SONICWALL®

SOLUTION BRIEF: WHAT TO LOOK FOR IN A NEXT-GEN VIRTUAL FIREWALL

Best practices for securing your public/private cloud environments

Abstract

To best capitalize on virtualization trends, IT must operationalize the complete virtualization of computing, networking, storage and security in a systematic way. A new approach is required to select an appropriate and effective next-generation virtual 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 application-centric, virtualized world, where data centers are virtualizing their infrastructure operations and application workloads. This means that the complete virtualization 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 virtual firewall that enables four fundamental capabilities:

1. Gain complete visibility into intra-host communication between virtual machines for threat prevention.
2. Ensure the appropriate placement of security policies for the application throughout the virtual environment.
3. Deliver safe application enablement policies by application, user and content, regardless of VM location.
4. Implement proper security zoning (i.e., VLANs) and isolation/segmentation.

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

Core requirement recommendations for next-generation virtual firewall

A next-generation virtual firewall must offer all the security advantages of a physical firewall, along with the operational and economic benefits of virtualization. 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. It should be strategically placed on the virtual network (VN), typically between VNs in multi-tenant ecosystem. The virtual firewall must capture virtual traffic between VNs for automated breach prevention, and establish access control measures for data confidentiality and VMs' 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 virtual 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 virtual firewall solutions that are optimized for broad range of public/private cloud/virtualized deployment use cases. A modern virtual firewall should be able to adapt to service-level increases, and ensure VNs safety and application workloads and data assets are available, as well as secure. To do so, it should have multi-Gbps performance for threat prevention and encrypted traffic inspection where necessary.

Ideally, virtual firewall deployments could be centrally managed using both 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 ultimate in visibility, agility and capacity to govern the entire virtual and physical firewall ecosystem with greater clarity, precision, and speed – optimally from a single pane of glass.

Best-practice capabilities to consider

When selecting your next-generation virtual 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 VMs that satisfy a given set of conditions are able to access data that belongs to another VM, using VLANs.
4. **User authentication**
   Create policies to control or restrict VM and workload access by unauthorized users.
5. **Data confidentiality**
   Block information theft and illegitimate access to protected data and services.
6. **Virtual application resilience and availability**
   Prevent disruption or degradation of application services and communications.
7. **System safety and integrity**
   Stop unauthorized takeover of VM systems and services.
8. **Traffic validation, inspection and monitoring mechanisms**
   Detect irregularities and malicious behaviors, and stop attacks targeting VM workloads.
9. **Deployment options**
   Deploy on a wide variety of virtualized and cloud platforms for various private/public cloud security use cases.

Conclusion

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

Learn more about SonicWall Virtual Firewall and SonicWall Web Application Firewall solutions.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com