ISTITUTO NAZIONALE DI FISICA NUCLEARE

Sezione di Firenze

<u>INFN/TC-04/17</u> 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
IPSEC e VPN
Virtual Private Network3
IPSec 3
Modalità Tunnel e Trasporto 4
Cisco VPN Concentrator 3005: configurazione6
Utilizzo di IPSec con autenticazione su Active Directory
IKE Proposal e Security Associations14
VPN IPSec con autenticazione tramite certificati digitali
Certificati rilasciati da una CA Microsoft16
Certificati gestiti tramite OpenSSL19
Certificati rilasciati dall'INFN CA 20
Configurazione del CISCO VPN Client 26
Piattaforma Windows 26
Piattaforma Linux 29
Esempio di connessione al VPN Concentrator
Problemi riscontrati
Conclusioni 38
Bibliografia 39

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

Network Layer	New IP Header	ESP/AH	IP Header	TCP Header	DATA	ESP TRL
------------------	---------------------	--------	--------------	---------------	------	------------

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.

🗿 Cisco Systems, Inc. VPN 3000 Concentrator [vpnbox] - Microsoft Internet Explorer								
File Edit View Favorites Tools Help 🥂								
🚱 Back 🔹 🐑 🔹 😫	🏠 🔎 Sear	ch 🤺 Favorites 🥝	8-6	🎍 👿 - 🔤	, 🔏			
Address 🙆 https://172.16.1.200/acces	s.html							💌 🄁 Go
msn ^M •	💌 🔎 Cer	ca 🔹 🥒 Evidenzia 🕺	Opzioni	🔀 Popup bloccat	e (8) 🔹 🔛 Hotma	il Messenger 😰 My	MSN	
VPN 3	000						Main Help S	upport Logout
K Concer	itrator Se	eries Manager					L	ogged in: admin
						Configu	ration Administrat	ion Monitoring
- <u>Configuration</u> <u>nterfaces</u>	Configurati	on Interfaces				Tue	esday, 12 October 2	004 16:36:59
							Save Needed	Refresh 🚱
Policy Management	mi ·		10010-004					
<u> —</u> <u>—</u>	Inis section	iets you configure the	VP14 500	JU Concentrator	s network intern	aces.		
	In the table	below, or in the picture	e, select a	and click the inte	rface you want to	o configure:		
								1
		Interface	Status	IP Address	Subnet Mask	MAC Address	<u>Default Gateway</u>	
		Ethernet 1 (Private)	UP	172.16.1.200	255.255.255.0	00.03.A0.89.8C.A2		
		Ethernet 2 (Public)	UP	192.84.145.24	255.255.255.0	00.03.A0.89.8C.A3	192.84.145.16	
		DNS Server(s)	192.84	. 145. 14				
		DNS Domain Name	i.infn.it					
		 Power Supply 						
			••••	1				
			. . .					
CISCO SYSTEMS								
e							🔒 🥥 Interi	net

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).
Configuring	Landing	munace	•	(LIIVACC).

Gener		TAGNALIA				
	General Parameters					
Sel	Sel Attribute Value		Description			
0	Disabled		Select to disable this interface.			
0	O DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.			
۲	Static IP Addressing					
	IP Address	172.16.1.200	Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface			
	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		1200	Enter the Maximum Transmit Unit for this interface (68 - 1500).			
		🔘 Do not fragment pric	or to IPSec encapsulation; fragment prior to interface transmission			
	Fublic Interface IPSec Fragmentation Policy	⊙ Fragment prior to IP	Sec encapsulation with Path MTU Discovery (ICMP)			
Fragmentation Foncy		\bigcirc Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF				

General RIP OSPF Bandwidth WebVPN

Apply Cancel

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

Configuration | Interfaces | Ethernet 2

Configuring Ethernet Interface 2 (Public).

Gener	General RIP OSPF Bandwidth WebvPN				
		Genera	l Parameters		
Sel	Attribute	Value	Description		
0	Disabled		Select to disable this interface.		
O DHCP Client			Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP.		
۲	Static IP Addressing				
	IP Address 192.84.145.24 Subnet Mask 255.255.255.0		Select to configure the IP Address and Subnet Mask. Enter the II Address and Subnet Mask for this interface		
	Public Interface		Check to make this interface a "public" interface.		
MAC Address 00.03.A0.89.8C.A3		00.03.A0.89.8C.A3	The MAC address for this interface.		
	Filter	2. Public (Default) 💌	Select the filter for this interface.		
	Speed	10/100 auto 💌	Select the speed for this interface.		
	Duplex	Auto 💌	Select the duplex mode for this interface.		
MTU 1200		1200	Enter the Maximum Transmit Unit for this interface (68 - 1500).		
Public Interface IPSec		🔘 Do not fragment prio	or to IPSec encapsulation; fragment prior to interface transmission		
		• Fragment prior to IPSec encapsulation with Path MTU Discovery (ICMP)			
	Fragmentation 1 oney	○ Fragment prior to IPSec encapsulation without Path MTU Discovery (Clear DF			

Apply Cancel

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:

Configuration System IP Routing Default Gateways					
Configure the default gateways for your system.					
Default Gateway	192.84.145.16	Enter the IP address of the default gateway or router. Enter 0.0.0.0 for no default router.			
Metric	1	Enter the metric, from 1 to 16.			
Tunnel Default Gateway	172.16.1.254	Enter the $I\!P$ address of the default gateway or router for tunnels. Enter 0.0.0.0 for no default router.			
Override Default Gateway		Check to allow learned default gateways to override the configured default gateway.			
Apply Cancel					

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.

Configuration | System | Servers | Authentication

Save Needed 🔒

This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, SDI or Kerberos/Active Directory server to access, or you can configure the internal server and <u>add users to the internal database</u>.

Click the Add button to add a server, or select a server and click Modify, Delete, Move, or Test.



Fig. 8. Impostazione server di autenticazione.

Configuration System Servers Authentication Modify	
Change a configured user authentication server.	
Server Type NT Domain	Selecting <i>Internal Server</i> will let you add users to the internal user database.
Authentication Server Address 172.16.0.100	Enter the IP address.
Server Port 139	Enter 0 for default port (139).
Timeout 4	Enter the timeout for this server (seconds).
Retries 2	Enter the number of retries for this server.
Domain Controller Name giove	Enter the NT Primary Domain Controller name for this authentication server.
Apply Cancel	

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.

General Parameters					
Attribute	Value	Description			
Access Hours	-No Restrictions- 💌	Select the access hours for this group.			
Simultaneous Logins	11	Enter the number of simultaneous logins for users in this group.			
Minimum Password Length	8	Enter the minimum password length for users in this group.			
Allow Alphabetic- Only Passwords		Enter whether to allow users with alphabetic-only passwords to be added to this group.			
Idle Timeout	30	(minutes) Enter the idle timeout for this group. Note: This value does not apply to WebVPN users. Set the WebVPN idle timeout in Configuration Tunneling and Security WebVPN HTTPS Proxy Default Idle Timeout.			
Maximum Connect time	0	(minutes) Enter the maximum connect time for this group.			
Filter	–None– 🛛 👻	Select the filter assigned to this group.			
Primary DNS	192.84.145.14	Enter the IP address of the primary DNS server for this group.			
Secondary DNS		Enter the IP address of the secondary DNS server.			
Primary WINS		Enter the IP address of the primary WINS server for this group.			
Secondary WINS		Enter the IP address of the secondary WINS server.			
Tunneling Protocols	□ PPTP □ L2TP □ IPSec □ L2TP over IPSec □ WebVPN	Select the tunneling protocols this group can connect with.			
Strip Realm		Check to remove the realm qualifier of the username during authentication.			
DHCP Network Scope		Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.			
Apply Cance	1				

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

Fig. 10. Proprietà del Base Group.

General IPSec Clie	ent Config Client FW HW Client PPTP/	LZTP 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 G	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.			
Туре	Internal 💌	<i>External</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> 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*.

IPSec Parameters							
Attribute	Value	Inherit?	Description				
IPSec SA	3DES-MD5		Select the group's IPSec Security Association.				
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	Paramet	ers				
Group Lock			Lock users into this group.				
Authentication	NT Domain 💌	V	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	V	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.				
Reauthentication on Rekey			Check to reauthenticate the user on an IKE (Phase-1) rekey.				
Client Type & Version Limiting		V	 Permit or deny VPN Clients according to their type and software version. Construct rules in the format p[ermit]/d[eny] <type> : <version>, For example, d VPN 3002 : 3.6*.</version></type> The * character is a wildcard. Use a separate line for each rule. Order rules by priority. For more instructions, <u>click here</u> . Check to initiate the exchange of Mode				
Mode Configuration		▼	Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the Altiga/Cisco client is being used by members of this group.				
Apply Cancel							

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

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.

Needed <mark>-</mark>

Configuration Tunneling and Security IPSec IKE Proposals	
	Save
Add. delete, prioritize, and configure IKE Proposals.	

Select an Inactive Proposal and click Activate to make it Active, or click Modify, Copy or Delete as appropriate. Select an Active Proposal and click Deactivate to make it Inactive, or click Move Up or Move Down to change its priority. Click Add or Copy to add a new Inactive Proposal. IKE Proposals are used by <u>Security Associations</u> to specify IKE parameters.



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.

Configuration Policy Management Tra	affic Management Security	Associations
		Save Needed 📊
This section lets you add, configure, modi <u>Proposals</u> to negotiate IKE parameters.	fy, and delete IPSec Security	Associations (SAs). Security Associations use $\underline{\mathrm{I\!K\!E}}$
Click \mathbf{Add} to add an SA, or select an SA	. and click \mathbf{Modify} or \mathbf{Delete}	9.
	TPSec SAs	Actions
	3DES-MD5 ESP-3DES-MD5	
	ESP-3DES-MD5-DH5 ESP-3DES-MD5-DH7 ESP-3DES-NONE ESD-4ES128-SHA	Add

Delete

ESP-DES-MD5

ESP-L2TP-TRANSPORT ESP/IKE-3DES-MD5

Configuration Policy Mana	igement Traffic Management Secur	ity Associations Modify			
Modify a configured Security	Association.				
SA Name	3DES-MD5	Specify the name of this Security Association (SA).			
Inheritance	From Rule 💌	Select the granularity of this SA.			
IPSec Parameters					
Authentication Algorithm	ESP/MD5/HMAC-128 🔽	Select the packet authentication algorithm to use.			
Encryption Algorithm	3DES-168 💌	Select the ESP encryption algorithm to use.			
Encapsulation Mode	Tunnel 💌	Select the Encapsulation Mode for this SA.			
Perfect Forward Secrecy	Disabled 💌	Select the use of Perfect Forward Secrecy.			
Lifetime Measurement	Time 💌	Select the lifetime measurement of the IPSec keys.			
Data Lifetime	10000	Specify the data lifetime in kilobytes (KB).			
Time Lifetime	28800	Specify the time lifetime in seconds.			
IKE Parameters					
IKE Peer	0.0.0.0	Specify the IKE Peer for a LAN-to-LAN IPSec connection.			
Negotiation Mode	Main 💌	Select the IKE Negotiation mode to use.			
Digital Certificate	None (Use Preshared Keys) 🔽	Select the Digital Certificate to use.			
Certificate Transmission	 Entire certificate chain Identity certificate only 	Choose how to send the digital certificate to the IKE peer.			
IKE Proposal	IKE-3DES-MD5	Select the IKE Proposal to use as IKE initiator.			
Apply Cancel					

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 <u>http://security.fi.infn.it/CA</u>.

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 <u>http://servername/certsrv</u> 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.

🗿 Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
🚱 Back 🔻 🐑 👻 📓 🏠 🔎 Search 🤺 Favorites 🤣 🔗 - 头 📧 - 🔜 🦓
Address 🗃 http://172.16.0.102/certsrv/certcarc.asp
msn 🗸 - 🔽 Cerca 🔹 🥜 Evidenzia 🛛 Opzioni 🔀 Popup bloccate (4) 🔹 🕁 Hotmail 🔉 Messenger 😰 My MSN
Manage MA all table Operations and an and a second s
Microsoff Certificate Services omero
Download a CA Certificate, Certificate Chain, or CRL
To trust certificates issued from this certification authority, install this CA certificate chain.
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.
CA certificate:
Current [omero]
Encoding method:
⊙ Base 64
Download CA certificate
Download CA certificate chain
Download latest base CRL
Domilioan isrear delta CKF
I Windows Media Hayer

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.

Microsoft Certificate Services -- omero

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:	
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	Acfvz/gvSTwOue5fc15r52j3dhajGP6588Onnm+p KoZIhvcNAQEEBQADgYEAhYSqYt8+hE32QttV4tet zgzf+SfAkW33VHpy3FwT6cngkjVmN19yZBV/HYOW CbkW1i1Sagt5hrF5HN3RJLkI4sWyx/AzYnoGa6n END CERTIFICATE REQUEST Browse for a file to insert.
Certificate Temp	late:
	vpn server 💌
Additional Attrib	utes:
Attributes:	<
	Submit >

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.

Microsoft (Certificate Services omero
Certificat	elssued
The certific	cate you requested was issued to you.
	⊙DER encoded or ⊙Base 64 encoded
	Download certificate

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 <u>http://servername/certsrv</u>, 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 (eq, 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.

Administration | Certificate Management | Enroll | Identity Certificate | PKCS10

Enter the information to be included in the certificate request. The CA's certificate **must** be installed as a Certificate Authority before installing the certificate you requested. Please wait for the operation to finish.

Common Name (CN)	vpnbox.fi.infn.it	Enter the common name for the VPN 3000 Concentrator to be used in this PKI.
Organizational Unit (OU)	Host	Enter the department.
Organization (O)	INFN	Enter the Organization or company.
Locality (L)	Firenze	Enter the city or town.
State/Province (SP)		Enter the State or Province.
Country (C)	IT	Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN)		Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.
Subject AlternativeName (E- Mail Address)	delcorso@fi.infn.it	Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.
Key Size	RSA 1024 bits 🐱	Select the key size for the generated RSA/DSA key pair.
Enroll Cancel		

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:

Subject			Issuer		Expir	ation	SCEP Issuer		Actions
INFN Certificatio INFN	n Authority at	INF1 INF1	∛ Certificati⊲ ∛	on Authority at	09/18/	2007	No	View Configure Del	
Identity Certif	icates (curren	: 1, maximu	um: 5)						
Subj	ect]	lssuer		Exp	piration	A	Actions
vpnbox.fi.infn.it at	: INFN	INFN Cer	tification Au	thority at INFN		10/12	/2005	/iew Ren	lew Delete
SSL Certificat Interface	es Subje	ct	Issuer	Expiration			Ad	tions	
Private	No Certif	icate Insta	lled.		Ge	enerate	Enroll Impor	<u>t</u>	
Public	No Certif	icate Insta	lled.		Ge	Generate Enroll Import			
SSH Host Key	,			[
Key Size		Key Ty	ре	Date Generated			Actions		
No SSH Host K	ey								
Enrollment St	atus [Remove A	11: Errored 1	<u> [imed-Out Re</u>	ejected Cancelled In	-Progress] (curre	nt: 0 availab	le: 5)	
Subject	Issuer	Date	Date Use Reason Method Status Actions				Actions		
									· · · · · · · · · · · · · · · · · · ·

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

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.

C C	 · · · · · · · · · · · · · · · · ·			
	a ana socuru	VIDSAC	haca c	
			MANDER 1	
the state of the s			and the state of t	

Proposal Name	CiscoVPNClient-3DES-MD5-RSA	Specify the name of this IKE Proposal.
Authentication Mode	RSA Digital Certificate (XAUTH) 🛛 👻	Select the authentication mode to use.
Authentication Algorithm	MD5/HMAC-128 🔽	Select the packet authentication algorithm to use.
Encryption Algorithm	3DES-168 🔽	Select the encryption algorithm to use.
Diffie-Hellman Group	Group 2 (1024-bits) 🔽	Select the Diffie Hellman Group to use.
Lifetime Measurement	Time 💌	Select the lifetime measurement of the IKE keys.
Data Lifetime	10000	Specify the data lifetime in kilobytes (KB).
Time Lifetime	86400	Specify the time lifetime in seconds.
Apply Cancel		

Modify a configured IKE Proposal.

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.

Configuration Policy Management Traffic Management Security Associations Modify				
Modify a configured Security	Association.			
SA Name	ESP-3DES-MD5	Specify the name of this Security Association (SA).		
Inheritance	From Rule 🔽	Select the granularity of this SA.		
IPSec Parameters				
Authentication Algorithm	ESP/MD5/HMAC-128 💌	Select the packet authentication algorithm to use.		
Encryption Algorithm	3DES-168 💌	Select the ESP encryption algorithm to use.		
Encapsulation Mode	Tunnel 💌	Select the Encapsulation Mode for this SA.		
Perfect Forward Secrecy	Disabled 🖌	Select the use of Perfect Forward Secrecy.		
Lifetime Measurement	Time 💌	Select the lifetime measurement of the IPSec keys.		
Data Lifetime	10000	Specify the data lifetime in kilobytes (KB).		
Time Lifetime	28800	Specify the time lifetime in seconds.		
IKE Parameters				
IKE Peer	0.0.0.0	Specify the IKE Peer for a LAN-to-LAN IPSec connection.		
Negotiation Mode	Main 🔽	Select the IKE Negotiation mode to use.		
Digital Certificate	vpnbox.fi.infn.it	Select the Digital Certificate to use.		
Certificate Transmission	 Entire certificate chain Identity certificate only 	Choose how to send the digital certificate to the IKE peer.		
IKE Proposal	CiscoVPNClient-3DES-MD5-RSA	Select the IKE Proposal to use as IKE initiator.		
Apply Cancel				

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.

Configuration | User Management | Groups | Modify servcal

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 Ge	eneral IPSec Clie	nt Config Client FW HW Client PPTP/L2TP WebVPN				
	Identity Parameters					
Attribute	Value	Description				
Group Name	servcal	Enter a unique name for the group.				
Password	•••••	Enter the password for the group.				
Verify	•••••	Verify the group's password.				
Туре	Internal 💌	<i>External</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator's Internal Database.				
	Cancel					

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

The new Selected in Sec Cherk Comp Cherk That The Cherk Thread The Sec Cherk Comp Cherk That The Sec Cherk Comp						
	IPSec Parameters					
Attribute	Value	Inherit?	Description			
IPSec SA	ESP-3DES-MD5 🛛 💌		Select the group's IPSec Security Association.			
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	V	(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	Paramet	ers			
Group Lock		✓	Lock users into this group.			
Authentication	None		Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication.			
Authorization Type	None	V	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	V	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.			

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

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).

Identity Gen		-21			
	Identity Parameters				
Attribute	Value		Description		
Username	cert_user		Enter a unique username.		
Password	•••••		Enter the user's password. The password must satisfy the group password requirements.		
Verify	•••••		Verify the user's password.		
Group	servcal	~	Enter the group to which this user belongs.		
IP Address			Enter the IP address assigned to this user.		
Subnet Mask			Enter the subnet mask assigned to this user.		
Apply	Cancel				

Identity General IPSec PPTP/L2TP

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

Identity	General	IPSec	PPTP/L2TP				
	IPSec Parameters						
1	Attribute		Va	alue	Inherit?	Description	
IPSec SA E		ESP-3DES-M	D5 🔽	~	Select the IPSec Security Association assigned to this user.		
Store Password on Client						Check to allow the IPSec client to store the password locally.	
Apply	/ Can	cel					

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).

Configuration | Policy Management | Certificate Group Matching | Rules | Modify

Modify the rule for certificate group matching.

Use the Distinguished Name, Operator, and Value fields to construct a rule component. Click **Append** to append the component to the **Matching Criteria** box below. The string in the Value field will be double-quoted automatically.

You can also modify a rule by editing its text directly in the **Matching Criterion** box. If you modify a rule in this way, separate the components with commas. Also, be sure to add double quotes around the value. If the value itself contains double quotes, replace them with two double quotes. For example, enter the value "*Tech*" Eng as: """Tech"" Eng". An example of a matching criterion is: OU="Engineering",ISSUER-O="Cisco"

Enable 🔽 Chec	ck to enable the rule.		
Group servcal 🛛 💙 Selec	ct the group to which this rule applie	S.	
Distinguished Name	Operator	Value	
Subject 🔽 Locality (L)	🖌 Equals (=)	Firenze	Append
	Matching Criterion		
Apply Cancel			

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.

Ø VPN Client 0	Create New VPN Connection Entry			
Connection Entry: INF	N-FI VPN			
Description:	S I S I S I S I S I S I S I S I S I S I			
<u>H</u> ost: 192.	84.145.24			
Authentication Tr	ansport Backup Servers Dial-Up			
Group Authentica	tion			
<u>N</u> ame:	VPNDomainUsers			
Password:	******			
Confirm Password:	*******			
C Certificate Auther	itication			
Name: Riccardo Veraldi (Microsoft)				
j s <u>e</u> no CA Cerar	uate unain			
Erase <u>U</u> ser Password	<u>S</u> ave Cancel			

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.

VPN Client	User Authentication for "INFN-FI VPN"	\mathbf{X}
Enter Username an CISCO SYSTEMS	d Password. Username: veraldi Password: *****	
	OK Cance	

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.

VPN Client Properties for "INFN-FI VPN cert"
Connection Entry: INFN-FI VPN cert
Description:
Host 192.84.145.24
Authentication Transport Backup Servers Dial-Up
C <u>G</u> roup Authentication
Name:
Password:
Confirm Password:
Certificate Authentication
Name: Riccardo Veraldi (Microsoft)
Send CA Certificate Chain
Erase User Password Save Cancel

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= 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).

VPN Client - Version 4.	0.4 (D)		
Connection Entries Status Cer	tificates <u>L</u> og <u>O</u> ptions <u>H</u>	<u>t</u> elp	
Cancel Connect New	F ன 🏹 Import Modify	X Delete	CISCO SYSTEMS
Connection Entries Certificat	es Log		
Connection Entry		Host	Transport
INFN VPN		192.84.145.24	IPSec/UDP
INFN VPN DOMAIN		192.84.145.24	IPSec/UDP
	VPN Client U	ser Authentication for "INFN	VPN DOM 🔀
	Enter Username and Pa	assword.	
	CISCO SYSTEMS U	sername: delcorso	
	IlluIllu	assword: ******	
•		ОК	Cancel
Authenticating user			

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.

Connection Entries, Status, Certificates, Log, Options, Hi					
Connection charles Status Certificates Eog Options Ti	elp				
Cancel Connect New Import Modify)) Delete	CISCO SYSTEMS author author			
Connection Entries Certaincates Ebg	11-4	Transact			
	192 94 145 24				
INFN VPN DOMAIN	192.84.145.24	IPSec			
Exporting yo	An application is requesting access	s to a Protected item			
	An application is requesting access	s to an indepted item.			
	CryptaAPI Private Key				
	OK Canc	el Details			

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.

Rilev su un	azione in massimo	stradament di 30 punt	to verso ti di pa	www.garr.it [193.206.158.2] ssaggio:
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.poo18021.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.

Scheda 🛛	Ethernet Connessione alla rete locale (L	AN> :
Comple	Suffisso DNS specifico per connessione Descrizione	3Com EtherLink XL 10/100 PCI 00-04-75-D8-57-DE No 172.16.16.1 255.255.255.0 172.16.16.100 172.16.16.100
Scheda I	Ethernet Connessione alla rete locale (L	AN> 2:
	Suffisso DNS specifico per connessioneDescrizioneIndirizzo fisicoDHCP abilitatoDHCP abilitatoSubnet maskGateway predefinitoServer DNS	fi.infn.it Cisco Systems UPN Adapter 00-05-9A-3C-78-00 No 172.16.1.201 255.255.255.0 172.16.1.201 192.84.145.14

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

Rilev su un	azione in massimo	nstradament di 30 punt	to verso ti di pa:	www.garr.it [193.206.158.2] ssaggio:
1	66 ms	67 ms	68 ms	vpnbox.fi.infn.it [192.84.145.24]
2	69 ms	67 ms	68 ms	eratostene-172-16-98.fi.infn.it [172.16.98.254]
3	68 ms	66 ms	73 ms	sw-gigac.fi.infn.it [192.84.145.16]
4	67 ms	69 ms	67 ms	ru-infnfi-rt-fi1.fi1.garr.net [193.206.136.73]
5	72 ms	67 ms	68 ms	rt-fi1-rt-bo1.bo1.garr.net [193.206.141.13]
6	71 ms	71 ms	66 ms	rt2-bo1-rt1-bo1.bo1.garr.net [193.206.134.237]
7	70 ms	72 ms	71 ms	rm-bo-g.garr.net [193.206.134.49]
8	75 ms	74 ms	76 ms	rt-rtg-1.rm.garr.net [193.206.134.225]
9	76 ms	81 ms	78 ms	rc-rt-1.rm.garr.net [193.206.134.162]
10	78 ms	113 ms	79 ms	dirgarrb2-rc.rm.garr.net [193.206.131.218]
11	84 ms	80 ms	79 ms	lx1.dir.garr.it [193.206.158.2]

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	Login Time	Duration	Bytes Tx	Bytes Rx		
No LAN-to-LAN Sessions								

Remote Access Sessions

[<u>LAN-to-LAN Sessions</u> | <u>Management Sessions</u>]

<u>Username</u>	Assigned IP Address Public IP Address	Group	<u>Protocol</u> Encryption	Login Time Duration	Client Type Version	<u>Bytes Tx</u> Bytes Rx
<u>Francesca Del Corso</u>	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
<u>Riccardo Veraldi</u>	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
<u>vpnuser</u>	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

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	0.0.0/255.255.255.255	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				

IKE (Phase 1) Statistics		IPSec (Phase 2) Statistics	
Active Tunnels	3	Active Tunnels	3
Total Tunnels	22	Total Tunnels	22
Received Bytes	118132	Received Bytes	917400
Sent Bytes	52950	Sent Bytes	1733864
Received Packets	610	Received Packets	3991
Sent Packets	256	Sent Packets	4542
Received Packets Dropped	27	Received Packets Dropped	3
Sent Packets Dropped	0	Received Packets Dropped (Anti-Replay)	0
Received Notifies	376	Sent Packets Dropped	0
Sent Notifies	166	Inbound Authentications	3988
Received Phase-2 Exchanges	22	Failed Inbound Authentications	0
Sent Phase-2 Exchanges	0	Outbound Authentications	4542
Invalid Phase-2 Exchanges Received	0	Failed Outbound Authentications	0
Invalid Phase-2 Exchanges Sent	0	Decryptions	3988
Rejected Received Phase-2 Exchanges	0	Failed Decryptions	0
Rejected Sent Phase-2 Exchanges	0	Encryptions	4542
Phase-2 SA Delete Requests Received	19	Failed Encryptions	0
Phase-2 SA Delete Requests Sent	0	System Capability Failures	0
Initiated Tunnels	0	No-SA Failures	0
Failed Initiated Tunnels	0	Protocol Use Failures	0
Failed Remote Tunnels	8		
Authentication Failures	1		
Decryption Failures	0		
Hash Validation Failures	0		
System Capability 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_e xample09186a00800949b4.shtml