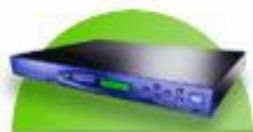


Sicurezza di rete in un apparato all-in-one!

Internet è oggi usata da aziende di qualsiasi dimensione per comunicare e collaborare con i propri partner, clienti e fornitori; grazie alla diffusione di connettività a banda larga di tipo "always-on", il numero e le potenzialità dei servizi a disposizione sono cresciuti enormemente. L'adozione di queste tecnologie aumenta però la vulnerabilità delle aziende a possibili attacchi ed intrusioni dall'esterno, che possono compromettere la sicurezza delle comunicazioni e la confidenzialità dei dati custoditi nei sistemi informativi aziendali.

COSI Internet Gateway® rappresenta la soluzione ideale di sicurezza "all-in-one" per tutte quelle piccole/medie imprese che non hanno grandi risorse da investire in sistemi di sicurezza complessi e costosi pensati e realizzati per ambiti ben più grandi.



Funzionalità

COSI Internet Gateway® racchiude, in un'unica piattaforma hardware/software, tutte le funzionalità di sicurezza necessarie a prevenire efficacemente la maggior parte delle possibili intrusioni attraverso la rete perimetrale:

1. Firewall
2. Traffic shaping
3. Intrusion detection
4. Transparent Proxy service
5. Content filtering

Tutte queste funzionalità possono essere amministrate remotamente tramite una comoda interfaccia Web integrata, che garantisce l'accesso da qualsiasi macchina in rete tramite browser.

Soluzione integrata per una protezione completa e multi-livello

Le funzionalità di firewall e intrusion detection consentono un controllo del traffico di rete, sia a livello TCP sia a livello IP, riuscendo ad intercettare fonti di probabile intrusione e applicando con-

tromisure appropriate come il blocco dei pacchetti sospetti.

Il servizio proxy, configurabile anche in modalità trasparente, oltre a velocizzare la navigazione attraverso le funzionalità di caching, mette a disposizione una vasta gamma di strumenti di content filtering per inibire l'accesso a tutti i siti potenzialmente pericolosi o non in linea con le politiche di navigazione su Internet dell'azienda.

Ogni attacco è diverso dall'altro e, ogni giorno, nuove metodologie d'attacco sono introdotte e scoperte. Per mantenere aggiornato ed efficiente il livello di sicurezza, il servizio di aggiornamento e monitoraggio remoto garantisce che tutte le componenti di sistema siano operative ed efficaci.

Interfaccia centralizzata per amministrazione controllo.

Tutte le funzioni di sicurezza di **COSI Internet Gateway®** possono essere controllate centralmente attraverso una comoda e intuitiva console web.

Dalla console è possibile definire le regole di protezione del firewall, fissare le politiche d'accesso per i vari utenti della rete locale, controllare lo stato del sistema e l'installazione degli eventuali upgrade disponibili oltre che compiere tutte le attività di configurazione di base del sistema.

Oltre a questo, la console dà accesso ad un sistema di monitoraggio e logging completo e configurabile che consente di controllare in modo semplice ed efficace tutte le attività della rete.

Servizi e supporto

Il mondo della sicurezza delle reti è in continua evoluzione; allo stesso modo, una soluzione di sicurezza integrata deve essere costantemente aggiornata e mantenuta.

A questo fine, COSI offre un servizio di supporto tecnico ed assistenza remota per tutte le funzioni di sicurezza, garantendo che il grado di sicurezza della vostra rete rimanga sempre elevato.

Per aggiungere valore alla soluzione, **COSI Internet Gateway®** include il supporto tecnico e l'assistenza remota per il primo anno.

Servizi	<ul style="list-style-type: none"> • Filtering Firewall - Controllo del traffico a livello di pacchetto. Regole di filtro definibili su indirizzi IP, porte TCP, tipologia di pacchetto applicabili su ogni singolo pacchetto. Possibilità di suddividere la rete in zone logiche (fino a 4), ognuna contenente sistemi con differenti caratteristiche d'accesso alle risorse di rete. • NAT - Attraverso il sistema firewall è possibile usufruire delle funzionalità di Network Address Translation (NAT). Tramite NAT, le varie postazioni sulla rete interna possono usufruire in modo controllato dei servizi Internet utilizzando un unico indirizzo IP pubblico. Le regole NAT sono definibili sulla base di IP, range di IP, e porte specifiche. • Intrusion Detection - Questo servizio analizza i pacchetti che transitano sulla rete e ne interpreta il contenuto, basandosi su set di regole configurabili, intercettando tutti quei flussi di dati "sospetti" che possono far parte di un attacco verso la rete. Il sistema è in grado di intercettare vari tipi di attacchi: Port-Scanning, DOS (Denial Of Service) e DDOS, SYN-Flood, ecc.. Inoltre, grazie a particolari set di regole, è anche in grado di intercettare il transito di alcune tipologie di virus e worm, indipendentemente dal protocollo usato per veicolarli. La possibilità di aggiornare le regole garantisce l'efficienza del sistema nel tempo. • Port Mapping/redirection - Utilizzando il port-mapping è possibile offrire servizi su Internet, distribuendoli su più server, anche con un singolo IP pubblico. Con questa funzionalità è, infatti, possibile re-dirigere il traffico diretto verso un particolare porta TCP verso la corrispondente porta TCP di una macchina nella rete interna. • Traffic shaping - Il sistema è in grado di controllare e limitare la banda utilizzata per ogni singola connessione TCP in modo dinamico. E' possibile assegnare un limite di banda ad un singolo IP, ad un range di IP o, anche, ad un protocollo specifico in ingresso o in uscita. • Proxy server - Tramite il caching dei contenuti Web, consente di velocizzare la navigazione dei siti visitati più frequentemente, riducendo anche l'occupazione di banda. Attraverso liste di controllo d'accesso configurabili, è possibile dare accesso ai vari utenti in modo molto flessibile. • Transparent Proxy - Utilizzare un proxy server significa riconfigurare i browser degli utenti in modo appropriato, cosa che richiede tempo. Con il proxy server fornito è possibile evitare questa attività: il sistema può, infatti, essere attivato in modalità trasparente. In questo caso, ogni richiesta http proveniente da qualsiasi macchina verrà re-diretta incondizionatamente al proxy senza la necessità di operare modifiche sulle macchine degli utenti. • Content Filtering - Un'altra attività importante svolta dal proxy è quella di content filtering. Il sistema analizza le richieste di navigazione e, basandosi su un database aggiornato periodicamente, decide se consentire l'accesso al sito richiesto. In questo modo, è possibile escludere dalla navigazione i siti con contenuti impropri, o potenzialmente pericolosi.
Funzionalità	<ul style="list-style-type: none"> • Web Administration - L'interfaccia di configurazione del sistema è costituita da una comoda interfaccia Web. Tutte le principali opzioni di configurazione sono raggiungibili da qualsiasi macchina in rete locale attraverso un comune web browser. Un'unica interfaccia con diversi livelli di dettaglio permette, sia ai meno esperti, sia al personale con esperienza, di trovare tutto ciò che serve per avviare ed ottimizzare ogni funzionalità del sistema. Per mantenere un elevato standard di sicurezza, la comunicazione fra sistema e browser avviene attraverso il protocollo https. • Secure Shell (SSH) Support - Per l'utenza più esigente è disponibile un accesso console al sistema attraverso una connessione criptata e sicura, che evita la possibilità che informazioni sensibili, come password e nomi utenti siano intercettate durante il passaggio sulla rete. Questa funzionalità rende ragionevolmente sicura anche l'amministrazione remota del sistema. • Activity log - Attraverso le interfacce di amministrazione si può accedere ad un completo sistema di log che tiene traccia di tutte le attività svolte dal sistema. • Alert agent - Gli eventi generati da un sistema di sicurezza sono, il più delle volte, asincroni: per questo motivo è stato creato un apposito agente software che si preoccupa di comunicare all'amministratore il verificarsi di particolari eventi che vanno dal rilevamento di possibili intrusioni all'avvenuto aggiornamento del sistema. • Remote update - Un apparato di sicurezza è un sistema fortemente dinamico. Le sue caratteristiche devono poter evolvere al presentarsi di nuove problematiche e tipologie d'attacco. Per questo è stato integrato nel sistema un servizio d'aggiornamento remoto automatico che, ad intervalli regolari, controlla la presenza di pacchetti d'aggiornamento, liberando l'amministratore da quest'attività che, se eseguita manualmente, richiederebbe parecchio tempo.