

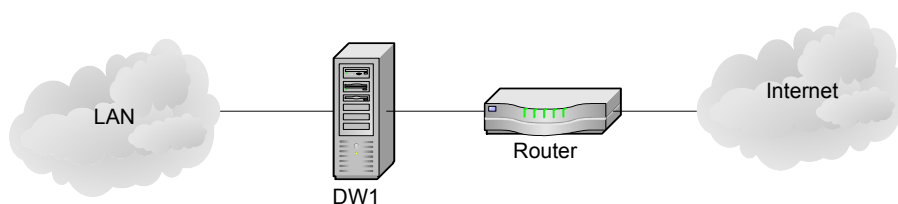
Funzionalità

DigiWall è un firewall per la protezione delle reti aziendali.

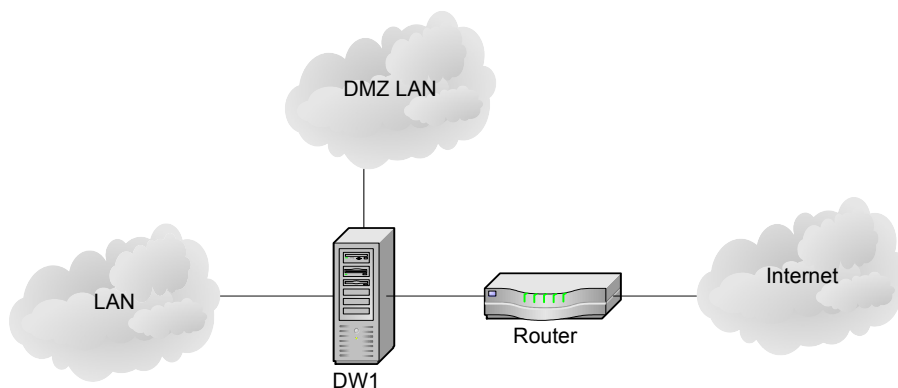
DigiWall è basato sul sistema operativo Linux e pertanto permette soluzioni estremamente flessibili ed adattabili alle esigenze del cliente.

DigiWall può essere usato come firewall perimetrale, come firewall interno (bastion host) o per isolare contemporaneamente più reti da Internet.

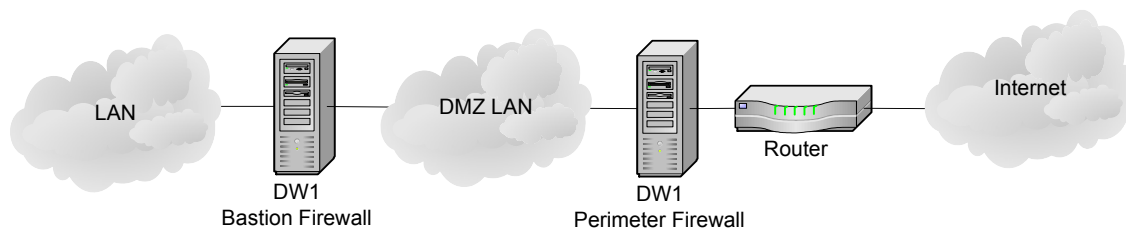
DigiWall può essere configurato in cluster ad alta disponibilità e dispone di un modulo aggiuntivo per il controllo dei servizi di rete con notifica via email e messaggi brevi (SMS) GSM.



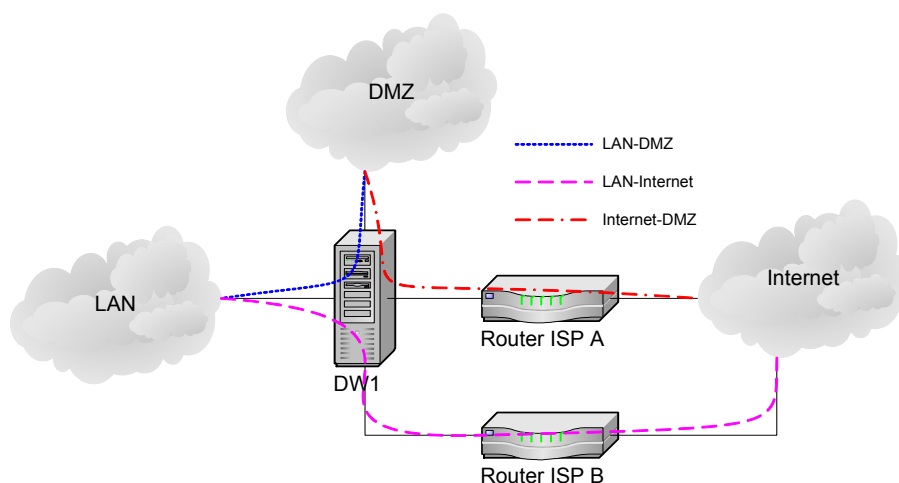
DigiWall come firewall perimetrale per la protezione di una rete locale.



DigiWall come firewall perimetrale per la protezione di reti multiple (rete aziendale e rete dei server pubblici).



DigiWall come firewall perimetrale e come firewall interno per aumentare il livello di protezione della rete aziendale in presenza di server pubblici.



DigiWall come firewall perimetrale per la protezione di reti multiple (rete aziendale e rete dei server pubblici) e con interfaccia verso due (diversi) ISP per funzioni di distribuzione del carico e failover.

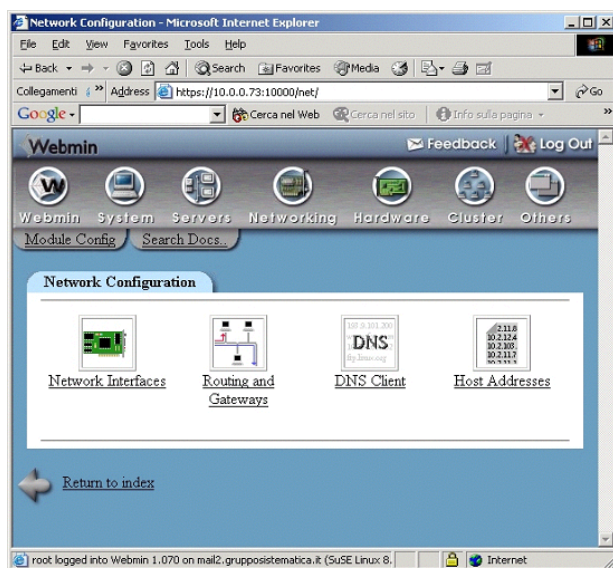
Il numero di utenti, di connessioni ed il volume di traffico supportati sono limitati solo dall'hardware usato. La configurazione standard è consigliata per reti con un numero massimo di 100 nodi, fino a 10000 connessioni contemporanee e un volume di traffico sostenuto di 10 Mbps¹.

- * Stateful packet filtering. DigiWall permette di selezionare i nodi IP e le porte autorizzate all'accesso (sia in ingresso che in uscita).
- * Network address translation. DigiWall permette una completa gestione delle traslazioni di indirizzi. È possibile reindirizzare una intera subnet verso un singolo indirizzo o verso un'altra subnet. Il reindirizzamento può essere impiegato sia in ingresso che in uscita (source e destination NAT).
- * HTTP proxy trasparente. È possibile attivare un proxy HTTP senza la necessità di configurare i nodi della LAN. È possibile indicare quali nodi dovranno passare attraverso il proxy e quali no. Il proxy permette di ridurre il traffico di rete e di definire, tra l'altro, filtri basati sul URL per impedire o limitare l'accesso ad alcuni siti.

¹ Megabit per secondo, con picchi fino a 100 Mbps.

- * DNS masquerading. È possibile attivare un servizio di caching DNS (Domain Name Service) per ridurre il traffico ed i tempi di latenza delle richieste di risoluzione dei nomi nel caso in cui non fossero disponibili dei server DNS interni.
- * DHCP server. È possibile attivare un servizio di assegnazione dinamica degli indirizzi IP ai nodi della rete locale nel caso in cui fosse necessario.
- * Statistiche. DigiWall genera giornalmente statistiche di traffico riferite alle ultime 24 ore. Le statistiche di traffico dell'HTTP proxy (se attivato) descrivono sia il traffico giornaliero che quello aggregato (dall'avvio dell'HTTP proxy)(incluso traffico WEB per ogni ora, giorno, mese; traffico per dominio e per singola URL, traffico per ogni client locale).
- * Amministrazione.
 - DigiWall viene amministrato da una console in locale o in remoto usando SSH (connessione cifrata e sicura). È disponibile anche un'interfaccia WEB accessibile tramite connessione sicura HTTPS.
 - È possibile definire gli host autorizzati a connettersi a DigiWall per l'amministrazione.
 - È possibile l'intervento in assistenza da remoto (teleassistenza).
 - In caso di necessità è possibile bloccare completamente l'accesso ed il transito di pacchetti da/per un certo indirizzo IP.
 - È possibile definire in modo sintetico a quali host permettere o negare alcuni servizi (WEB, EMAIL, FTP, etc.).
 - È possibile controllare le connessioni attive in ogni istante.
 - È possibile controllare quali host generano più traffico e verso quali host lo generano.

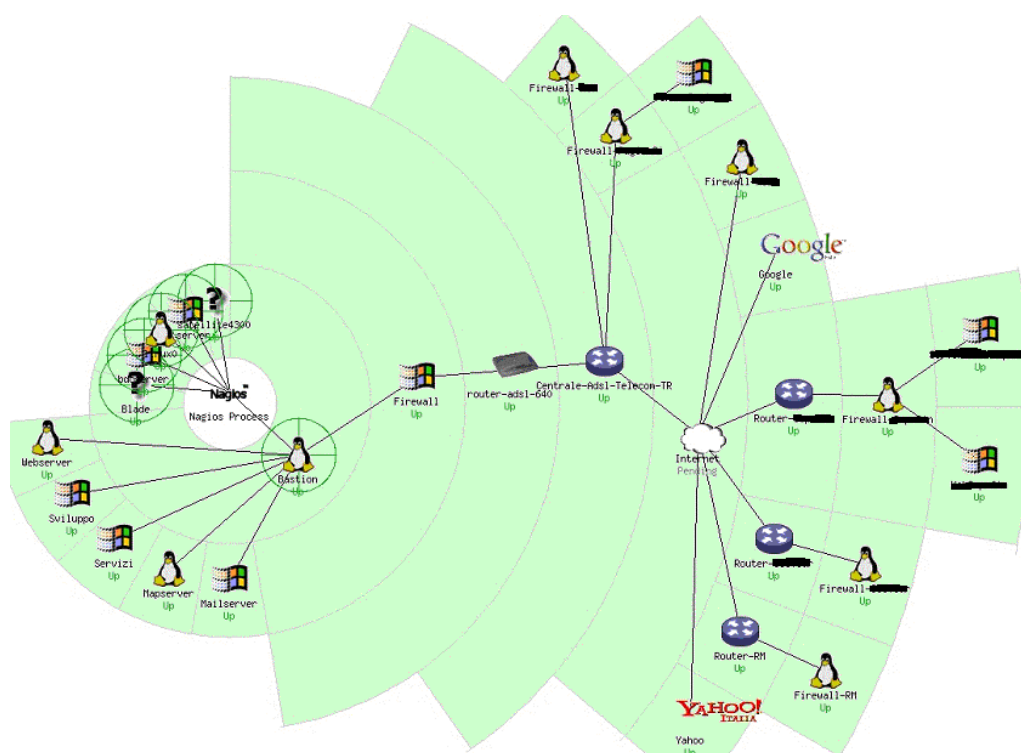
Screenshot



Network Monitoring

Principali caratteristiche.

- * Il sistema di network monitoring è basato su Nagios (www.nagios.org).
- * Definizione di gruppi di host e gerarchie di host.
- * Monitoring dei servizi (ping, ssh, telnet, smtp, pop3, imap, lotus, http, https, generico servizio TCP).
- * Report dei tempi di risposta con generazione delle statistiche di disponibilità dei servizi.
- * Definizione di operatori con relativi scope e tempi di competenza.
- * Alerting degli operatori con email e SMS.
- * Esempio di vista dello stato complessivo del sistema controllato.



Campi di applicazione

- * DigiWall è particolarmente indicato per la protezione di reti aziendali di dimensioni medio/piccole (fino a 100 nodi) dove l'adozione di firewall con caratteristiche superiori non sarebbe giustificata.

Caratteristiche Tecniche

- * Stateful packet filtering
- * Traslazione degli indirizzi (NAT – Network Address Translation) estesa (Source e Destination NAT, portmapping, redirectione dei flussi)
- * HTTP Proxy trasparente (non richiede la configurazione dei client) Squid 2.4

- * DNS masquerading.
- * DHCP service.
- * Backup automatico della configurazione.
- * Generazione automatica dei report di traffico per ogni coppia di indirizzi IP.
- * Generazione automatica dei report di traffico del proxy.
- * Limitazione degli effetti di attacchi DOS², ICMP³, SYN⁴
- * Logging degli eventi e notifica di quelli rilevanti all'amministratore (via email e/o SMS⁵)
- * Sistema operativo Suse Linux 8.1, kernel 2.4.19
- * Amministrazione remota via SSH.
- * Gestione gruppo di continuità (tipo APC Smart-UPS, rileva l'assenza di alimentazione ed eventualmente procede allo shutdown).

Case history

- * Installazione presso la ASL N.4 di Terni. DigiWall è dislocato come bastion host di un firewall CISCO PIX. Sono abilitate le funzionalità di firewall, smart relay host per il dominio asl4.terni.it, proxy trasparente per la rete aziendale (LAN e WAN) (circa 500 nodi).
- * Installazione presso ASM S.p.A. di Terni. DigiWall è dislocato come firewall perimetrale in configurazione ad alta disponibilità (cluster) con funzioni di network monitoring e sms alerting. Sono abilitate le funzionalità di firewall e proxy trasparente per la rete aziendale LAN (circa 100 nodi).
- * Installazione presso PagineSì S.r.l. di Terni. DigiWall è dislocato come firewall perimetrale. I server pubblici sono isolati nella DMZ e l'accesso ad Internet avviene per mezzo di due provider diversi. Il traffico da e per i server pubblici è instradato sulla una rete mentre il traffico da e per la LAN è instradato sull'altra rete.

² Denial Of Service.

³ ICMP flood, Ping of death.

⁴ SYN flood.

⁵ Richiede hardware addizionale e la copertura del campo GSM.