What to Look For in a Next-Gen Cloud Firewall

Best practices for securing your public/private cloud environments.

ABSTRACT

To best capitalize on the latest cloud computing trends, IT must operationalize the cloud migration of computing, networking, storage and security in a systematic way. A new approach is required to select an appropriate and effective next-generation cloud firewall solution. This brief explores:

- *Fundamental capabilities*
- *Core solution requirements*
- *Best-practice feature sets*

Introduction

With information technologies and business processes becoming tightly interdependent, business stakeholders expect IT to keep pace with technology innovations and modernize data center operations and services to position the organization for growth.

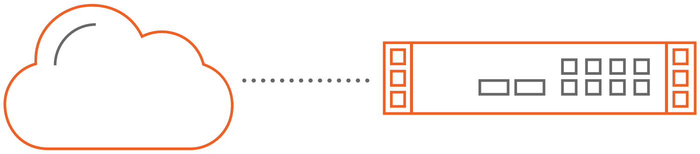
To succeed, IT must embrace today's digital transformation to the cloud, where organizations are moving their infrastructure operations and application workloads are moving to the cloud. This means that the cloud migration of computing, networking, storage and security must be operationalized in a systematic way. These components must be tightly integrated to deliver application services safely, efficiently and in a scalable manner.

A Sound Approach

To address the security challenges facing public/private cloud environments, a sound approach would be to design, implement and deploy a cloud firewall that enables five fundamental capabilities:

1. Gain complete visibility into communication between cloud workloads for threat prevention.
2. Ensure the appropriate placement of security policies for the application throughout the cloud environment.
3. Deliver safe application enablement policies by application, user and content, regardless of location.
4. Implement proper security zoning (i.e., VLANs) and isolation/segmentation.
5. Extend the effectiveness of security policies with contextual-based rules and automated monitoring.

When applying a software-defined data center model (SDDC), best practices suggest deployment of a next-generation cloud firewall. The firewall should leverage advanced security tools and services that protect the entire private and public cloud environment.



SOLUTION BRIEF

Core Requirement Recommendations for Next-generation Cloud Firewall

A next-generation cloud firewall must offer all the security advantages of a physical firewall, along with the operational and economic benefits of the cloud. These include system scalability and agility, speed of system provisioning, simple management, and cost reduction.

Optimally, it should consist of a full-featured firewall service capable of performing deep packet inspection, security controls and networking services equivalent to a physical firewall. The cloud firewall must capture between cloud workloads for automated breach prevention and establish access control measures for data confidentiality safety and integrity.

Bottom line, it should effectively shield all critical components of the private/public cloud environments from resource misuse attacks, cross-virtual-machine attacks, side-channel attacks, common network-based intrusions, and application and protocol vulnerabilities. Infrastructure support for firewall high availability (HA) implementation is also recommended. This fulfills SDDC scalability and availability requirements by ensuring system resiliency, operational uptime, service delivery and uptime, and conformance to regulatory requirements.

Look for cloud firewall solutions that are optimized for a broad range of public/private cloud/virtualized deployment use cases. A modern cloud firewall should be able to ensure cloud workloads' safety while making sure application and database servers are accessible at all times. To do so, it should have multi-Gbps performance for threat prevention and encrypted traffic inspection where necessary.

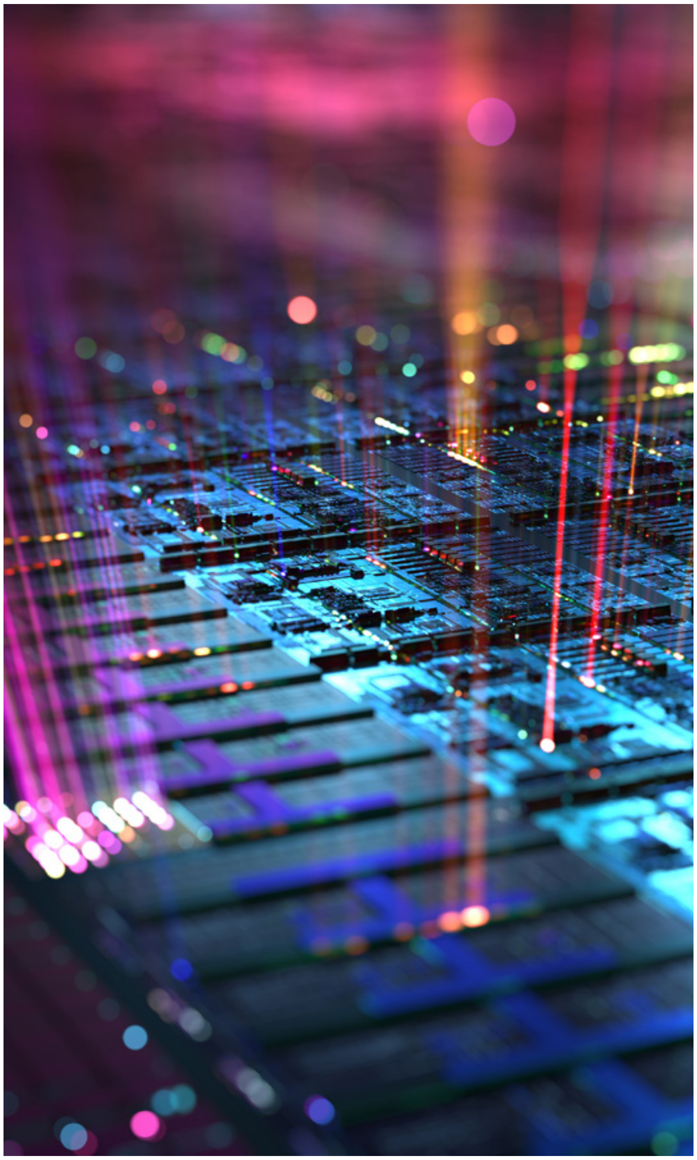
Ideally, cloud firewall deployments could be centrally managed on-prem or via an open, scalable cloud-based security management platform that is delivered as a cost-effective software-as-a-service (SaaS). This would provide the visibility, agility and capacity to govern the entire cloud and physical firewall ecosystem with greater clarity, precision and speed – optimally from a single pane of glass.

The policy effectiveness for gateway antivirus, antispyware, content filtering, intrusion prevention, geo-IP filtering and deep-packet inspection of encrypted traffic should be presented in a format that is easy to understand and actionable.

Best-practice Capabilities to Consider

When selecting your next-generation cloud firewall solution, look for the following feature-set capabilities.

1. **Automated breach prevention**
   Deliver complete advanced threat protection, including high-performance intrusion and malware prevention and cloud-based sandboxing.
2. **Secure communications**
   Ensure data exchange between groups of virtual machines are done securely including isolation, confidentiality, integrity and information flow control within these networks via the use of segmentation.
3. **Access control**
   Validate that only workloads that satisfy a given set of conditions are able to access data that belongs to other workloads using VLANs.
4. **User authentication**
   Create policies to control or restrict workload access by unauthorized users.
5. **Data confidentiality**
   Block information theft and illegitimate access to protected data and services.
6. **Cloud application resilience and availability**
   Prevent disruption or degradation of application services and communications.
7. **System safety and integrity**
   Stop unauthorized takeover of systems and services.
8. **Traffic validation, inspection and monitoring mechanisms**
   Detect irregularities and malicious behaviors and stop attacks targeting workloads.
9. **Deployment options**
   Deploy on a wide variety of virtualized and cloud platforms for various private/public cloud security use cases.
10. **Deliver a streamlined user experience**
    Reduce configuration errors and deployment time for a better overall security posture.



Conclusion

Organizations are increasingly embracing cloud migration to offset operational overhead and enable business flexibility and scalability. Today's IT requires cloud firewall solutions that are just as robust as physical firewalls while accommodating the security needs and challenges of the cloud environment.

To learn more about SonicWall Virtual Firewalls, contact your SonicWall representative today or click here.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com