FireGte 10NX

Manuale Operativo
rev. 1.0 del 09/2006

digicom
http://www.digicom.it

INDICE

PREMESSA

PRECAUZIONI

Al fine di salvaguardare la sicurezza, l'incolumità dell'operatore e il funzionamento dell'apparato, devono essere rispettate le seguenti norme per l'installazione. Il sistema, compresi i cavi, deve venire installato in un luogo privo o distante da:

- Polvere, umidità, calore elevato ed esposizione diretta alla luce del sole.
- Oggetti che irradiano calore. Questi potrebbero causare danni al contenitore o altri problemi.
- Oggetti che producono un forte campo elettromagnetico (altoparlanti Hi-Fi, ecc.)
- Liquidi o sostanze chimiche corrosive.

CONDIZIONI AMBIENTALI

Temperatura ambiente da -5 a +45°C Umidità relativa dal 20 a 80% n.c.
Si dovrà evitare ogni cambiamento rapido di temperatura e umidità.

AVVERTENZE GENERALI

Per evitare scosse elettriche, non aprite l'apparecchio o il trasformatore. Rivolgetevi solo a personale qualificato. Scollegate il cavo di alimentazione dalla presa a muro quando non intendete usare l'apparecchio per un lungo periodo di tempo. Per scollegare il cavo tiratelo afferrandolo per la spina. Non tirate mai il cavo stesso.
In caso di penetrazione di oggetti o liquidi all'interno dell'apparecchio, scollegate il cavo di alimentazione e fatelo controllare da personale qualificato prima di utilizzarlo nuovamente.

PULIZIA DELL'APPARATO

Usate un panno soffice asciutto senza l'ausilio di solventi.

VIBRAZIONI O URTI

Attenzione a non causare vibrazioni o urti.

DICHIARAZIONE CE DI CONFORMITA'

Noi, **Digicom S.p.A. via Volta 39 - 21010 Cardano al Campo (Varese - Italy)**, dichiariamo sotto la nostra esclusiva responsabilità, che il prodotto a nome **Firegate 10NX**, soddisfa la direttiva 89/336/CEE (solo compatibilità elettromagnetica). Le norme sono:

EN 55022 classe B EN 61000-3-2 EN 61000-3-3 EN 55024

Smaltimento delle apparecchiature obsolete

Tutti i prodotti elettrici ed elettronici devono essere smaltiti separatamente rispetto alla raccolta differenziata municipale, mediante impianti di raccolta specifici designati dal governo o dalle autorità locali. Quando sul prodotto è riportato il simbolo di un bidone della spazzatura barrato da una croce, significa che l'apparato è coperto dalla direttiva europea 2002/96/EC (WEEE).
Sono previste sanzioni in caso di smaltimento abusivo di detti prodotti.

1. INTRODUZIONE

1

Grazie per la fiducia accordataci nell'acquistare un prodotto Digicom!

Con FireGate 10NX le sarà possibile collegare il suo ufficio o dipartimento aziendale ad Internet in modo semplice ed efficiente.
Fino a 253 stazioni della sue rete locale LAN avranno la possibilità di accedere ad Internet per la navigazione (WWW, HTTP) o l'accesso alla posta elettronica (e-mail) utilizzando un modem* ADSL, xDSL o Cable Modem ed un abbonamento per singolo utente.
La sua LAN sarà inoltre protetta dai più comuni attacchi di hacker che potenzialmente possono provenire da Internet. FireGate 10NX supporta trasparentemente i protocolli L2TP, PPTP e IPSEC per il VPN passthrough oltre che le funzioni native per stabilire connessioni VPN con altri dispositivi su IPSEC, IKE e Microsoft VPN.
Tutte le operazioni di linea saranno gestite in modo completamente automatico e trasparente da FireGate 10NX, senza intervento alcuno da parte degli utilizzatori della rete.
Potrà inoltre sfruttare le funzionalità avanzate di FireGate 10NX per gestire in modo efficiente l'accesso ad Internet dei suoi computer, realizzando esportazioni di servizi, gruppi di utenti a cui permettere/negare l'accesso, bloccare protocolli o applicazioni e molto altro.
In questo manuale troverà tutte le informazioni necessarie per collegare FireGate 10NX alla sua rete di computer e configurare opportunamente l'insieme in pochi minuti.

* Per comodità, per indicare il modem connesso alla porta WAN, questo verrà convenzionalmente chiamato "Modem xDSL", indipendentemente dalla sua tipologia (ADSL, HDSL, SDSL, Cable o altra tecnologia similare).

1.1. CARATTERISTICHE

LAN

- **Switch 10/100 BaseT integrato**
  Fino a 4 stazioni di rete possono essere collegati direttamente al dispositivo. La velocità e modalità di funzionamento della LAN viene riconosciuta ed impostata automaticamente.
- **Porta DMZ 10/100 BaseT separata**
  Per il collegamento dei server o PC che saranno ulteriormente protetti rimanendo fisicamente separato dalla LAN
- **Supporto DHCP Server**
  Un server DHCP (Dynamic Host Configuration Protocol) interno è in grado di assegnare gli indirizzi IP ai computer della rete che ne fanno richiesta.
- **Supporto RIP e Tabelle di Routine statiche**
  E' supportato il protocollo RIP ed è possibile configurare le tabelle di routing statiche per interagire con altri router connessi in LAN.
- **Pc Database**
  Database di tutte le macchine connesse alla LAN, con possibilità di gestire fino a 5 gruppi differenti e di bloccare la connessione a qualsiasi dispositivo non riconosciuto.

WAN

- **Porta WAN 10/100BaseT**
  A questa porta è possibile connettere il Modem xDSL.
- **Supporto protocollo PPPoE e PPTP**
  FireGate 10NX è in grado di generare una chiamata automatica verso il provider Internet (se necessario), utilizzando il protocollo PPP over Ethernet integrato e supportare il protocollo PPTP.
- **Connessione diretta al provider Internet**
  FireGate 10NX può effettuare una "connessione diretta", senza protocollo PPPoE, se il provider Internet richiede questo tipo di funzionamento o se si collega il dispositivo ad un router intermedio.

ACCESSO AD INTERNET / ROUTING AVANZATO

- **Accesso condiviso ad Internet**
  Fino a 253 computer connessi alla rete LAN (opportunamente configurati) possono usufruire dell'accesso Internet contemporaneamente e in modo trasparente.
- **Abbonamento per singolo utente**
  Tramite un abbonamento Internet per singolo utente, gli utenti della LAN hanno l'accesso simultaneo ad Internet.
- **Nat disattivabile**
  Disattivando il NAT è possibile utilizzare il dispositivo come un normale Router ethernet con la possibilità di filtrare il traffico indesiderato per ottimizzare il traffico in rete

FUNZIONI INTERNET AVANZATE

- **Virtual Servers**
  Permette a utenti Internet di accedere a servizi presenti sulla propria LAN (Server Web, Ftp…)
- **Special Internet Applications**
  Permette di utilizzare applicazioni Internet speciali come Internet Videoconferencing*, Telephony, Games Servers ecc.
- **Vpn passtrought**
  Permette il passaggio in trasparente dei protocollo IPSEC, L2TP e PPTP.
- **Multi DMZ**
  Possibilità di associare contemporaneamente fino a 7 indirizzi IP Internet (per abbonamenti multiutente) con 7 indirizzi IP di LAN, queste macchine pur essendo completamente esposte, rimarranno comunque pretette dagli attacchi base

Alcune applicazioni potrebbero non essere supportate

CONFIGURAZIONE E MONITOR

- Configurazione semplice ed immediata attraverso un comune browser (Explorer, Netscape, ecc.)
- Gestione e monitoraggio da una qualsiasi stazione di LAN locale o remota
- Supporto protocollo UpnP (Universal Plug and Play) per Windows XP, 2000 e Me.

SICUREZZA E PROTEZIONE DEI DATI

- Accesso alla configurazione protetto da password
- Tutti i pacchetti di dati provenienti dal link WAN vengono controllati e verificati.
- Tutte le richieste di accesso a stazioni presenti in LAN, WAN o DMZ sono controllati da regole di Firewall definibili dall'utente.
- Protezione automatica da attacchi di tipo Denial of Service.

FUNZIONI DI VPN GATEWAY

- Supporto IPSec standards, incluso IKE e Certificati, DES, 3DES, AES
- Supporto VPN Microsoft (PPTP) con autenticazione PAP, CHAP, MS-CHAP, MSCHAP-v2
- Supporto fino a 10 Tunnel VPN .
- Engine di crittografia hardware ad alte prestazioni per mantenere un throughput elevato anche in presenza di protocollo 3DES o AES.

1.2. CONTENUTO DELLA CONFEZIONE

- 1 FireGate 10NX
- 1 Alimentatore 12V dc
- 1 Manuale di configurazione rapida
- 1 Cd-Rom con il manuale completo

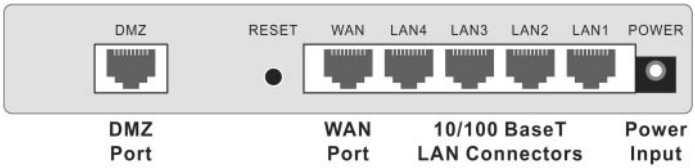
1.3. DESCRIZIONE PORTE, LED E DIP SWITCH

Fig. 1.1. Vista dei Led

1.3.1. DESCRIZIONE DEI LED

Power	Acceso – Dispositivo Acceso Spento – Dispositivo Spento
Status (Rosso)	Acceso – Condizione di errore Spento – Stato normale Lampeggiante - Durante il selftest di accensione
LAN	2 led per ogni porta ● Link/Act ● Acceso – Porta LAN attiva ● Spento – Porta Lan non attiva ● Lampeggiante - Attività dati sulla porta ● 100 ● Acceso - La porta sta operando a 100Mbit/s ● Spento - La porta sta operando a 10Mbit/s (se Link/Act acceso)
WAN	Acceso - connessione con il modem xDSL sulla porta WAN stabilita e attiva Lampeggiante - Attività dati sulla porta WAN
PPPoE	Acceso - Connessione PPPoE stabilita Spento – Nessuna Connessione PPPoE
DMZ	● Link/Act ● Lampeggiante – Attività dati sulla porta ● 100 ● Acceso - La porta sta operando a 100Mbit/s ● Spento - La porta sta operando a 10Mbit/s (se Link/Act acceso)

1.3.2. POSTERIORE



DMZ Usare un normale cavo per collegare la porta ad un HUB o Switch

Reset Pulsante di Reset. Ha due funzioni:

- Reboot. Premendo e rilasciando il pulsante si effettua un riavvio del dispositivo.
- Reset di tutte le impostazioni. Per riportare tutte le impostazioni al default di fabbrica:

1. Spegnere il dispositivo.
2. Tenere premuto il pulsante e riaccendere il dispositivo.
3. Mantenere il pulsante premuto per circa 10 secondi o finche il led di status sarà acceso per 2 volte.
4. Rilasciare il pulsante. Il dispositivo è ora tornato alle impostazioni di fabbrica.

WAN (10/100BaseT) Porta per la connessione del modem xDSL. Usare il cavo fornito con il modem o un normale cavo di LAN.

LAN1-4 (10/100BaseT) Porte LAN (MDI-X/MDI automatiche). Usare normali cavi LAN (CAT5 per 100Mbit/s). Tutte le porte si tramutano, se necessario, in "Uplink" (MDI) in modo automatico

Power port Ingresso per il cavo proveniente dall'alimentatore. Utilizzare unicamente l'alimentatore fornito nella confezione. L'utilizzo di alimentatori diversi può comportare il danneggiamento del dispositivo con conseguente invalidazione delle condizioni di garanzia.

2. INSTALLAZIONE E CABLAGGI

2

Posizione

Scegliete una posizione che sia vicina:

- Al modem xDSL
- Alla presa di alimentazione
- Ad un Hub o presa di rete se la vostra rete è composta da più di 4/5 dispositivi di rete.

Accensione e connessione alla LAN

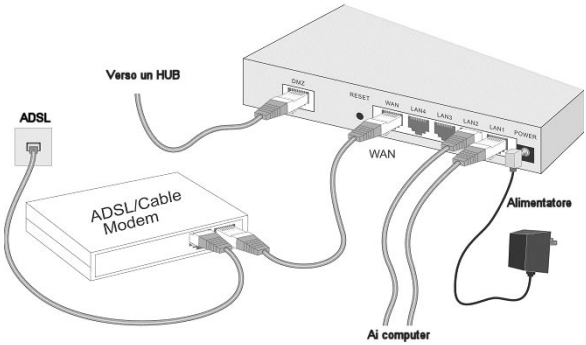
Alimentate il dispositivo utilizzando SOLO l'alimentatore fornito nella confezione e verificate che si accenda il led **Power.**

Collegate un Pc al connettore LAN1 e verificate che si accenda il led **Link/Act 1.**

Connessione alla porta DMZ

Utilizzate un normale cavo Ethernet per collegare la porta DMZ ad un Pc o ad un hub o switch (di un segmento diverso della rete).

La porta DMZ non dispone della funzionalità MDI / MDI-X



Connessione del modem xDSL

Utilizzate un normale cavo Ethernet per collegare la porta WAN del dispositivo alla porta ethernet (LAN) del vostro modem xDSL.

Verificate che si accenda il led WAN del dispositivo.

Nota: la lunghezza di ogni cavo deve essere inferiore a 100mt. I cavi devono essere Cat.5

Trovate un corretto schema di cablaggio dei cavi alla pagina:
http://www.digicom.it/digisit/faq2.nsf/numeratxt/1177?OpenDocument

2.1. CENNI PRELIMINARI PER LA CONFIGURAZIONE

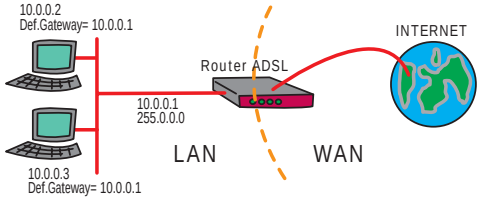
CONFIGURAZIONE FIREWALL

Questa sezione descrive gli scenari della vostra rete LAN, prima e dopo l'inserimento del Firewall, fornendovi le indicazioni principali necessarie alla corretta impostazione dell'intero sistema.

Nota: Nel nostro esempio assumiamo che gli indirizzi IP siano stati configurati in modalità fissa e non tramite DHCP (Indirizzi assegnati automaticamente, solitamente dal router ADSL). La descrizione generale è comunque valida. Fate riferimento alle sezioni DHCP e DNS per le descrizioni specifiche.

PRIMA

Ipotizziamo la tipica situazione di una rete LAN che accede ad Internet tramite un router ADSL. Tutto il sistema è già installato, configurato e funzionante.



Gli indirizzi IP e la Subnet Mask

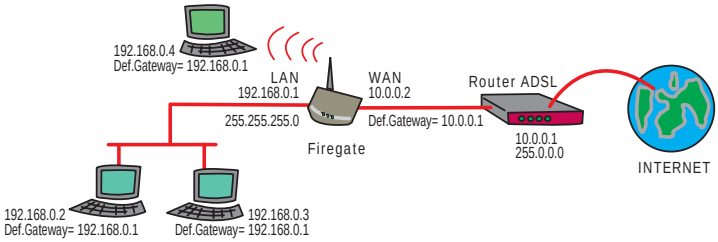
Nell'esempio illustrato, tutti i computer della rete LAN hanno un indirizzo IP appartenente alla stessa classe 10.0.0.x con Subnet Mask 255.0.0.0.
Affinchè i computer possano comunicare tra di loro tramite il protocollo TCP/IP, gli indirizzi e Subnet Mask assegnati alle stazioni di rete devono necessariamente appartenere alla stessa classe.
In questo contesto anche il Router ADSL fa parte della rete LAN e pertanto ha anch'esso un indirizzo appropriato.

Il Default Gateway

Il **Router ADSL** svolge la funzione fondamentale di fornire l'accesso ad Internet a tutti i componenti della rete LAN, pertanto ne è la "porta di uscita" verso il mondo esterno, in altre parole, il **Gateway** della rete.
Per questo motivo, tutti i computer che debbano poter accedere ad Internet dovranno avere **l'indirizzo IP del Router ADSL** impostato nel campo **Default Gateway** (o Gateway) delle impostazioni di rete TCP/IP.

DOPO

La caratteristica principale del Firewall è quella di interporre una "barriera" a protezione della rete locale, tra la LAN (Local Area Network) ed il mondo esterno, convenzionalemte chiamato "WAN" (Wide Area Network).
Il Firewall considera i due network LAN e WAN come due reti separate e distinte aventi indirizzi diversi.
Per questo motivo, inserendo il Firewall nella nostra rete sarà necessario modificare gli indirizzi IP della parte LAN come di seguito descritto (1).



Gli indirizzi IP di LAN

Nell'esempio illustrato, tutti i computer della rete LAN dovranno modificare le proprie impostazioni per "passare" alla nuova classe di indirizzi 192.168.0.x e Subnet Mask 255.255.255.0.

Il Default Gateway

Il **Firewall** svolgerà ora la funzione di punto di accesso verso il mondo esterno e pertanto diventerà il nuovo **Gateway** della rete.
Per questo motivo, tutti i computer che debbano poter accedere ad Internet dovranno avere l'indirizzo IP del Firewall impostato nel campo **Default Gateway** (o Gateway) delle impostazioni di rete TCP/IP.

Resta ora da configurare il "**lato WAN" del Firewall** per farlo comunicare con il Router ADSL.
Lasciando invariata la configurazione del router ADSL, l'impostazione della porta WAN del Firewall andrà a "sostituire" quella che era l'impostazione di una stazione di rete LAN, prima dell'inserimento del Firewall stesso.
Essendo 10.0.0.1 l'indirizzo IP del Router ADSL assegneremo alla porta WAN del Firewall un indirizzo IP appartenente alla stessa classe, ad esempio 10.0.0.2 e Subnet mask 255.0.0.0.

Dovremo anche specificare un indirizzo per il **Default Gateway** della porta **WAN**. In questo caso sarà ancora l'indirizzo IP 10.0.0.1 del Router ADSL che è di fatto il Gateway di accesso ad Internet per il Firewall.

A questo punto le stazioni della rete rete LAN saranno in grado di navigare in Internet in virtù del fatto che, di default, il Firewall non limiterà alcun accesso dalla LAN verso l'esterno mentre qualsiasi tentativo di intrusione, proveniente dall'esterno ed indirizzato verso la LAN del Firewall, verrà automaticamente impedito e bloccato.

DNS

Una volta che una stazione di rete ha la possibilità di accedere ad Internet, un'altra impostazione fondamentale è quella relativa ai DNS (Domain Name Server). In una rete TCP/IP il servizio DNS svolge la funzione di **tradurre gli URL** (ad esempio www.digicom.it) nei corrispondenti **indirizzi IP globali** (ad esempio 195.103.9.66).
Se le impostazioni DNS sono assenti o incorrette, di fatto le stazioni di rete non possono navigare in Internet.
Tutte le stazioni di rete dovranno avere **almeno un indirizzo IP configurato nel campo DNS** delle impostazioni di rete TCP/IP. Questo indirizzo è solitamente fornito dal provider Internet.
Nota: Se il router ADSL supporta la funzione di **DNS Autodiscovery/Proxy**, l'impostazione del server DNS sulle stazioni di LAN può essere l'indirizzo IP del router ADSL stesso (10.0.0.1 nel nostro esempio); sarà il router ad occuparsi di svolgere il servizio di risoluzione dei nomi DNS per la rete LAN.

DHCP

La descrizione fin qui fornita fa riferimento alle impostazioni degli indirizzi in modo "fisso" o statico.
E' possibile che una rete LAN si avvalga del servizio DHCP (Domain Host Control Protocol) per la configurazione automatica degli indirizzi. Questo servizio è svolto da un **DHCP server**, solitamente attivato sul Router ADSL, ed ha il compito di assegnare in modo automatico gli indirizzi IP, Subnet Mask, Default Gateway e DNS alle stazioni di LAN che ne fanno esplicita richiesta.

Una stazione di rete Microsoft Windows opera in **modalità DHCP** quando nelle impostazioni del protocollo TCP/IP della scheda di rete ha selezionato la voce "Ottieni automaticamente un indirizzo IP"; opera invece in modalità **fissa o statica** quando ha selezionato la voce "Utilizza il seguente indirizzo IP". La stessa cosa vale per le impostazioni dei server DNS.
Detto ciò, se la nostra rete LAN utilizzava il **servizio DHCP prima dell'inserimento del Firewall**, affinchè si possano lasciare invariate le impostazioni delle stazioni di LAN sarà necessario attivare il servizio DHCP anche nel Firewall. Si dovranno configurare un numero sufficientemente grande di indirizzi disponibili ma anche gli indirizzi dei server DNS da utilizzare in modo che, quando le stazioni di LAN ne faranno richiesta, il Firewall possa soddisfare tali richieste assegnando tutti i parametri necessari alla navigazione.

(1) Se avete libero accesso alla configurazione del Router ADSL ed avete ben compreso la descrizione della sezione “DOPO”, potete anche optare per l’alternativa di lasciare invariata la configurazione dell’intera LAN ma modificare opportunamente l’indirizzo IP del Router ADSL.

2.2. ACCESSO ALLA CONFIGURAZIONE

FireGate 10NX è interamente configurabile utilizzando un comune browser internet (come Explorer o Netscape). Per accedere alla configurazione è necessario disporre:

- Pc connesso alla LAN del firewall
- Indirizzo IP della stessa rete del firewall
- Browser con supporto Javascript

2.2.1. IMPOSTARE L’INDIRIZZO IP

Il firewall all’acquisto (o dopo un reset) è configurato con indirizzo:

IP: **192.168.0.1**
SM: **255.255.255.0**
Dhcp Server **abilitato**

Configurate il vostro Pc come Client Dhcp oppure con indirizzo IP statico 192.168.0.x(2-254) e subnet mask 255.255.255.0
Fate riferimento al **Capitolo 6.1.** per la procedura di configurazione del PC.

3. CONFIGURAZIONE BASE

3

Configurazione via Browser

1. Avviate il vostro Browser (Explorer, Netscape, ecc.)
2. Nel campo Indirizzo URL inserite "HTTP://" e l'indirizzo IP (usando l'indirizzo impostato di fabbrica: HTTP://192.168.0.1)

Se non vedete apparire la schermata iniziale verificate che:

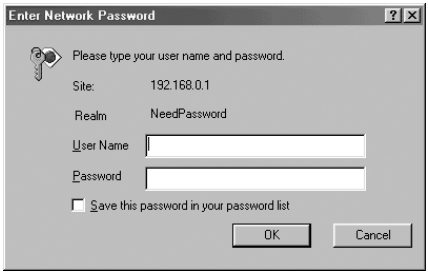
- Il dispositivo sia acceso ed il cavo di LAN è correttamente collegato.
- Il dispositivo ed il computer dal quale state tentando di accedere alla configurazione si trovino sullo stesso segmento di rete
- Nessun altro computer o dispositivo di rete stia utilizzando l'indirizzo 192.168.0.1. Se così fosse, scollegate la stazione dalla rete e modificatene l'indirizzo IP prima di ricollegarla alla rete oppure spegnetela finchè non avrete assegnato un diverso indirizzo IP Il dispositivo.
- Il vostro computer abbia un indirizzo IP compatibile. Per verificare quale sia l'indirizzo IP attualmente utilizzato dal vostro computer, dalla barra di Avvio di Windows® selezionate Esegui, inserite winipcfg (Win98) o ipconfig (WinMe/2000/XP) e cliccate OK.
- Verificate che sia selezionata la vostra scheda di rete. Verificate che l'indirizzo IP sia compreso tra 192.168.0.2 e 192.168.0.254 e il Subnet Mask sia uguale a 255.255.255.0
- Il vostro browser non sia configurato per utilizzare un Proxy server.
- Se utilizzate Internet Explorer verificate il menu Visualizza -> Opzioni -> Connessione.
- Se utilizzate Netscape verificate Opzioni -> Preferenze di rete -> Proxy.

Configurazione via UPnP

Se il vostro sistema operativo supporta UPnP, una icona per il vostro Router apparirà nel system tray notificandovi che un nuovo dispositivo di rete è stato trovato e proponendovi un collegamento.

- Se non intendete cambiare l'indirizzo IP potete accettare di creare il collegamento.
- Che accettiate o meno di creare il collegamento il router sarà raggiungibile dalle Risorse di Rete.
- Fate doppio click sull'icona del Router (Collegamento o Risorse di Rete) per iniziare la configurazione.

Se non è mai stata impostata una password vedrete la seguente schermata:



- Inserite **admin** nel campo User Name e lasciate il campo **password vuoto**.
- Cliccate su OK

Vi consigliamo di modificare successivamente user name e password tramite il menu ***Admin Login***.

3.1. CONFIGURAZIONE WAN CON "SETUP WIZARD"

Dovete avere a disposizione i dati relativi al tipo di connessione Internet con il vostro ISP.
Di seguito un riassunto delle tipologie più comuni:

Modem xDSL (ADSL, HDSL, SDSL, ecc)

Tipo	**Dettagli**	**Dati ISP richiesti**
Dynamic IP address	Indirizzo IP dinamico. L'indirizzo IP è allocato automaticamente quando ci si connette con l'ISP	Nessuno
Static (Fixed) IP Address	Indirizzo IP assegnato staticamente.	Indirizzi e Subnet mask a voi assegnate.
PPPoE	Connessione all'ISP in modalità PPP over Ethernet. L'assegnazione dell'indirizzo è automatica.	User name e password.
PPTP	Connessione all'ISP in modalità Point to Point Tunneling. L'assegnazione dell'indirizzo è solitamente dinamica ma può essere statica.	· Indirizzo IP del PPTP Server. · User name e password. · Indirizzi e Subnet mask a voi assegnate (se statico)

Other Modems (Altri modem, Router o Wireless)

Tipo	**Dettagli**	**Dati ISP richiesti**
Dynamic IP Address	Indirizzo IP dinamico. L'indirizzo IP è allocato automaticamente quando ci si connette con l'ISP	Nessuno
Static (Fixed) IP Address	Indirizzo IP assegnato staticamente.	Indirizzi e Subnet mask a voi assegnate.

Cable Modems

Tipo	**Dettagli**	**Dati ISP richiesti**
Dynamic IP Address	Indirizzo IP dinamico. L'indirizzo IP è allocato automaticamente quando ci si connette con l'ISP	Generalmente nessuno. L'ISP potrebbe richiedere delle impostazioni come Hostname, Domain name, o MAC Address.
Static (Fixed) IP Address	Indirizzo IP assegnato staticamente.	Indirizzi e Subnet mask a voi assegnate. L'ISP potrebbe richiedere delle impostazioni come Hostname, Domain name, o MAC Address.

Big Pond (Australia) e SingTel RAS

- Non utilizzati in Europa

Selezionate la modalità in base alla vostra tipologia di collegamento e proseguite nella configurazione cliccando su Next. Inserite i dati nelle apposite caselle.

Esempi di configurazione:

- **Accesso Internet tramite modem (Bridge) ADSL* e protocollo PPPoE:**

Selezionate DSL/ADSL modem, selezionate PPPoE, inserite User name e password, deselezionate le voci "Connect automatically…" e "Disconnect after idle…", selezionate "Dynamic" per gli accessi con IP dinamico, selezionate "Static" se l'indirizzo IP è statico, inserite l'IP di WAN e l'indirizzo del DNS (fornito dall'ISP) in DNS.

- **Accesso ad Internet tramite Router ADSL* con NAT e IP dinamico:**

Se la vostra LAN (e di conseguenza il Router ADSL) sta utilizzando gli indirizzi IP del range 192.168.0.x, modificate l'IP del router ADSL (ad esempio 10.0.0.1/255.0.0.0).
Selezionate Other, selezionate "Static" IP address, inserite un indirizzo IP libero appartenente al range assegnato al router ADSL, Subnet mask e Gateway (ad esempio rispettivamente 10.0.0.2, 255.0.0.0 e 10.0.0.1. Inserite l'indirizzo del DNS (o un indirizzo fittizio) in DNS

- **Accesso ad Internet tramite Router ADSL* con IP pubblico:**

Selezionate Other, selezionate "Static" IP address, inserite uno degli indirizzi IP pubblici disponibili in IP address, inserite la Subnet mask, inserite l'indirizzo IP del router ADSL in Gateway, inserite l'indirizzo del DNS (fornito dall'ISP) in DNS.

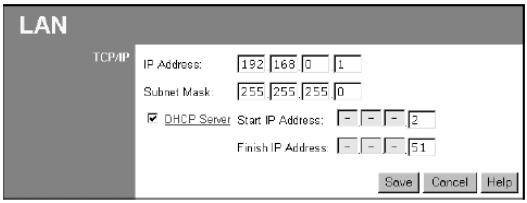
**** La porta LAN del Bridge o Router ADSL deve essere collegata alla porta WAN del dispositivo.***

Al termine cliccate su **Finish**. Se avete selezionato "Test Internet connection" verrà verificata la raggiungibilità della parte WAN.
Cliccate su **Close** per chiudere il Wizard.

3.2. CONFIGURAZIONE LAN

LAN

Cliccate su LAN per accedere ai parametri della sezione LAN.



TCP/IP

IP Address	Queste impostazioni dipendono dalle impostazioni della vostra LAN:
Network Mask	Se utilizzate il DHCP server (consigliato): Generalmente nessun cambiamento è richiesto per queste impostazioni. Comunque tutti i dispositivi in rete devono essere impostati come DHCP Client oppure utilizzare un indirizzo IP e Subnet mask compatibile. Se in LAN è già presente un DHCP server: De-selezionate il DHCP server interno per non incorrere in conflitti Se la LAN utilizza indirizzi IP statici: Impostate per il router un indirizzo IP tra quelli non utilizzati della LAN. La Network Mask deve essere la stessa utilizzata per i PC in rete.

Se abilitato (default), il router fornirà gli indirizzi IP e dati relativi ai computer DHCP client che ne faranno richiesta.
Se necessario modificate i campi Start IP Address e Finish IP Address per adattarli alla vostra LAN.
Queste impostazioni determinano anche quanti client saranno gestiti.

Save	Salva nel dispositivo le modifiche apportate
Cancel	Ignora le modifiche apportate e ricarica I parametri dal dispositivo

3.3. CONFIGURAZIONE PC PER ACCESSO AD INTERNET

Dopo aver configurato la sezione di WAN ed aver eventualmente modificato la sezione di LAN, tutti i Pc correttamente configurati possono già accedere ad Internet.
Tutti i Pc dovranno essere configurati in Dhcp Client oppure con indirizzo IP statico compatibile con l'indirizzo ipostato nella sezione LAN del firewall.

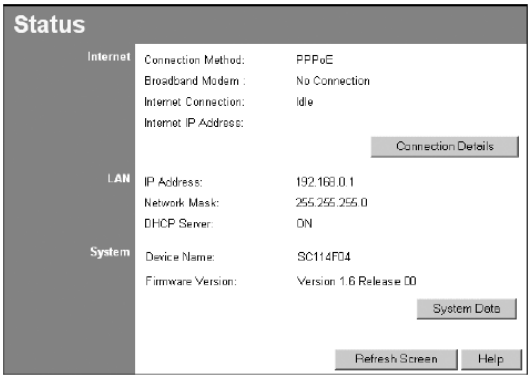
Esempio:

	Indirizzo IP (LAN)	**Subnet Mask (LAN)**	**Gateway**	**DNS**
FireGate 10NX	192.168.0.1	255.255.255.0	----------	Forniti dall'ISP
PC	192.168.0.xxx (2-254)	255.255.255.0	192.168.0.1 (indirizzo FireGate)	Forniti dall'ISP

3.4. STATUS

Status

La finestra di Status permette di verificare lo stato della connessione WAN, della sezione LAN e del Sistema.



Internet

Connection Method	Indica il metodo di connessione, come impostato nel Wizard
Broadband Modem	Stato della connessione (WAN)
Internet Connection	Stato della connessione Internet: · Active (attivo) · Idle (a riposo) · Unknown (sconosciuto) · Failed (fallito)

In caso di errori potete cliccare “Connection Details” per maggiori dettagli.

Internet IP Address	L’indirizzo IP assegnato dall’ISP (Internet Service Pr ovider).
“Connection Details”	Descrizione dettagliata della connessione corrente

LAN

IP Address	Indirizzo IP del dispositivo
Network Mask	Network Mask (Subnet Mask) associata all’indirizzo IP
DHCP Server	Stato del DHCP Server interno: “Enabled” (abilitato) o “Disabled” (disabilitato).

System

Device Name	Identificativo del dispositivo.
Firmware Version	Versione del firmware attualmente a bordo del dispositivo.
System Data	Informazioni varie di sistema.

Bottoni

Connection Details	Finestra dei dettagli relativi alla connessione
System Data	Visualizza ulteriori informazioni varie di sistema
Refresh Screen	Aggiorna le informazioni visualizzate.

4. CONFIGURAZIONE AVANZATA

4

FireGate 10NX mette a disposizione una serie di funzioni avanzate che permettono una completo controllo delle sessioni in Ingresso ed in Uscita dal Firewall.

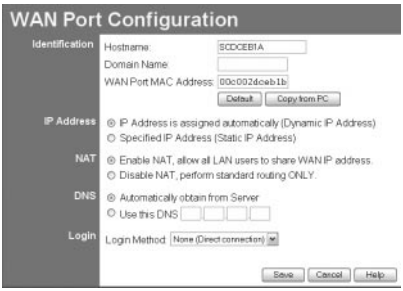
Questo manuale tratta la descrizione delle funzionalità della versione Firmware **"Version 1.0 Release 02".** Eventuali differenze con versioni firmware successive saranno descritte direttamente negli aggiornamenti scaricabili dal sito www.digicom.it

La struttura attuale dei menù di configurazione avanzata è la seguente:

4.1. INTERNET

4.1.1. WAN PORT

In questa schermata è possibile impostare l'indirizzo IP di WAN del Router, la configurazione è alternativa al *Setup Wizard* spiegato nei capitoli precedenti.



Identification:

Hostname:	imposta il nome del dispositivo
Domain name:	imposta il dominio di rete a cui, eventualmente, appartiene il dispositivo
WAN Port MAC Address:	al default viene mostrato il MAC address del dispositivo, se il vostro abbonamento prevede che a collegarsi sia un solo MAC address specificato, è possibile impostare un MAC address a scelta. *Copy from PC* imposta il MAC copiandolo dalla scheda di rete del PC utilizzato per la configurazione.

IP Address:

IP A. Assigned automatically: abilita la funzione DHCP Client sulla porta WAN

Specified IP A.:	Se selezionato apre la finestra dove impostare Indirizzo IP, Subnet Mask e Gateway per la porta WAN.

NAT:

Enable:	NAT abilitato, questa opzione abilita l'utilizzo del NAT e tutte le funzionalità del Firewall.
Disable:	NAT disabilitato, tutte le funzionalità del firewall associate all'utilizzo di un NAT (Virtual Server, Multi-DMZ, etc.) sono disabilitate. Il dispositivo si comporta come un normale router Ethernet, con l'aggiunta della possibilità di gestire direttamente il passaggio di protocolli e indirizzi IP.

DNS:

Automatic obtain from Server: l'indirizzo del Server DNS viene chiesto al provider Internet.

Use this DNS:	inserite il DNS che volete utilizzare nella connessione.

Login:

se necessario selezionate il metodo di autenticazione per la connessione con il provider Internet. I tipi di autenticazione possibili e i loro parametri sono elencati nella descrizione del Setup Wizard.

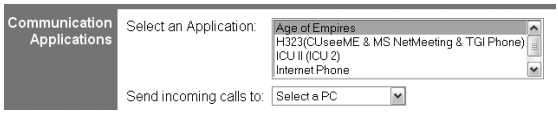
Cliccate sul tasto **Save** per salvare le modifiche effettuate in questa pagina.

Nota! Se utilizzate un indirizzo IP fisso sulla WAN e non c'è Login con il server Internet, non è possibile utilizzare la funzione Automatic obtain from Server. Se l'indirizzo DNS non viene inserito o non viene assegnato il dispositivo utilizzerà i due Backup DNS impostabili nella finestra di configurazione Options.

4.1.2. ADVANCED SETUP

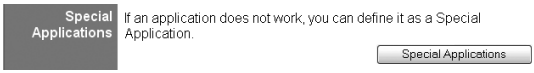
La pagina di configurazione **Advanced Setup** permette la configurazione delle seguenti sezioni:

4.1.2.1. Communication Applications

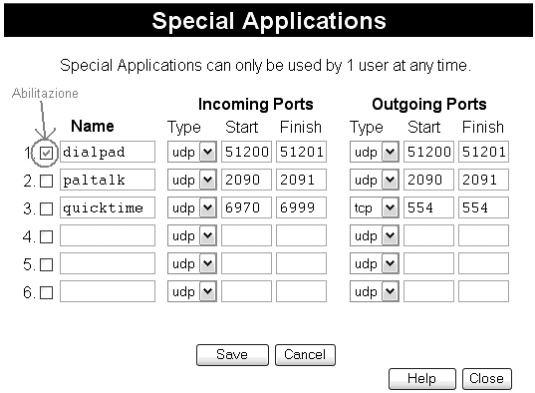


La maggior parte delle applicazioni sono supportate in modo trasparente dal dispositivo, tuttavia alcune particolari applicazioni possono non funzionare correttamente in presenza del protocollo NAT. Se dovete utilizzare una delle applicazioni indicate nella lista, selezionatela e associatela ad una macchina di LAN selezionandolo dalla lista *Send incoming calls to:*
La lista dei PC di LAN è personalizzabile con l'apposita funzione *PC Database* descritta più avanti.

4.1.2.2. Special Applications



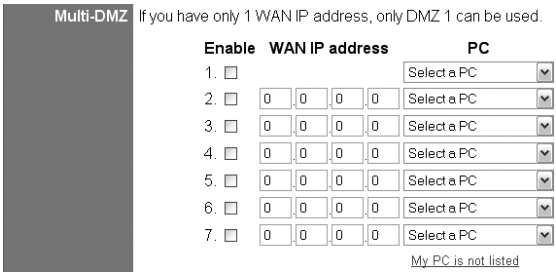
Alcune applicazioni utilizzano gruppi di porte differenti in ingresso e in uscita.
Selezionando **Special Applications** è possibile definire il range di porte utilizzate da un applicazione.



Name: inserite il nome dell'aplicazione che volete configurare
Incoming Port: selezionate il protocollo (*Type*, TCP o UDP) e definite il range di porte (da *Start* a *Finish*) che l'applicazione utilizza in ingresso.
Outgoing Port: selezionate il protocollo (*Type*, TCP o UDP) e definite il range di porte (da *Start* a *Finish*) che l'applicazione utilizza in uscita dal Firewall.

Abilitate l'applicazione mettendo una spunta nella casella a fianco del nome e selezionate **Save** per salvare le impostazioni.
Quando una macchina in rete utilizza l'applicazione definita impegnando in uscita una delle porte definite in Outgoing Port verranno automaticamente aperte le porte definite in Incoming Port verso l'indirizzo IP della macchina in oggetto. Questo permette potenzialmente l'utilizzo dell'applicazione a TUTTE le macchine presenti in rete anche se **una sola macchina alla volta potrà utilizzare questo servizio.**

4.1.2.3. Multi-DMZ



Multi-DMZ 1

La prima Multi-DMZ (1.) configurabile è una funzionalità standard che viene solitamente definita come DMZ Software. La sua funzione è quella di rendere completamente visibile da Internet una macchina presente in LAN.

Abilitando questa funzione, tutte le sessioni in ingresso non riconosciute (non specificate in altre regole) vengono passate alla macchina posta in Multi-DMZ 1.

Multi-DMZ 2-7

Questa funzionalità è disponibile solo se il vostro abbonamento Internet prevede l'utilizzo di n (più di uno) indirizzi IP pubblici.
Fino ad un massimo di 6 macchine connesse alla vostra rete interna (indirizzi privati) potranno essere completamente raggiungibili dall'esterno utilizzando tutti gli indirizzi IP pubblici del vostro abbonamento.

Il dispositivo effettua una associazione 1 ad 1, la macchina indicata nel campo **PC** inivierà in Internet i pacchetti con l'indirizzo IP specificato nel campo **WAN IP Address** della stessa riga.

Tutti gli indirizzi di WAN dovranno necessariamente appartenere alla stessa subnet dell'indirizzo IP di WAN principale.

Note sulla sicurezza.

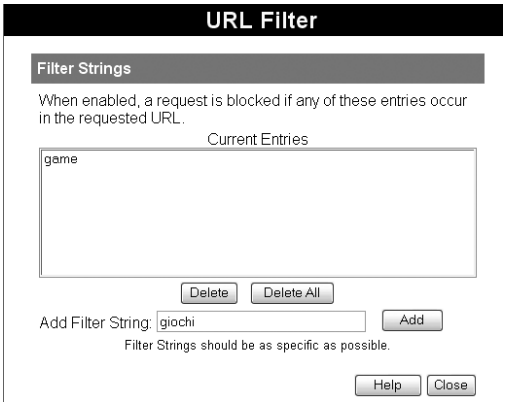
Configurando una macchina in DMZ si viene a creare una situazione di potenziale rischio, perché il PC riceve direttamente tutte le sessioni indirizzate all'indirizzo di WAN associato.
E' consigliabile l'utilizzo di questa funzione SOLO se assolutamente necessario.
Mantenete sempre aggiornati i server che lavorano sulle macchine in DMZ, per sistemare tutti i bug che vegono costantemente scoperti.

Un PC posto in DMZ è comunque più sicuro di un PC non collegato al firewall perché le funzionalità base di protezione dagli attacchi DoS restando attive.

4.1.2.4. URL Filter

Questa funzionalità permette di abilitare il filtraggio delle pagine Web visualizzabili.
Ogni pagina Web è raggiungibile tramite un URL (http://www.digicom.it/...../.....); utilizzando questa funzione è possibile bloccare l'accesso ad indirizzi che contengono parole specifiche (ad esempio sex , game , giochi etc.)

Selezionate il tasto **Configure URL Filter** per definire l'elenco di parole da bloccare.



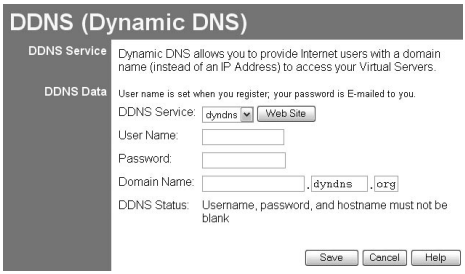
Inserite le parole da cercare nella casella **Add Filter String** e cliccate sul tasto **Add.**
La parola verrà inserita nell'elenco.

Le parole inserite devono essere il più specifico possibile, per evitare che vengano bloccate anche pagini utili.

4.1.3. DYNAMIC DNS

Utilizzando un abbonamento Internet con un indirizzo IP dinamico, si ha lo svantaggio di non poter offrire servizi all'esterno perché di volta in volta si utilizza un indirizzo differente.

Il servizio Dynamic DNS offre la possibilità di essere sempre raggiungibili (con qualsiasi indirizzo IP) utilizzando un nominativo come ***vostronome.dyndns.org***
Per poter utilizzare questa funzionalità è necessario effettuare una registrazione gratuita al servizio Dynamic DNS, alla pagina www.dyndns.org



DDNS Service: Selezionate il provider del servizio di Dynamic DNS che volete utilizzare. (dyndns è il più utilizzato, eventualmente potete utilizze gli altri che compaiono in lista)
User Name: Inserite il nome con cui vi siete registrati al servizio
Password: Inserite la password con cui vi siete registrati al servizio.
Domain Name: Inserite il dominio che avete abilitato.

Cliccate sul tasto **Save** per salvare le impostazioni ed effettuare il primo aggiornamento.

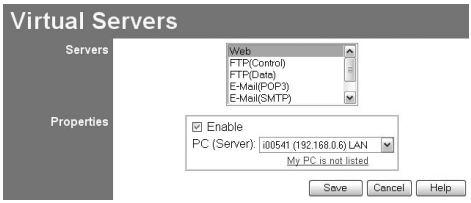
DDNS Status indicherà lo stato della registrazione al servizio.

4.1.4. VIRTUAL SERVERS

La funzione **Virtual Server** permette ad utenti localizzati in Internet di avere accesso a Server presenti in LAN attraverso il Firewall.

Normalmente un utente presente in Internet non ha accesso ai Server della vostra LAN perché:

- Il Server non ha un indirizzo IP globale
- Il NAT blocca ogni sessione originata da in Internet e diretta al suo indirizzo di WAN, perché non può sapere a priori a quale macchina di LAN la sessione è realmente indirizzata.



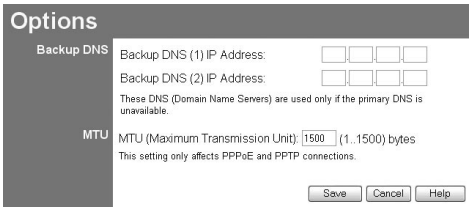
In questa finestra è possibile abilitare in modo rapido l'esportazione dei principali Server.

Selezionate il servizio da esportare dalla lista **Servers**
Nella finestra **Properties** selezionate **Enable** ed indicate dalla lista **PC (Server)** la macchina che offre tale servizio.
L'elenco della macchine è personalizzabile dal menù **PC Database** (spiegato nel capitolo **Other**)

Per gestire l'esportazioni di Server differenti a quelli presenti in lista è necessario utilizzare la funzione **Firewall Rules** (capitolo **Security**).

Cliccate su **Save** per salvare le impostazioni effettuate.

4.1.5. OPTIONS



Backup DNS

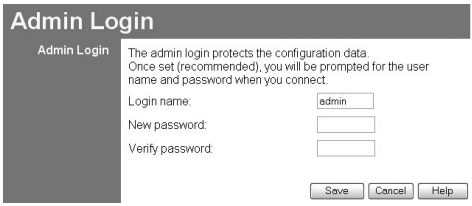
In questa sezione è possibile definire due indirizzi DNS di Backup.
Se l'indirizzo DNS impostato nella sezione WAN non è raggiungibile, il dispositivo utilizzerà i DNS indicati in questa pagina.

MTU

Il parametro MTU viene sempre impostato a 1500, alcuni provider Internet possono richiedere un valore inferiore per ottimizzare il traffico.
Modificate questo valore secondo le indicazioni del vostro ISP.

4.2. SECURITY

4.2.1. ADMIN LOGIN



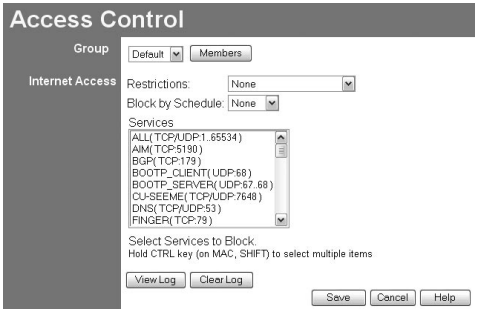
In questa sezione è possibile impostare un username ed una password per l'accesso alla configurazione del dispositivo.
E' sempre consigliata l'impostazione di una password, per evitare l'accesso ad utenti indesiderati; questa impostazione diventa obbligatoria se intendete abilitare la configurazione da remoto.

Login name: inserite l'User Name che volete utilizzare
New password: inserite la password per l'accesso
Verify password: ripetete l'inserimento della password per verifica.

4.2.2. ACCESS CONTROL

La funzione Access Control permette all'amministratore di rete di porre delle restrizioni per l'accesso ad Internet per le macchine di LAN.

Al Default le restrizioni di accesso sono disabilitate, cioè tutte le macchine connesse in LAN possono accedere a tutti i servizi disponibili in Internet.



Group

E' possibile definire fino a 5 gruppi di PC a cui applicare regole differenti.
Selezionate il gruppo che voltete configurare e cliccate sul tasto **Members** per aggiungere la macchine al gruppo; la selezione delle macchine si basa sulla lista **PC Database** (descritta nel capitolo **Other**).
Il gruppo **Default** invece racchiude tutte le macchine che non sono esplicitamente inserite in altri gruppi.

Internet Access

In questa sezione potete selezionare la restrizione da applicare al gruppo selezionato.
Restrictions – Block all Internet access Blocca TUTTE le sessioni in Ingresso/Uscita per le macchine inserite nel gruppo.
Restrictions – Block selected Services Blocca solamente i servizi selezionati dalla lista **Services**

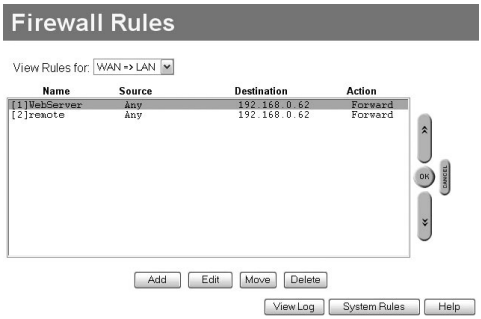
Block by Schedule se abilitato (selezione **Default**) applica le restrizioni SOLO negli orari definiti nella sezione **Scheduling.**

Cliccando sul tasto **View Log** è possibile visualizzare i tentativi di accesso che sono stati bloccati dal Firewall ed il nome della macchina che li ha generati.
Cliccate sul tasto **Clear Log** per cancellare il Log.

Terminata la configurazione cliccate sul tasto **Save** per salvare le impostazioni.

4.2.3. FIREWALL RULES

La funzione primaria del Firewall è quella di bloccare gli attacchi DoS (Denial of Service) attacks.
Un attacco DoS non mira a penetrare le difese del Firewall per accedere a dati riservati ma a saturare la banda disponibile per la connessione Internet rendendola di fatto inutilizzabile.
Oltre alla protezione DoS il Firewall permette di creare "regole" per gestire direttamente (bloccare o permettere) il passaggio di qualsiasi sessione dati.
La configurazione delle Firewall Rules richiede un attenta pianificazione per evitare di incorrere in situazioni di compromissione della sicurezza.
Queste configurazioni devono essere effettuate da Amministratori di sistema.



La finestra principale mostra un riassunto di tutte le regole di Firewall configurate, divise per direzione e priorità.

View Rules for:

Indica la direzione presa in considerazione, per ogni direzione verranno visualizzate le rispettive regole nella finestra sottostante. Le direzioni possibili sono:

WAN => LAN	gestione dei pacchetti in ingresso verso le macchine collegate alla LAN
WAN => DMZ	gestione dei pacchetti in ingresso verso le macchine collegate alla porta fisica DMZ
LAN => WAN	gestione dei pacchetti in uscita dalla LAN verso la WAN
DMZ => WAN	gestione dei pacchetti in uscita dalla DMZ verso la WAN

Nella finestra di gestione delle regole vengono visualizzati i seguenti campi:

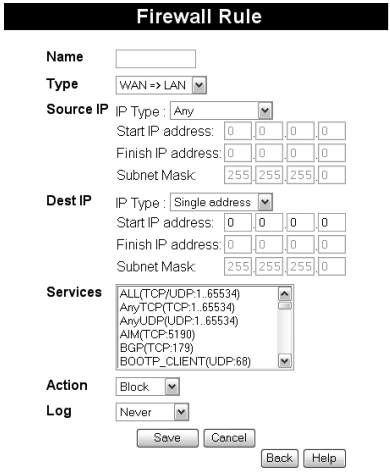
Indicatore di priorità	Il primo campo è racchiuso tra due parentesi quadre **[**xx**]**; la regola **[**01**]** verrà applicata prima della regola **[**02**]...**
Name	Viene visualizzato il nome mnemonico associato alla regola.
Source	Sorgente del traffico, definito da un indirizzo IP.
Destination	Destinatario del traffico, definito da un indirizzo IP.
Action	Indica l'azione intrapresa dal Firewall se riconosce un pacchetto appartenente alla sessione descritta nella regola; **Forward** permette il passaggio, **Block** scarta il pacchetto.

I tasti effettuano le seguenti operazioni:

Add	Aggiunge una nuova regola
Edit	Modifica la regola selezionata
Move	Cambia la posizione alla regola selezionata (prioprità). Cliccate su **Move** ed indicate il nuovo indice di priorità.
Delete	Elimina la regola selezionata.
View Log	Visualizza il **Firewall Rules Log**
System Rules	Visualizza un report di tutte le regole inserite nel Firewall

4.2.3.1. Aggiunta / modifica di una regola

Aggiungendo o modificando una regola si accede alla seguente finestra di configurazione:



Name

Inserite il nome mnemonico da associare alla regola

Type

Selezionate la direzione del pacchetto che volete controllare

Source IP / Dest IP

Indicate il sorgente ed il destinatario del pacchetto.
Il tipo di selezione effettuabile è:

Any	da qualsiasi indirizzo IP / Subnet Mask
Single Address	dall'indirizzo IP specifico indicato nel campo *Start IP Address*
Address Range	dal tutti gli indirizzi IP compresi in *Start IP Address* e *Finish IP Address*
Subnet Address	da tutti gli indirizzi IP appartenenti alla rete definita da *Start IP Address* e *Subnet Mask*

Services

Selezionate il servizio (protocollo/porte) del pacchetto da gestire.
Se necessario è possibile aggiungere nuovi Services dall'apposito menù.

Action

Impostate l'azione da applicare alla regola: **Forward** permette il passaggio oppure **Block** blocca, scarta il pacchetto.

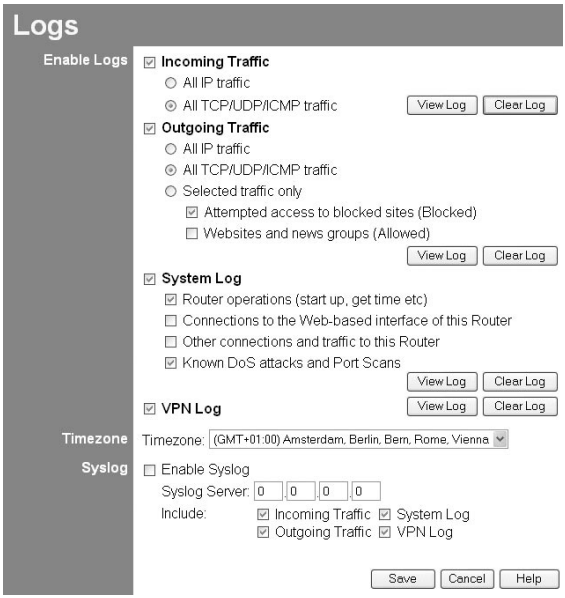
Log

Indica se e quando inserire nel Log il traffico corrispondente a questa regola, le opzioni selezionabili sono:

Never	non inserire nei Log
Always	inserisci sempre nei Log
Match	inserisci solo per i pacchetti corrispondenti alla regola
Not Match	inserisci solo per i pacchetti non corrispondenti alla regola

4.2.4. LOGS

I log tracciano e registrano vari tipi di attività svolte dal dispositivo. L' utilità dei log è fondamentale per la determinazione e risoluzione di eventuali problemi, ma può generare un gran numero di dati e influire sulle prestazioni generali del dispositivo. Date le basse capacità di memorizzazione del dispositivo stesso, i log possono essere inviati via email ad un indirizzo predeterminato.



Data - Logs Screen

Enable Logs

Incoming Traffic Selezionare l'opzione desiderata:

- **All IP traffic** – effettua il log di tutte le connessioni TCP/IP entranti, di qualsiasi tipo. Questa opzione genera dei log molto corposi, riempendo I buffer molto velocemente.
- **All TCP/UDP/ICMP traffic** – Questi 3 protocolli sono quelli più spesso utilizzati nelle connessioni Internet. TCP è utilizzato per HTTP, FTP, Telnet, E-mail e altre applicazioni tipiche. UDP è spesso utilizzato per Video streaming e altre comunicazioni dove la velocità è più importante del recapito garantito dei pacchetti. ICMP è utilizzato per diagnostiche tipo "ping" e "trace route".

Outgoing Traffic Selezionare l'opzione desiderata:

- **All IP traffic** - - effettua il log di tutte le connessioni TCP/IP uscenti, di qualsiasi tipo. Questa opzione genera dei log molto corposi, riempendo I buffer molto velocemente.
- **All TCP/UDP/ICMP traffic** – Vedi sopra.

Siccome verranno loggate la maggiorparte delle connessioni, i log rimarranno molto corposi.

- **Selected Traffic only** – Questa selezioni riduce sensibilmente la dimensione dei log. Saranno loggate solamente le connessioni HTTP. Selezionare il traffico che desiderate includere:
- *Attempted access to blocked sites* – Solamente connessioni bloccate da URL filter.
- *Websites and news groups* – Solamente le connessioni riuscite a siti Web e server Newsgroup.

System Log Selezionare l'opzione desiderata:

- **Router operations (start up, get time etc)** – Normali operazioni di routers.
- **Connections to the Web - based interface of this Router** – Connessioni all'interfaccia Web del dispositivo.

	● **Other connections and traffic to this Router** – Altre connessioni e traffico verso il dispositivo, come PINGS o pacchetti RIP (Router Information Protocol). ● **Known DoS attacks and Port Scans** – Attacchi DoS (Denial of Service) che sono stati bloccati dal Firewall integrato. Il Firewall utilizza la tecnologia "Stateful Inspection" per bloccare pacchetti che possono essere individualmente validi ma che collettivamente possono rappresentare un attacco. Vengono anche loggati Scan ad una serie di porte, per determinare se queste sono aperte
VPN	Se abilitato, vengono loggate le connessioni VPN entranti ed uscenti
View Log Button	Viasualizza il log
Clear Log Button	Cancella il log

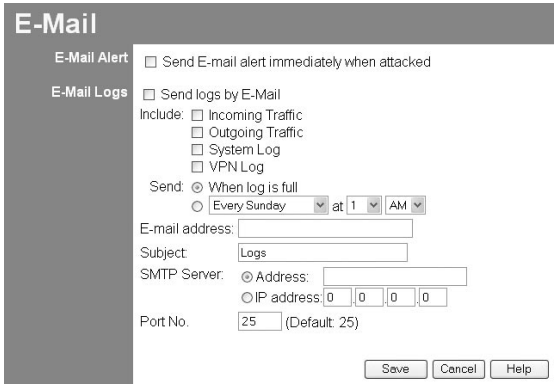
Timezone

Timezone	Selezionare la Timezone corretta al fine di associare la corretta data/ora alle informazioni dei log

Syslog Server

Enable Syslog	Se abilitato, I log verranno inviati al Syslog Server.
Syslog Server	Inserire l'indirizzo IP del Syslog Server.
Include	Selezionare I log da inviare al Syslog Server.

4.2.5. EMAIL



E-Mail

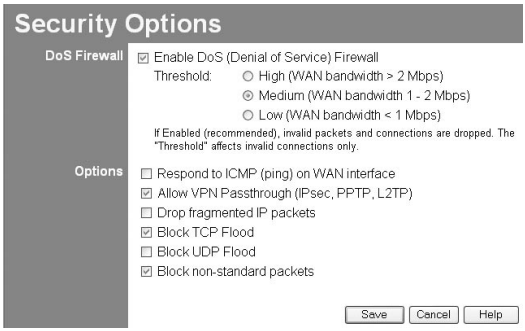
E-Mail Alerts

Send E-Mail alert	Se selezionato una E-mail viene inviata immediatamente in caso di un attacco DoS (Denial ofService).

E-Mail Logs

Send Logs by E-Mail	Se abilitato I log veraano inviati via email all'indirizzo configurato
Include	Selezionare quali log si desidera ricevere via e-mail
Send	● Selezionare quando si desidera ricevere I log via e-mail. **When log is full** - Quando il log raggiunge la massima capacità di memorizzazione. **Every day, Every Monday...** - Il log viene inviato agli intervalli selezionati. · Selezionando "Every day" il log verrà inviato all'ora selezionata. · Selezionando un giorno specifico, il log verrà inviato una volta alla settimana. · Se il log si riempie prima della data/ora specificata, questo verrà inviato comunque subito.
E-mail address	Inserire l'indirizzo e-mail al quale inviare il log. Questo indirizzo comparirà anche come mittente.
Subject	Inserire il "soggetto" per l'e-mail.
SMTP Server	Inserire l'indirizzo IP del server SMTP (Simple Mail Transport Protocol) per la posta in uscita.
Port No.	Inserire il numero di porta del server SMTP, generalmente 25.

4.2.6. SECURITY



Security

SPI Firewall

Enable DoS Firewall Se abilitato gli attacchi di tipo DoS (Denial of Service) saranno intercettati e bloccati. Si raccomanda di lasciare questa opzione abilitata.
Note:
· Un attacco DoS non mira a penetrare le difese e carpire dati ma piuttosto a saturare la banda disponibile sulla connessione Internet rendendola di fatto inutilizzabile.
· Il dispositivo utilizza la tecnologia "Stateful Inspection" in grado di determinare quando singoli pacchetti TCP/IP possono essere validi ma in situazioni particolari e ben precise, questi rappresentano un DoS attack.

Threshold Questa impostazione interviene sul numero massimo di connessioni "half-open" accettate e permesse.
· Una connessione "half-open" si verifica quando un client remoto apre una sessione con il server senza poi proseguire a fronte delle richieste del server.
· Mentre il numero ottimale delle connessioni "half-open" permesse può dipendere da molti fattori, il fattore primario è la capacità di banda della vostra connessione Internet.
· Selezionare l'opzione che corrisponde alla vostra bada per la connessione Internet.

Options

Respond to ICMP Il protocollo ICMP è utilizzato da programmi tipo "ping" e "traceroute", di monitor o discovery.
· Se selezionato il dispositivo risponderà a pacchetti ICMP provenienti da Internet.
· Se non selezionato il dispositivo non risponderà a pacchetti ICMP provenienti da Internet, ignorandoli e accrescendo la sicurezza.

Allow VPN pass-through ● Se selzionato, I computer della LAN potranno stabilire delle connessioni VPN direttamente (VPN non stabiliota dal FireGate), utilizzando l protocolli IPSEC, PPTP, L2TP.

Drop fragmented IP packets Se abilitato, I pacchetti frammentati vengono scartati, forzando una ritrasmissione. Ciò può impedire il funzionamento di applicazioni. Normalmente questa opzione dovrebbe rimanere disabilitata.

Block TCP Flood Un TCP flood è un numero estremamente alto di richieste di connessioni TCP. Solitamente identifica un attacco DoS (Denial of Service). Normalmente questa opzione dovrebbe rimanere abilitata

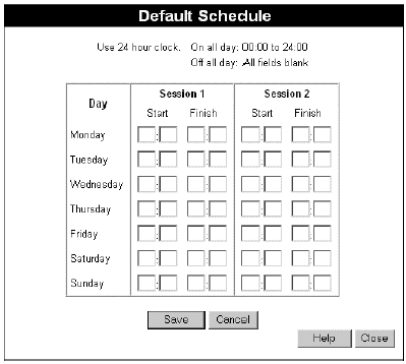
Block UDP Flood Un UDP flood è un numero estremamente alto di pacchetti UDP. Spesso identifica un attacco DoS (Denial of Service).
Normalmente questa opzione dovrebbe rimanere abilitata

Block non-standard packets Pacchetti di dimensioni o formati abnormi sono sopesso utilizzati daglu hacker per condurre degli attachi DoS. Possono anche essere generati da dispositivi di rete guasti o malconfigurati.
This setting should normally be enabled.
Normalmente questa opzione dovrebbe rimanere abilitata

4.2.6. SCHEDULING

Scheduling

- Lo scheduling può essere (opzionalmente) applicato ad un gruppo Access Control.
- Il blocco dei servizi avverrà durante il periodo definito (tra “Start” e “Finish”)
- Possono essere definiti due (2) sessioni o periodi differenti
- Il formato di inserimento è quello 24 ore.
- I campi vuoti non definiscono alcuno scheduling.

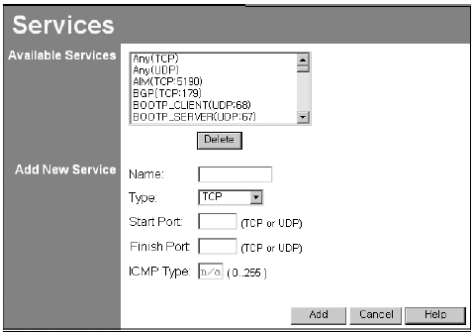


Data - Default Schedule Screen

Day	Giorno della settimana
Session 1 - Session 2	Possono essere definiti due (2) sessioni o periodi differenti. La sessione 2 può essere lasciata vuota.
Start Time	Ora di inizio (24h) della restrizione.
Finish Time	Ora di termine (24h) della restrizione.

4.2.7. SERVICES

Questa funzione può essere usata per definire dei servizi che possono essere filtrati o permessi in Access Control e Firewall Rules. Sono presenti molti servizi comuni pre-definiti ed è possibile aggiungere de nuovi servizi definiti dall'utente.



Services

Available Services

Available Services	Lista dei servizi disponibili
"Delete"	Cancella I servizi aggiunti manualmente. I servizi predefiniti non possono essere eliminati.

Add New Service

Name	Nome mnemonico del servizio, senza spazi o punti.
Type	Selezionare il protocollo (TCP, UDP, ICMP) usato dal servizio.
Start Port	Inizio del range di porte utilizzato dal servizio. Se la porta è singola specificare lo stesso numero sia in "Start" che "Finish".
Finish Port	Fine del range di porte utilizzato dal servizio. Se la porta è singola specificare lo stesso numero sia in "Start" che "Finish".
ICMP Type	Per servizi basati su ICMP inserire il tipo (numero) del servizio

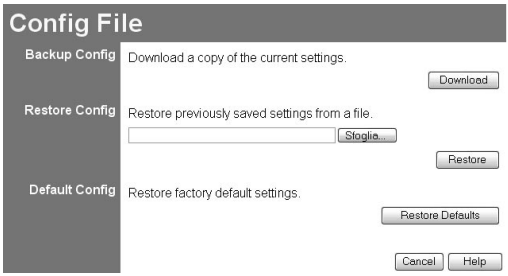
Bottoni

Delete	Cancella il servizio selezionato dalla lista
Save	Aggiunge il servizio alla lista usando i dati presenti in "Add New Service".
Cancel	Azzera l'area "Add New Service " per l'aggiunta di una nuova entry.

4.3. OTHER

4.3.1. CONFIG FILE

Questa funzionalità offre la possibilità di salvare la configurazione del dispositivo su file.
In questo modo è possibile disporre di "profili" preconfigurati e di avere una copia di backup della configurazione in caso di problemi.



Backup Config

Effettua il salvataggio della configurazione attuale; cliccate su **Download** per salvare il file di configurazione sul PC.

Restore Config

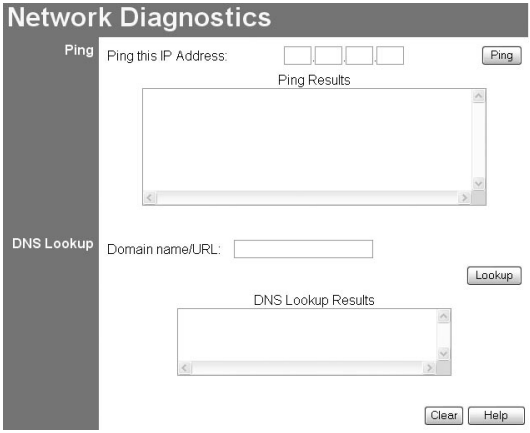
Effettua il ripristino di una configurazione salvata; cliccate su **Sfoglia...** per selezionare il file di configurazione dal vostro PC e successivamente cliccate su **Restore** per avviare il ripristino.

Default Config

Effettua il rispristino alle impostazioni di fabbrica; cliccate su **Restore Defaults** per ripristinare la configurazione dei fabbrica.

4.3.2. NETWORK DIAG

In questa sezione è possibile effettuare dei ping verso l'esterno direttamente dall'interfaccia WAN del Firewall e testare il funzionamento dei server DNS tramite il DNS Lookup.



Ping

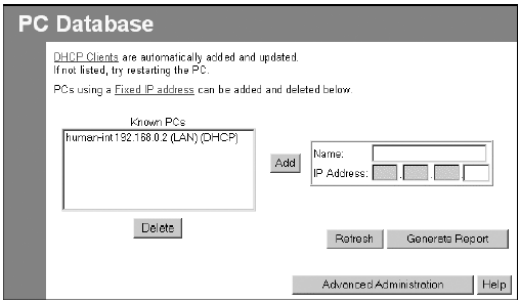
Inserite l'indirizzo IP sul quale effettuare il Ping nel campo **Ping this IP Address.**
Cliccate su **Ping** per effettuare l'operazione.
Nella finestra **Ping Status** verrà visualizzato il risultato dell'operazione.

DNS Lookup

Inserite il nome o l'URL da risolvere nel campo **Domain name/URL** e cliccate su **Lookup.**
Nella finestra **DNS Lookup result** verrà visualizzato il risultato dell'operazione.

4.3.3. PC DATABASE

La funzione di PC Database viene utilizzata ogni qualvolta sia necessario inserire un determinato PC nella configurazione di altre funzioni, ad esempio DMZ e Access Control.



- I PC configurati come "DHCP Clients" (Ottieni un indirizzo IP automaticamente) vengono inseriti automaticamente nel database.
- Il dispositivo utilizza il MAC address per identificare ogni PC, non il nome o l'indirizzo IP in quanto questi possono variare.
- Il database non contiene I PC che operano con indirizzi IP statici a meno che non vengano manualmente inseriti.

PC Database

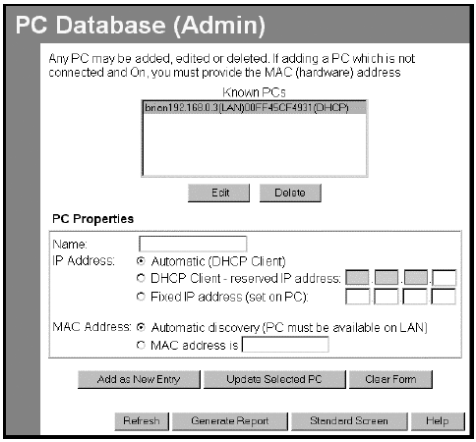
Known PCs	Lista delle entry correnti. Sono visualizzati nome, indirizzo IP e tipo.
Name	Per aggiungere un nuovo PC alla lista inserire un nome mnemonico, possibilmente il nome dell'host per comodità.
IP Address	Inserire l'indirizzo IP del PC. Al PC verrà inviato un PING per determinarne il MAC Address. Se il PC non è raggiungibile non sarà possibile inserirlo nella lista.

Bottoni

Add	Aggiunge il PC alla lista.
Delete	Cancella il PC dalla lista
Refresh	Aggiorna i dati visualizzati
Generate Report	Visualizza una lista completa e dettagliata.
Advanced Administration	Visualizza il menu in modalità *Advanced*.

PC Database (Admin)

Visualizzazione in modalità "Advanced Administration"



PC Database (Admin)

Known PCs	Lista delle entry correnti. Sono visualizzati nome, indirizzo IP e tipo.

PC Properties

Name	Per aggiungere un nuovo PC alla lista inserire un nome mnemonico, possibilmente il nome dell'host per comodità.
IP Address	Selezionare l'opzione appropriata: · **Automatic** – Il PC è impostato come DHCP client. Il dispositivo allocherà un indirizzo per il PC quando questo ne farà. L'indirizzo potrebbe cambiare. · **DCHP Client - Reserved IP Address** - Il PC è impostato come DHCP client. Il dispositivo allocherà sempre lo stesso indirizzo IP per il PC quando questo ne farà richiesta. · **Fixed IP Address** – Il PC è impostato con un indirizzo IP statico.
MAC Address	Select the appropriate option · **Automatic discovery** – Il dispositivo cercherà in LAN il PC per scoprirne il MAC address. Il PC deve essere raggiungibile in LAN. · **MAC is** – Inserire il MAC address del PC. Il MAC address è anche chiamato "Hardware Address", "Physical Address", o "Network Adapter Address".

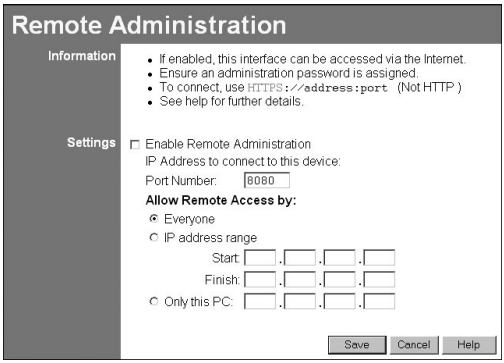
Bottoni

Add as New Entry	Aggiunge l'indirizzo IP del PC usando i dati in "Properties" . Se "Automatic discovery" è selezionato al PC verrà inviato un PING per determinarne il MAC Address, pertanto il PC deve essere raggiungibile in LAN.
Update Selected PC	Aggiunge (modifica) l'indirizzo IP del PC usando i dati in "Properties"
Clear Form	Azzera l'area " Properties" per l'aggiunta di una nuova entry.
Refresh	Aggiorna i dati visualizzati
Generate Re port	Visualizza una lista completa e dettagliata.
Standard Screen	Visualizza il menu in modalità *Standard*.

4.3.4. REMOTE ADMIN

Remote Administration

Questa funzione permette di accedere alla configurazione del dispositivo da Internet.



Enable Remote Management Se abilitato permette di accedere alla configurazione del dispositivo da Internet (porta WAN).
Se disabilitato, il dispositivo ignorerà qualsiasi tentativo di accesso alla configurazione dalla porta WAN.

Port Number Inserite un numero di porta compreso tra 1024 e 65535 (**8080 consigliato**)
Questo numero di porta deve essere specificato in fase di accesso remoto (vedi esempio).

Nota: la porta di default per il servizio HTTP è 80 mentre HTTPS è 443, ma così facendo si inibisce la possibilità di utilizzare un Virtual Server Web e HTTPS.

Allow Remote Access Permette di stabilire quali indirizzi IP avranno accesso al dispositivo da remoto

- **Everyone** – Chiunque. L'indirizzo IP del remoto viene ignorato
- **IP address range** – Solamente un indirizzo IP compreso nel range Start-Finish (campi obbligatori)
- **Only this PC** – Solamente l'indirizzo IP specificato (campo obbligatorio)

Esempio di accesso alla configurazione da un browser remoto: **https**://10.10.10.10:8080
Questo esempio assume che l'indirizzo IP sulla porta WAN sia 10.10.10.10 e il numero di portaimpostato sia 8080.

NOTA: utilizzare **HTTPS://....,** non utilizzare HTTP://....

4.3.5. ROUTING

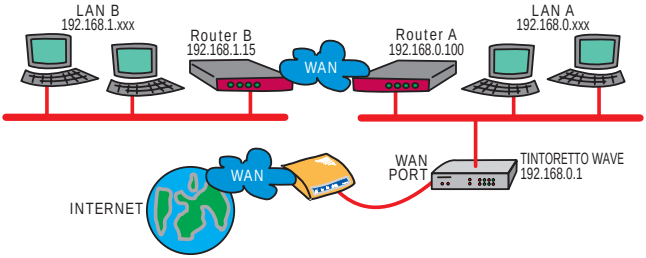
Questa sezione può essere ignorata se sulla vostra LAN **non** sono presenti Router.

Se invece sulla vostra rete sono presenti altri Router, sarà necessario intervenire sulla configurazione di FireGate 10NX e su quella dei Router, per permettere il corretto funzionamento dell'intero sistema.
Se i computer serviti da FireGate 10NX non devono accedere alla rete remota o se i computer sulla rete remota non devono accedere ad Internet potete ignorare questa sezione.
Se gli altri router in LAN utilizzano il protocollo **RIP** potete abilitarlo anche sul dispositivo ed ignorare la sezione di Routing statico.
Se preferite assegnare manualmente ed in modo **statico** tutti gli instradamenti dovrete configurare la sezione di Routing statico.

Per effettuare correttamente questo tipo di operazioni fatevi assistere dall'amministratore di rete o dal personale preposto all'installazione e manutenzione dei Router. Per comodità e maggiore chiarezza disegnate uno schema dell'attuale impostazione della rete, riportando gli indirizzi IP delle reti e dei router connessi.

Esempio di Routing

L'esempio che segue prevede l'inserimento di FireGate 10NX in un sistema composto da due LAN (LAN A, 192.168.0.x e LAN B 192.168.1.x) indipendenti ed interconnesse da due router (ROUTER A e ROUTER B).



In questa situazione le tabelle di routing dei due router contengono le informazioni su come raggiungere le rispettive reti remote.

Esemplificando, il ROUTER A connesso alla propria rete 192.168.0.x, sa che per raggiungere una qualsiasi stazione della rete 192.168.1.x deve inoltrare i pacchetti dati all'indirizzo 192.168.1.15, ovvero il ROUTER B.
Il ROUTER B a sua volta sa che se dalla propria rete 192.168.1.x si deve raggiungere una qualsiasi stazione della rete 192.168.0.x, esso deve inoltrare i pacchetti dati all'indirizzo 192.168.0.100, ovvero il ROUTER A.
All'inserimento del dispositivo nel sistema, affinchè tutto continui a lavorare correttamente, i vari componenti dovranno disporre delle seguenti informazioni:

FireGate 10NX

La rete remota 192.168.1.x (Destination IP Address) è raggiungibile attraverso il router all'indirizzo 192.168.0.100 (Gateway Address).

ROUTER A (Router locale)

La rete remota 192.168.1.x è raggiungibile attraverso il router all'indirizzo 192.168.1.15 (Informazione già presente nella routing table).
Ogni altra destinazione (Default route, Internet in questo caso) è raggiungibile attraverso il router all'indirizzo 192.168.0.1 (Informazione da aggiungere).

ROUTER B (Router remoto)

La rete remota 192.168.0.x è raggiungibile attraverso il router all'indirizzo 192.168.0.100, informazione già presente nella routing table. Ogni altra destinazione (Default route, Internet in questo caso) è raggiungibile attraverso il router all'indirizzo 192.168.0.100 (Informazione da aggiungere).

In questo caso specifico è possibile configurare la tabella di routing del ROUTER B con un'unica entry che contenga l'informazione che qualsiasi destinazione (LAN A e Internet) sono raggiungibili attraverso un'unica default route che punta all'indirizzo 192.168.0.100.

Riassumendo, le tabelle di routing dei tre dispositivi dovranno contenere le seguenti informazioni:

FireGate 10NX		**Note**
Destination IP Address	192.168.1.0	LAN B
Network Mask	255.255.255.0	
Gateway IP Address	192.168.0.100	Router A
Metric	1	

ROUTER A		**Note**
Destination IP Address	192.168.1.0	LAN B
Network Mask	255.255.255.0	
Gateway IP Address	192.168.0.15	Router B
Default Route		
Destination IP Address	0.0.0.0	*
Network Mask	0.0.0.0	*
Gateway IP Address	192.168.0.1	FireGate 10NX

ROUTER B		**Note**
Destination IP Address	192.168.0.0	LAN A
Network Mask	255.255.255.0	
Gateway IP Address	192.168.0.100	Router A
Default Route**		
Destination IP Address	0.0.0.0	*
Network Mask	0.0.0.0	*
Gateway IP Address	192.168.0.100	Router A

*Questa è la sintassi normalmente utilizzata per indicare una default route. Verificate che sia valida anche per i vostri router.

**In questo esempio potrebbe essere l'unica entry nella routing table del Router B.

Enable RIP

E' possibile utilizzare il protocollo RIP versione 1 in alternativa le tabelle di routing statico.

4.3.6. ROUTING

RIP

Rip version, selezionare l'opzione desiderata

Disabled. Il router ignora i pacchetti RIP di qualsiasi tipo ed utilizza solamente le tabelle di routing statico inserite.

RIP_1. Il router utilizza le informazioni ricevute via RIP versione 1.

RIP_2B. Il router utilizza le informazioni ricevute via RIP versione 2 in Broadcast.

RIP_2M. Il router utilizza le informazioni ricevute via RIP versione 2 in Multicast.

Static Routing

Static Routing Table Entries Lista della route statiche attualmente inserite

· I dettagli della route sono mostrati in "Properties".

· Modificare i parametri come desiderato e cliccare "Update" per salvare le modifiche.

Properties

· **Destination Network** – L'indirizzo di rete della LAN remota. Per una LAN in classe C standard, i primi tre campi identificano l'indirizzo di rete, il quarto va lasciato a zero, ad esempio 192.168.1.0.

· **Network Mask** – La Subnet Mask della LAN remota. Per una LAN in classe C standard, questa è 255.255.255.0

Gateway IP Address – Indirizzo IP del Gateway o Router in LAN (locale) al quale il dispositivo deve far riferimento per raggiungere la rete remota)

Interface. Normalmente impostare LAN (NAT abilitato)

Se il **NAT è disabilitato** è possibile creare dell router per destinazioni raggiungibili attraverso la WAN

Metric – Numero di salti o "hops" (routers) da attraversare per raggiungere la LAN remota. Verrà utilizzata la via più breve. Il default è 1.

Bottoni

Save	Salva l'impostazione RIP. Non ha effetto sulle tabelle di routing statiche.
Add	Aggiunge una nuova entry alla tabella di routing statica con I parametri presenti in "Properties".
Update	Aggiorna una nuova entry alla tabella di routing statica con I parametri presenti in "Properties".
Delete	Cancella la entry corrente
Clear Form	Azzera I parametri in "Properties" per l'inserimento di una nuova entry.
Generate Report	Visualizza una lista completa e dettagliata.

4.3.7. UPGRADE FW

Il firmw are del dispositivo può essere aggiornato dal browser.
Scaricate sul PC il file di aggiornamento, poi selezionate *Upgrade* dal menu Advanced.

Per effettuare un aggiornamento del firmware:
Cliccate su "**Browse**".
Selezionate il file di aggiornamento.
Cliccate su "**Start Upgrade**" per iniziare l'aggiornamento.

Effettuare questa operazione solamente a fronte di una effettiva necessità, dopo aver consultato il personale del Supporto Tecnico.
Durante l'aggiornamento il dispositivo non è operativo ed effettue rà un restart a fine procedura. Ogni connessione attiva sarà terminata.

4.3.8. UPNP

UPnP

Enable UPnP Services · UPnP (Universal Plug and Play) permette la rilevazione automatica e configurazione del dispositivo connesso in LAN. UpnP è supportato da Windows® ME/XP.
· Se Enabled, il dispositivo è visibile via UPnP.
· Se non Enabled, il dispositivo non è visibile via UPnP.

Allow Configuration... · Se selezionato, si potrà modificare la configurazione via UPnP.
· Se non selezionato gli utenti potranno solamente visualizzare la configurazione via UPnP.

Allow Internet access to be disabled
· Se selezionato, si potrà disabilitare l'accesso ad Internet via UPnP.
· Se non selezionato, non si potrà disabilitare l'accesso ad Internet via UPnP

5. SERVER VPN

5

Firegate 10NX integra nativamente un Server VPN.
Una connessione VPN (Virtual Private Network) è una connessione protetta tra due punti attraverso una rete "non sicura" (solitamente Internet).
Esistono molti standard e protocolli per la VPN, gli Standard supportati dal Firegate 10NX sono:

IPSec
Microsoft VPN

5.1. NOZIONI BASE

5.1.1. VPN (IPSEC)

Questa sezione descrive il supporto VPN fornito dal dispositivo.
Una VPN (Virtual Private Network) crea una connessione protetta tra due punti attraverso una rete "non sicura", solitamente Internet. Questa connessione protetta è chiamata **VPN Tunnel**.
Esistono molti standard e protocolli per le VPN. Lo standard implementato dal dispositivo è **IPSec**.

IPSec

IPSec è uno standard di sicurezza VPN "near-ubiquitous" per reti basate su TCP/IP. Lavora a livello di pacchetto per autenticare e crittografare tutti i pacchetti che attraversano il VPN Tunnel. Ciò non influenza le applicazioni in uso che "vedono" il tunnel VPN come una qualsiasi connessione di rete.
Le VPN basate su IPsec scambiano le informazioni attraverso connessioni logiche chiamate **SA** (Security Associations). Una SA è semplicemente una definizione di protocolli, algoritmi e chiavi in uso tra I due dispositivi (endpoints) VPN.
Ogni IPsec VPN usa due SA, una per ogni direzione. Se si utilizza il protocollo **IKE** (Internet Key Exchange) per generare e scambiare le chiavi saranno presenti delle SA anche per la connessione IKE.
IPSEC prevede due modalità di security:

- **Transport Mode** – la porzione di dati (payload) del pacchetto è incapsulata e crittografata mentre l'IP header rimane in chiaro (invariato).
  Questa modalità NON è supportata dal dispositivo.
- **Tunnel Mode** – Tutto il pacchetto è incapsulato, compreso l'IP header originale, e un nuovo header viene generato. L'header generato è l'unico parte in chiaro. Ciò aumenta il grado di sicurezza dei dati originari.
  Il dispositivo utilizza sempre il Tunnel Mode.

IKE

IKE (Internet Key Exchange) è una parte opzionale ma largamente utilizzata di IPsec. IKE fornisce un metodo di negoziazione e generazione delle chiavi necessarie per IPSec. Se si utilizza IKE solamente una chiave verrà richiesta in fase di configurazione. Inoltre IKE supporta l'uso di **Certificati** (forniti da CA - Certification Authorities) per autenticare l'identità dell'utente o gateway VPN remoto.
Se IKE non è utilizzato, tutte le chiavi e ID (SPI) devono essere inserite manualmente e non si potranno utilizzare Certificates. Questa modalità è chiamata "Manual Key Exchange".
Quando si utilizza IKE, il tunnel VPN richiede 2 fasi per essere stabilito:

- **Fase 1,** la negoziazione e instaurazione della connessione IKE.
- **Fase 2,** la negoziazione e instaurazione della connessione IPSec.

Essendo le due connessioni IKE e IPsec separate, queste hanno SA (Security Associations) diverse.

Policies

Le impostazioni delle configurazione VPN sono salvate in apposite **Policies**.
Ogni policy definisce:

- L'indirizzo IP dell'endpoint VPN remoto
- Il traffico che è ammesso a transitare attraverso la VPN.
- I parametri per le IPsec SA (Security Association)
- Se IKE è utilizzato, i parametri per le IKE SA (Security Association)
- Generalmente è necessaria almeno una (1) VPN Policy per ogni destinazione remota con la quale si desidera stabilire una connessione VPN.

E' possibile, a volte necessario, definire più Policies per una stessa destinazione remota. In questo caso l'ordine (sequenza) delle policy è importante. Le policy sono esaminate in ordine fino a trovarne ed utilizzarne una che corrisponde ai dati.

Configurazione VPN

La regola generale è che ognuno degli endpoint deve avere Policies corrispondenti:

Remote VPN address	Ogni endpoint VPN deve essere configurato per iniziare o accettare connessioni con il client o gateway VPN remoto. Solitamente ciò richiede un indirizzo IP statico. Tuttavia un VPN Gateway può accettare connessioni in ingresso da un client remoto del quale non conosce l'indirizzo IP.
Traffic Selector	Determina quale traffico uscente instaurerà una connessione VPN e quale traffico entrante verrà accettato. Ognuno degli endpoint deve essere configurato per inviare ed accettare il traffico dell'endpoint remoto. Se si interconnettono 2 LAN è necessario che: · Ognuno degli endpoint deve conoscere gli indirizzi IP usati sull'altro endpoint. · Le due LAN devono utilizzare range di indirizzi IP differenti.
IKE parameters	Se si usa IKE (consigliato), le impostazioni IKE devono corrispondere (eccetto che per SA lifetime che può essere diverso).
IPsec parameters	Le impostazioni IPsec devono corrispondere su entrambi gli endpoint.

5.1.2. MICROSOFT VPN

PPTP (VPN)

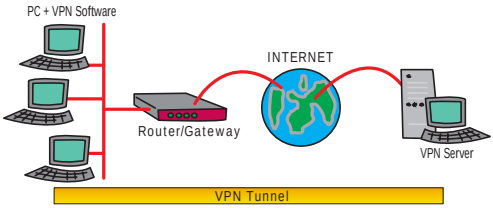
Il protocollo supportato per la Microsoft VPN è il PPTP (Point-to-Point Tunneling Protocol).
Il protocollo PPTP è un'estensione del protocollo standard di comunicazione Internet PPP definito nella RFC 1661 e del TCP/IP. PPP è multi protocollo ed offre autenticazione, sicurezza e compressione dei dati.
In pratica, PPTP realizza una sessione PPP in tunnel attraverso una connessione IP già esistente, senza considerare la configurazione di quest'ultima.
Il tunneling viene creato dal protocollo PPTP che fornisce l'incapsulamento e l'adattamento dei pacchetti di informazione (che possono essere IP, IPX o NetBEUI) all'interno dei pacchetti IP per la trasmissione in Internet.
In questo modo, grazie all'incapsulamento viene permesso il trasporto di pacchetti con indirizzi IP privati, che altrimenti non rientrerebbero negli indirizzi standard Internet. Viene inoltre garantito un livello di sicurezza maggiore, perchè i pacchetti non transitano "in chiaro" in Internet.

Autenticazione

La connessione avviene utilizzando una User Name e Password.
Il FireGate supporta lo scambio di password con protocollo PAP, CHAP, MS-CHAP, MS-CHAP v2.

5.1.3. APPLICAZIONI VPN CLASSICHE

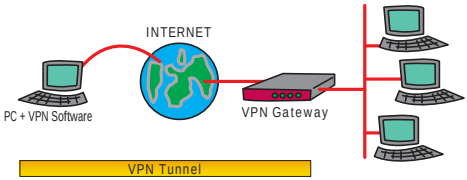
VPN Pass-through



In questa situazione un PC sulla LAN servita dal dispositivo, utilizza un software VPN. Il dispositivo non si comporta come un VPN endpoint. Si limita a permettere trasparentemente il passaggio dei pacchetti di una connessione VPN.

- Il software VPN del PC può utilizzare un qualsiasi protocollo VPN supportato dal VPN server remoto.
- Il VPN Server remoto deve supportare PC client che si trovano dietro ad un NAT router e che utilizzano indirizzi IP che non sono validi su Internet.
- Il dispositivo Router/Gateway non richiede alcuna configurazione VPN in quanto non si comporta come un VPN endpoint.

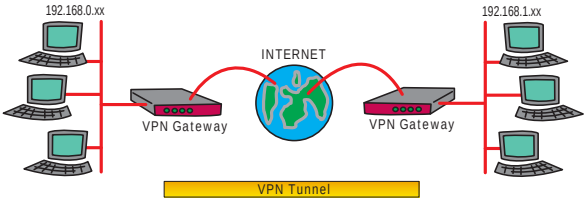
Client PC verso VPN Gateway



In questa situazione un PC deve utilizzare un software VPN appropriato per collegarsi via Internet al dispositivo VPN Gateway. Una volta connesso il PC client avrà le stesse possibilità di accesso alle risorse della LAN dei PC fisicamente localizzati sulla LAN stessa (salvo restrizioni applicate dall'amministratore).

- IPsec non è l'unico protocollo che può essere utilizzato in questa situazione, ma è l'unico supportato dal VPN Gateway.
- Windows 2000 e Windows XP includono un programma client VPN Ipsec. La configurazione di questo client è descritta più avanti.

Connessione di 2 LAN via VPN



Questa situazione permette di collegare due reti LAN. I PC serviti dai due endpoint remoti avranno la possibilità di sfruttare un accesso protetto alle risorse remote.

- Le due LAN devono usare range di indirizzi IP differenti.
- Le VPN Policies ai due estremi determinano quando una connessione VPN viene stabilita e quali risorse saranno accessibili una volta stabilita la connessione VPN.
- E' possibile stabilire altre connessioni VPN simultanee verso molte destinazioni remote.

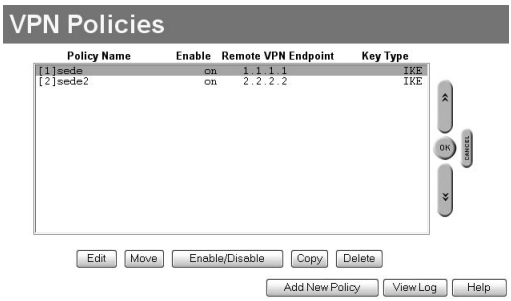
5.2. CONFIGURAZIONE SERVER VPN

5.2.1. VPN (IPSEC)

Cliccando sul collegamento "**VPN (IPSec)**" è possibile accedere alle seguenti pagine di configurazione:

5.2.1.1. VPN Policies

In questa finestra vengono mostrale tutte le VPN Policies esistenti.



Indicatore di priorità

L'ordine delle Policies è importante perché il dispositivo analizza le policies dalla prima [1] all'ultima, pertanto se esistono più policies con la stessa destinazione verrà attivata la prima valida in ordine di priorità.

Policy Name	Nome mnemonico associato alla policy
Enable	*On* policy attiva *Off* policy non attiva
Remote VPN Endpont	Indirizzo IP o nome del VPN Endpoint
Key Type	Indica la modalità di scambio delle chiavi, *IKE* (Internet Key Exchange) oppure *Manual* (Manual Key Exchange)

I tasti hanno le seguenti funzioni:

Edit	Apre la finestra di modifica per la Policy selezionata
Move	Cambia la posizione della Policy selezionata (priorità). Cliccate su *Move* e successivamente indicate il nuovo indice [x] della Policy
Enable/Disable	Abilita / Disabilita l'utilizzo della Policy selezionata
Copy	Apre la finestra di creazione di una nuova Policy caricando le impostazioni della Policy selezionata.
Delete	Cancella la Policy selezionata.
Add New Policy	Apre la finestra di creazione di una nuova Policy.
View Log	Visualizza il VPN Log.

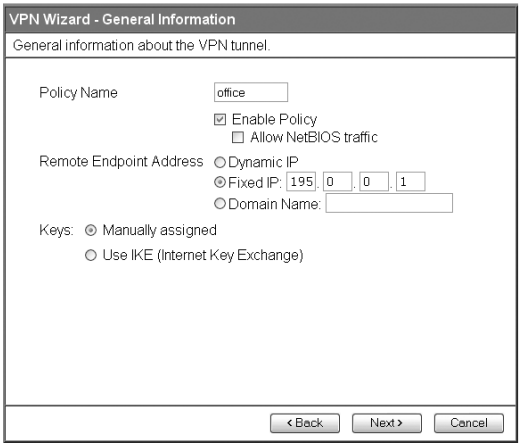
5.2.1.2. Creazione di una nuova Policy

Cliccando sul tasto *Add New Policy* viene visualizzata la seguente finestra:

Prima di proseguire nella configurazione verificate di avere a disposizione le seguenti informazioni:

- Configurazione del remote VPN Gateway/Server
- Se dovete utilizzare dei certificati, verificate di averli già a disposizione.

Selezionate **Next** per procedere nella configurazione della Policy utilizzando il Wizard (procedura guidata), oppure cliccate sul tasto **Setup Screen** per accedere direttamente alla finestra di configurazione (consigliato per utenti esperti).



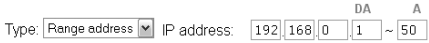
Policy Name Inserite il nome della Policy. (non inserite spazi " " nel nome).
Enable Policy Selezionate quest'opzione per rendere la Policy attiva già al termine della configurazione.
Allow NetBIOS traffic Selezionate quast'opzione per permettere il passaggio del protocollo NetBIOS nel tunnel VPN.
Remote Endpoint Address *Dynamic IP* selezionate quest'opzione se la connessione avviene con un Client di cui non conoscete l'indirizzo IP; il FireGate in questo casò non sarà in grado di attivare autonomamente la connessione ma dovrà essere il Client a richiederne l'attivazione.
Fixed IP selezionate quest'opzione se il Client/Server remoto dispone di un indirizzo IP fisso ed inserite l'indirizzo IP del VPN Endpoint.
Domain Name selezionate quest'opzione se è possibile risalire all'indirizzo IP del VPN Endpoint tramite un dominio (tramite Dyndns per esempio) ed inserite il nome nella casella a fianco.
Keys Selezionate il metodo che intendete utilizzare:
Manually assigned
IKE (Internet Key Exchange)

Selezionate **Next** per proseguire.

In questa finestra è necessario definire le reti Locale e Remota che possono attraversare il Tunnel VPN.

Local IP addresses Indica la rete / le macchine che possono accedere al tunnel VPN e quindi alla rete remota.
Remote IP addresses Indica la rete /le macchine raggiungibili solo attraverso il tunnel VPN; le macchine poste alle spalle del VPN Endpoint.

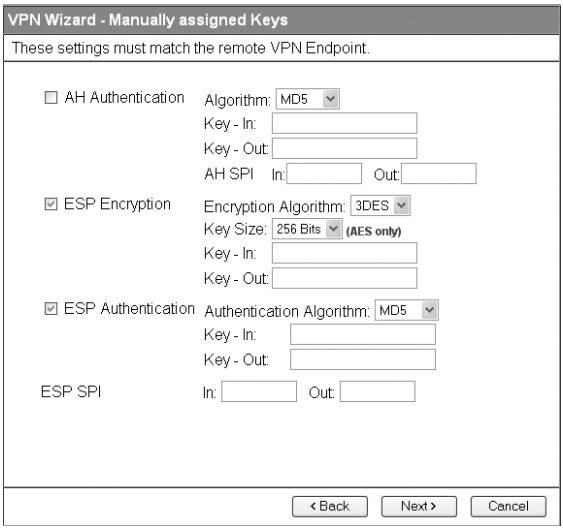
Per indicare gli indirizzi locali e remoti si hanno a disposizione differenti metodi, selezionabili tramite **Type:**
Any Indica qualsiasi indirizzo IP (selezionabile solo per il campo Local IP addresses)
Single Address Indica un solo indirizzo IP, inserite l'indirizzo nel campo *IP address*
Range Address Indica un gruppo sequenziale di indirizzi IP, definiti da un indirizzo IP di partenza e uno di arrivo. Inserite il gruppo nel campo *IP address*, il range viene definito dall'ultimo campo dell'indirizzo IP.



Subnet address Indica tutti gli indirizzi appartenenti alla rete descritta da un indirizzo IP (*IP address*) e la relativa Subnet Mask (*Subnet Mask*)

Cliccate su **Next** per proseguire nella configurazione.

Se state configurando una Policy con **Keys –** *Manually assigned* la finestra di configurazione sarà la seguente:



Tutte le impostazioni devono corrispondere a quelle impostate nel VPN Endpoint, tutte che chiavi impostate come **In** devono corrispondere alle chiavi impostate come **Out** nel VPN Endpoint remoto e viceversa.
Key Size, valido solo per AES

Le chiavi inserite possono essere scritte in ASCII oppure in Esadecimale (Hex) e hanno lunghezza:
Alghoritm MD5 32 caratteri Hex oppure 16 ASCII
Alghoritm SHA-1 40 caratteri Hex oppure 20 ASCII
Alghoritm 3DES 48 caratteri Hex oppure 24 ASCII
Alghoritm DES 16 caratteri Hex oppure 16 ASCII
Alghoritm AES 16, 24 o 32 caratteri per rispettivamente 128, 192 o 256 bits

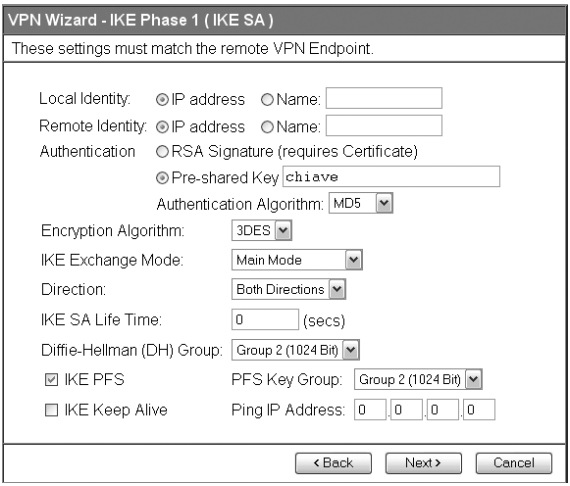
Le chiavi SPI devono essere di almeno 4 caratteri.

AH Authentication Authentication Header specifica il protocollo di autenticazione per l'header VPN. Il suo utilizzo è alternativo all'ESP.

ESP Encryption – Authentication
Encapsulating Security Payload provvede alla sicurezza dei datie dell'autenticazione attraverso il tunnel VPN.

La configurazione è completa, cliccate su **Next** per acceder all'ultima finestra; cliccate su **Finish** per salvare le impostazioni e su **Close** per uscire dal Wizard.

Se state configurando una Policy con **Keys –** *IKE* la finestra di configurazione sarà la seguente:



Local Identity Questa impostazione deve corrispondere a "Remote Identity" sul VPN Endpoint remoto. *WAN IP Address* è il metodo utilizzato più comune.

Remote Identity Questa impostazione deve corrispondere a "Local Identity" sul VPN Endpoint remoto. *WAN IP Address* è il metodo utilizzato più comune.

VPNID

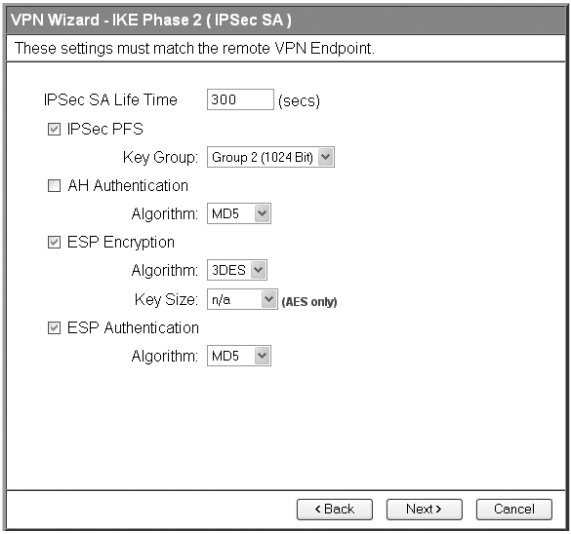
Local Identity Type Tipologia per l'identità locale (vedi sotto)
Local Identity Data Inserire il valore per l'identità locale
Remote Identity Type Tipologia per l'identità del remoto (vedi sotto)
Remote Identity Data Inserire il valore per l'identità del remoto

Tipologia per l'identità

WAN IP address L'indirizzo IP di WAN del dispositivo locale
Remote WAN IP L'indirizzo IP di WAN del dispositivo remoto
Fully Qualified Domain Name (FQDN) Un nome di dominio, ad esempio www.digicom.it
Fully Qualified User Name (FQUN) Un ID, nome o indirizzo email, ad esempio FG, FireGate oppure support@digicom.it
DER ASN.1 DN Binary DER encoding del proprio ASN.1 X.500 Distinguished Name.
Authentication *RSA Signature* richiede che entrambi gli Endpoint dispongano di certificati validi rilasciati da CA (Certification Authority)
Pre-shared Key inserite la stessa Key su entrambi gli Endpoint, la key deve essere di almento 8 caratteri e massimo di 128.

	Questa Key viene utilizzata solo con la fase IKE SA, per le seguenti fasi le Key vengono generate in automatico. *Authentication Algorithm* selezionate l'algoritmo di crittografia che volete utilizzare, **MD5** oppure **SHA-1**
Encryption Algorithm	Selezionate la stesso algoritmo su entrambi gli Endpoint. **3DES** è più sicuro ma, **DES** è molto più veloce.
IKE Exchange Mode	Selezionate la stessa opzione su entrambi gli Endpoint VPN. *Main Mode* fornisce un livello di sicurezza maggiore, ma ha bisogno di conoscere a priori l'indirizzo del remoto; non è utilizzabile per connessioni con Client dinamici. *Aggressive Mode* non effettuata controlli sull'identità degli Endpoint ma è molto più veloce.
Direction	Definisce in queale direzione il Tunnel VPN può essere creato: *Initiator* il tunnel può essere aperto solo in uscita dal Firewall *Responder* il tunnel può essere aperto solo in ingresso sul Firewall *Both* entrambi i VPN Endpoint possono aprire il tunnel
IKE SA Life Time	Questa impostazione può differire tra i due Endpoint e verrà utilizzata quella convalore minore. L'unità di misura è in secondi e spesso vengono impostati periodi di diverse ore come 28800.
Diffie-Hellman (DH) Group	Selezionate lo stesso gruppo su entrambi gli Endpoint. Il gruppo 1 è più veloce del gruppo 2.
IKE PFS	Questa funzione, se abilitata, controlla che le key IPSec siano modificate regolarmente durante lo scambio di dati. Deve essere abilitata su entrambi gli Endpoint. Selezionate lo stesso **PFS Key Group.**
IKE Keep Alive	Questa funzione permette di riattivare il tunnel VPN in caso di "caduta" effettuando un controllo di connessione tramite Ping, inserite l'indirizzo dell'Endpoint nel campo *Ping IP Address*. E' possibili inserire sia l'indirizzo di WAN sia quello di LAN del VPN Endpoint, l'indirizzo di LAN è consigliato.

Cliccate su **Next** per passare alla seconda finestra di configurazione dell'IKE.



IPSec SA Life Time	Questa impostazione può differire sugli endpoint VPN, verrà utilizzata quella con tempo minore. Unità di misura in secondi, spesso impostati a periodi di diverse ore, come 28800 secondi.
IPSec PFS	Se abilitata, PFS (Perfect Forward Security) incrementa ulteriormente la sicurezza cambiano le key IPsec ad intervalli di tempo regolari e verificando che le nuove chiavi non abbiano alcuna relazione con le precedenti. In questo modo se una chiave viene scoperta, questa non è di nessuna utilità per scoprire la successiva.
AH Authentication	AH (Authentication Header) specifica il protocollo di autenticazione per l'header VPN header, se utilizzato.

AH solitamente non è utilizzato. Se si, abilitare su entrambi gli endpoint VPN.

ESP Encryption ESP (Encapsulating Security Payload) provvede alla security per I dati (payload) inviati attraverso il VPN tunnel. Generalmente si attiveranno sia Encryption che Authentication.

- Gli algoritmi 3DES e AES forniscono maggior sicurezza rispetto a DES, ma sono più "lenti".

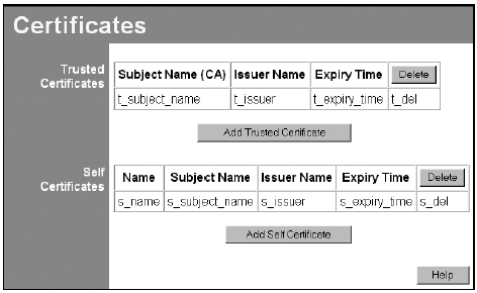
Selezionare lo stesso metodo su entrambi gli endpoint VPN.

ESP Authentication Generalmente si abilita ESP Authentication. Ci sono piccole differenze tra i diversi algoritmi disponibili. Assicurarsi di usare le stesse impostazioni sui due endpoint.

Cliccate su **Next** per accedere alla schermata finale; Cliccate su **Finish** per salvare i paramentri e su **Close** per uscire.

5.2.1.3. Utilizzo di certificati

I Certificates sono utilizzati per autenticare gli utenti. Questi Certificati sono rilasciati da appositi CA (Certification Authorities) e sono chiamati "Self Certificates".
Ogni CA rilascia anche un certificato a se stesso. Quest'ultimo è necessario per permettere le comunicazioni con il CA. Questi sono chiamati "Trusted Certificates."
Il pannello ***Certificates*** mostra entrambi I certificati, il Trusted Certificate – per il CA stesso – e il Self Certificates – rilasciato a voi.



Trusted Certificates

Subject Name (CA) Il "Subject Name" indica sempre la persona o azienda al quale il certificato è stato rilasciato. Per i trusted certificates indicherà un CA.

Issuer Name CA (Certification Authority) che ha rilasciato il certificato.

Expiry Time Data di scadenza del certificato, da rinnovare prima della scadenza.

Delete Cancella un Trusted Certificate. Selezionare un checkbox nella colonna *Delete* per I certificati che si desidera cancellare, quindi cliccare su "Delete".

Self Certificates

Name Il nome che intendete assegnare al certificato. Utilizzare un nome facilmente associabile e richiamabile.

Subject Name L'azienda o persona alla quale il cetificato è stato rilasciato.

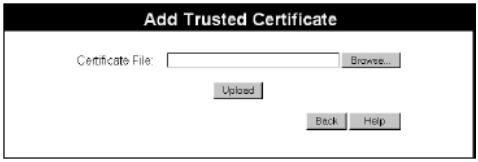
Issuer Name CA (Certification Authority) che ha rilasciato il certificato.

Expiry Time Data di scadenza del certificato, da rinnovare prima della scadenza.

Delete Cancella un Self Certificate. Selezionare un checkbox nella colonna *Delete* per I certificati che si desidera cancellare, quindi cliccare su "Delete".

Aggiungere un Trusted Certificate

1. Una volta ottenuto un nuovo Certificato dal CA è necessario caricarlo sul VPN Gateway.
2. Nel pannello "**Certificates**" cliccare su "**Add Trusted Certificate**"

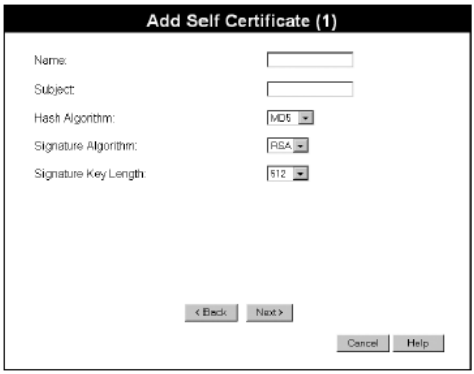


3. Cliccare su "**Browse**" e selezionare il file del certificato sul PC
4. Selezionare il file il cui nome verrà visualizzato nel apposito campo.
5. Cliccare su "**Upload**" per caricare il file sul VPN Gateway.
6. Cliccare su "**Back**" per tornare alla lista dei Trusted Certificate. Il nuovo certificato apparirà in lista.

Aggiungere un Self Certificate

Il processo è diverso dall'ottenere un Trusted Certificate. Il VPN Gateway deve generare un richiesta per il CA. Non potete richiedere un un Certificato direttamente. Effettuare la seguente procedura:

7. Nel pannello "Certificates" cliccare su "**Add Self Certificate**"



8. Completare I parametri.

Name	Il nome che intendete assegnare al certificato. Utilizzare un nome facilmente associabile e richiamabile.
Subject Name	Il nome con cui altre organizzazioni "vedranno" il "proprietario" del presente certificato, generalmente l'ufficiale nome dell'azienda o persona. Lo stesso nome dovrebbe comparire in tutti i subject name dei certificati.
Hash Algorithm	Selezionare l'opzione desiderata.
Signature Algorithm	Selezionare l'opzione desiderata, si consiglia RSA.
Signature Key Length	Selezionare l'opzione desiderata, normalmente 1024 bits offrono una adeguata sicurezza.

9. Cliccare su "**Next**" per proseguire.

10. Verificare che I *Certificate Details* siano corretti. Queste informazioni sono utilizzate per generare la richiesta del Certificato. Se i dati non fossero corretti, cliccare su "**Back**" per correggerle.
11. Se I dati sono corretti copiare il testo contenuto in *Data to supply to CA* negli appunti.
12. Richiedere un certificato:
    - Connettersi al sito Internet del CA.
    - Iniziare la procedura per la richiesta di un Self Certificate.
    - Quando vi verrà richiesto di fornire I dati, incollate I dati (incluso "——BEGIN CERTIFICATE REQUEST——" e "——END CERTIFICATE REQUEST——") dagli appunti nel form del CA.
    - Inviare il form del CA (Submit)
    - Se non si verificano problemi, vi verrà fornito il Cerificato.
13. Una volta ottenuto il nuovo certificato come descritto sopra, dovrete caricarlo nel VPN Gateway. Cliccare su "**Next**" per proseguire.

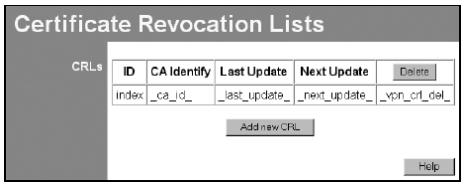
14. Caricamento del Certificato:
    - Cliccare su "**Browse**" e selezionare il file del certificato sul PC
    - Selezionare il file il cui nome verrà visualizzato nel apposito campo.
    - Cliccare su "**Upload**" per caricare il file sul VPN Gateway .
    - Cliccare su "**Finished**" per tornare alla lista dei Cerificati. Il nuovo certificato apparirà in lista.

La Certificate Revocation List (CRL)

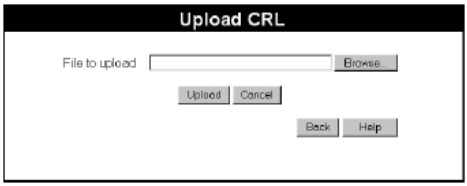
Le CRL sono necessario solamente se si utilizzano i Certificati.
I file CRL (Certificate Revocation List) mostrano I certificati che sono stati revocati e pertanto non più validi.

Ogni CA fornisce le proprie liste di CRL.
E' MOLTO IMPORTANTE mantenere aggiornate le proprie CRL, richiedendole con intervalli regolari ai propri CA.
Il campo "**Next Update**" nel CRL mostra quando sarà disponibile il prossimo aggiornamento.

Per aggiungere un nuovo CRL
15. Ottenere il file CRL dal CA.
16. Selezionare *CRL* dal menu VPN.



17. Cliccare su "**Add New CRL**"



18. Caricare il file CRL:
    - Cliccare su "**Browse**" e selezionare il file CRL sul PC
    - Selezionare il file il cui nome verrà visualizzato nel apposito campo.
    - Cliccare su "**Upload**" per caricare il file sul VPN Gateway.
    - Cliccare su "**Back**" per tornare alla lista dei CRL. Il nuovo CRL apparirà in lista.
19. Usare "**Delete**" per cancellare il precedente CRL ora non più aggiornato.

5.2.1.4. VPN Status

In questa finestra è possibile vedere quali VPN sono attualmente attive.

5.2.2. MICROSOFT VPN

Cliccando sul collegamento "**Microsoft VPN**" è possibile accedere alle seguenti pagine di configurazione:

5.2.2.1. Server

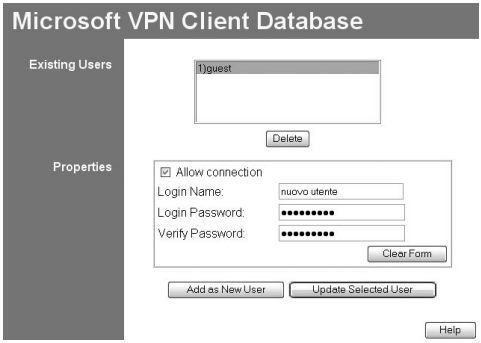
Selezionate l'opzione **Enable PPTP (VPN) Server** per abilitare questa questo tipo di server VPN.
L'autenticazione di un utente può avvenire utilizzando dei protocolli differenti, selezionate nelle 4 opzioni seguenti quale protocollo accettare.
I protocolli sono:

MS-CHAP v2
MS-CHAP
CHAP
PAP

Verificate i protocolli che possono utilizzare i vostri Client prima di procedere, è consigliabile lasciare abilitati solo i protocolli necessari e se possibile non utilizzare il PAP. (PAP non utilizza la crittografia per l'autenticazione).

Cliccate sul tasto **Save** per salvare le impostazioni.

5.2.2.2. Client



In questa finestra è possibile definire gli utenti che possono accedere alla nostra rete, tramite una Login (Username e Password).

Aggiunta di un utente	Inserite lo username nel campo *Login Name* Inserite la password nei campi *Login Password* e *Verify Password* Selezionate l'opzione *Allow connection* se voltete abilitare subito l'utente che state inserendo. Cliccate sul tasto **Add as New User**
Modifica di un utente	Selezionate l'utente che volete modificare dalla lista **Existing Users** Effettuate le modifiche Salvate le nuove impostazioni con il tasto **Update Selected User**
Eliminazione di un utente	Selezionate l'utente che volete modificare dalla lista **Existing Users** Cliccate sul tasto **Delete**

5.2.2.3. Status

In questa finestra potete verificare il numero di connessioni al server attive e potete leggere il Log del server.

6. ESEMPI DI CONFIGURAZIONE

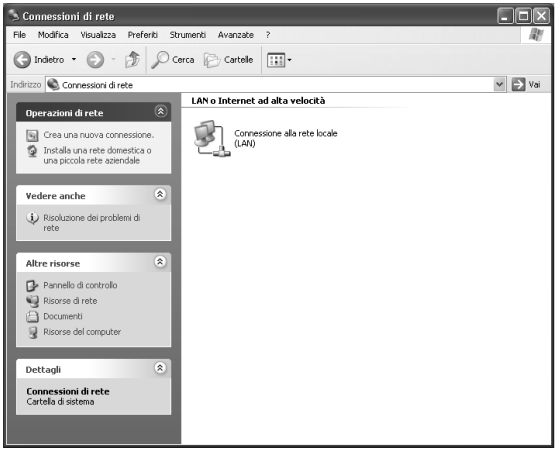
6

6.1. CONFIGURAZIONE INDIRIZZO IP

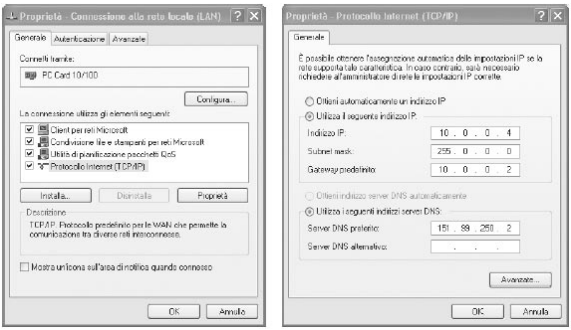
6.1.1. IMPOSTAZIONE COME CLIENT DHCP

Windows® XP

1. Dal menù **Start** selezionate **-> Pannello di Controllo -> Rete e Connessioni Internet, Risorse di rete** e selezionate **Visualizza risorse di rete**.



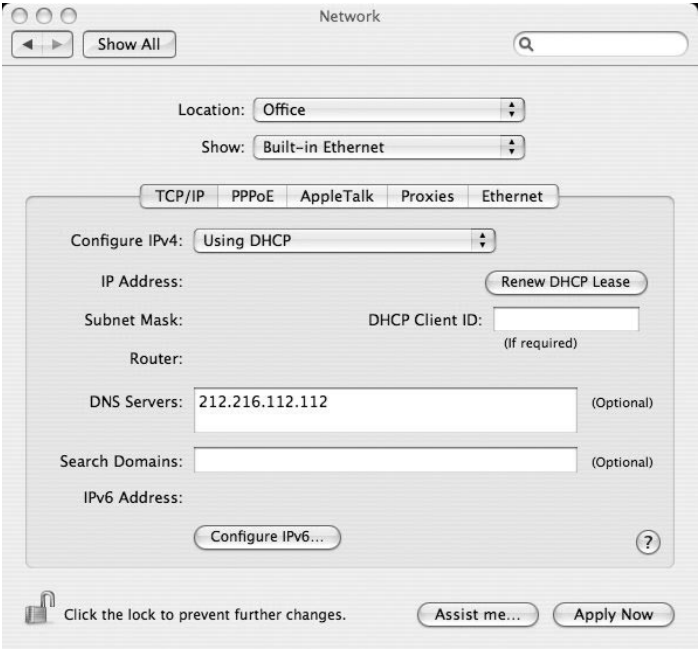
2. Selezionate **Connessione alla rete locale (LAN)** e visualizzate le **Proprietà**, selezionate **Protocollo Internet (TCP/IP)** e premete sul pulsante **Proprietà**.



3. Per impostare il Computer come client DHCP dovete selezionare **Ottieni automaticamente un Indirizzo IP**, a questo punto potete chiudere le finestre confermanto con **OK**.
4. Riavviate Windows® per rendere attive le nuove impostazioni.

Macintosh®

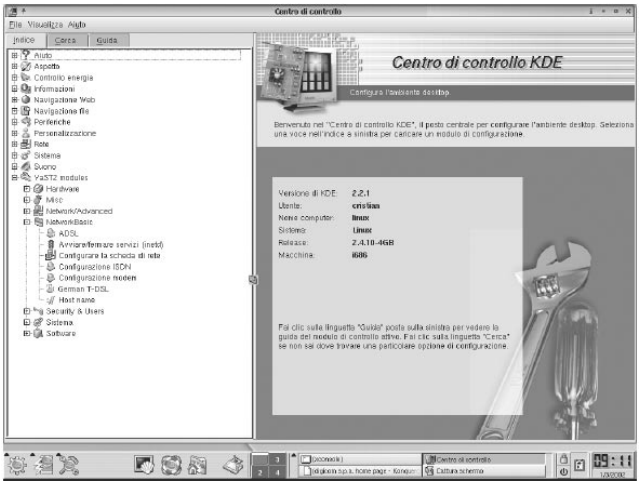
1. Dal Pannello di controllo selezionate **Preferenze di Sistema** (System Preferences).
2. Cliccate sull'icona **Network.**
3. Selezionate Mostra: **Ethernet Integrata** (Built-in Ethernet).
4. Cliccate sul pulsante **TCP/IP.**
5. Selezionate **Utilizzo di DHCP** (Using DHCP).
6. Chiudete il pannello **Network**.

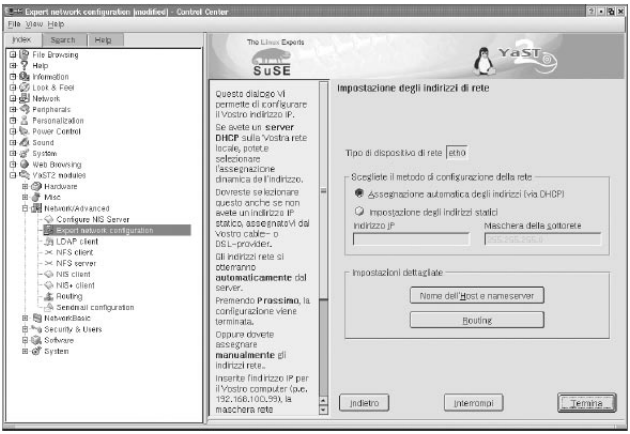


Linux

Di seguito verranno date alcune informazioni su come configurare le risorse di rete utilizzando il Centro di Controllo KDE, con la distribuzione Suse 6.2.

1. Attivate il Control Center.
2. Selezionate **Configurare la scheda di rete** nel menù **Network Basic**.



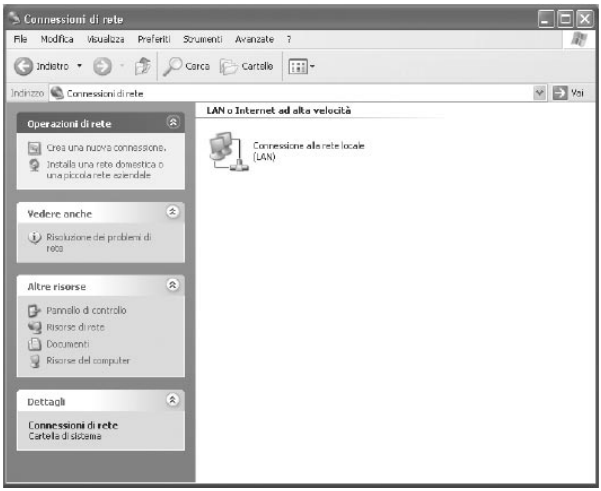


3. Selezionate Assegnazione automatica degli indirizzi (via DHCP).
4. Confermate con **Termina**.

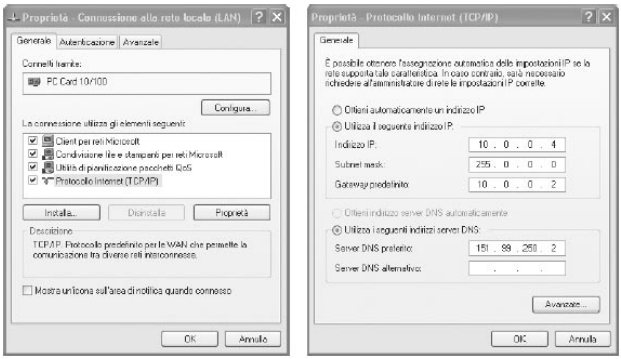
6.1.2. INDIRIZZI IP STATICI

Windows® XP

1. Dal menù **Start** selezionate **-> Pannello di Controllo -> Rete e Connessioni Internet , Risorse di rete** e selezionate **Visualizza risorse di rete**.



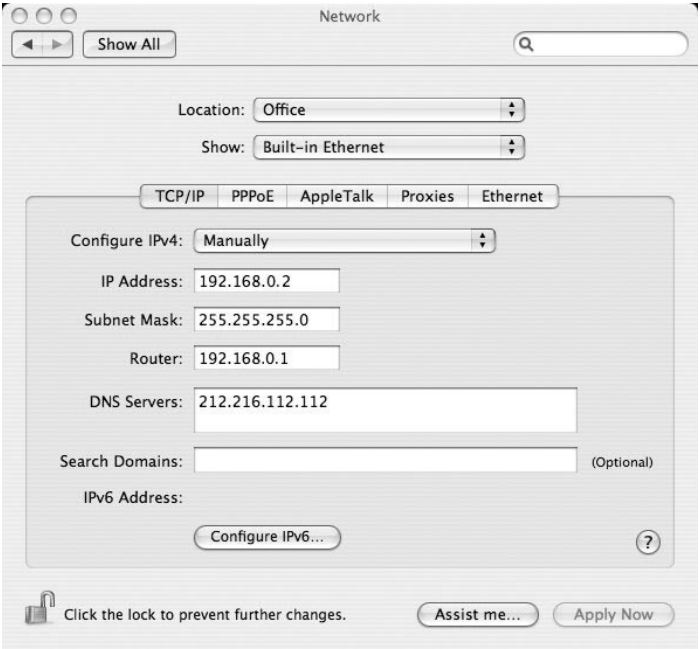
2. Selezionate **Connessione alla rete locale (LAN)** e visualizzate le **Proprietà**, selezionate **Protocollo Internet (TCP/IP)** e premete sul pulsante **Proprietà**.



3. Per impostare un indirizzo IP dovete selezionare **Utilizza il seguente indirizzo IP:** ed inserire Indirizzo IP, la Subnet mask ed il Gateway predefinito come in figura. Confermate con **OK** le nuove impostazioni.
4. Riavviate Windows® per rendere attive le nuove impostazioni.

Macintosh®

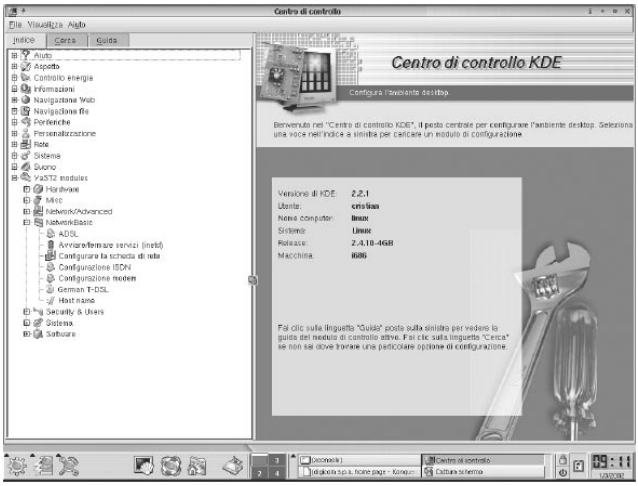
1. Dal Pannello di controllo selezionate **Preferenze di Sistema** (System Preferences).
2. Cliccate sull'icona **Network.**
3. Selezionate Mostra: **Ethernet Integrata** (Built-in Ethernet).
4. Cliccate sul pulsante **TCP/IP.**
5. Selezionate **Manualmente** (Manually).
6. Inserite i valori per **IP** 192.168.0.2, **Maschera di sottorete** (Subnet Mask) 255.255.255.0 e **Router** 192.168.0.1.
7. Chiudete il pannello **Network.**



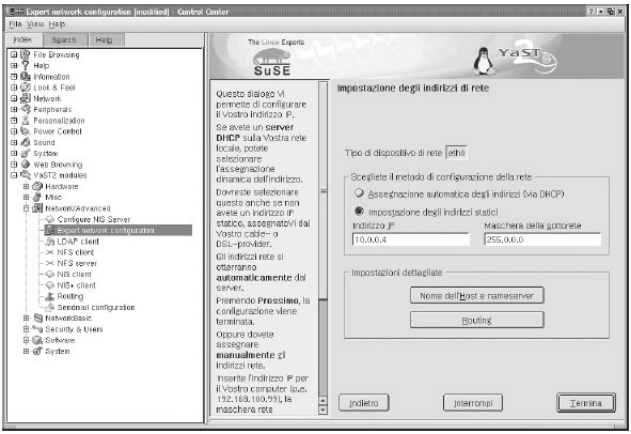
Linux

Di seguito verranno date alcune informazioni su come configurare le risorse di rete utilizzando il Centro di Controllo KDE, con la distribuzione Suse 6.2.

1. Attivate il Control Center.
2. Selezionate **Configurare la scheda di rete** nel menù **Network Basic**.



3. Selezionate **Impostazione degli indirizzi statici**, ed inserite gli indirizzi come riportato in figura.



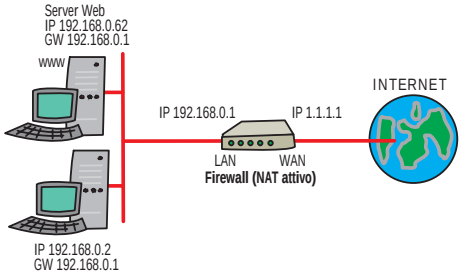
4. Per impostare il gateway, cliccate su Routing e inserite l'indirizzo 10.0.0.2 nel campo Gateway predefinito.

6.2. ESPORTAZIONE DI SERVIZI

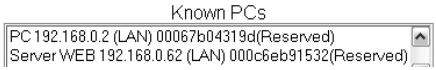
Come descritto nel manuale, volendo rendere disponibili agli utenti Internet dei servizi offerti da alcune macchine nella nostra LAN è necessario configurare delle “esportazioni”.

Le esportazioni basilari possono essere effettuate dall’apposito menù **Internet - Virtual Server.**

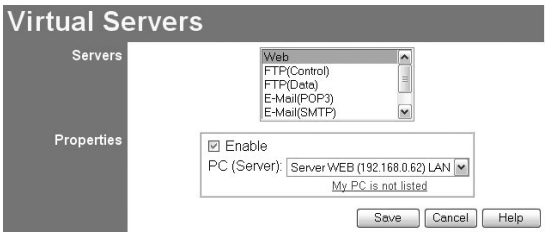
Volendo realizzare l’applicazione descritta nell’immagine sotto (rendere accessibile il server WEB 192.168.0.62) occorre:



- Verificare che il Server WEB (192.168.0.62) sia inserito nel PC Database



- Nella finestra di configurazione **Virtual Server** impostare:



Cliccare su **Save** per salvare le impostazioni.

Terminata la configurazione, da Internet si potrà accedere al Server Web (192.168.0.62) tramite l’auttuale indirizzo di WAN. L’utente dovrà inserire nel proprio browser l’URL http://1.1.1.1

6.3. ESPORTAZIONE DEI SERVIZI TRAMITE FIREWALL RULES

Come descritto nel manuale, volendo rendere disponibili agli utenti Internet dei servizi offerti da alcune macchine nella nostra LAN è necessario configurare delle "esportazioni".

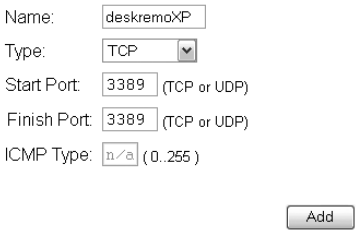
Se avete la necessità di esportare dei servizi differenti da quelli disponibili nella finestra di configurazione Virtual Server (WEB, FTP, POP3, SMTP, DNS, Telnet) è necessario aggiungerli manualmente, tramite la funzione **Security – Firewall Rules.**

In quest'esempio effettueremo l'esportazione del servizio "Condivisione Desktop Remoto" di Windows® Xp.

Prima di procedere alla configurazione è necessario disporre delle seguenti informazioni:

- **Indirizzo IP del PC che offre tale servizio**
  Verificate che il PC in questione sia configurato con indirizzo **IP Statico**, oppure che sia inserito nel PC Database come "**DHCP Client - reserved IP address**" (è necessario che abbia sempre lo stesso indirizzo).
- **Porta utilizzata dal servizio da esportare**
  Generalmente queste informazioni sono fornite dal produttore del Software se la porta è fissa e non modificabile, oppure è un parametro che è possibile impostare.
  In questo caso, Windows® XP utilizza la porta 3389 con protocollo TCP.

Accedete alla finestra di configurazione **Security – Services**
Verificate se nella lista **Available Services** è già disponibile un servizio associato alla porta TCP:3389
Al default questo servizio non è presente, pertanto dovrete aggiungere un nuovo servizio:



- Cliccate su **Add** per aggiungere il servizio alla lista.

Accedete alla configurazione delle regole del Firewall e cliccate sul tasto **Add** per inserire una nuova regola.

Name nome della regola

Type la direzione da impostare per esportare un servizio è dalla WAN (esterno) alla LAN (interno); se il PC si trova collegato alla porta fisica DMZ la direzione sarà WAN => DMZ

Souce IP *Any* qualsiasi utente Internet

Dest IP Inserite l'indirizzo IP della macchina che offre il servizio

Services selezionate il servizio precedentemente creato

Action *Forwar,d* permettere il passaggio di questo servizio

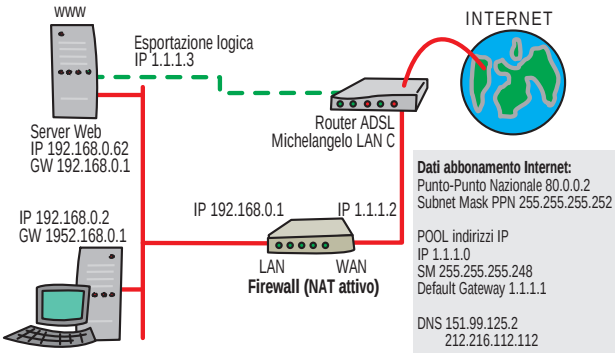
Log *Always* per registrare sempre nel LOG gli accessi effettuati

Cliccate sul tasto **Save** per salvare la configurazione.

A questo punto un utente connesso ad Internet potrà accedere al servizio esportato, "puntando" all'indirizzo IP di WAN del Firewall.

6.4. MULTI-DMZ – UTILIZZO DI UN RANGE DI INDIRIZZI PUBBLICI

In quest'esempio vedremo come utilizzare abbonamenti con **n IP Pubblici.**



Utilizzando un abbonamento Internet come quello riportato nell'esempio solitamente sfruttiamo SOLO i primi due indirizzi IP dei 5 utilizzabili:

1.1.1.1 assegnato alla LAN del router Adsl
1.1.1.2 asseganto alla WAN del Router

Volendo inserire un Server (WEB) con indirizzo pubblico 1.1.1.3 siamo costretti a posizionare il server nella porzione di rete tra il Firewall ed il router Adsl privandolo completamente di qualsiasi protezione.

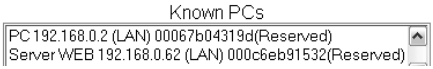
Grazie alla funzionalità Multi-DMZ possiamo (come nell'immagine) mantenere il Server Web collegato alla LAN con un indirizzo IP Privato (192.168.0.62) e rendere disponibile il Server con l'indirizzo pubblico 1.1.1.3

Il vantaggi di questa operazione sono:

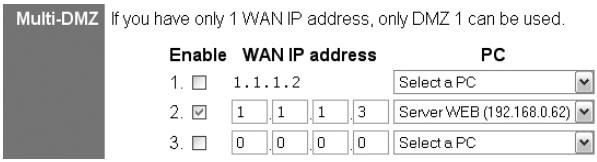
- Mantenere il Server connesso alla LAN
- Rendere visibile il Server con Indirizzo IP diverso da quello del Firewall
- Avere ancora libere tutte le porte del Firewall per altri Virtual Server verso altre stazioni di rete
- Mantenere attivo sul Server WEB la **protezione DoS** fornita dal Firewall

La configurazione da effettuare è la seguente:

Inserite il Server WEB (192.168.0.62) nel PC Database



Accedete alla finestra di configurazione **Internet – Advanced Setup.**
Attivate la funzionalità Multi-DMZ come indicato nell'immagine.



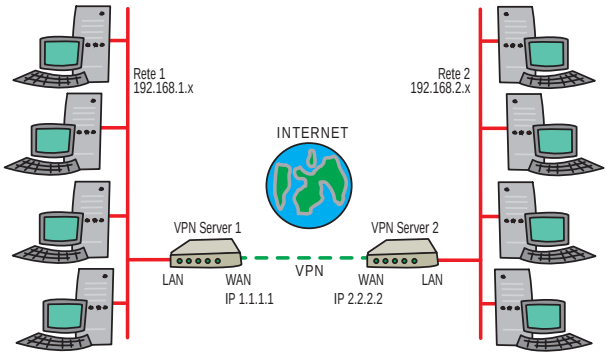
Cliccate su **Save** in fondo alla pagina per attivare la configurazione.

Tutti i servizi disponibili sul Server WEB sono ora raggiungibili tramite l'indirizzo IP 1.1.1.3 , in questo caso qualsiasi utente Internet può raggiungere questo Server tramite l'URL http://1.1.1.3

6.5. CONNESSIONE DI DUE RETI LAN CON IPSEC

L'applicazione descritta prevede la connessione, generalmente chiamata Lan-to-Lan tra due reti tramite Internet, con un tunnel VPN IPSec.

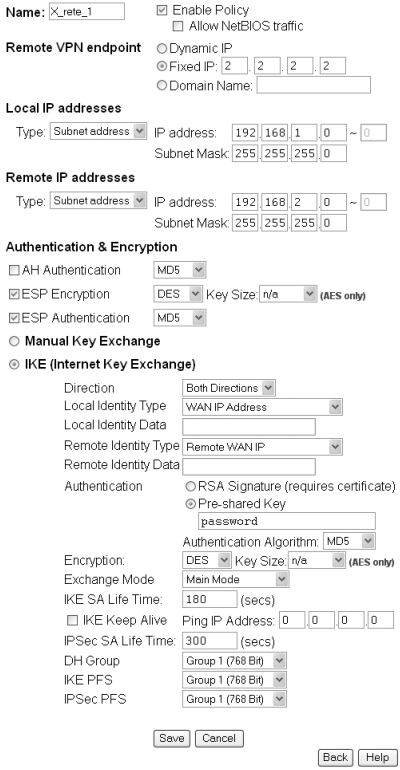
Lo schema dell'applicazione è il seguente:



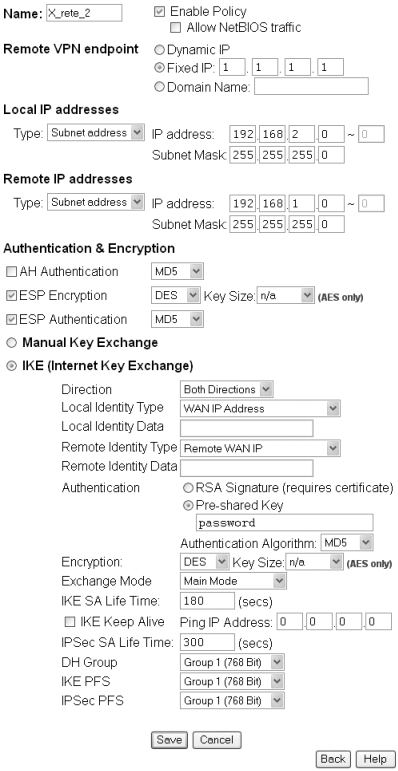
Le due LAN devono necessariamente utilizzare **indirizzi IP differenti.**
I due Endpoint devono avere indirizzi IP di WAN **Statici** e **Pubblici** (1.1.1.1 e 2.2.2.2)

Un esempio di configurazione è il seguente:

VPN Server RETE 1



VPN Server RETE 2

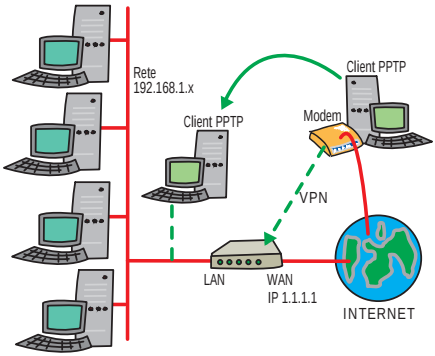


Cliccate **Save** per salvare la configurazione.

Dopo aver configurato le Policy è sufficiente aprire una sessione verso un indirizzo IP della rete remota (anche un ping) per attivare automaticamente il Tunnel VPN.

6.6. ACCESSO ALLA LAN DA CLIENT WINDOWS® CON MICROSOFT VPN

L'applicazione descritta permette l'accesso alla rete locale da parte di un PC connesso in Internet.



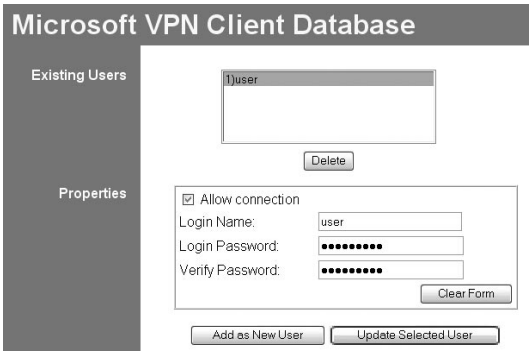
Dopo aver aperto il tunnel VPN PPTP il PC (Client PPTP) risulterà virtualmente collegato alla RETE LAN, disporrà di un indirizzo IP della RETE (192.168.1.x) e potrà liberamente accedere a tutte le risorse locali.

Per abilitare questo seguite queste semplici istruzioni:

nel menù **Microsoft VPN – Server**

Abilitate il server selezionando le opzioni che vedete nell'immagine (PAP è disabilitato per garantire maggiore sicurezza).

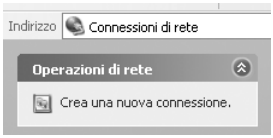
Nel menù **Microsoft VPN – Client**



Aggiungete un utente inserendo il nome in **Login Name** e la password in **Login Password** e **Verify Password,** verificate che sia selezionata l'opzione **Allow connection** e cliccate sul tasto **Add as New User.**

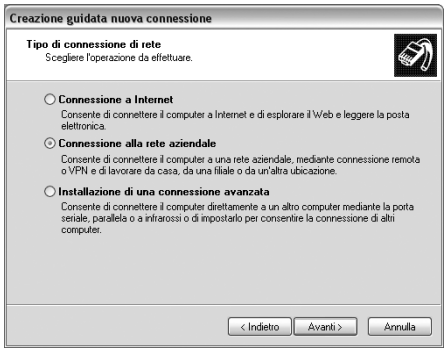
Terminata questa fase, l'utente inserito può connettersi alla nostra rete.

6.6.1. CONFIGURAZIONE WINDOWS® XP PER ACCESSO MICROSOFT VPN



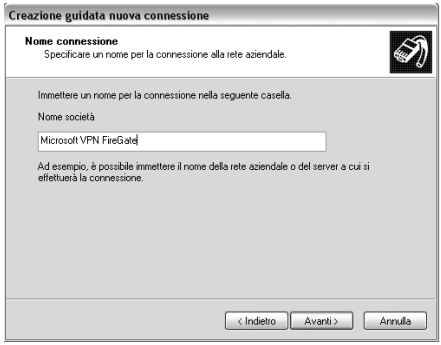
Dal menù **Connessioni di rete** selezionate l'opzione **Crea una nuova connessione.**

Selezionate **Avanti.**

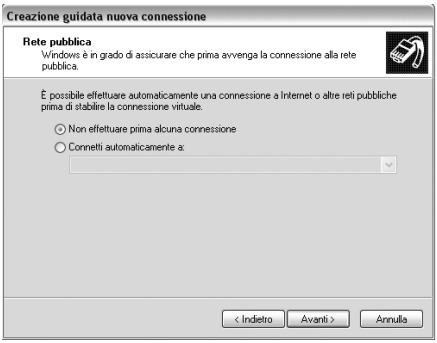


Selezionate **Connessione alla rete aziendale** e cliccate su tasto **Avanti.**

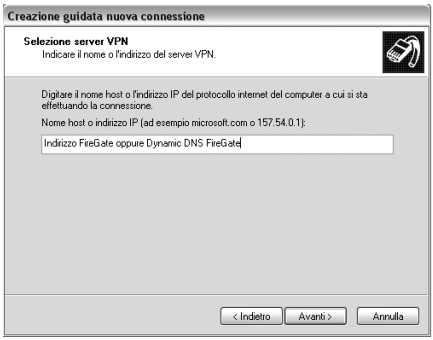
Selezionate **Connessione VPN** e cliccate su tasto **Avanti.**



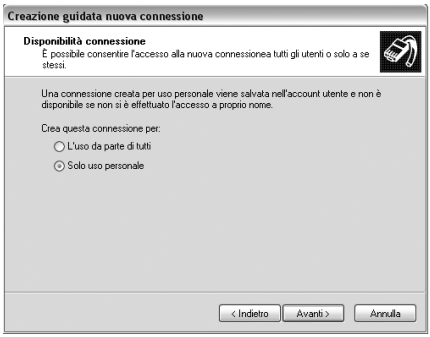
Inserite un nome mnemonico per la connessione e cliccate su tasto **Avanti.**



Selezionate la voce **Non effettuate prima alcuna connessione** se accedete ad Internet tramite Ethernet oppure se non volete effettuare automaticamente una connessione remota e cliccate su tasto **Avanti.**



Inserite l'indirizzo IP del FireGate 10 oppure il nome corrispondente all'IP del FireGate e cliccate su tasto **Avanti.**



Selezionate **Solo uso personale** se volete abilitare questa connessione solo per il Vostro profilo di Windows® Xp e cliccate su tasto **Avanti.**

Cliccate sul tasto **Fine** per terminare la configurazione.

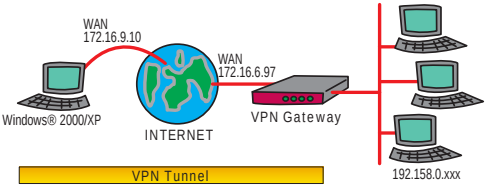
Eseguite la nuova connessione creata ed inserite l'username e la password inserite nel FireGate per accedere alla LAN remota.

Nota! Se sul FireGate è stato disabilitato il DHCP Server sulla LAN, dovete inserire un indirizzo IP statico nella configurazione di questo accesso VPN.

6.7. CONFIGURAZIONE WINDOWS® 2000 / XP PER ACCESSO CON IPSEC

Esempio 2: Windows® 2000/XP Client che accede ad una LAN

In questo esempio, un client Windows® 2000/XP si connette al VPN Gateway ed ottiene l'accesso alla LAN locale.

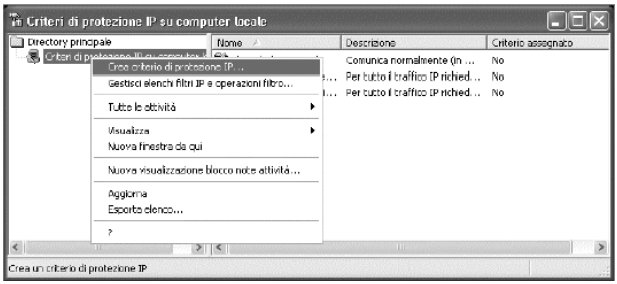


Configurazione VPN Gateway

Impostazione	**Valore**	**Note**
Name	Win Client	Nome mnemonico
Remote Endpoint	172.16.9.10	Indirizzo IP di WAN (Internet) dell'altro endpoint.
Local IP addresses	Subnet address: 192.168.0.0 255.255.255.0	Permette l'accesso all'intera LAN. Usare la definizione il più possibile restrittiva.
Remote IP addresses	172.16.9.10	Per un singolo client equivale al Gateway.
Key Exchange	IKE	Devono corrispondere
IKE SA Parameters		
IKE Direction	Booth	Permette l'attivazione del tunnel da entrambi gli endpoint
Local Identity	WAN IP address	Richiesto
Remote Identity	WAN IP address	Richiesto
IKE Authentication method	Pre-shared Key	I Certificati non sono largamente utilizzati.
Pre-shared Key	Xxxxxxxxxx	Deve corrispondere all'impostazione del client
IKE Authentication algorithm	SHA-1	Deve corrispondere all'impostazione del client
IKE Encryption	3DES	Deve corrispondere all'impostazione del client
IKE Exchange mode	Main Mode	Deve corrispondere all'impostazione del client
DH Group	Group 1 (768 bit)	Deve corrispondere all'impostazione del client
IKE SA Life time	28800	Può differire dall'impostazione del client, verrà utilizzata quella con tempo minore
IKE PFS	Disable	Deve corrispondere all'impostazione del client
IPSec SA Parameters		
IPSec SA Life time	28800	Può differire dall'impostazione del client, verrà utilizzata quella con tempo minore
IPSec PFS	Disable	Deve corrispondere all'impostazione del client
AH authentication	Non Selezionato	AH è raramente utilizzato
ESP authentication	Selezionato /MD5	Deve corrispondere all'impostazione del client
ESP encryption	Selezionato /DES	Deve corrispondere all'impostazione del client

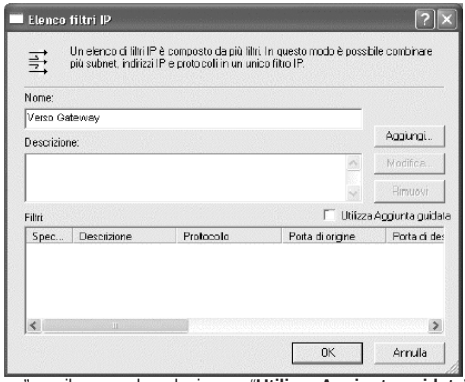
Configurazione client Windows®

1. Selezionare Start - Programmi – Strumenti di Amministrazione – Criteri di protezione locali.
2. Right click *IP Security Policy on Local Machine* and select *Create IP Security Policy*

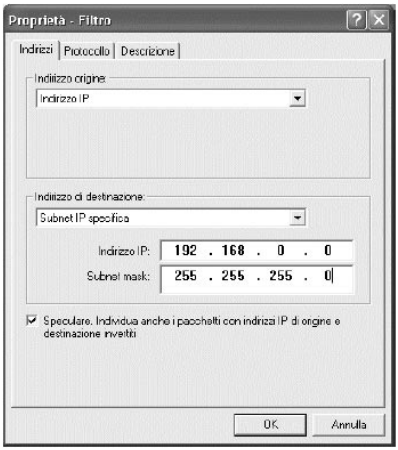


3. Cliccare su “Avanti”, inserire un nome per la policy, ad esempio “Gateway_Win2k”, cliccare “ Avanti “.
4. Deselezionare *Attiva regola predefinita.* Cliccare “ Avanti “, cliccare “Fine”. La nuova regola verrà inserita in lista.
5. Fare click con il tasto destro e selezionare “Proprietà”. Vedrete una finestra come quella nell’esempio sotto.
   - Notare che non esistono filtri. Dovranno essere aggiunti 2 filtri, entrante e uscente.
   - Aggiungiamo il filtro uscente per primo.

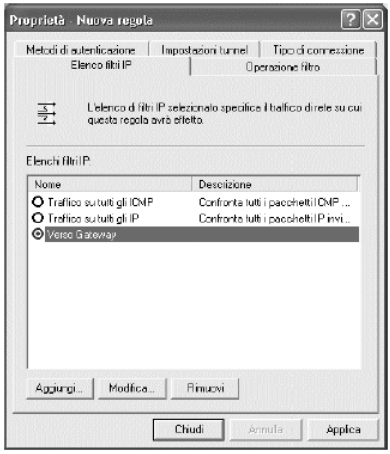
6. Deselezionare “Utilizza Aggiunta guidata” e cliccare “Aggiungi”, poi nuovamente su “Aggiungi”



7. Digitare "**Verso Gateway**" per il nome, de-selezionare **"Utilizza Aggiunta guidata**" e cliccare "**Aggiungi**".
8. Siccome questo è il filtro uscente, **l'Indirizzo origine** equivale all'Indirizzo IP del client e **l'indirizzo destinazione** equivale alla rete remota.
   Verificare che l'opzione "**Speculare...**" sia selezionata.



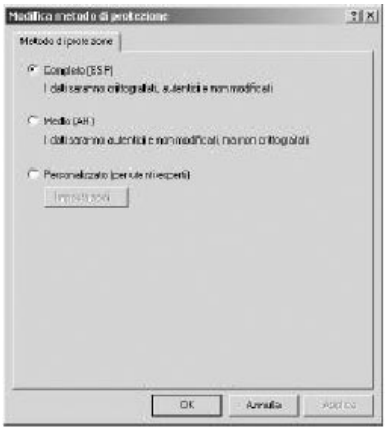
9. Cliccare "**OK**" per salvare le impostazioni e chiudere il pannello.



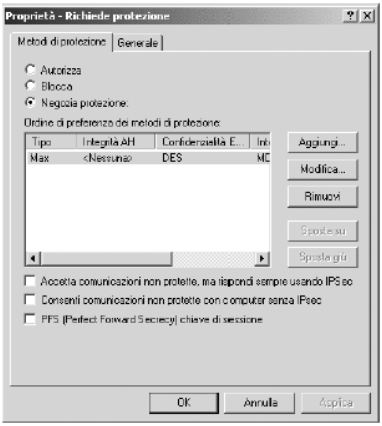
10. Nel pannello (sopra) assicurarsi che il filtro "**Verso Gateway**" sia selezionato, cliccare su "**Operazione Filtr*o***"

11. Selezionare "**Richiedi**" protezione e cliccare su "**Modifica**".

12. Selezionare "**Negozia protezione**" (questo seleziona IKE) e cliccare su "**Aggiungi**".



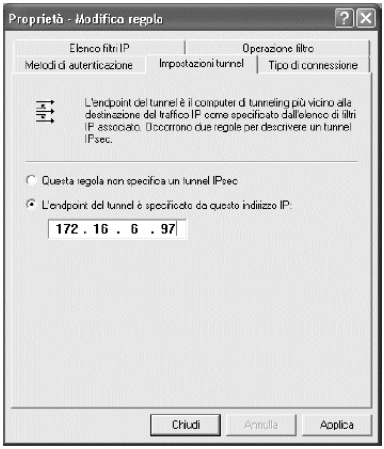
13. Nel pannello (sopra), selezionare **Completo** *[ESP]* e cliccare "**OK**" per salvare le impostazioni e tornare al pannello **"Richiedi protezione"**.



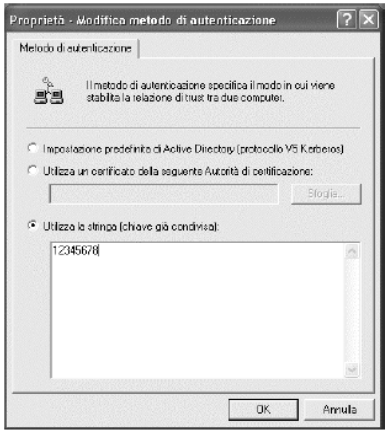
14. Verificare che le seguenti impostazioni siano corrette.

VPN	**Windows®**
IKE abilitato	Negozia protezione
AH disabilitato	Integrità AH: <Nessuna>
ESP encryption: Abilitata/DES	Confidenzialità :DES
ESP authentication: Abilitata /MD5	Integrità ESP: MD5

15. Cliccare "**OK**" per tornare al pannello "**Operazione filtro"** di "**Modifica Regola**".
16. Cliccare "**Impostazioni Tunnel"** , selezionare "**l'endpoint del tunnel è specificato da questo indirizzo IP**" ed inserire l'indirizzo IP di WAN (Internet) del VPN Gateway.

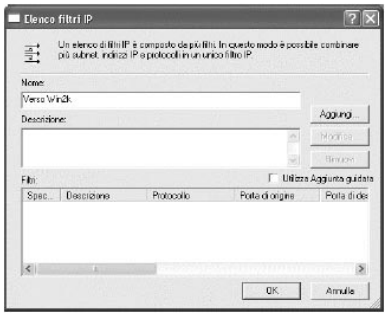


17. Cliccare su "**Metodi di autenticazione**", cliccare "**Modifica**".
18. Selezionate "**Utilizza stringa**" *(chiave condivisa)*, inserire una chiave nel campo a disposizione.

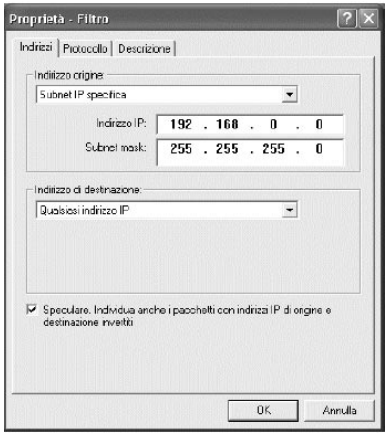


19. Cliccare su "**OK**" per salvare le impostazioni e tornare al pannello *Metodi di autenticazione* di "**Modifica regole**".
20. Cliccare su "**Chiudi**" per tornare a Proprietà gateway_Win2k. Apparirà il filtro "**Verso Gateway**".

21. Aggiungiamo ora la seconda regola (entrante).
Deselezionare "**Utilizza Aggiunta guidata**" e cliccare "**Aggiungi**", poi nuovamente su "**Aggiungi**".



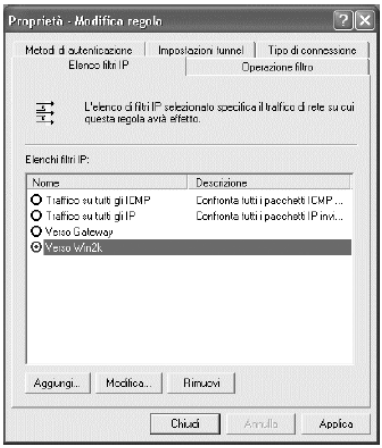
22. Digitare "**Verso Win2k**" per il nome, de-selezionare "**Utilizza Aggiunta guidata**" e cliccare "**Aggiungi**".



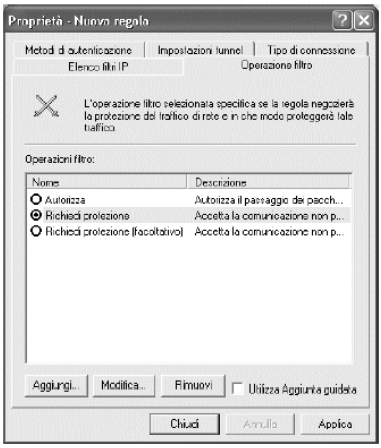
Siccome questo è il filtro entrante, **l'Indirizzo origine** equivale alla rete remota e **l'indirizzo destinazione** equivale all'Indirizzo IP del client.

Verificare che l'opzione "**Speculare...**" sia selezionata.

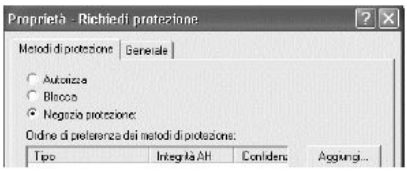
23. Cliccare su "**OK**" per salvare le impostazioni.

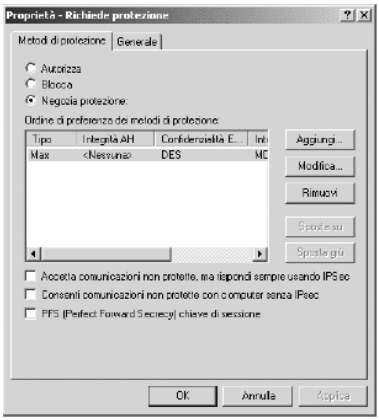


24. Nel pannello (sopra) assicurarsi che il filtro "**Verso Win2k**" sia selezionato, cliccare su "**Operazione Filtro**".

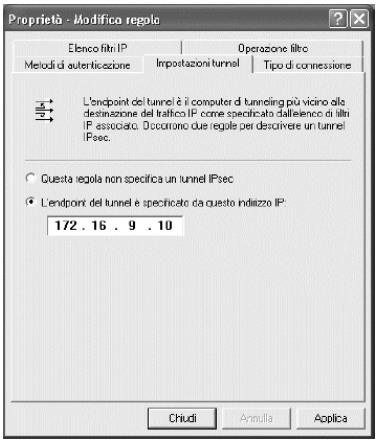


25. Selezionare "**Richiedi protezione**" e cliccare su "**Modifica**".

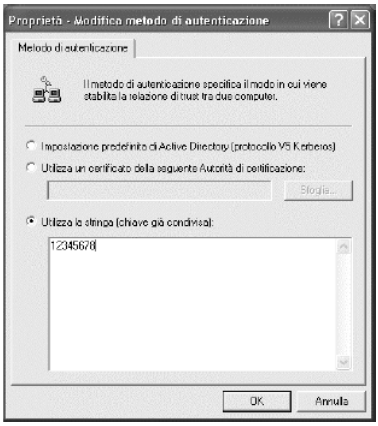




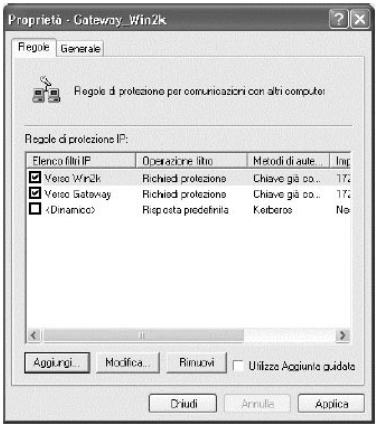
27. Cliccare "**OK**" per salvare le impostazioni e poi nuovamente "**OK**" per tornare al pannello Operazione filtro.
28. Selezionare "**Impostazioni Tunnel**" ed inserire l'indirizzo IP del PC client che corrisponde di fatto al suo indirizzo di WAN (Internet).



29. Selezionare il pannello Metodi di autenticazione, cliccare "**Modifica**".
30. Selezionate "**Utilizza stringa**" *(chiave condivisa)*, inserire una chiave nel campo a disposizione.



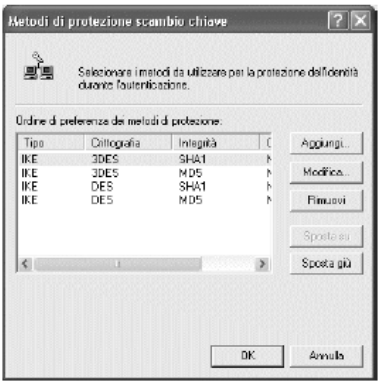
31. Cliccare su "**OK**" per salvare le impostazioni e tornare al pannello *Metodi di autenticazione* di "**Modifica regole**".
32. Cliccare su "**Chiudi**" per tornare a Proprietà Gateway_Win2k.



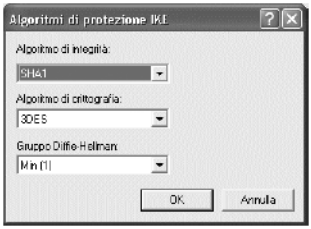
33. Selezionare il pannellino *Generale.*

34. Cliccare su "**Avanzate**"

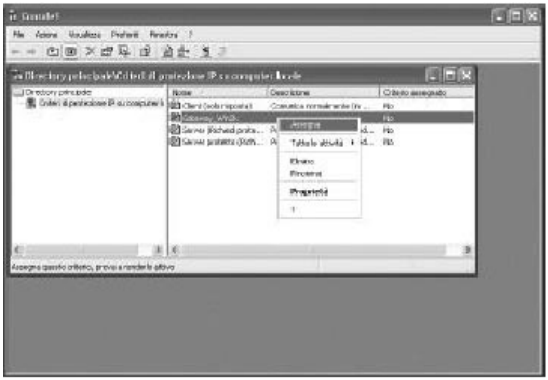
35. Cliccare su "**Metodi**".

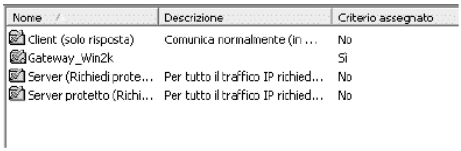


36. Selezionare la prima entry, cliccare su "**Modifica**".



37. Selezionare "**SHA1**" per *Algoritmo di integrità*, "3DES" per *Algoritmo di crittografia*, "Min o Low (1)" per *Gruppo Diffie-Hellman*.
38. Cliccare "**OK**" per salvare le impostazioni, nuovamente "**OK**" poi "**Chiudi**" per tornare a *Criteri di protezione locali*.
39. Fate doppio click sulla policy Gateway_Win2k e selezionate "**Assegna**" per attivare la policy.





La configurazione è completa.

21010 Cardano al Campo VA
via A. Volta 39