

SOLUZIONE PER NEXT GENERATION FIREWALL

La diffusione dell'uso di applicazioni Web 2.0 (applicazioni con un'elevata interazione sito-utente quali, blog, peer-to-peer, social network, ecc) e delle SaaS (Software as a Service) accentua la problematica di avere una piena visibilità delle applicazioni che transitano nella rete aziendale.

I classici strumenti di difesa in questo scenario denotano limiti sia in efficacia che efficienza.

l'esigenza

Queste le principali esigenze che emergono rispetto a questo tema:

- **Definire politiche di autorizzazione per Utente/Gruppo** oltre per indirizzo IP.
- Controllare le applicazioni che transitano attraverso il firewall anche su protocollo criptato https (es. applicazione Web 2.0 come blog, peer-to-peer, VoIP, social network, ecc.).
- Soddisfare requisiti di **Compliance**, analizzando le applicazioni utilizzate, per utente, e definendo regole che in base alle policy di riferimento.
- Definire politiche di **URL filtering** sul traffico passante per prevenire la frequentazione di siti vettori di minacce o non conformi alle politiche aziendali.
- Mantenere alto il livello di protezione dalle vulnerabilità (**Intrusion Prevention System**) e dal codice malevole (**Antivirus/Antispyware**).

la soluzione

Si propone un cambiamento radicale dell'approccio alla gestione della sicurezza perimetrale, **spostando il focus della definizione delle regole di autorizzazione nei firewall dal binomio Indirizzo-IP/Protocollo al binomio Utente/ Applicazione**.

Queste le principali caratteristiche:

- funzionalità standard firewall (policy enforcement, statefull inspection, packet filtering, NAT, VPN client-to-site e site-to-site);
- funzionalità Intrusion Prevention (IPS) per il blocco delle minacce;
- riconoscimento applicativo e visibilità su tutto lo "stack" al fine di controllare le applicazioni che transitano attraverso il firewall;

- raccolta delle informazioni esterne all'infrastruttura firewall per aumentare l'efficacia decisionale
- supporto per l'inserimento dei firewall in modo trasparente (in gergo: bump-in-the-wire) per non impattare sull'operatività della rete;

i vantaggi

La soluzione in cui un unico apparato accorpa funzionalità di

- firewall;
 - concentratore VPN;
 - gestione della banda (quality of services - QoS);
 - protezione dalle vulnerabilità (IPS) o da malware (Antivirus/Antispyware);
 - analisi dei contenuti in generale (File blocking; Data filtering) controllo della navigazione (URL filtering)
 - pieno controllo delle applicazioni, analizzate anche su traffico cifrato SSL (non solo le "porte aperte", ma anche tipologia di traffico che passa all'interno di tali porte),
- contribuisce significativamente ad una **riduzione di costi e di risorse impiegate** ma anche al **raggiungimento ed al mantenimento dello stato di Compliance a normative e Security Policy**.

Inoltre la visibilità che la soluzione offre su ciò che accade nella rete in tempo reale, grazie a reportistica e analisi forense, permette una visibilità di livello superiore rispetto ai firewall tradizionali.

Inoltre, è progettata per ridurre al minimo gli impatti di nuovi componenti applicativi sull'operatività della rete e dei sistemi di sicurezza perimetrale esistenti.

About IKS

IKS, nata alla fine degli anni novanta focalizzando il proprio agire sui principali temi dell'Information e Communication Technology, è in grado di fornire servizi e soluzioni utili a migliorare i processi aziendali, con competenza e approccio innovativi. IKS può vantare tra i propri Clienti le principali aziende del panorama nazionale.

Alcune idee maturate nel corso di esperienze reali sono diventate "soluzioni a valore" che permettono di proporsi sul mercato in modo esclusivo.

www.iks.it
informazioni@iks.it
+39 049.8701010

padova
corso Stati Uniti, 14 bis - 35127



appassionati all'eccellenza