FireGATE 30 DUAL

DESCRIZIONE

La soluzione avanzata per la piccola e media impresa che vuole rendere disponibile le risorse di rete application-based, fornendo nel contempo sicurezza, prestazioni e ridondanza del link Internet agli utenti locali, remoti e mobili.

La presenza di **2 porte WAN** fornisce all'amministratore di rete la possibilità di definire la gestione del traffico in ingresso ed uscita, ottimizzando la banda a disposizione in base a utenti, applicazioni o protocolli in transito. Per le situazioni in cui l'accessibilità alle risorse di rete è prevalente, è possibile utilizzare la **seconda porta WAN** come **backup automatico** della prima, in modalità Link Failover.

Un completo **Firewall integrato** sovraintende alla **sicurezza generale** proteggendo la rete da accessi indiscriminati e da attacchi provenienti da Internet, mentre l'**accesso protetto** è gestito da un **server VPN** in grado di realizzare **fino a 30 tunnel IPSEC** site-to-site ad alte prestazioni e **fino a 4 link PPTP** user-to-site.

La recente diffusione di applicazioni VoIP e IPTV richiede alle moderne infrastrutture di rete di essere adeguatamente predisposte, al fine di poter correttamente supportare e distribuire questi servizi agli utenti. FireGATE 30 DUAL può essere un componente primario di questo scenario, integrando le **funzionalità di SIP pass-trough**, **IGMP Snooping** e **IGMP Proxy**, oltre alla gestione del **Quality of Service** inbound e outbound che permetta di ottenere sempre il **massimo della banda disponibile** minimizzando le congestioni di traffico.

FireGATE 30 DUAL **racchiude** in un singolo dispositivo **tutte le funzionalità** che un moderno sistema di accesso ad Internet per piccola e media impresa deve avere, ad un prezzo di gran lunga inferiore all'insieme dei diversi dispositivi. **Gateway Internet**, **Firewall**, **VPN server**, **Application server**, **Traffic management** e ridondanza del link All-inside-the-box!

Codice: 8E4335

Hardware

- **2 porte WAN 10/100 Auto MDI-MDI-X**
- **8 porte LAN 10/100 Auto MDI-MDI-X**
- **Chassis metallico, montabile a rack 19"**

Supporto Load Balancing e Traffic Management

- **Load balancing in ingresso ed uscita su IP, Protocolli, Servizi e Volume del traffico**
- **Gestione DNS su load Balance in ingresso**

Supporto Backup su guasto del link principale

- **Modalità di Failover e ripristino automatico del link principale**

Supporto VPN IPSEC

- **Fino a 30 tunnel con throughput di oltre 30Mbps**
- **Supporto IKE e Manual Keying**
- **Crittografia e Autenticazione DES, 3DES, AES, MD5, SHA1, AH, ESP**
- **Dynamic IPSec, IPSec NAT Traversal**
- **DPD (Dead Peer Detection)**
- **NetBios over VPN**
- **Client software VPN IPSec incluso**

Supporto VPN PPTP

- **Fino a 4 tunnel con throughput fino a 10Mbps**

Funzioni di Sicurezza Firewall

- **Stateful Packet Inspection (SPI)**
- **Protezione da attacchi Denial of Service (DoS)**
- **Policy based IP e MAC Packet Filtering in ingresso ed Uscita**
- **URL filter, Access Control, gestione blocco Java Applet/Active X/Web Proxy/ Cookie**

NETWORKING - FIREWALL

FireGATE 30 DUAL

NETWORKING - FIREWALL

Supporto Quality of Service

- Prioritizzazione del traffico e gestione della banda su protocolli, indirizzi e porte
- Supporto DiffServ

Configurazione e gestione

- Interfaccia grafica Web based
- Supporto configurazione guidata VPN
- Management locale e remoto via HTTP e HTTPS

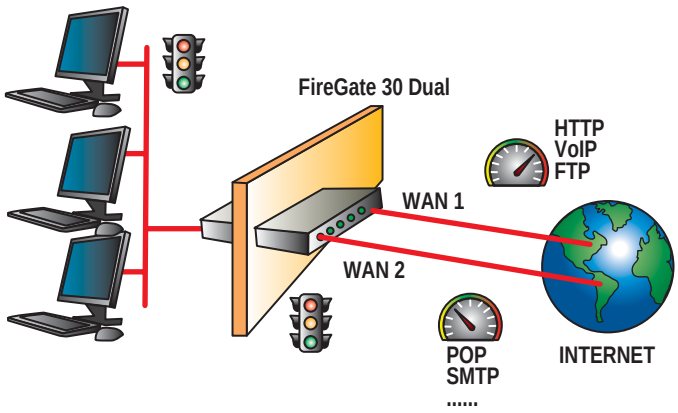
Supporto protocolli e funzioni

- System Logvia email e Syslog
- Accesso WAN IP statico, DHCP, PPPoE, PPTP
- Router mode con e senza NAT
- Supporto Multiple NAT su Multiple LAN e WAN
- Supporto Dynamic DNS, Routing statico e RIP-2
- SupportoVirtual Server DMZ,DHCP Server, NTP, SMTP Client, SNMP
- Supporto SIP Pass-through, IGMP snooping e IGMP Proxy
- Supporto Port based VLAN Bridge

Caratteristiche salienti

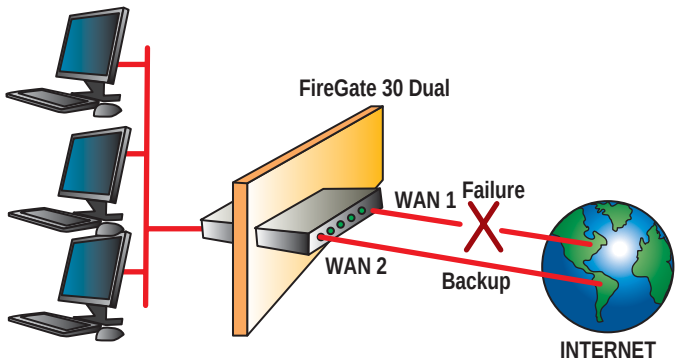
Incremento, Scalabilità e Ripristino della banda.

La **doppia porta WAN** è uno dei principali punti di forza di FireGATE 30 DUAL. Potendo combinare **due connessioni Internet distinte e separate**, permette di trarne i vantaggi intrinsechi come la possibilità di sommare la velocità e la capacità dei due link, condividerne la banda in modo ottimizzato e suddividerla per tipo di utenti, applicazioni o protocolli. L'**amministratore può definire come distribuire** il carico ed i servizi sulle 2 WAN in base a **regole personalizzate**, compresa la gestione dei valori DNS (record NX, MX e CNAME) associabili.



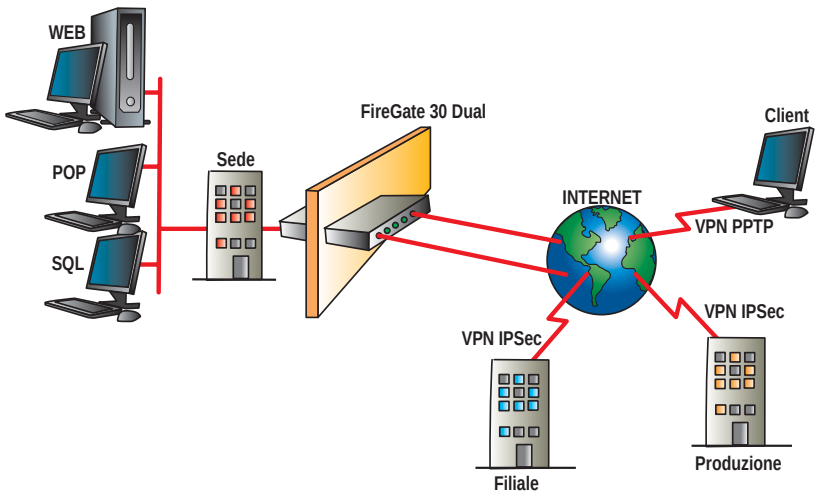
FireGATE 30 DUAL

L'altra possibilità è quella di privilegiare la stabilità della connessione e la fruibilità dei servizi interni o esterni, configurando la **seconda porta WAN come backup** del link primario. In caso di caduta o blocco della connessione Internet principale, FireGATE 30 DUAL attiverà automaticamente la seconda porta WAN trasferendo su di essa tutte le connessioni uscenti ed i servizi interni pubblicati, ripristinando la porta WAN principale non appena possibile, per supportare al meglio l'up-time dei servizi e minimizzare il rischio di perdita di produttività e relativo business. La funzione di Backup è utilizzabile anche in presenza di connessioni VPN IPSec dinamiche.



Accesso protetto e condivisione delle risorse di rete via VPN.

Laddove sia necessario fornire accesso attraverso Internet alle risorse aziendali in modo condiviso, con altre realtà come filiali o aziende partner piuttosto che singoli utenti come dipendenti o servizi in dial-up, la sicurezza è l'aspetto più importante e imprescindibile. A tale scopo FireGATE 30 DUAL è **dotato di un server VPN (Virtual Private network) IPSec/PPTP** in grado di realizzare fino a **30 connessioni simultanee**, **protette** e **crittografate** con throughput di oltre 30Mbps e **4 connessioni PPTP simultanee** (fino a 10Mbps).

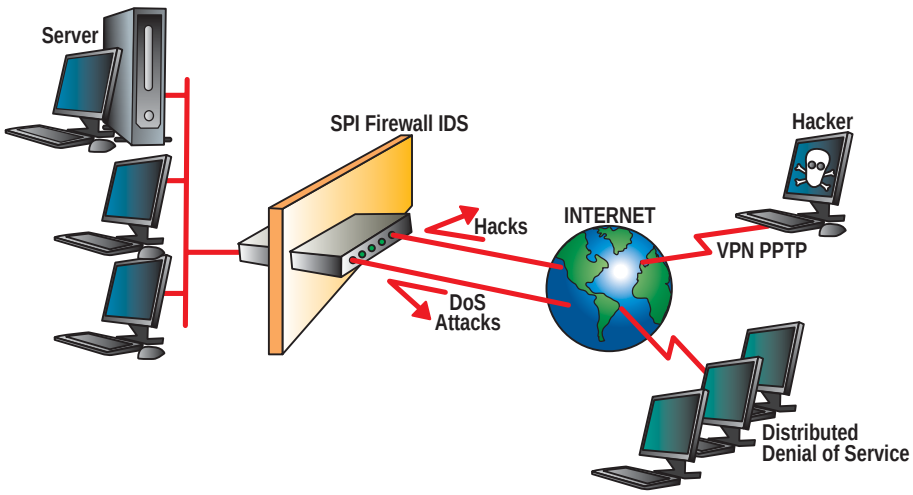


Protezione da attacchi e accessi indesiderati.

La grande diffusione degli accessi broadband alla rete Internet ha portato con se, insieme agli innegabili vantaggi, anche un enorme ed inevitabile dilagare dei tentativi di intrusione e hacking dei computer ad essa collegati. Generalmente parlando, una connessione ad Internet effettuata a 'schermi abbassati' comporta **tentativi d'intrusione** pressochè immediati da parte di sistemi automatizzati e non, che sono pronti ad infettare le macchine con virus, backdoor e trojan, 24 ore al giorno/365 giorni all'anno. **E' quindi indispensabile** interporre delle **barriere efficaci** e **impenetrabili a difesa dei propri server**, dei dati e degli utenti della rete locale.

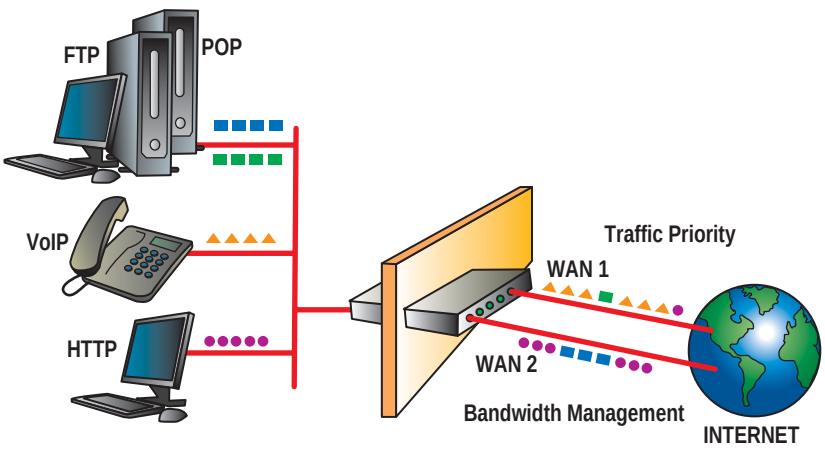
FireGATE 30 DUAL

FireGATE 30 DUAL **implementa un potente Stateful Packet Inspection Firewall** in grado di **riconoscere e bloccare** i tentativi di attacco di tipo **Denial of Service** ed i tentativi di intrusione. Ulteriormente è possibile limitare l'accesso verso l'esterno a determinati protocolli, porte, indirizzi IP e MAC, siti web, applicazioni (Java, Activex, Cookie, ecc) in modo flessibile e totalmente personalizzato. Ogni attività e operazione del firewall può essere inviata sotto forma di log via email o a server syslog.



Gestione Priorità del traffico e Bandwidth Management.

Altro punto di forza di FireGATE 30 DUAL è l'**engine di Traffic and Bandwidth Management**, in grado di **gestire l'utilizzo della banda** ed **assegnare le priorità** di traffico a qualsiasi tipo di dato in transito, assicurando lo smistamento prioritario dei pacchetti mission-critical definibili dall'utente anche in condizioni di forte carico. L'amministratore ha il **totale controllo** e la possibilità di **personalizzare** le soglie massime di traffico ad utenti, applicazioni e servizi, sia in ingresso che in uscita, evitando così la saturazione dei link e garantendo sempre una riserva di banda ai servizi desiderati.



Funzioni di rete.

FireGATE 30 DUAL implementa un **set completo di funzioni di rete** necessarie per realizzare gli scenari e le applicazioni avanzate che è in grado di supportare. Oltre a funzioni standard come **Virtual Server**, **DMZ**, **Routing Statico** e **DDNS** (Dynamic DNS), sono supportate funzioni speciali come **LAN Address Mapping** e **VLAN Bridge**. Quest'ultima funzione permette di realizzare delle reti virtuali VLAN, in modalità Bridge o Tagged, tra gruppi di porte LAN e le porte WAN del dispositivo al fine di delimitare il traffico oppure trasferire sulle porte LAN uno o più indirizzi IP aggiuntivi di WAN.