collegano in VPN (**Use Address Pools**), mentre nella sezione **Pools** è stato definito l'intervallo di indirizzi IP 172.16.1.201 - 172.16.1.211 che veranno assegnati agli utenti che si collegheranno in VPN.

Nella sezione **Configuration** > **System** > **Management Protocols** vengono configurati i protocolli di accesso all'interfaccia di management (Telnet, SNMP, HTTP, ecc.).

Nella sezione **Configuration** > **System > Events** si può configurare la gestione degli eventi a livello di syslog, notifica via email e trap SNMP. In particolare in **Configuration** > **System > Events > Classes** si impostano i tipi di eventi da monitorare. Quelli che abbiamo impostato per avere un log completo in caso di problemi sono stati CERT 1-13, IKE 1-6, IKEDBG 1-10, IPSEC 1-6, IPSECDBG 1-10.

Il Cisco VPN Concentrator è stato configurato per accettare connessioni client in VPN attraverso IPSec con autenticazione su Active Directory (Windows Server 2003 domain controller sul dominio INFN-FI) oppure autenticazione PKI con utilizzo di certificati rilasciati dall'INFN Certification Authority.
La configurazione generale del Cisco VPN Concentrator appena descritta è indipendente dal tipo di autenticazione utilizzato per il client.

Utilizzo di IPSec con autenticazione su Active Directory

Per effettuare autenticazione con Active Directory sono necessarie alcune impostazioni sul domain controller; nel nostro caso il domain controller giove.fi.infn.it ha come sistema operativo Microsoft Windows Server 2003.
In *Active Directory Users and Computers* per gli utenti abilitati ad utilizzare la connessione VPN va impostato la proprietà *Allow access* nella sezione *Dial-in / Remote Access Permission.*

Sul Cisco VPN Concentrator nella sezione **Configuration** > **System** > **Servers** > **Authentication** vengono configurati i server di autenticazione per gli utenti VPN. Può essere impostata l'autenticazione tramite server RADIUS, dominio NT, SDI (Security Dynamics International) server , Kerberos/Active Directory. La nostra impostazione è stata quella di definire un NT Domain, come mostrato in Fig. 8 e 9. Il Cisco VPN box ha per default un tipo di autenticazione definita come *Internal Server* che utilizza per autenticare gli utenti e gruppi interni e gli utenti che utilizzano un certificato.

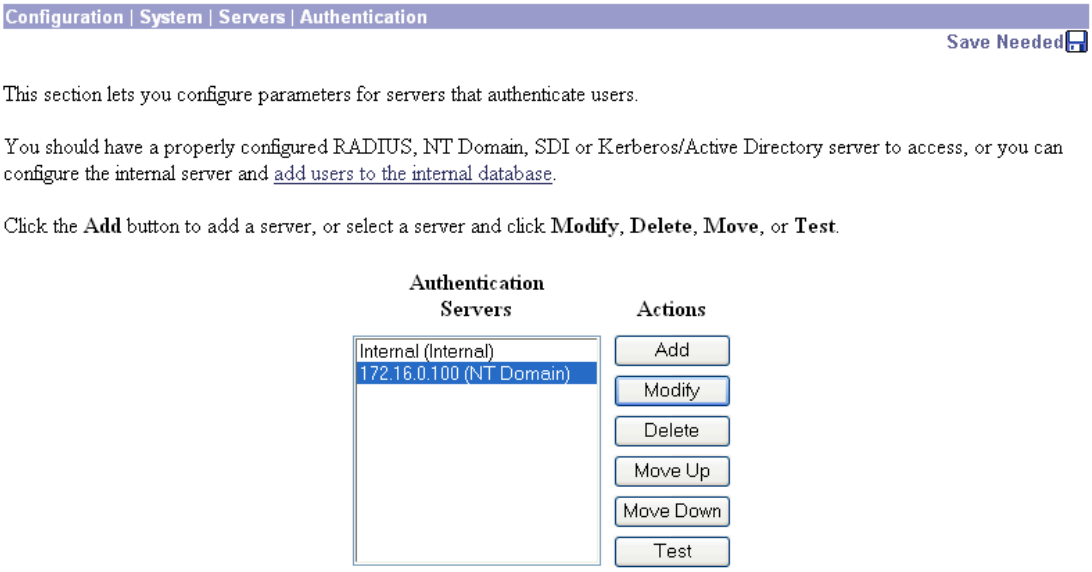


Fig. 8. Impostazione server di autenticazione.

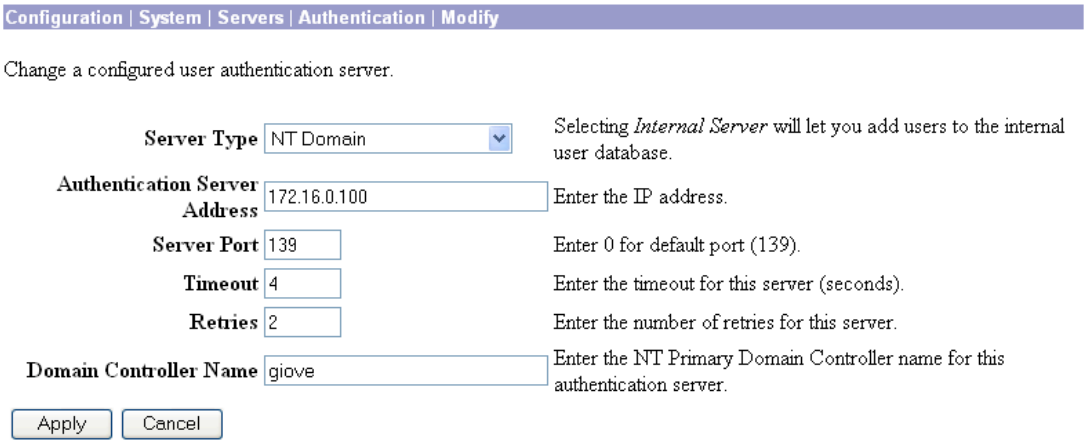


Fig. 9. NT Domain come Autentication Server.

In **Configuration** > **User Management** vengono impostate le proprietà del *Base Group* e degli altri gruppi creati, che ereditano le proprietà del gruppo di base.
Le proprietà del gruppo base che abbiamo impostato sono mostrate in Fig. 10 ed 11.

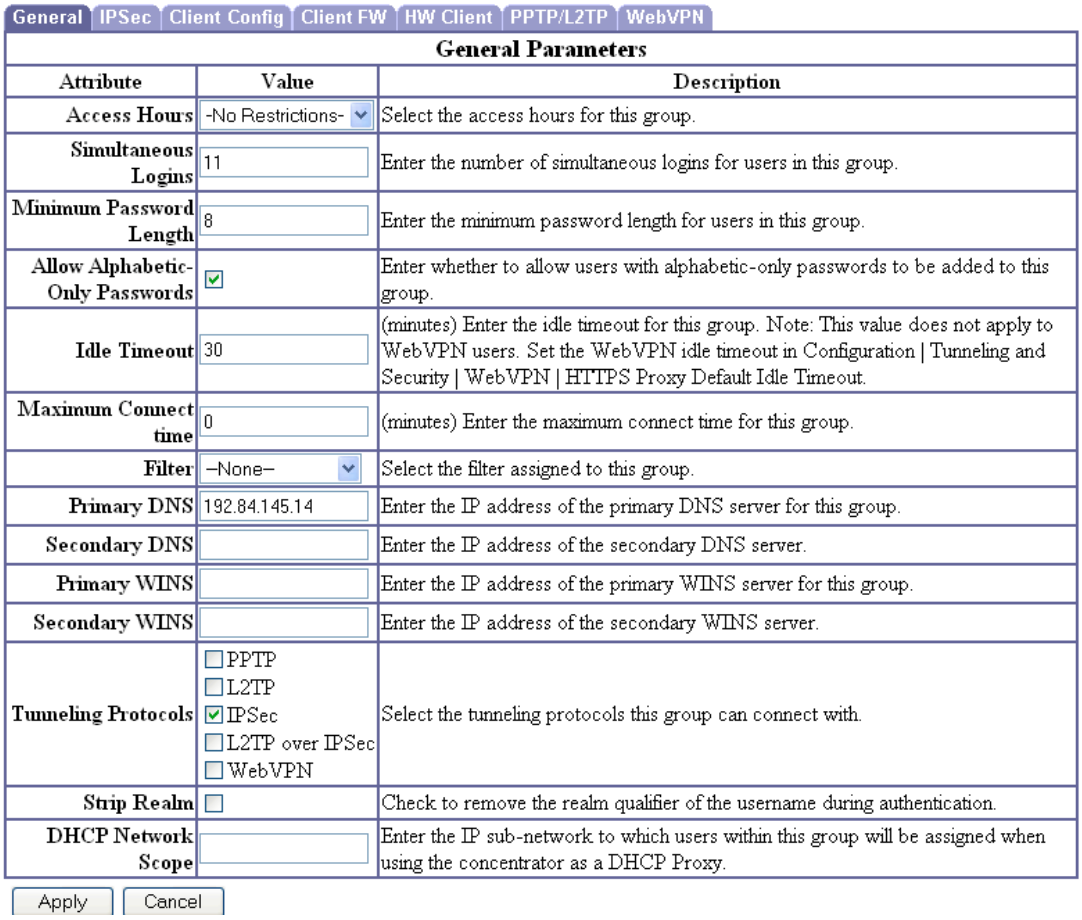


Fig. 10. Proprietà del Base Group.

General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN

IPSec Parameters		
Attribute	**Value**	**Description**
IPSec SA	ESP-3DES-MD5	Select the IPSec Security Association assigned to this group.
IKE Peer Identity Validation	If supported by certificate	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	Check to enable the use of IKE keepalives for members of this group.
Confidence Interval	300	(seconds) Enter how long a peer is permitted to idle before the VPN Concentrator checks to see if it is still connected.
Tunnel Type	Remote Access	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters		
Group Lock	☐	Lock the users into this group.
Authentication	NT Domain	Select the authentication method for members of this group. This parameter does not apply to **Individual User Authentication**.
Authorization Type	None	If members of this group need authorization in addition to authentication, select an authorization method. If you configure this field, you must also configure an Authorization Server.
Authorization Required	☐	Check to require successful authorization.
DN Field	CN otherwise OU	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.
IPComp	None	Select the method of IP Compression for members of this group.
Default Preshared Key		Enter the preshared key to be used with clients that do not support groups.

Fig.11. Sezione IPSEC del Base Group.

In **Configuration** > **User Management** > **Groups** abbiamo creato il gruppo specifico per l'autenticazione con il domain controller, *VPNDomainUsers*. Di questo gruppo sono state impostate nella sezione *Identity* una password (che viene usata come preshared-key IPSec dal client VPN) ed il tipo di autenticazione *Internal*.

Configuration | User Management | Groups | Modify VPNDomainUsers

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN

Identity Parameters		
Attribute	**Value**	**Description**
Group Name	VPNDomainUsers	Enter a unique name for the group.
Password	••••••••••••••••	Enter the password for the group.
Verify	••••••••••••••••	Verify the group's password.
Type	Internal	*External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator's Internal Database.

Apply | Cancel

Fig.12. Configurazione di una pre-shared key per il gruppo VPNDomainUsers.

Nella sezione *IPSec* è stata impostata IPSec SA 3DES-MD5, precedentemente creata nella sezione specifica, tipo di tunnel *Remote Access*, autenticazione *NT Domain*.

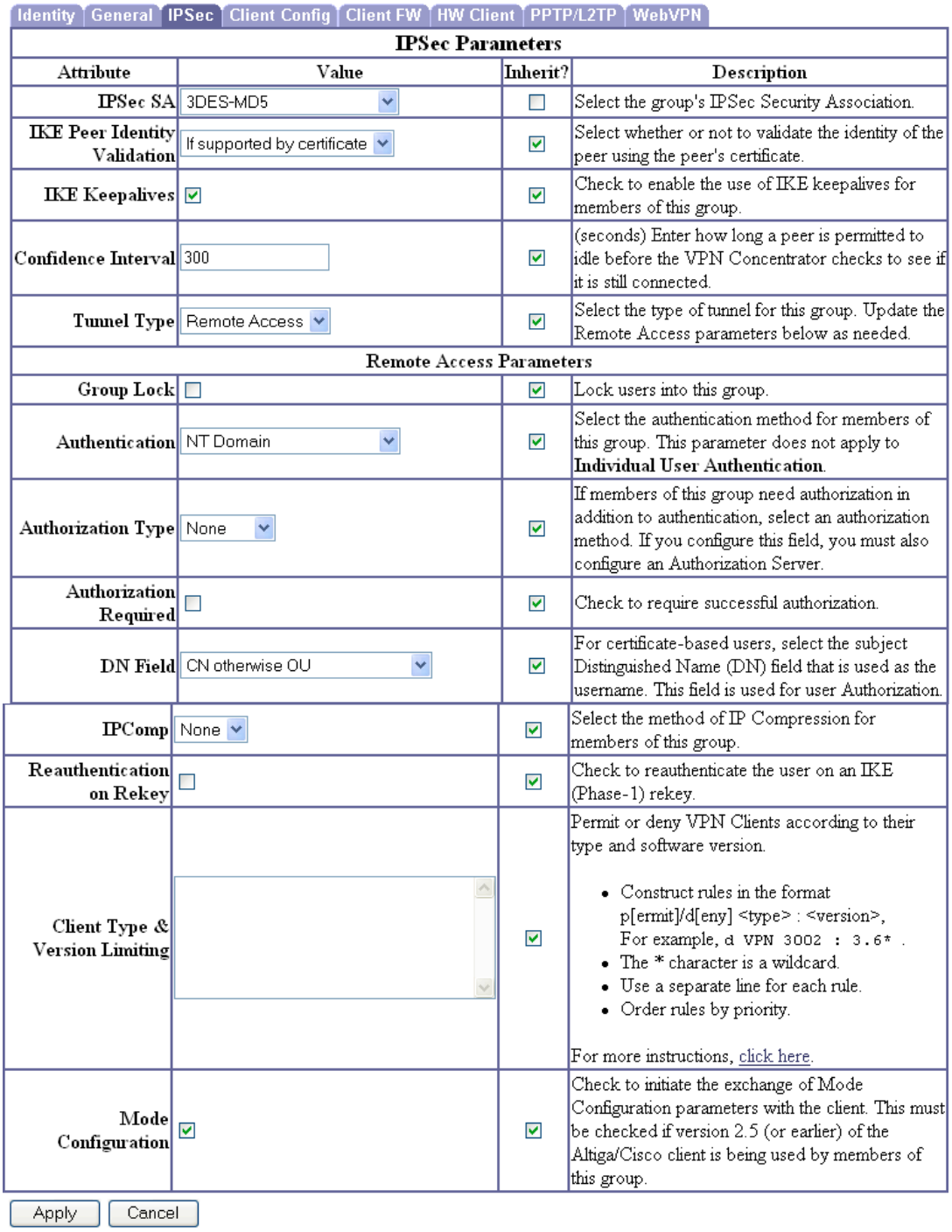


Fig.13. Sezione IPSec per il gruppo VPNDomainUsers.

IKE Proposal e Security Associations

Nella sezione **Configuration** > **System** > **Tunneling Protocols** > **IPSec** > **IKE Proposals** sono stati attivati i proposal opportuni, in particolare per l'IKE-3DES-MD5 è stato impostato un *authentication mode* appropriato, come mostrato nelle Fig. 14 e 15. È stato poi impostato un determinato ordine degli *active proposals* in quanto il sistema sceglie quelli che soddisfano le Security Association impostate, scandendoli nell'ordine impostato.

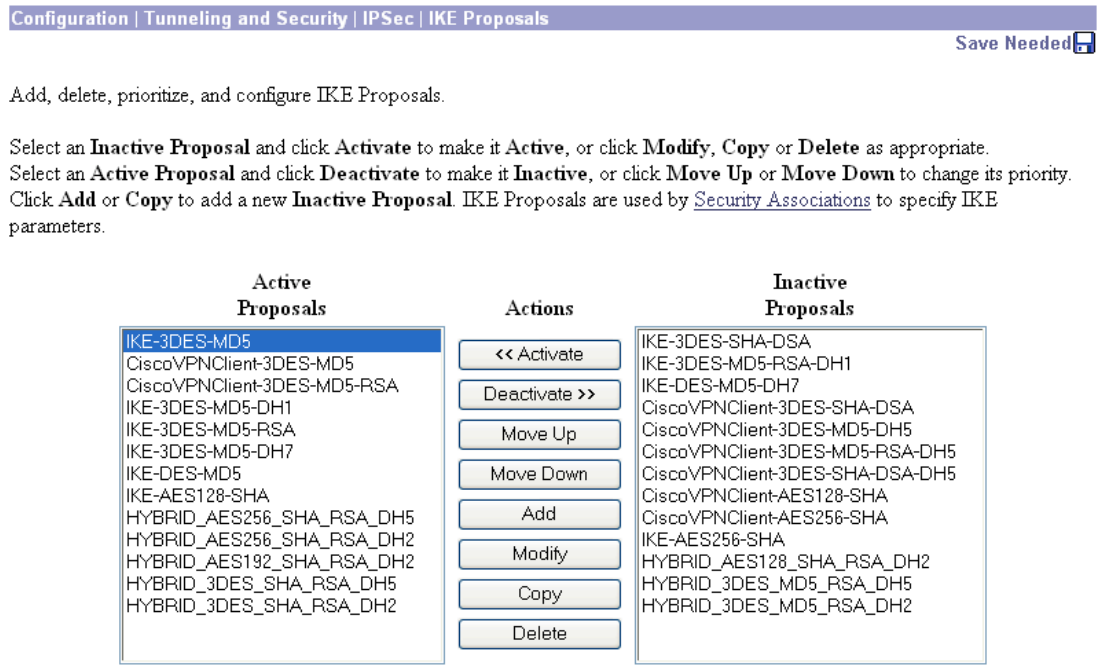


Fig.14. Elenco dei proposals attivi e inattivi.

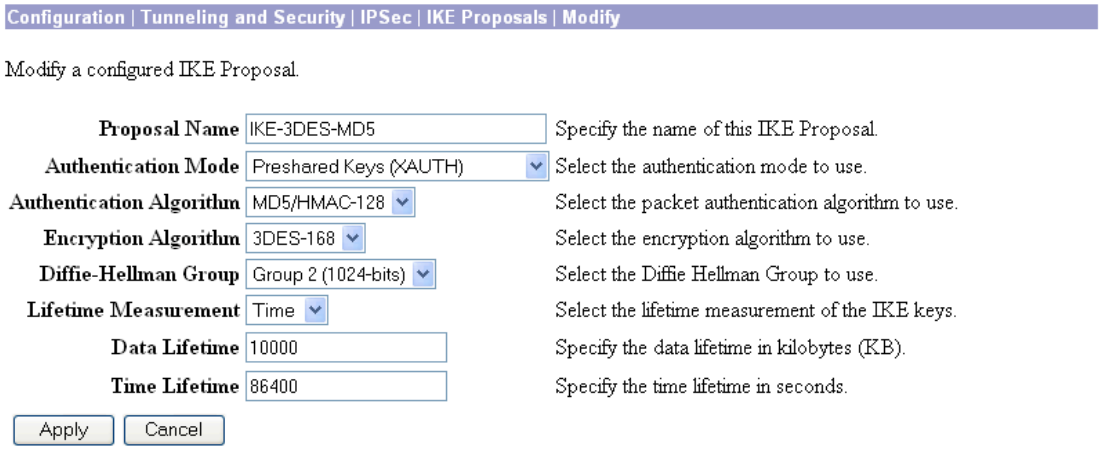


Fig.15. Proprietà del Proposal IKE-3DES-MD5.

Nella sezione **Configuration** > **Policy Management** > **Traffic Management** > **Security Associations** è presente la lista delle Security Associations (Fig. 16). Per consentire l'autenticazione attraverso le *preshared keys* è stata creata la SA 3DES-MD5 (Fig. 17). È importante notare che nelle proprietà della SA creata i parametri IKE devono essere impostati in modo da utilizzare una preshared key nel campo *Digital Certificate* e di utilizzare un IKE proposal che abbia lo stesso metodo di autenticazione.

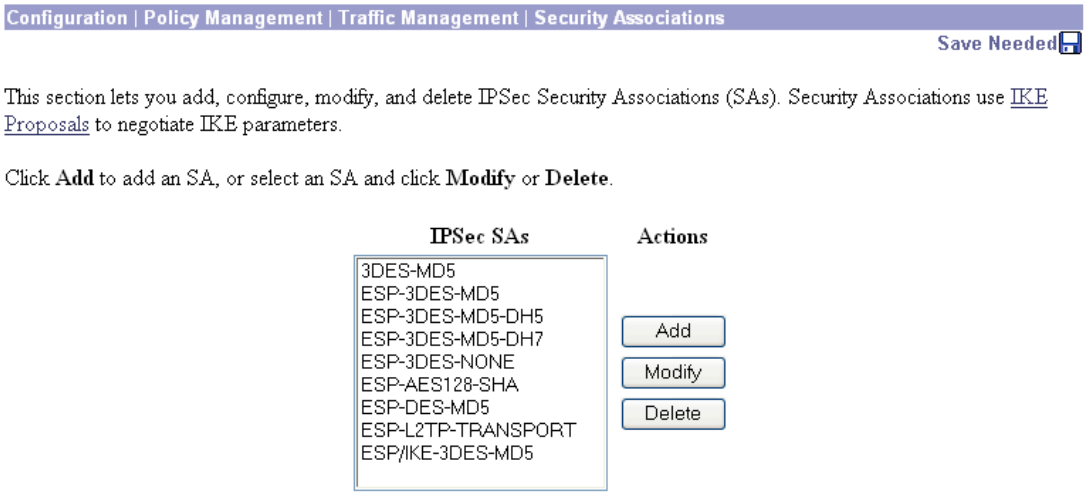


Fig. 16. Lista delle Security Associations.

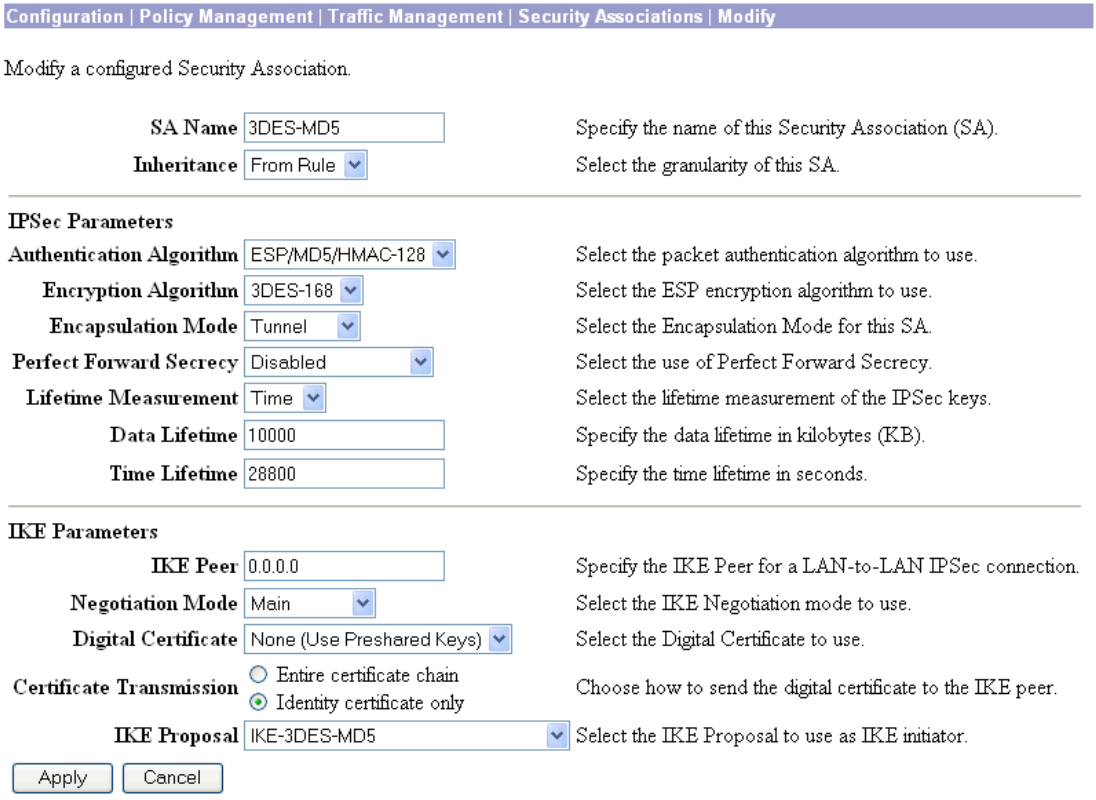


Fig. 17. Creazione della Security Association 3DES-MD5.

VPN IPSec con autenticazione tramite certificati digitali

Per utilizzare l'autenticazione tramite certificato digitale occorre installare come prima cosa il certificato della *Certification Authority* che validerà l'identità dei certificati utenti, quindi il certificato per il VPN Concentrator. Per quest'ultimo occorre effettuare l'*enrollment* del certificato host per vpnbox.fi.infn.it. La richiesta di certificato così sottomessa deve essere firmata dalla CA.
All'interno del Cisco VPN Concentrator nella sezione **Administration** > **Certificate Management** > può essere installato un certificato di una qualunque CA.
Abbiamo testato tre diverse configurazioni: la prima basata su una CA Microsoft, la seconda basata su una CA creata con *OpenSSL*, la terza (attualmente in produzione) basata su una vera Certification Authority, quella dell'INFN, consultabile al sito http://security.fi.infn.it/CA.

Certificati rilasciati da una CA Microsoft

Per utilizzare una Certification Authority Microsoft è stata utilizzata una macchina con sistema operativo Windows Server 2003, inserita nel dominio INFN-FI, dove sono stati installati i *Certificate Services* per gestire una CA ed il *Certificate Services Web Enrollment Support*.
Il certificato per la CA lo si può scaricare collegandosi al sito http://servername/certsrv e selezionando la voce '*Download a CA certificate, certificate chain, or CRL'*, come mostrato in Fig. 18.

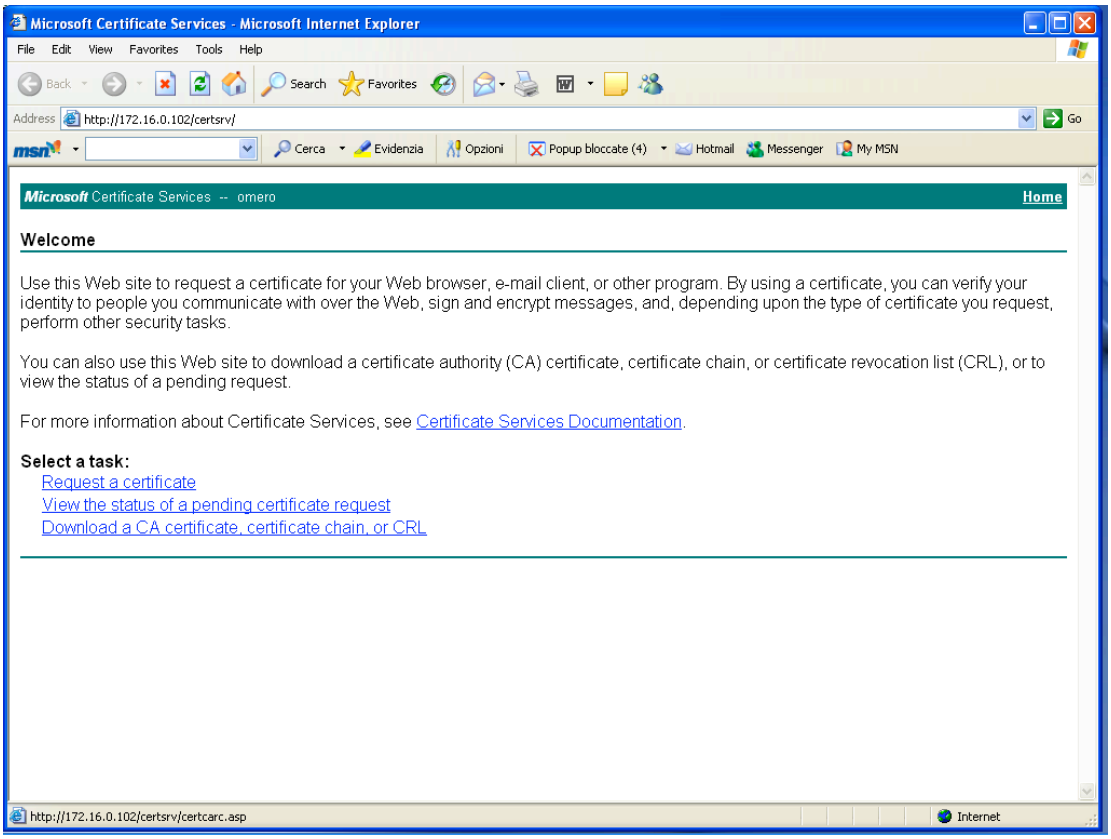


Fig. 18. Richiesta di un certificato ad una CA Microsoft.

Nella pagina seguente scegliere il metodo di *Encoding Base 64* e selezionare *Download CA certificate*; in questo modo viene scaricato un file *certnew.cer* in formato PEM che verrà successivamente importato all'interno del browser Internet Explorer.

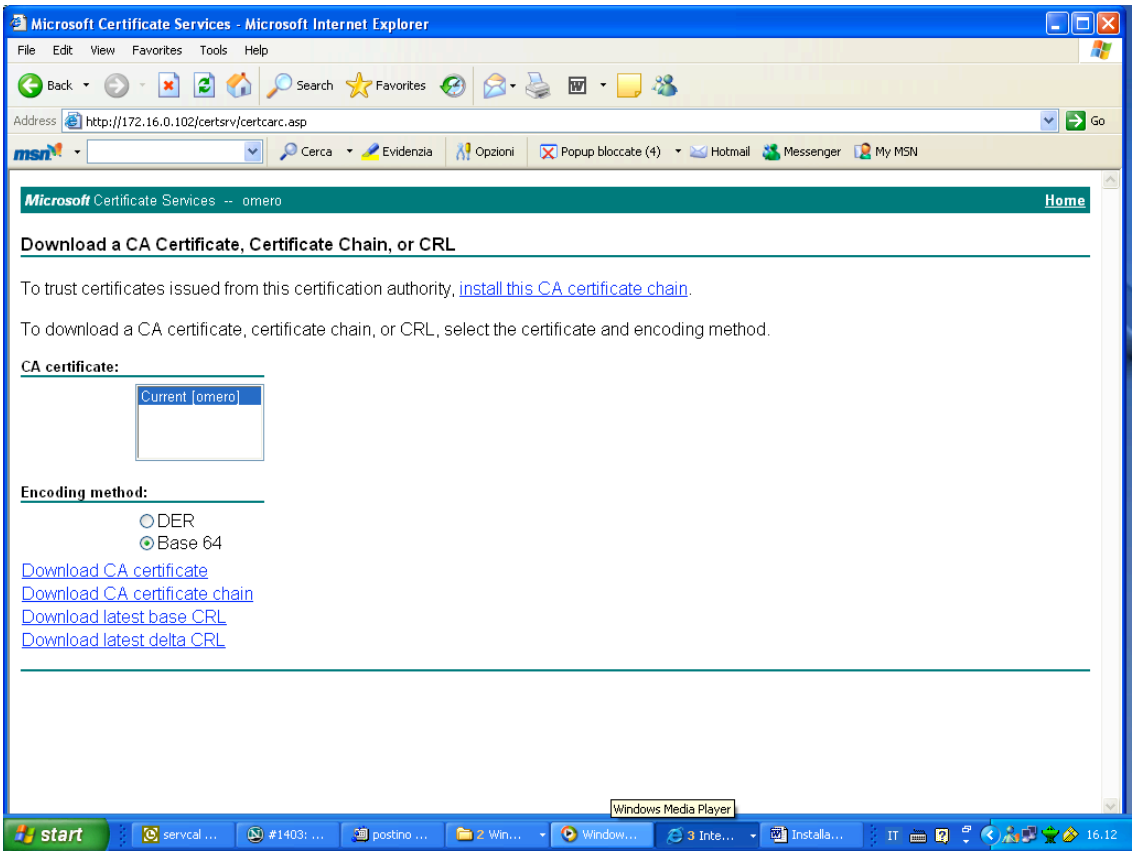


Fig 19. Download del certificato della CA.

A questo punto si richiede un certificato host per il VPN Concentrator tramite il form di enrollment in **Administration > Certificate Management > Enroll > Identity Certificate > PKCS10.**
Facendo riferimento alla Fig. 18 selezionare '*Request a Certificate'* e successivamente *'Advanced Certificate Request*'. A questo punto selezionare '*Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file'*. Inserire la richiesta di certificato generata tramite l'enrollment sul VPN Concentrator come mostrato in Fig. 20 selezionando un template opportuno per il certificato ed eseguire il *Submit* della richiesta.
Nel nostro caso abbiamo creato sulla CA Microsoft, utilizzando il *Certificate Template,* un template ad hoc chiamato *vpn_server*. Nelle proprietà del template, nella sezione *Subject Name* è stata selezionata l'opzione *Supply in the request* per poter utilizzare determinati campi nel certificato che siano riconosciuti dal VPN Concentrator.

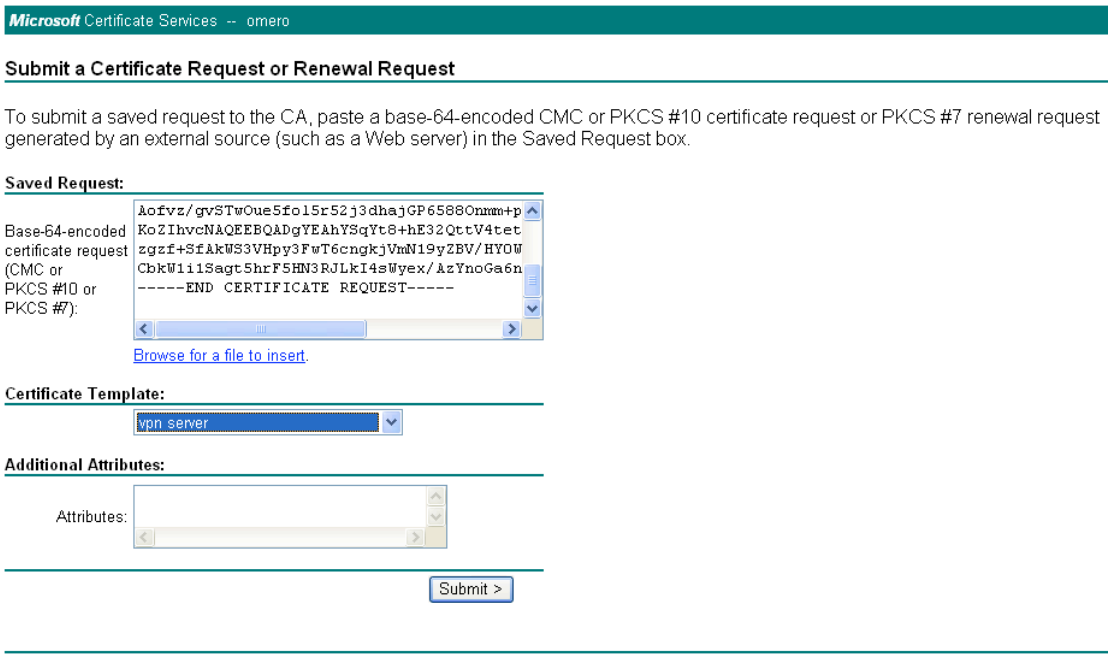
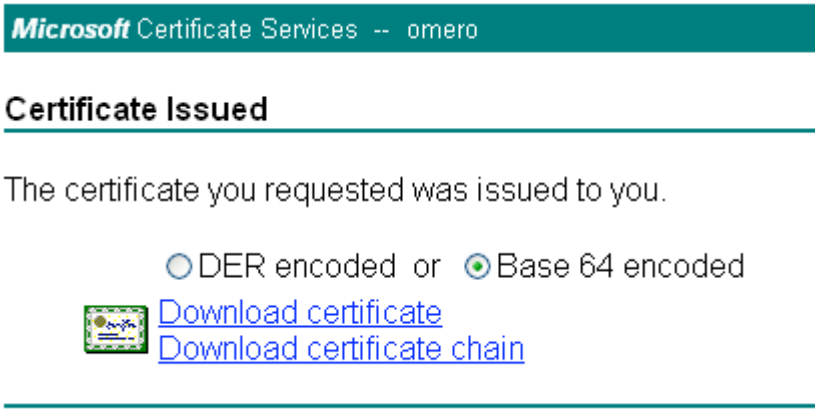


Fig. 20. Sottomissione di una richiesta di certificato.

A questo punto si esegue il download del certificato in formato *Base 64 encoded* e lo si installa sul Cisco VPN Concentrator nell'apposita sezione.



Per poter utilizzare l'autenticazione tramite certificati utilizzando il software CISCO VPN client è necessario richiedere un certificato utente. Per fare questo occorre collegarsi a http://servername/certsrv, selezionare '*Request a Certificate'* e scegliere '*User Certificate'*. Scaricare ed installare il certificato così ottenuto.

Certificati gestiti tramite OpenSSL

Prima di tutto bisogna creare una Certification Authority. A tal fine si utilizza lo script *CA.sh* presente nelle distribuzioni di OpenSSL.

```
> CA.sh –newca
CA certificate filename (or enter to create)

Making CA certificate ...
Generating a 1024 bit RSA private key
..............................++++++
.....................................++++++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IT
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:Firenze
Organization Name (eg, company) [Internet Widgits Pty
Ltd]:INFN
Organizational Unit Name (eg, section) []:myCA
Common Name (eg, YOUR name) []:Riccardo Veraldi
Email Address []:Riccardo.Veraldi@fi.infn.it
```

A questo punto si può procedere con la richiesta di certificato per il VPN Concentrator utilizzando la procedura di *enrollment* in **Administration > Certificate Management > Enroll > Identity Certificate > PKCS10**.

Si salva la richiesta di certificato in un file *vpnbox.pem* e si firma utilizzando OpenSSL:

```
> openssl ca -policy policy_anything -out vpnbox.crt -
infiles vpnbox.pem
```

Nel file *vpnbox.crt* sarà contenuto il certificato da installare sul VPN Concentrator.

Occorre ora richiedere un certificato personale per l'utente client della VPN:

```
> openssl req -new -keyout veraldi.key -out veraldi.pem -
nodes -days 365
```

e successivamente firmarlo:

```
> openssl ca -policy policy_anything -out veraldi.crt -
infiles veraldi.pem
```

a questo punto occorre trasformare il certificato appena rilasciato in formato pkcs12:

```
> openssl pkcs12 -export -out veraldi.p12 -inkey
veraldi.key  -in veraldi.crt
```

Il certificato così esportato può essere importato all'interno del browser Internet Explorer per essere utilizzato in fase di autenticazione da parte del CISCO VPN Client.

Certificati rilasciati dall'INFN CA

Nel nostro sistema in produzione abbiamo installato il certificato dell'INFN CA. Per fare questo nella sezione **Administration > Certificate Management** selezionare la voce relativa all'installazione di un certificato e successivamente di un certificato di una CA. E' stata scelta la modalità *Cut & Paste Text*.
In **Administration > Certificate Management > Enrollment** selezionare *Enroll via PKCS10 Request (Manual)*. Abbiamo successivamente impostato i campi della richiesta di certificato come mostrato in Fig. 21.

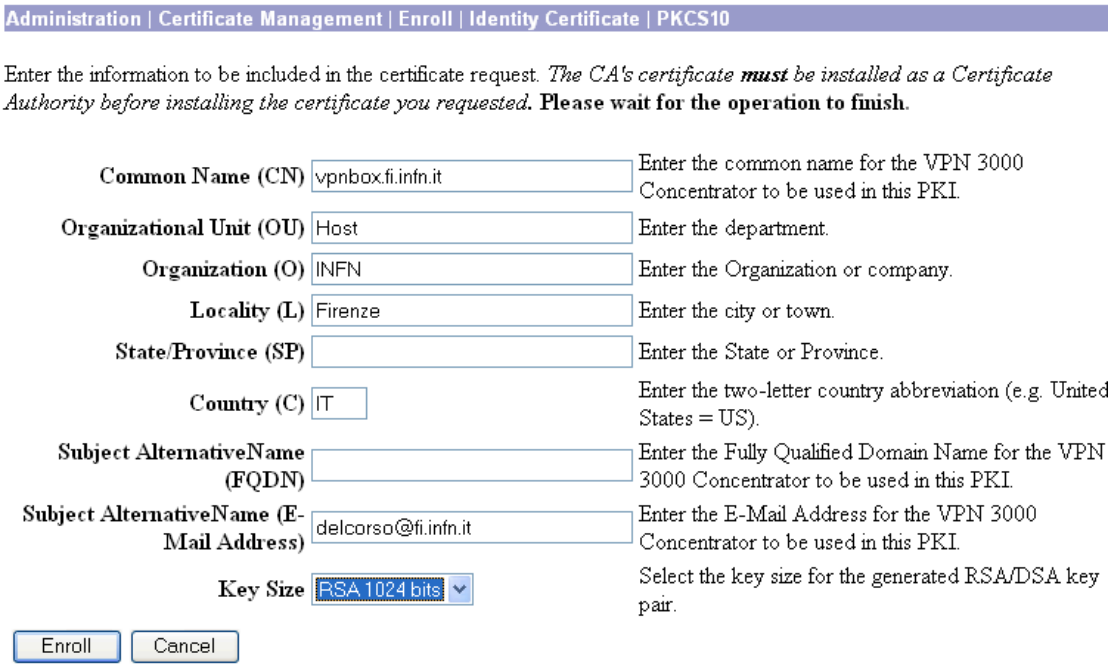


Fig. 21. Informazioni incluse nella richiesta di certificato.

Abbiamo inviato la richiesta all'INFN CA e successivamente abbiamo installato il certificato rilasciato selezionando in **Administration > Certificate Management** l'opzione di installazione del certificato associato all'*Enrolment Status*.
La configurazione finale è quella mostrata in Fig. 22:

Certificate Authorities [View All CRL Caches | Clear All CRL Caches] (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
INFN Certification Authority at INFN	INFN Certification Authority at INFN	09/18/2007	No	View | Configure | Delete

Identity Certificates (current: 1, maximum: 5)

Subject	Issuer	Expiration	Actions
vpnbox.fi.infn.it at INFN	INFN Certification Authority at INFN	10/12/2005	View | Renew | Delete

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	No Certificate Installed.			Generate | Enroll | Import
Public	No Certificate Installed.			Generate | Enroll | Import

SSH Host Key

Key Size	Key Type	Date Generated	Actions
No SSH Host Key			

Enrollment Status [**Remove All:** Errored | Timed-Out | Rejected | Cancelled | In-Progress] (current: 0 available: 5)

Subject	Issuer	Date	Use	Reason	Method	Status	Actions
No Enrollment Requests							

Fig. 22. Certificati installati sul Cisco VPN Concentrator in produzione.

Nella sezione **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals** è stato attivato il proposal *CiscoVPNClient-3DES-MD5-RSA* ed è stato scelto un *authentication mode* appropriato per l'autenticazione RSA con certificato (Fig. 23). È stato inoltre impostato un ordine opportuno degli *active proposals* in quanto il sistema sceglie i proposal scandendoli nell'ordine dall'alto al basso fino ad incontrare quello che soddisfa le Security Associations impostate.

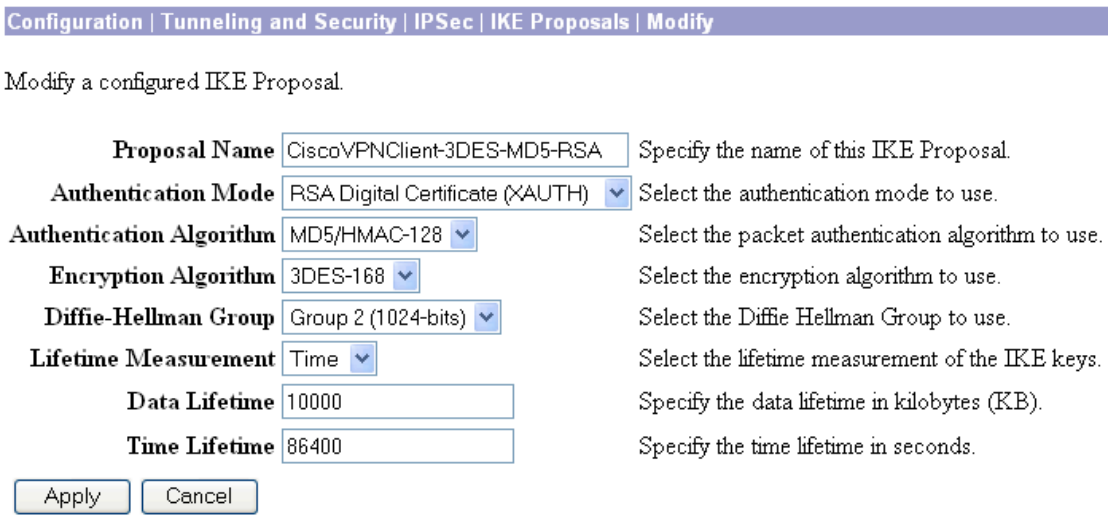


Fig. 23. Proprietà dell'IKE proposal CiscoVPNClient-3DES-MD5-RSA.

Nella sezione **Configuration** > **Policy Management** > **Traffic Management** > **Security Associations** è presente la lista delle Security Associations. Per consentire l'autenticazione attraverso i certificati è stata modificata la SA ESP-3DES-MD5 (Fig. 24). È importante notare che nelle proprietà della SA creata, i parametri IKE devono essere impostati in modo da utilizzare il certificato host del VPN Concentrator nel campo *Digital Certificate* ed un IKE Proposal che abbia lo stesso metodo di autenticazione cioè il CiscoVPNClient-3DES-MD5-RSA.

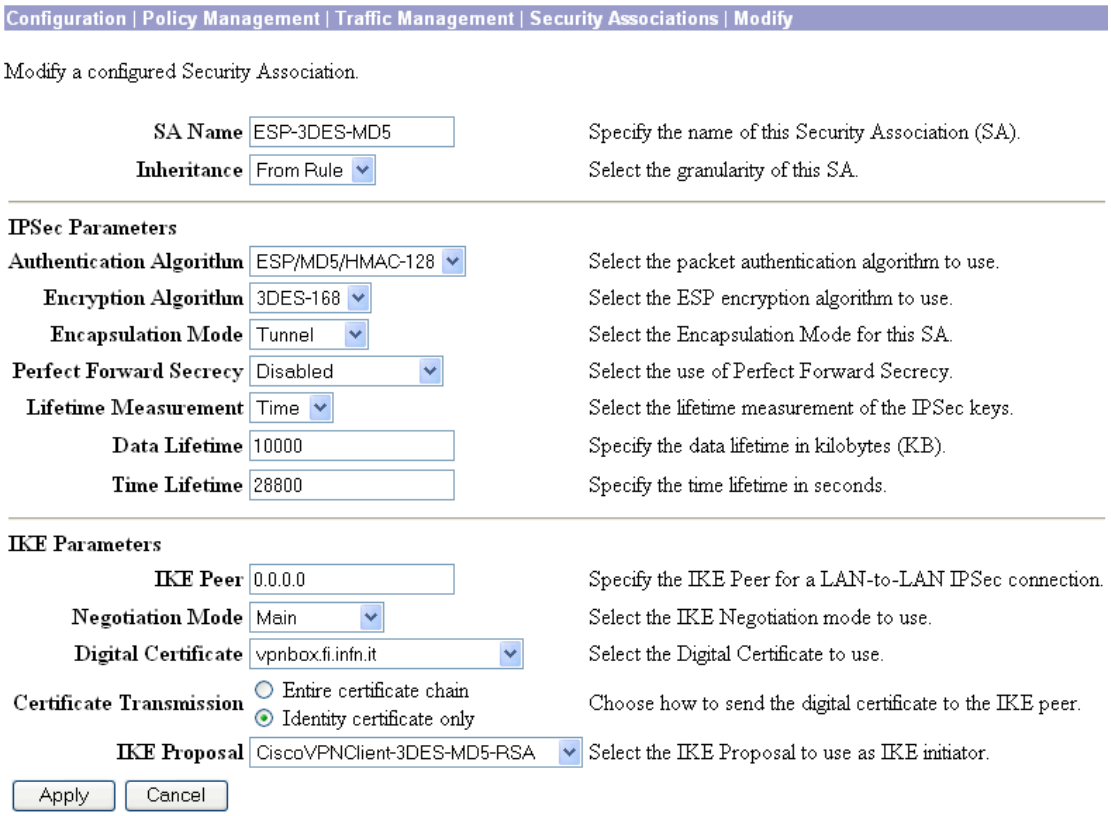


Fig.24. Proprietà della SA ESP-3DES-MD5.

Bisogna quindi creare un nuovo gruppo relativo agli utenti che utilizzano il certificato. Abbiamo così creato il gruppo *servcal* in **Configuration** > **User Management** > **Groups**, le cui proprietà sono mostrate in Fig. 25 e 26. In particolare nella sezione IPSec bisogna selezionare una SA (ESP-3DES-MD5) che faccia parte degli IKE Proposal che utilizzano il certificato come mostrato precedentemente.
È importante notare che il nome di questo gruppo deve corrispondere al campo OU del certificato utente perché per default è impostata in **Configuration > Policy Management > Certificate Group Matching > Policy** la policy *Obtain Group from OU*. Se questa impostazione automatica viene rimossa questo vincolo decade e può essere scelto un nome per il campo OU del certificato diverso dal nome del gruppo. Noi abbiamo fatto questa scelta.

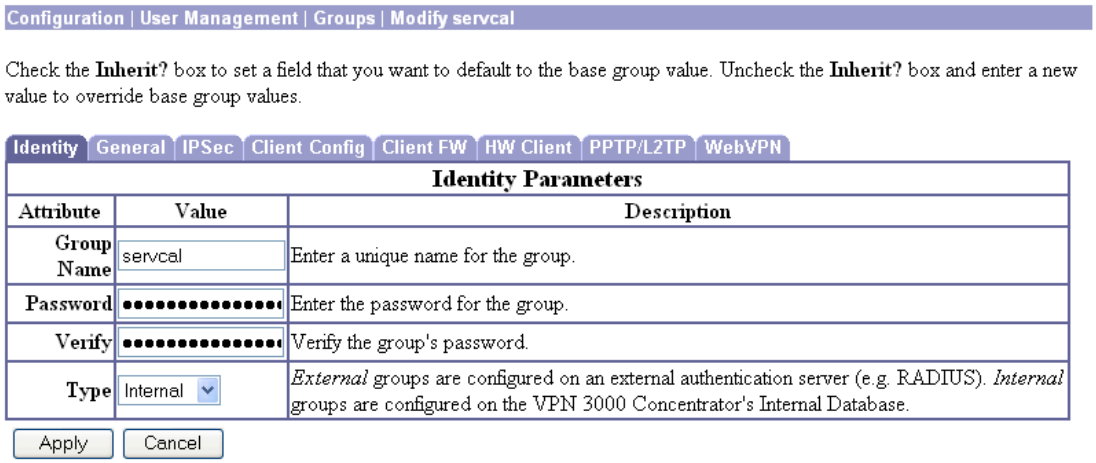


Fig. 25. Proprietà di u nuovo gruppo per gli utenti che utilizzano PKI.

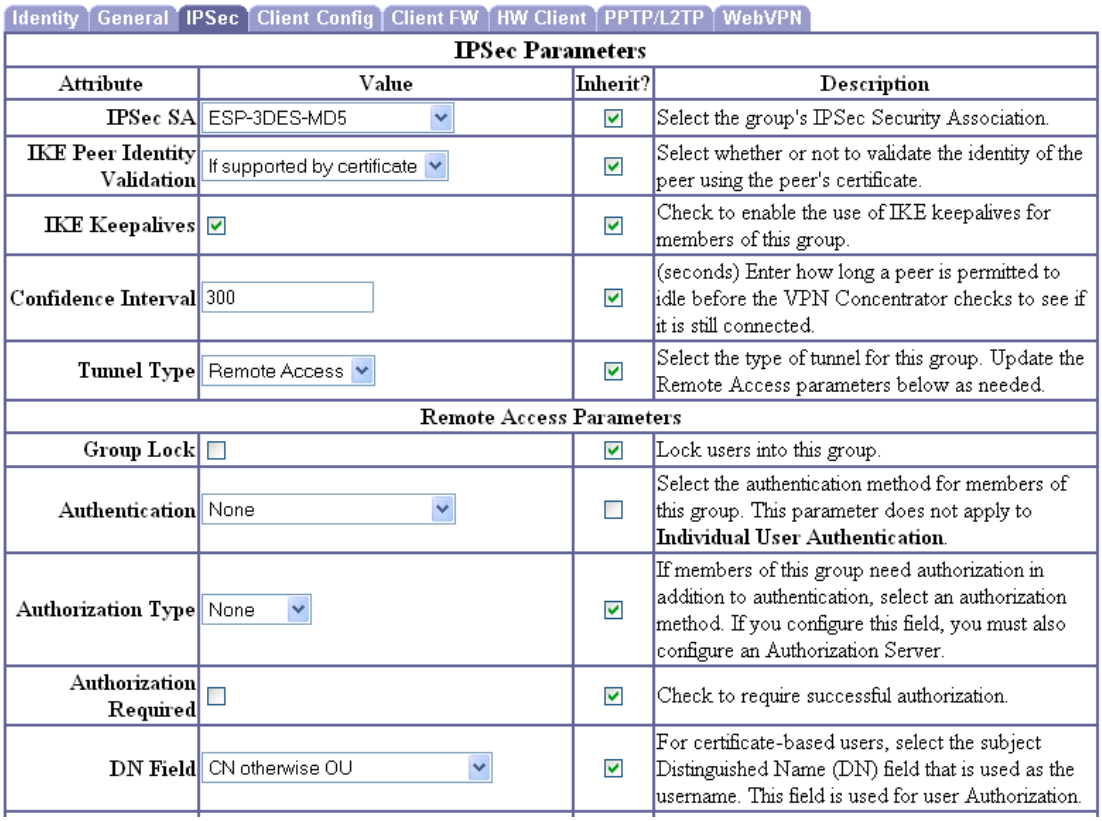


Fig. 26. Sezione IPSec per il gruppo servcal.

Successivamente in **Configuration** > **User Management > Users** viene aggiunto un nuovo utente, *cert_user*, il cui profilo è utilizzato internamente dal sistema per tutti gli utenti che utilizzano questo tipo di autenticazione (Fig. 27 e 28). Nelle proprietà dell'utente sono impostate una password (che non viene richiesta al momento dell'autenticazione) e il gruppo al quale associare l'utente. Il gruppo da selezionare deve essere quello relativo all'utilizzo dei certificati, nel nostro caso *servcal*. Nelle proprietà IPSec, come per il gruppo di appartenenza, va impostata la SA opportuna (ESP-3DES-MD5).

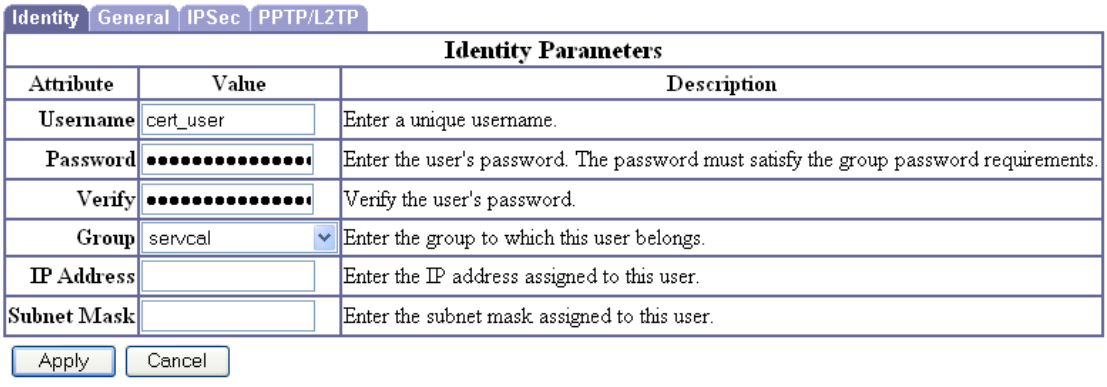


Fig. 27. Proprietà dell'utente che utilizza un'autenticazione PKI.

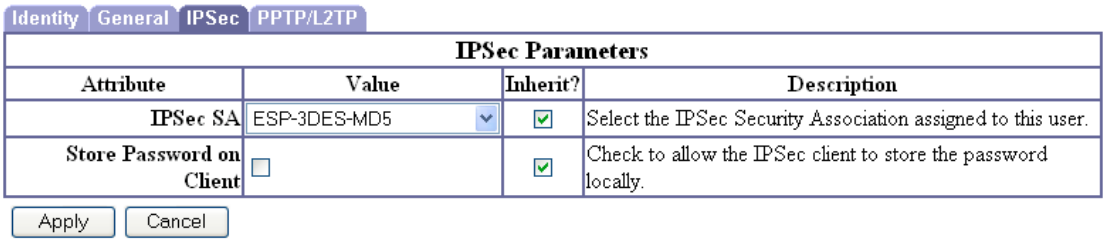


Fig. 28. Proprietà IPSec dell'utente cert_user.

Abbiamo deciso di impostare una policy secondo regole personalizzate che discriminino opportunamente le proprietà del certificato utente ai fini dell'autenticazione. In tal senso abbiamo deciso di utilizzare il campo **L** (locality) del certificato come criterio per consentire l'autenticazione solo ai client possessori di certificato facenti capo alla sezione di Firenze. In questo modo non viene consentito l'accesso in VPN agli utenti afferenti ad altre sezioni che abbiamo un certificato rilasciato dall'INFN CA. Per fare questo in **Configuration > Policy Management > Certificate Group Matching > Policy** bisogna selezionare l'opzione *Match Group from Rules* e successivamente in **Configuration > Policy Management > Certificate Group Matching > Rules** occorre aggiungere una nuova regola. Nel nostro caso abbiamo aggiunto la regola L=Firenze (vd. Fig. 29).

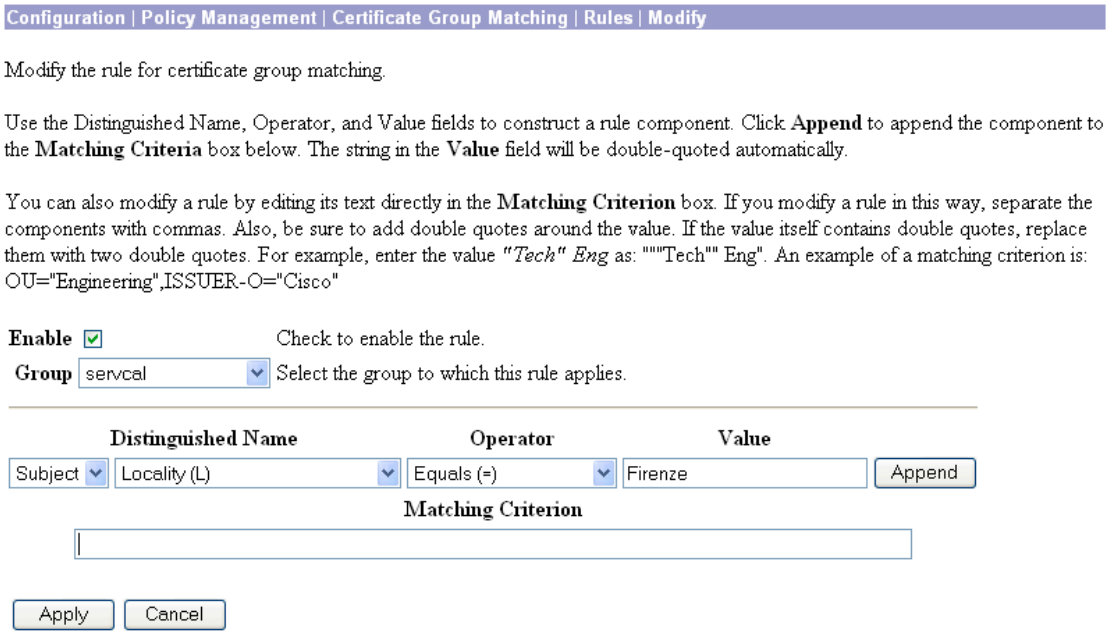


Fig. 29.Iimpostazione delle regole di match per i certificati.

Configurazione del CISCO VPN Client

Piattaforma Windows

Il client si collega alla pagina http://www.fi.infn.it/calcolo/vpn, scarica la versione aggiornata del Cisco VPN Client, la versione 4.0.4.D ad ottobre 2004, in base al proprio sistema operativo (Unix o Windows) e procede alla sua installazione.
La compatibilità software del Cisco VPN Client installato su MS Windows XP, 98, ME, NT 4.0, e Linux supporta IPSec puro. Per utilizzare L2TP/IPSEC come protocollo di tunnelling vanno utilizzati altri software client come quello Microsoft (L2TP/IPSec per Windows 2000/XP, 98, ME, ecc.), come riportato a http://www.cisco.com/en/US/products/hw/vpndevc/ps2284
La configurazione del software client per Windows 2000/XP è mostrata in Fig. 30:

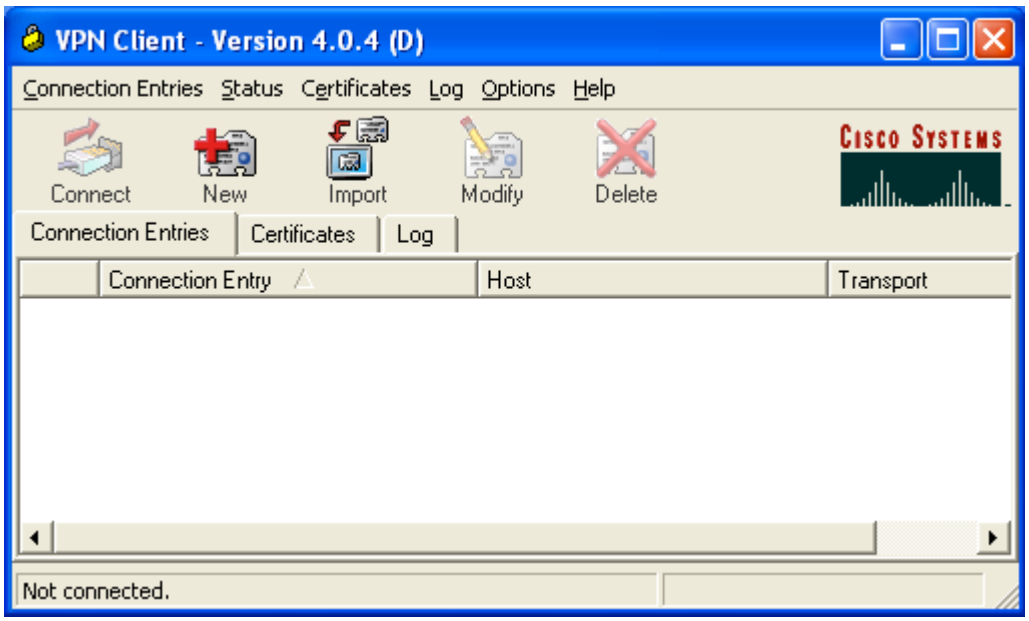


Fig. 30. Schermata principale del software VPN client CISCO per Windows.

Nella caso della configurazione di una connessione con utilizzo di username/password con autenticazione su dominio NT si impostano i parametri di nuova connessione **Connection Entries > New** come mostrato in Fig. 31. Nella sezione *Authentication* abbiamo definito un nome per la connessione e specificato l'indirizzo IP del VPN Concentrator ed i parametri per il gruppo *VPNDomainUsers* inserendo la *pre-shared key* configurata all'interno del VPN Concentrator per tale gruppo.

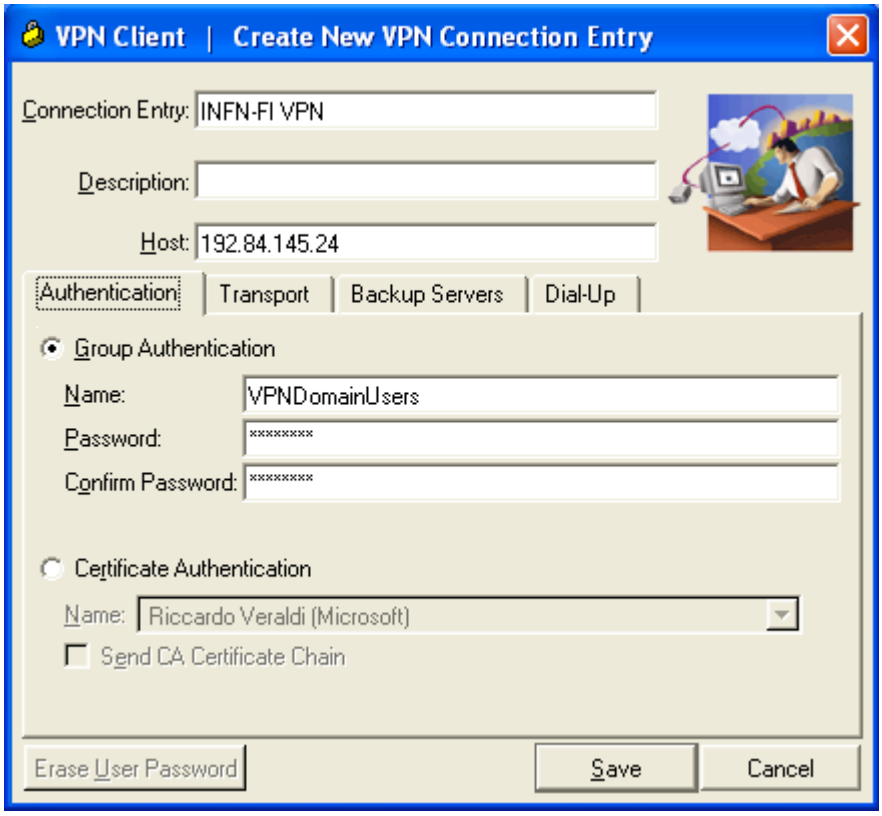


Fig. 31. Configurazione delle proprietà di connessione VPN.

A questo punto è possibile stabilire una connessione con il VPN Concentrator dopo avere salvato la configurazione. Il software client chiede all'utente le credenziali per l'accesso al dominio INFN-FI.

Fig. 32.: Richieste credenziali di dominio.

Per quanto riguarda la configurazione per l'accesso VPN con autenticazione tramite certificato abbiamo importato il certificato personale dell'utente ed il certificato dell'INFN CA all'interno del browser Internet Explorer. A questo punto il certificato utente sarà visibile automaticamente anche dal software CISCO VPN Client. Abbiamo creato il profilo di una nuova connessione come mostrato in Fig. 33. Rispetto al caso precedente l'unico cambiamento è l'impostazione di una *Certificate*

Authentication invece di una *Group Authentication*. Abbiamo poi selezionato il certificato personale dell'utente rilasciato dall'INFN-CA. A questo punto il nuovo profilo può essere salvato ed è pronto per l'utilizzo. In questo caso non verranno chieste credenziali all'utente per potere accedere alla VPN e verrà utilizzato il proprio certificato personale come mezzo di autenticazione.

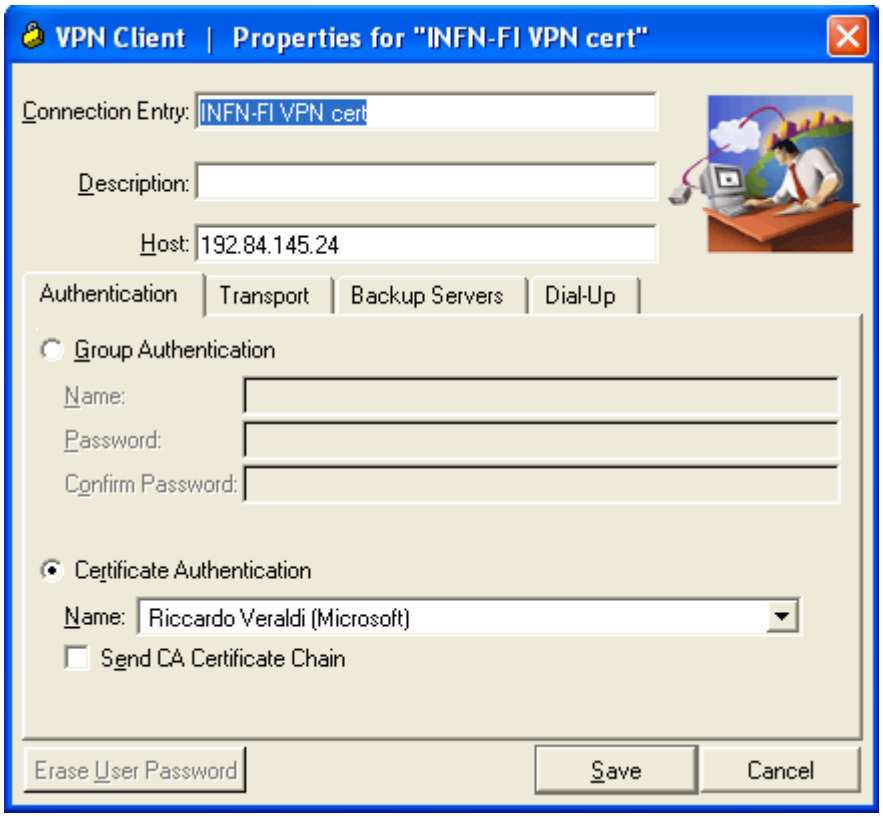


Fig. 33. Configurazione parametri per l'autenticazione con certificato.

Piattaforma Linux

Il sistema operativo su cui è stato testato è Linux RedHat 9, con versione del kernel 2.4.20-8. La versione client installata è la CISCO VPN client 4.0.4.B-K9.

Passi da eseguire: scompattare l'archivio vpnclient-linux-4.0.4.B-k9.tar.gz; verrà creata una directory *vpnclient*; eseguire lo script *vpn_install*. I binari verranno installati in */usr/local/bin* mentre i file di configurazione sono memorizzati in */etc/CiscoSystemsVPNClient/Profiles/*.
Lo script installerà un kernel module *cisco_ipsec*.
Va creato un file *ipsec.pcf* modificando il file sample.pcf, che nel nostro caso è stato configurato nel modo seguente:

[main]
Description=sample user profile
Host=192.84.145.24
AuthType=1
GroupName=VPNDomainUsers
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=veraldi
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
UserPassword=
enc_UserPassword=
GroupPwd=
enc_GroupPwd=
ISPPhonebook=
NTDomain=
EnableMSLogon=1
MSLogonType=0
TunnelingMode=0
TcpTunnelingPort=10000
SendCertChain=0
PeerTimeout=90
EnableLocalLAN=0

Successivamente va caricato il kernel module del vpn client il quale crea un'interfaccia virtuale *cipsec0*, visibile digitando il comando ifconfig –a:

cipsec0 Link encap:Ethernet HWaddr 00:00:00:00:00:00
BROADCAST MULTICAST MTU:1400 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

Per fare questo utilizzare lo script vpnclient_init

A questo punto siamo pronti per lanciare la connessione in VPN invocando il comando vpnclient con il profile ipsec appena configurato:

% vpnclient connect ipsec
Cisco Systems VPN Client Version 4.0.4 (B)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.4.20-8 #1 Thu Mar 13 17:18:24 EST 2003 i686

Enter a group password:
Initializing the VPN connection.
Contacting the gateway at 192.84.145.24
User Authentication for ipsec...

Enter Username and Password.

Username [veraldi]: veraldi
Password []:
Authenticating user.
Negotiating security policies.
Securing communication channel.
Your VPN connection is secure.

VPN tunnel information.
Client address: 172.16.1.202
Server address: 192.84.145.24
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is inactive
Local LAN Access is disabled

Ora l'utente e' collegato in VPN e inserito nella LAN.
Se viene eseguito il comando traceroute il risultato ottenuto è il seguente:

```
[root@test bin]# traceroute www.fi.infn.it
traceroute to www.fi.infn.it (192.84.145.38), 30 hops max, 38 byte packets
 1  vpnbox.fi.infn.it (192.84.145.24)  1.789 ms  1.735 ms  1.630 ms
```

```
 2  eratostene-172-16-98.fi.infn.it (172.16.98.254)  1.794 ms  1.832 ms  1.754 ms
 3  www.fi.infn.it (192.84.145.38)  1.717 ms  1.779 ms  1.757 ms

[root@test bin]# traceroute www.cern.ch
traceroute to webr2.cern.ch (137.138.28.230), 30 hops max, 38 byte packets
 1  vpnbox.fi.infn.it (192.84.145.24)  84.694 ms  1.618 ms  1.779 ms
 2  eratostene-172-16-98.fi.infn.it (172.16.98.254)  1.680 ms  1.759 ms  1.619 ms
 3  sw-gigac.fi.infn.it (192.84.145.16)  2.209 ms  3.041 ms  2.045 ms
 4  ru-infnfi-rt-fi1.fi1.garr.net (193.206.136.73)  2.114 ms  2.080 ms  1.961 ms
 5  rt-fi1-rt-bo1.bo1.garr.net (193.206.141.13)  3.283 ms  3.322 ms  3.320 ms
… …
```

Esempio di connessione al VPN Concentrator

Abbiamo eseguito dei test di connessione con il VPN Concentrator da una rete esterna alla LAN della sezione, utilizzando un client Windows XP.
Abbiamo creato due profili, uno per l'autenticazione con utilizzo di Active Directory (username e password) INFN VPN DOMAIN, e l'altro con utilizzo di certificati rilasciati dall'INFN CA, INFN VPN (Fig. 34).

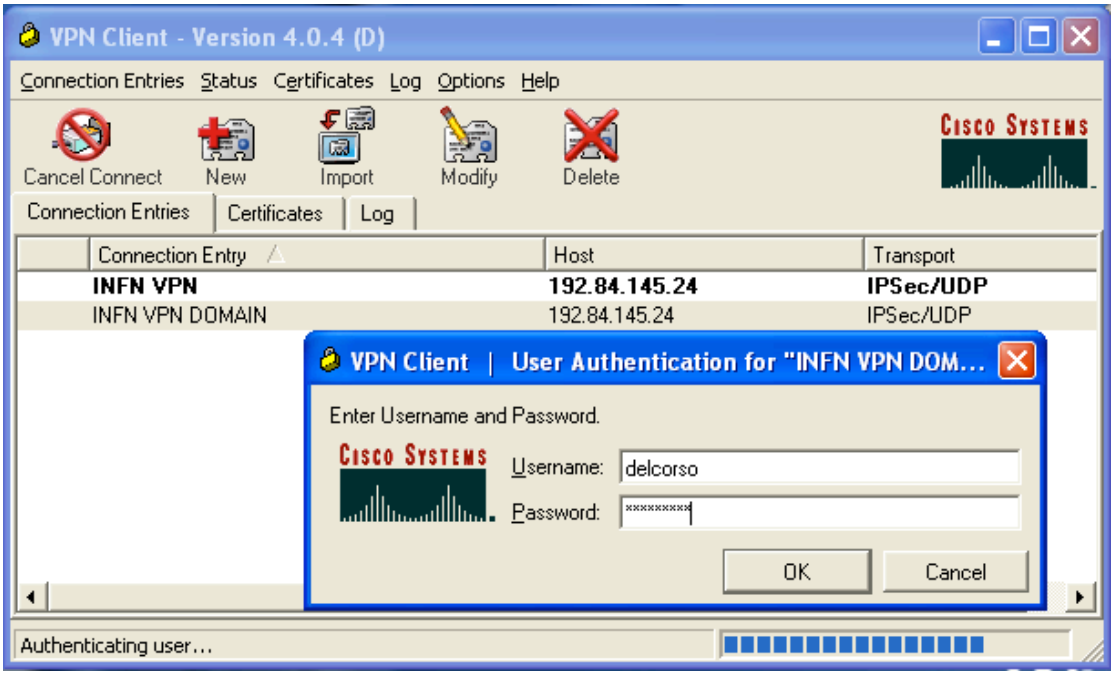


Fig. 34. Autenticazione con utilizzo di Active Directory.

Utilizzando i certificati per l'autenticazione non vengono richieste credenziali username/password, come mostrato in Fig. 35.

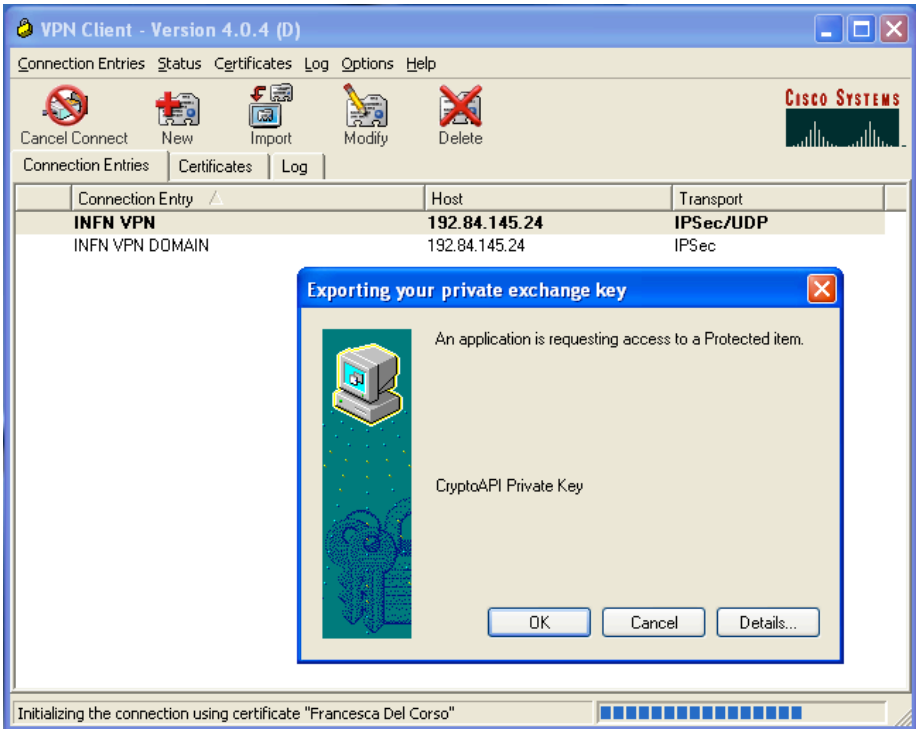


Fig. 35. Autenticazione con utilizzo di PKI.

Senza l'utilizzo della VPN i pacchetti seguono un certo percorso di instradamento, dato dalle regole di routing dell'ISP al quale l'utente è collegato.

```
Rilevazione instradamento verso www.garr.it [193.206.158.2]
su un massimo di 30 punti di passaggio:

  1    <1 ms    <1 ms    <1 ms  venus.casalecchio.org [172.16.16.100]
  2    53 ms    51 ms    52 ms  192.168.100.1
  3    51 ms    51 ms    51 ms  host23-70.pool8021.interbusiness.it [80.21.70.23]
  4    49 ms    52 ms    51 ms  r-bo74-bo83.opb.interbusiness.it [151.99.101.121]
  5    56 ms    55 ms    56 ms  r-rm213-bo74.opb.interbusiness.it [151.99.101.197]
  6    58 ms    58 ms    61 ms  r-rm156-v13.opb.interbusiness.it [151.99.29.144]
  7    59 ms    59 ms    56 ms  host10-8.pool8020.interbusiness.it [80.20.8.10]
  8    58 ms    56 ms    55 ms  garr-nap.namex.it [193.201.28.15]
  9    58 ms    58 ms    57 ms  rt-rtg-2.rm.garr.net [193.206.134.229]
 10    56 ms    55 ms    56 ms  rc-rt-1.rm.garr.net [193.206.134.162]
 11    63 ms    61 ms    70 ms  dirgarrb1-rc.rm.garr.net [193.206.131.166]
 12    64 ms    65 ms    64 ms  lx1.dir.garr.it [193.206.158.2]
```

Fig. 36. Instradamento dei pacchetti senza VPN.

Una volta stabilita la connessione in VPN l'utente è automaticamente proiettato all'interno della LAN della Sezione di Firenze. Al computer del client viene assegnato un indirizzo IP appartenente al range precedentemente configurato all'interno del VPN Concentrator come si può vedere in Fig 37 e in Fig 38.

Fig. 37. Interfaccia di rete reale del client e virtuale con indirizzo IP assegnato dal VPN Concentrator.

Fig. 38. Instradamento dei pacchetti dopo avere stabilito una VPN IPSec.

Dal lato del VPN Concentrator nella sezione **Monitoring** > **Sessions** vengono mostrate tutte le sessioni attive in un dato momento, i dettagli e le statistiche per sessioni IKE ed IPSec (Fig. 39).

Monitoring | Sessions — Friday, 15 October 2004 10:47:36

Reset Refresh

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name.

Group –All–

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Weighted Active Load	Percent Session Load	Concurrent Sessions Limit	Total Cumulative Sessions
0	3	1	4	4	3	1.50%	200	40

LAN-to-LAN Sessions

[Remote Access Sessions | Management Sessions]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
No LAN-to-LAN Sessions							

Remote Access Sessions

[LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx
Francesca Del Corso	172.16.1.201 192.84.145.20	servcal	IPSec/UDP 3DES-168	Oct 15 10:20:42 0:26:54	WinNT 4.0.4 (D)	348808 303448
Riccardo Veraldi	172.16.1.202 172.16.0.1	servcal	IPSec 3DES-168	Oct 15 10:36:48 0:10:48	WinNT 4.0.5 (B)	21456 39296
vpnuser	172.16.1.203 80.104.165.147	VPNDomainUsers	IPSec/UDP 3DES-168	Oct 15 10:45:37 0:01:58	WinNT 4.0.4 (D)	1552 5528

Monitoring | Sessions | Detail — Friday, 15 October 2004 10:49:26

Reset Refresh

Back to Sessions

Username	Public IP Address	Assigned IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
vpnuser	80.104.165.147	172.16.1.203	IPSec/UDP	3DES-168	Oct 15 10:45:37	0:03:48	1552	5528

IKE Sessions: 1
IPSec/UDP Sessions: 1

IKE Session			
Session ID	1	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**Diffie-Hellman Group**	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys (XAUTH)		
UDP Source Port	500	**UDP Destination Port**	500
IKE Negotiation Mode	Aggressive	**Rekey Time Interval**	86400 seconds
IPSec/UDP Session			
Session ID	2	**Remote Address**	172.16.1.203
Local Address	0.0.0.0/255.255.255.255	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**Idle Time**	0:03:27
Encapsulation Mode	Tunnel		
UDP Source Port	10000	**UDP Destination Port**	10000
Rekey Time Interval	28800 seconds		
Bytes Received	5528	**Bytes Transmitted**	1552

Monitoring | Statistics | IPSec — Friday, 15 October 2004 10:51

Reset Refresh

IKE (Phase 1) Statistics	
Active Tunnels	3
Total Tunnels	22
Received Bytes	118132
Sent Bytes	52950
Received Packets	610
Sent Packets	256
Received Packets Dropped	27
Sent Packets Dropped	0
Received Notifies	376
Sent Notifies	166
Received Phase-2 Exchanges	22
Sent Phase-2 Exchanges	0
Invalid Phase-2 Exchanges Received	0
Invalid Phase-2 Exchanges Sent	0
Rejected Received Phase-2 Exchanges	0
Rejected Sent Phase-2 Exchanges	0
Phase-2 SA Delete Requests Received	19
Phase-2 SA Delete Requests Sent	0
Initiated Tunnels	0
Failed Initiated Tunnels	0
Failed Remote Tunnels	8
Authentication Failures	1
Decryption Failures	0
Hash Validation Failures	0
System Capability Failures	0

IPSec (Phase 2) Statistics	
Active Tunnels	3
Total Tunnels	22
Received Bytes	917400
Sent Bytes	1733864
Received Packets	3991
Sent Packets	4542
Received Packets Dropped	3
Received Packets Dropped (Anti-Replay)	0
Sent Packets Dropped	0
Inbound Authentications	3988
Failed Inbound Authentications	0
Outbound Authentications	4542
Failed Outbound Authentications	0
Decryptions	3988
Failed Decryptions	0
Encryptions	4542
Failed Encryptions	0
System Capability Failures	0
No-SA Failures	0
Protocol Use Failures	0

Fig. 39. Statistiche IKE ed IPSec.

Problemi riscontrati

I problemi rilevati con l'utilizzo del Cisco VPN Concentrator 3005 sono stati essenzialmente due: il primo riguarda l'enrollment dei certificati: Talvolta accade che la procedura di enrollment del certificato host (*Identity Certificate*) fallisca perché il sistema non riesce a scrivere sulla flash memory. Una possibile soluzione consiste nel riformattare la flash memory del VPN Concentrator ma non è stata da noi testata.
L'altro problema riguarda la memorizzazione dei certificati: effettuando il reboot dell'appliance vengono persi i certificati installati, sia quelli della CA che quelli host. Questo problema riscontrato nel modello 3005, l'entry level della serie 3000, potrebbe essere sempre legato alla flash memory. Per ripristinare la configurazione precedente occorre reinstallare i certificati.

CONCLUSIONI

Il sistema presentato è attualmente in produzione nella Sezione INFN di Firenze, e consente agli utenti un accesso remoto alla LAN in modo trasparente, in particolare a risorse che normalmente non sono disponibili se non in sede locale (stampanti, pagine Web protette, consultazione riviste scientifiche, accesso alle risorse critiche locali). L'utilizzo dei certificati digitali consente un'autenticazione sicura senza l'utilizzo di credenziali tradizionali come username e password, senza la gestione aggiunta di dovere registrare l'utente del servizio VPN in un qualche tipo di database.
Per chi non possiede un certificato l'autenticazione su dominio Windows è comunque sempre disponibile abilitando la proprietà di accesso remoto per l'utente che richieda l'utilizzo del servizio VPN.

BIBLIOGRAFIA

Cisco VPN Solutions
http://www.cisco.com/warp/public/779/largeent/learn/technologies/vpn/
http://www.cisco.com/warp/public/779/servpro/solutions/vpn/

IPSec
http://www.cisco.com/warp/public/cc/cisco/mkt/security/encryp/tech/ipsec_wp.htm

Active Directory
http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_configuration_example09186a00800949b4.shtml