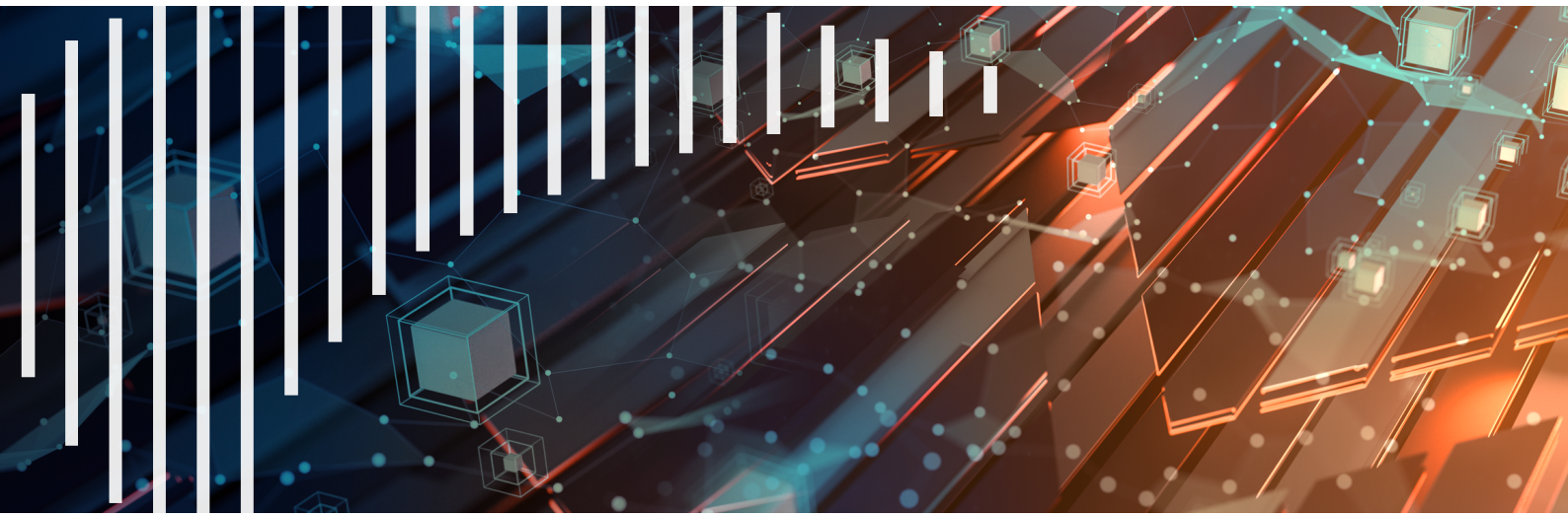


Cosa deve offrire un firewall cloud di nuova generazione

Le migliori pratiche per proteggere ambienti cloud pubblici e privati

SINTESI

Per trarre il maggior vantaggio dalle nuove tecnologie di cloud computing, i responsabili IT devono attuare la migrazione in cloud dei processi di calcolo, connettività di rete, storage e sicurezza in modo sistematico. La scelta di un firewall cloud di nuova generazione adeguato ed efficace richiede un nuovo approccio. Questo documento esamina i temi seguenti:

- *funzionalità essenziali*
- *requisiti chiave di una soluzione*
- *caratteristiche consigliate*

Introduzione

Con tecnologie informatiche e processi aziendali sempre più interdipendenti, i dirigenti aziendali si aspettano che l'IT tenga il passo con le innovazioni tecnologiche e modernizzi la gestione dei data center e i servizi per consentire all'organizzazione di crescere.

Per fare questo, l'IT deve adottare l'attuale trasformazione digitale verso il cloud, con cui le aziende trasferiscono le attività della propria infrastruttura e i carichi di lavoro delle applicazioni nel cloud. Ciò significa attuare una migrazione sistematica delle risorse di calcolo, connettività di rete, archiviazione e sicurezza nel cloud. Queste componenti devono essere strettamente integrate per fornire servizi per le applicazioni in modo sicuro, efficiente e scalabile.

L'approccio ottimale

Per affrontare le sfide di sicurezza relative agli ambienti cloud pubblici/privati, un approccio ottimale consisterebbe nel progettare, implementare e utilizzare un firewall cloud che disponga di cinque capacità fondamentali:

1. Fornire visibilità completa sulle comunicazioni tra i carichi di lavoro in cloud per prevenire le minacce.
2. Garantire la corretta applicazione delle policy di sicurezza per le applicazioni nell'intero ambiente cloud.
3. Offrire policy per l'abilitazione sicura delle applicazioni in base ad applicativo, utente e contenuto, indipendentemente dalla loro posizione.
4. Implementare un'adeguata ripartizione in zone (ad es. VLAN) e isolamento/segmentazione della sicurezza.
5. Estendere l'efficacia delle policy di sicurezza con regole contestuali e monitoraggio automatizzato.

Quando si applica un modello di data center definito dal software (SDDC), le best practice suggeriscono di utilizzare un firewall cloud di nuova generazione, che dovrebbe offrire strumenti e servizi di sicurezza avanzati per proteggere l'intero ambiente cloud pubblico e privato.

SOLUTION BRIEF

Requisiti chiave consigliati per un firewall cloud di nuova generazione

Un firewall cloud di nuova generazione deve offrire tutti i vantaggi di sicurezza di un firewall fisico combinati ai vantaggi operativi ed economici di una soluzione cloud, tra cui scalabilità e agilità del sistema, velocità di provisioning dei sistemi, semplicità di gestione e riduzione dei costi.

La soluzione ottimale sarebbe un servizio firewall completo in grado di svolgere l'ispezione approfondita dei pacchetti, controlli di sicurezza e servizi di connettività di rete analogamente a un firewall fisico. Il firewall cloud deve analizzare il traffico tra i carichi di lavoro in cloud per prevenire le violazioni in modo automatico e implementare misure di controllo degli accessi per garantire la riservatezza, la sicurezza e l'integrità dei dati.

In sostanza, dovrebbe proteggere efficacemente tutti i componenti critici degli ambienti cloud privati/pubblici da attacchi che implicano un uso illecito delle risorse, attacchi tra macchine virtuali o di tipo side-channel, comuni intrusioni via rete e vulnerabilità delle applicazioni e dei protocolli. È inoltre consigliata un'infrastruttura che supporti l'implementazione dell'alta disponibilità (HA) per i firewall. In tal modo è possibile soddisfare i requisiti di scalabilità e disponibilità dei data center SDDC garantendo la resilienza dei sistemi, tempi di operatività adeguati, tempi di attività e fornitura dei servizi nonché il rispetto dei requisiti normativi.

È consigliabile una soluzione firewall cloud ottimizzata per un'ampia gamma di casi d'implementazione virtualizzati e in cloud pubblici/privati. Un moderno firewall cloud dovrebbe essere in grado di garantire la sicurezza dei carichi di lavoro nel cloud e l'accesso continuo ai server di applicazioni e database. A tale scopo occorrono prestazioni di vari gigabit al secondo per la prevenzione delle minacce e, laddove necessario, per l'ispezione del traffico crittografato.

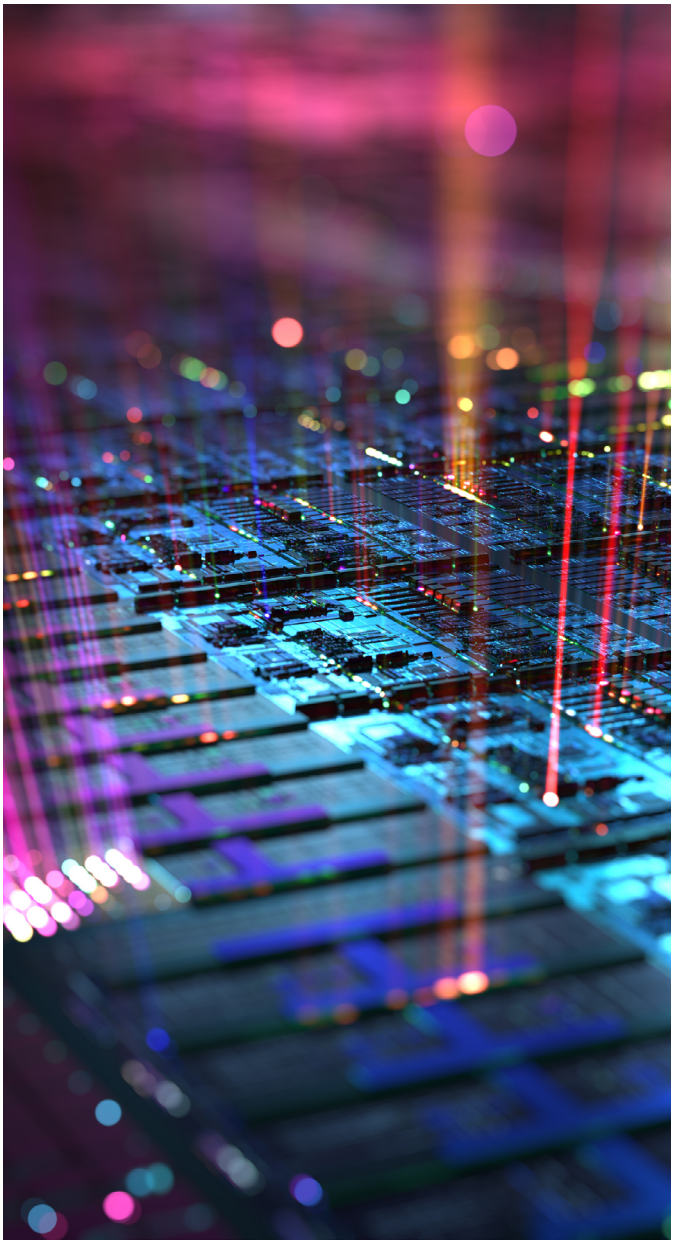
La soluzione ideale sarebbe quella di gestire centralmente i firewall cloud in loco o tramite una piattaforma di gestione della sicurezza aperta, scalabile e basata sul cloud, disponibile come software-as-a-service (SaaS) conveniente. Questa soluzione fornirebbe visibilità, agilità e la capacità di governare l'intero ecosistema di firewall fisici e cloud, offrendo maggiore chiarezza, precisione e velocità – meglio ancora se da un unico pannello di controllo.

Per garantire la massima efficacia, le policy per gateway antivirus, anti-spyware, filtraggio dei contenuti, prevenzione delle intrusioni, filtraggio degli IP in base all'area geografica e ispezione approfondita del traffico crittografato dovrebbero essere disponibili in un formato facilmente comprensibile e fruibile.

Best practice da prendere in considerazione

Per la scelta di una soluzione firewall cloud di nuova generazione è opportuno cercare le seguenti caratteristiche.

1. **Prevenzione automatica delle violazioni**
   Protezione completa contro le minacce avanzate, inclusa la prevenzione di intrusioni e malware ad alte prestazioni e una sandbox basata sul cloud.
2. **Comunicazioni sicure**
   Lo scambio di dati tra gruppi di macchine virtuali deve avvenire in completa sicurezza tramite funzioni di isolamento, riservatezza, integrità e controllo dei flussi di informazioni all'interno di queste reti tramite l'uso della segmentazione.
3. **Controllo degli accessi**
   Garanzia che solo i carichi di lavoro che soddisfano determinate condizioni possano accedere tramite VLAN ai dati appartenenti ad altri carichi di lavoro.
4. **Autenticazione degli utenti**
   Creazione di policy specifiche per controllare o limitare l'accesso ai carichi di lavoro da parte di utenti non autorizzati.
5. **Riservatezza dei dati**
   Blocco del furto di informazioni e dell'accesso illecito a dati e servizi protetti.
6. **Resilienza e disponibilità delle applicazioni cloud**
   Prevenzione di interruzioni o di degrado delle comunicazioni e dei servizi per le applicazioni.
7. **Sicurezza e integrità dei sistemi**
   La soluzione deve impedire che terzi non autorizzati assumano il controllo dei sistemi e dei servizi.
8. **Meccanismi di convalida, monitoraggio e ispezione del traffico**
   Rilevamento di irregolarità e comportamenti malevoli e blocco di attacchi rivolti ai carichi di lavoro.
9. **Opzioni di implementazione**
   Capacità di implementazione in un'ampia varietà di piattaforme cloud e virtualizzate per diversi scenari di sicurezza in cloud pubblici/privati.
10. **Esperienza d'uso semplificata**
    Riduzione degli errori di configurazione e dei tempi d'installazione, a tutto vantaggio della sicurezza generale.



Conclusioni

Le organizzazioni adottano in misura crescente la migrazione al cloud per compensare i costi operativi e ottenere scalabilità e flessibilità. Il panorama IT attuale necessita di firewall cloud che siano potenti come quelli fisici e in grado di soddisfare le esigenze di sicurezza e le sfide di un ambiente cloud.

Per maggiori informazioni sui firewall virtuali di SonicWall, contattate subito il vostro rappresentante SonicWall o fate clic qui.

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative per la nuova normalità iperdistribuita, in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibili economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni visitare www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

© 2023 SonicWall Inc. TUTTI I DIRITTI RISERVATI.
SonicWall è un marchio o marchio registrato di SonicWall Inc. e/o delle sue affiliate negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi e marchi registrati appartengono ai rispettivi proprietari. Le informazioni contenute nel presente documento si riferiscono ai prodotti di SonicWall Inc. e/o delle sue affiliate. Né il presente documento né la vendita di prodotti SonicWall costituiscono alcuna licenza, espressa o implicita, di estoppel o di altro tipo, né garantiscono diritti di proprietà intellettuale. Salvo quanto specificato nei termini e nelle condizioni stabiliti nel contratto di licenza di questo prodotto, SonicWall e/o le sue affiliate non si assumono alcuna responsabilità ed escludono garanzie di qualsiasi tipo, esplicite, implicite o legali, in relazione ai propri prodotti, incluse, in via esemplificativa, qualsiasi garanzia implicita di commerciabilità, idoneità a scopi specifici o violazione di diritti altrui. SonicWall e/o le sue affiliate declinano ogni responsabilità per danni di qualunque tipo, siano essi diretti, indiretti, consequenziali, punitivi, speciali o incidentali (inclusi, senza limitazioni, danni per mancato guadagno, interruzioni dell'attività o perdite di dati) derivanti dall'utilizzo o dall'impossibilità di utilizzare il presente documento, anche nel caso in cui SonicWall e/o le sue affiliate siano state avvertite dell'eventualità di tali danni. SonicWall e/o le sue affiliate non rilasciano alcuna garanzia o dichiarazione relativamente alla precisione o completezza dei contenuti del presente documento e si riservano il diritto di apportare modifiche, in qualsiasi momento e senza preavviso, alle specifiche e alle descrizioni dei prodotti. SonicWall Inc. e/o le sue affiliate non si assumono alcun impegno di aggiornare le informazioni contenute in questo documento.