FireGATE 10 C

Codice: 8E4205

DESCRIZIONE

La soluzione ideale per l'accesso protetto ad Internet e la condivisione remota di risorse aziendali.

La crescente diffusione delle linee di tipo Broadband rende l'accesso ad Internet via ADSL (o xDSL in generale) la soluzione più vantaggiosa ed attrattiva.

FireGATE 10 C sfrutta una connessione xDSL già esistente per far navigare tutti i computer della rete, in modo efficiente e trasparente.
Se lo si desidera, si possono configurare le modalità ed i servizi Internet ai quali i computer della rete potranno accedere, creando diversi gruppi con diversi permessi, restringendo o abilitando selettivamente l'utilizzo del servizio di accesso ad Internet.

Se da un lato le caratteristiche di velocità ed economicità delle linee Broadband sono un indiscutibile vantaggio, non bisogna sottovalutare o dimenticare l'aspetto della "sicurezza" che ne deriva.
Essere sempre On-Line equivale ad essere sempre connessi, sempre "raggiungibili", e di fatto, sempre esposti agli eventuali attacchi provenienti da malintenzionati o semplici buontemponi.

Firewall
Quando una rete è connessa ad Internet gli attacchi provenienti dall'esterno possono essere molteplici, di varia natura e con scopi ed effetti diversi.
Si può attaccare una "rete" per arrivare fino ai Server e carpirne, modificarne o cancellarne i dati.

Qualche volta gli hacker si accontentano semplicemente di curiosare, oppure se i dati presenti sui computer non hanno un qualche valore interessante o commerciabile, usano piazzare dei "cavalli di troia" sui server o sui computer client.

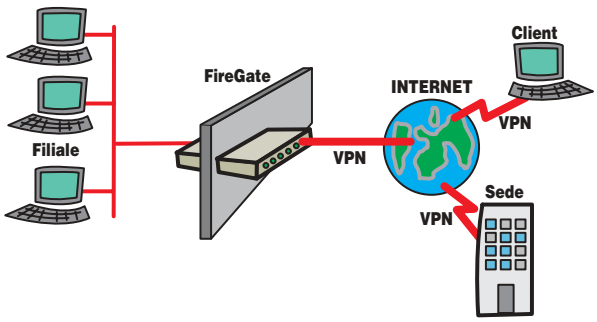
- **Switch 3 porte 10/100Mbit/s integrato**
- **1 porta WAN 10/100 Mbit/s**
- **1 porta DMZ 10/100 Mbit/s**
- **Firewall Stateful Packet Inspection**
- **Supporto VPN IPSec Tunnel (fino a 10) tramite acceleratore hardware: MD5-HMAC/SHA1-HMAC authentication, DES-CBC, 3DES-CBC encryption, AES, Internet Key Exchange, Manual Key Negotiation**
- **Supporto VPN Microsoft® (PPTP) con autenticazione PAP, CHAP, MS-CHAP, MSCHAP-v2**
- **Supporto protocolli NAT, PPPoE, HTTP, DHCP, TCP/IP, UDP, PAP, CHAP, RIP1, RIP2, DDNS, UpnP, Syslog**
- **Supporto DHCP Server e Client**
- **Supporto esportazione di servizi interni NAT e NAPT**
- **Funzione NAT disattivabile**
- **Supporto VPN Passthrough PPTP, IPSec, L2TP**
- **Supporto Multi-DMZ (fino a 7 indirizzi IP Internet)**
- **Funzioni di sicurezza Firewall: Attack Alert (Email) log, Policy Based Packet Filter, Stateful Packet Inspection, DoS (Denial of Service), URL filter, Access Control**
- **Configurazione e Management protetto da password via Browser, locale e remoto**
- **Configurazione salvabile**
- **Firmware aggiornabile**
- **Dimensioni: 170 x 148 x 28 mm**
- **Peso: 300 gr.**
- **Alimentazione: 12Vcc 1A**
- **Marcatura CE**

NETWORKING - FIREWALL

FireGATE 10 C

Una volta "infettato" un computer o server si può successivamente prenderne remotamente il controllo oppure "ordinargli" di condurre a sua volta un attacco verso altri server. Tracciando questo tipo di evento sembrerà che l'attaccante sia il vostro computer e non quello dell'hacker!

Questi e altri motivi possono bastare per decidere di cautelarsi e non offrire la propria rete su di un piatto di argento a chiunque abbia le intenzioni e le capacità per farne un uso non appropriato o illegale.
Proteggere la propria rete è quindi non solo ragionevole ma praticamente indispensabile.
FireGATE 10 C nasce anche con questo scopo. Le sue funzioni di sicurezza includono il riconoscimento e il blocco di attacchi di tipo Denial of Service, Stateful Packet Inspection, URL Filtering ed Access Control.

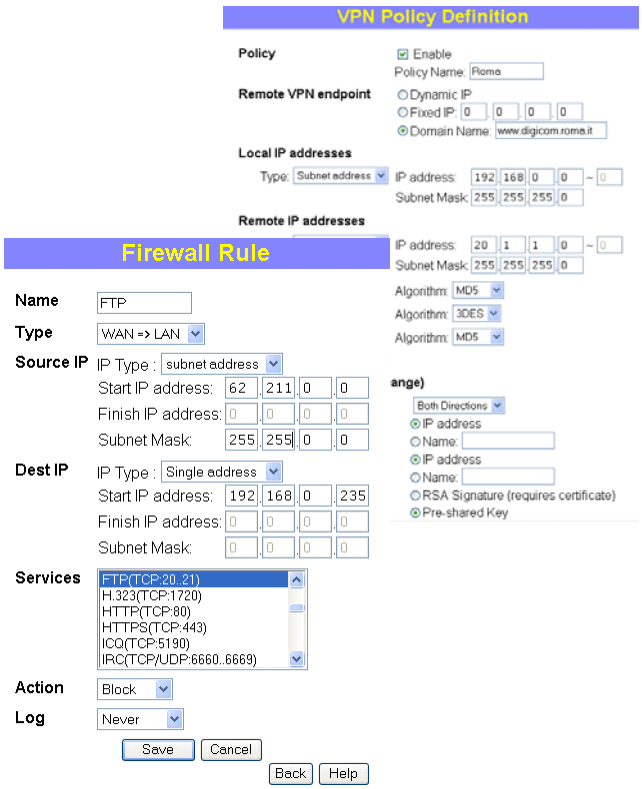


VPN/IPSec Tunnels

Un'altra caratteristica tipica dell'utilizzo di linee broadband è la possibilità di realizzare delle interconnessioni protette con altre reti o computer attraverso Internet.
Per garantire la sicurezza e la riservatezza dei dati circolanti sulla rete "pubblica" FireGATE 10 C supporta le VPN (Virtual Private Networks) con protocolli di crittografia ed autenticazione IPSec o IKE.
Le chiavi di protezione possono essere inserite manualmente, negoziate o gestite da “certificati” di validazione.
Alte prestazioni sono garantite da un apposito engine acceleratore hardware dedicato.

In questo modo si possono creare dei veri e propri "tunnel" protetti (fino a 10) tra i vostri computer e la rete remota, condividendone le risorse esattamente come se le due reti fossero direttamente interconnesse tra loro.

Per facilitare ulteriormente l’accesso sicuro alla rete da parte di Client remoti,
FireGATE 10 C può sfruttare il protocollo PPTP funzionando come Server. In questo modo, configurando opportunamente le opzioni disponibili in Windows®, il vostro PC remoto apparterrà a tutti gli effetti alla rete a cui si è connesso tramite Internet in modo semplice e sicuro. Tutto ciò si può realizzare anche se gli abbonamenti che avete sottoscritto con il vostro ISP prevedono indirizzi IP dinamici.



NETWORKING - FIREWALL