Sistemi firewall

sicurezza reti

ICT Information &
Communication Technology

TiLAK

Firewall sicurezza

In informatica, nell'ambito delle reti di computer, un firewall è un componente passivo di difesa perimetrale di una rete informatica, che può anche svolgere funzioni di collegamento tra due o più tronconi di rete, garantendo dunque una protezione in termini di sicurezza informatica della rete stessa.
Di norma, la rete viene divisa in due sottoreti: una, detta esterna, comprende interamente Internet mentre l'altra interna, detta LAN (Local Area Network), comprende una sezione più o meno grande di un insieme di computer host locali. In alcuni casi è possibile che nasca l'esigenza di creare una terza sottorete detta DMZ (o zona demilitarizzata) adatta a contenere quei sistemi che devono essere isolati dalla rete interna, ma che devono comunque essere protetti dal firewall ed essere raggiungibili dall'esterno (server pubblici).

Definizione e funzionalità

Una prima definizione chiusa di firewall è la seguente: Apparato di rete hardware o software di ingresso-uscita bidirezionale che, opportunamente configurato o settato e agendo in maniera centralizzata, filtra tutti i pacchetti entranti ed uscenti, da e verso una rete o un computer, secondo regole prestabilite che contribuiscono alla sicurezza della stessa.
Un firewall può essere realizzato con un semplice computer (con almeno due schede di rete, una per l'input l'altra per l'output, e software apposito), può essere una funzionalità logica (software) inclusa in un router oppure può essere implementato su un apparato hardware dedicato. Esistono inoltre i cosiddetti "firewall personali", che sono programmi installati sui normali calcolatori client, che filtrano solamente i pacchetti che entrano ed escono da quel calcolatore, utilizzando in tal caso solo una scheda di rete.

Definizione e funzionalità

La funzionalità principale in sostanza è quella di creare un filtro sulle connessioni entranti ed uscenti, innalzando il livello di sicurezza della rete e permettere sia agli utenti interni che a quelli esterni di operare nel massimo della sicurezza. Il firewall infatti agisce sui pacchetti in transito da e per la zona interna potendo eseguire su di essi operazioni di:

controllo;
modifica;
monitoraggio.

"aprendo" in tutti i casi il pacchetto IP e leggendo le informazioni presenti sul suo header, e in alcuni casi anche sul suo contenuto o payload.

Una funzione spesso associata al firewall è quella di NAT (traduzione degli indirizzi di rete), che può contribuire a rendere inaccessibili i calcolatori sulla rete interna mascherandone gli indirizzi IP. Molti firewall possono registrare tutte le operazioni fatte (logging), effettuare registrazioni più o meno selettive (ad esempio, registrare solo i pacchetti che violano una certa regola, non registrare più di N pacchetti al secondo), e tenere statistiche di quali regole sono state più violate. La registrazione integrale dell'attività di un firewall può facilmente assumere dimensioni ingestibili, per cui spesso si usa il logging solo temporaneamente per diagnosticare problemi, o comunque in modo selettivo (logging dei soli pacchetti rifiutati o solo di alcune regole). Tuttavia, l'analisi dei log di un firewall (o anche dei contatori delle varie regole) può permettere di individuare in tempo reale tentativi di intrusione. Talvolta ad un firewall è associata anche la funzione rilevamento delle intrusioni (IDS), un sistema basato su euristiche che analizza il traffico e tenta di riconoscere possibili attacchi alla sicurezza della rete, e può anche scatenare reazioni automatiche da parte del firewall (Intrusion prevention system).

Filtraggio contenuti

Una funzione che alcuni firewall prevedono è la possibilità di filtrare ciò che arriva da Internet sulla base di diversi tipi di criteri non relativi alla sicurezza informatica, ma volti a limitare gli utilizzi della rete sulla base di decisioni politiche, in particolare vietando la connessione su determinate porte o, per quanto riguarda il web, a determinate categorie di siti:

contenuti non adatti ai minori (ad esempio in una rete domestica con postazioni libere non protette individualmente);

contenuti ritenuti non pertinenti con l'attività lavorativa (in una rete aziendale);

contenuti esclusi in base alle informazioni veicolate, su base politica, religiosa o per limitare la diffusione della conoscenza (in questi casi il firewall è uno strumento di censura).

Alcune nazioni arrivano a filtrare tutto il traffico internet proveniente dal proprio territorio nazionale nel tentativo di controllare il flusso di informazioni.
Spesso l'attivazione di questa funzionalità è demandata a software e/o hardware aggiuntivi appartenenti alla categoria dell'URL filtering. Ai firewall viene però richiesto di impedire che gli utenti aggirino tali limitazioni.

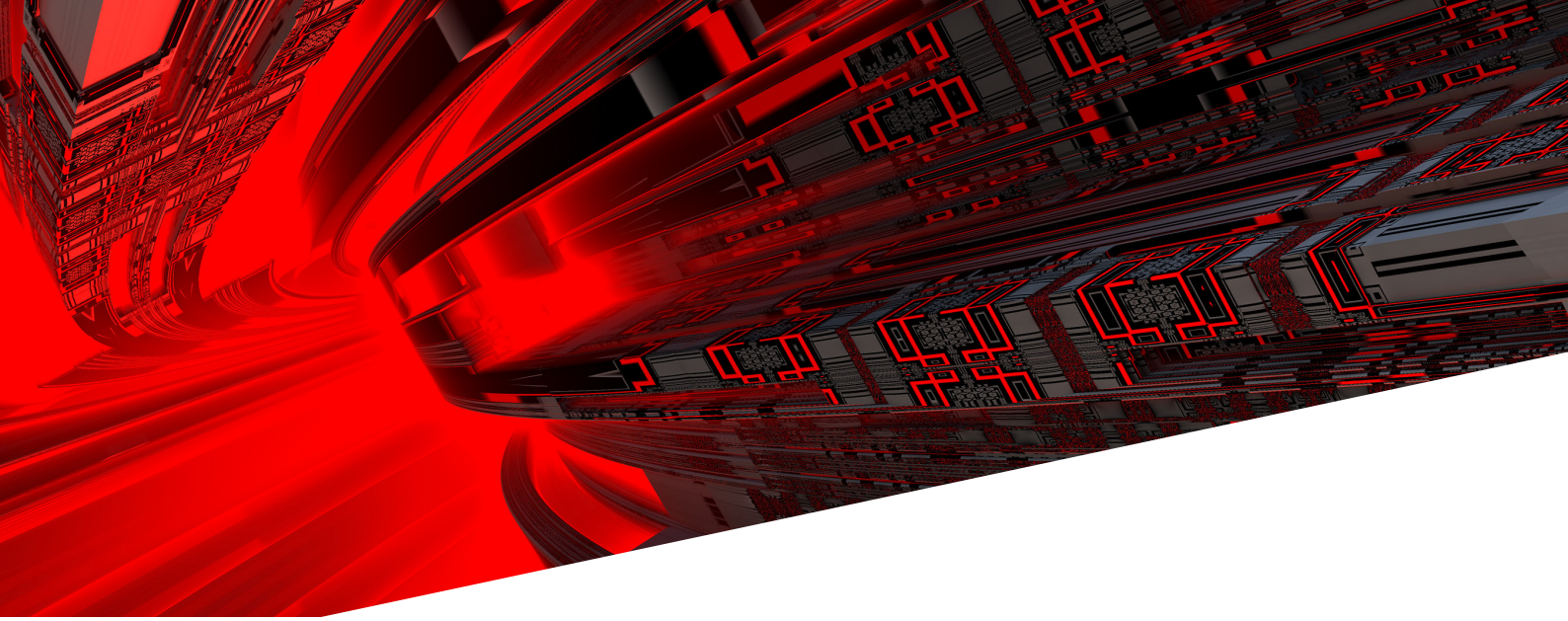
WatchGuard per medie imprese

Scalabilità con progressi hardware:
l'uso degli hardware standard del settore da parte di WatchGuard assicura che le prestazioni del prodotto si adattino ai progressi dei processori Intel e Freescale.

Tecnologia migliore del settore:
l'architettura modulare di WatchGuard è basata sul sistema operativo proprietario Fireware, in grado di eseguire le versioni complete dei maggiori motori di scansione di terze parti. Ciò offre la sicurezza migliore del mercato per ogni fascia di prezzo, insieme alla massima flessibilità per soddisfare un panorama di minacce in continua evoluzione.

Gestibilità della categoria:
La console di gestione basata sulle policy di WatchGuard offre una singola interfaccia per configurare e controllare facilmente tutti i motori di sicurezza, insiema alla flessibilità per gestire la sicurezza di rete da qualunque luogo (per esempio, sede o succursali), senza dover installare ulteriore software di gestione.

Visibilità premiata:
il premiato strumento di visibilità di WatchGuard, Dimension™, trasforma grandi masse di dati sulla sicurezza in tendenze chiave ed eventi critici per identificare rapidamente ed efficacemente minacce potenziali e problematiche di produttività. Operando da qualsiasi cloud pubblico o privato, Dimension non necessità di installazione ed è eseguibile da qualsiasi browser.



Controllo totale

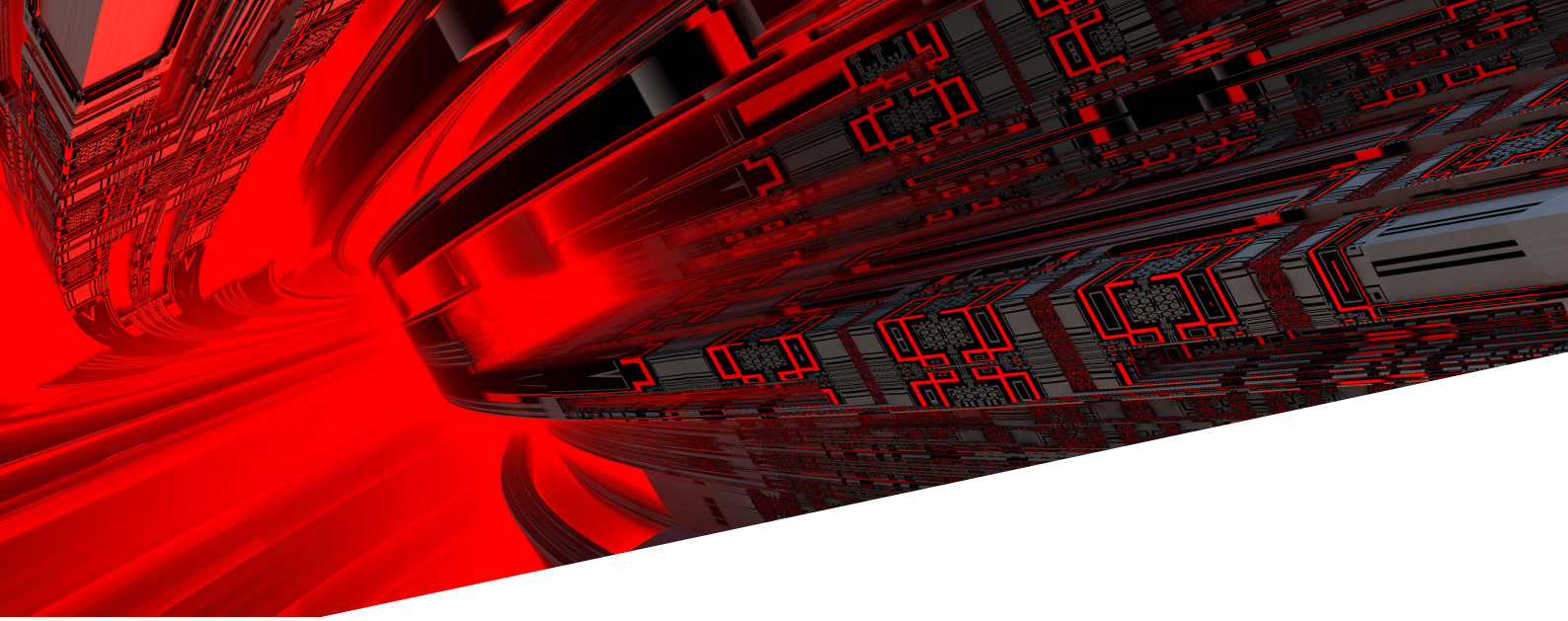
Devi mantenere al sicuro la tua azienda e vuoi farlo dettando le tue condizioni. Noi sappiamo come aiutarti. Puoi posizionare il potente NGFW di WatchGuard ai confini della tua rete e ampliarlo nel corso del tempo, aggiungendo le funzionalità di sicurezza di cui necessiti, quando le necessiti. Otterrai le massime prestazioni e la massima protezione, alle tue condizioni.

Sicurezza implacabile

La gestione unificata delle minacce (Unified Threat Management (UTM)) di WatchGuard è la piattaforma all-in-one per la sicurezza di rete più performante del settore. Ciò significa nessun compromesso. Mai. Si tratta di un'appliance di sicurezza completa, implacabile e velocissima che si adatta alle dimensioni della tua azienda e al tuo budget, facile da distribuire su tutte le reti che devi gestire.

Accesso wireless e sicurezza assoluta

Le minacce alle reti di oggi non sono legate al desktop. E neanche la tua sicurezza può esserlo. WatchGuard estende la sicurezza UTM completa e veloce fino alla WLAN, con una gamma di punti di accesso wireless per l'utilizzo in ambienti interni ed esterni. Inoltre, ti consentiamo di configurare e gestire facilmente tutte le tue reti cablate e da un'unica console intuitiva.



Nessun pericolo nella tua posta

I nostri gateway protetti per le e-mail si ispirano ai nostri peggiori incubi: spam, virus, malware, minacce combinate, spyware, phishing, attacchi di rete - oltre all'estrapolazione dei dati in uscita. Il risultato? E-mail protette per le reti di messaggistica più esigenti, in modo da dormire sonni tranquilli.

Sicurezza reali per minacce virtuali

Guardati intorno: tutto è cambiato. Negli ambienti virtualizzati, dove i flussi di dati tra applicazioni, reparti e aziende attraversano raramente un percorso di rete fisico, l'imposizione perimetrale assume tutto un altro significato. WatchGuard permette di proteggere i 'confini interni' di applicazioni e organizzazioni - dai piccoli uffici alle grandi imprese e ai fornitori di servizi. Virtuali? Certo. Ma la sicurezza è più che reale.

WatchGuard™

cloud service support
sicurezza informatica
hardware **consulenza IT**
networking solutions RF-ID
disaster recovery
backup virtualizzazione
connettività internet posta
business intellinge
WIFI *gestione reti* VMWare
terminali radio frequenza SERVER
cablaggio **documentale**
raccolta dati di produzione

ICT Information &
Communication Technology

TiLAK

TiLAK

ICT Information &Communication Technology

Tilak Srl Unipersonale
25125- Brescia Via Orzinuovi 55
Tel. +39 348 5923187

www.tilak.it
commerciale@tilak.it