5 Suggerimenti per la scelta di un firewall di nuova generazione

Investi in un Next-Generation Firewall (NGFW) incentrato sulle minacce. Chiedi se può offrirti...

1 Difesa integrata dalle minacce

Protezione interattiva su più livelli.

Le minacce multivettoriali e persistenti si insinuano nelle falle dei sistemi di protezione ed eludono il rilevamento. Un NGFW incentrato sulle minacce offre le più avanzate tecnologie per la sicurezza che interagiscono tra loro su tutta la rete e endpoint e vengono gestite mediante una console centralizzata. Basate su un'infrastruttura di firewall stateful completa, le tecnologie NGFW incentrate sulle minacce devono includere:

- IPS di nuova generazione
- Advanced Malware Protection
- Application Visibility and Control
- Filtro URL basato sulla reputazione
- VPN a livello di applicazioni

▸ Grazie alla protezione integrata dalle minacce e dal malware avanzato che effettua costantemente correlazioni delle informazioni su tutti i livelli di sicurezza, vengono identificati gli attacchi più sofisticati e ci si può proteggere.

Risorse

Next-Generation Firewall: guida all'investimento

Ottieni l'elenco completo delle caratteristiche necessarie per proteggere la tua azienda dagli attacchi in questo white paper.
Leggi.

Maggiore visibilità, maggiore protezione

Scopri un approccio innovativo per la difesa dalle minacce che offre la protezione continua.
Guarda il video.

Sito Web di Cisco NGFW

Rimani aggiornato sulle ultime tendenze e scopri le novità per la sicurezza di Cisco.
Ulteriori informazioni.

2 Indicatori di compromissione interattivi

Rilevamento più rapido del malware per ridurre i rischi.

L'attuale tempistica standard del settore per il rilevamento di una minaccia varia tra i 100 e i 200 giorni, un periodo di tempo decisamente troppo lungo. Un NGFW deve fornire indicatori di compromissione (IoC) interattivi in grado di:

- Correlare le informazioni sulla sicurezza a livello di rete con quella degli endpoint
- Fornire visibilità estremamente accurata sul comportamento di file e host dannosi e sospetti
- Assegnare priorità agli host infetti per una rapida risoluzione dei problemi

▸ Gli IoC interattivi consentono di visualizzare l'attività del malware su host ed endpoint, comprenderne l'impatto e intervenire rapidamente con azioni di contenimento e correzione.

3 Visibilità complessiva della rete

Più efficacia della sicurezza con una panoramica olistica.

È impossibile proteggere ciò che non si vede. È necessario monitorare costantemente quello che accade nella rete. Un NGFW deve fornire un'analisi completa del contesto di numerosi fattori:

- Utenti, sistemi operativi e dispositivi
- Comunicazioni tra macchine virtuali
- Minacce e vulnerabilità
- Applicazioni e accessi ai siti Web
- Trasferimenti di file e altro ancora

▸ Questo livello di dettaglio delle informazioni aiuta a identificare e correggere le carenze di sicurezza, nonché di ottimizzare le policy per ridurre il numero di eventi significativi che richiedono ulteriori azioni.

4 Meno complessità e meno costi

Livelli di sicurezza unificati e automazione per migliorare l'efficienza.

La combinazione di minacce avanzate e carenza di esperti della sicurezza IT intensifica le pressioni sui reparti IT. La soluzione NGFW ideale deve essere in grado di:

- Consolidare più livelli di difesa in un'unica piattaforma
- Offrire una sicurezza elevata e coerente su vasta scala
- Automatizzare le attività di sicurezza di routine come la valutazione dell'impatto, l'ottimizzazione delle policy e l'identificazione degli

▸ Grazie alla riduzione di complessità e costi il tuo team potrà concentrarsi sugli eventi più importanti.

5 Integrazione con soluzioni di terze parti

Ottimizzazione degli investimenti esistenti nella sicurezza

È necessario condividere le informazioni e sfruttare al meglio le tecnologie di sicurezza esistenti per consolidare e semplificare la risposta. La soluzione NGFW ideale deve essere aperta e perfettamente integrabile in un ecosistema di soluzioni di sicurezza di terze parti tra cui:

- Sistemi di gestione delle vulnerabilità
- Sistemi SIEM e di visualizzazione della rete
- Sistemi di correzione del flusso di lavoro e creazione di ticket
- Sistemi di controllo dell'accesso alla rete (NAC) e altro ancora

▸ L'integrazione di soluzioni di terze parti riduce il carico di lavoro per l'IT e il TCO, rafforzando la protezione su più livelli.

Gli attacchi continueranno ad evolversi parallelamente all'ambiente IT che devi proteggere. Assicurati di scegliere un NGFW che offra funzioni di **protezione dalle minacce perfettamente integrata e su più livelli**. Grazie alla condivisione di contesto e informazioni tra le funzioni di sicurezza, puoi accelerare il processo di rilevamento e risposta alle minacce in tutta l'azienda e sfruttare al massimo gli investimenti.

Non è quello che facciamo, ma ciò che rendiamo possibile.

Trasformare in realtà il concetto di Security Everywhere.

Visita la pagina www.cisco.com/go/ngfw

Seguici su Twitter @CiscoSecurity