ANALYST BRIEF

Sponsored by: Zscaler

Cloud firewalls are the future, but legacy hurdles remain. Practical, real-world, and artificial limitations can be overcome to achieve a modern enterprise security posture.

Why True Security Transformation Requires Cloud Firewalls

September 2022

Written by: Christopher Rodriguez, Research Director, Security and Trust

AT A GLANCE

KEY STATS

According to IDC research:

- 41.6% of organizations invested in "modernized cybersecurity infrastructure" to improve organizational trust in 2021.
- 38.7% of organizations invested in "automating IT security management" in 2021.
- When asked to identify which IT infrastructure delivery models their organization is using/planning to use for security in the short term, 52.5% of survey respondents chose either mostly or entirely cloud, hosted, and SaaS security. Only 15.8% identified the delivery model as mostly or entirely on premises.

Introduction

The move to the cloud is a strategic, if not necessary, opportunity for businesses to implement a modern approach to security. As IT buyers plan their future security architecture, long-standing security practices are worth rethinking. The network firewall — a time-tested staple of security architectures — has struggled to match the scale and presence of digital transformation. Cloud environments and workloads, edge computing, IoT, OT, and BYOD are all challenging the relevancy of traditional firewall approaches. This paper describes what firewall as a service can do for organizations that use it properly and discusses key considerations and supporting trends.

Cloud Firewall Advantages

The cloud is now an accepted aspect of enterprise IT environments, offering infamous benefits of scale and efficiency. The cloud delivery model offers several advantages in cybersecurity too. Notably, 82% of organizations expected to use the cloud for IT infrastructure security delivery models by 2022 (IDC's *Future of Trust Survey,* February 2021, n = 507).

The cloud delivery model also makes sense for firewalls, including the following benefits:

- **Enterprise-scale efficiency.** Firewalls seem simple on paper. Users request access to a particular resource, a determination is made whether they should be granted network access, and then a rule is changed accordingly — all simple concepts. The default deny stance ensures that no unauthorized users are allowed in the network. However, enterprises have thousands of users requiring network access. While a one-off policy change is not difficult, the process can quickly become a treadmill of endless requests and rule changes. The challenge is multiplied for each permutation of firewall that requires a different process for policy changes, including on premises, branch offices, private cloud, public cloud, or edge. Firewall as a service provides a universal layer of coverage from which to create and change policies by removing redundancy from the process.

- **Flexibility.** The enterprise IT environment is dynamic; change is a given. Workloads may rely on public cloud or private cloud for certain audiences, use cases, or seasons. A hybrid workforce opens the possibility that workers may log on at home one day and in the office the next day. While an employee's log-in from an airport may rightfully require closer scrutiny, blocking access is not appropriate either. As buyers evaluate zero trust approaches to implement more robust security, cloud firewalls offer the ability to extend fine-grained zero trust policies across all environments and resources, including applications that require nonstandard ports and protocols. Importantly, cloud firewalls can enforce zero trust policies that are adjusted based on environmental and use case–specific risk factors, instead of brittle "block or allow" controls. Employees can remain secure and productive on the road or via BYOD instead of submitting help desk tickets.

- **Future proofing.** Digital transformation is upon us. Businesses are implementing the infrastructure that applications, sensors, devices, and users rely on for performant, highly reliable connectivity. While this means that organizations are currently implementing a hybrid infrastructure, the cloud is here to stay. The next objective is to ensure that security does not become a bottleneck in the transformation process. Cloud firewalls offer advantages over traditional firewalls, such as scalability and ubiquity, which are best attuned to the needs of complex, distributed, and demanding modern enterprise networks.

- **Threat detection.** Similarly, the increase in the complexity, ferocity, and ubiquity of advanced threats, ransomware, and insider threats requires an evolutionary leap in security technologies to keep up. Cloud firewalls now feature advanced security analytics, machine learning, and AI technology that is required to detect sophisticated multivector attacks and zero-day exploits with low false positives. Cloud firewalls leverage the scalability of cloud computing to perform these advanced security inspections without introducing latency, whereas on-premises firewalls force businesses to make a trade-off between security and performance.

- **Value enhancing.** Traditional firewalls have been challenged to adapt to myriad threats (especially in replacing campus and branch firewalls), increasing traffic loads, and expanding encryption. By comparison, cloud firewalls present an edge access point that is nearest to the user in question, thus preventing the long backhaul trips to traditional firewalls for inspection. As a result, security can be implemented without creating performance bottlenecks and therefore can eliminate many complaints related to poor performance. The advantage is pronounced in the campus and branch offices, where security must support existing corporate policies rather than facilitate silos.

Considerations for Cloud Firewall Buyers

In a world of mixed marketing messaging and complexity, the firewall has been a constant factor. However, the concept of firewall is changing as the technology moves to the cloud. Differences between traditional firewall appliances ported to the cloud and true born-in-the-cloud and built-for-the-cloud firewalls translate to important customer outcomes in terms of security and technical requirements. This section discusses the key factors that IT buyers should keep in mind as they evaluate cloud firewalls.

Understanding Cloud Performance

Cloud firewalls are better suited to the needs of the digital transformation era than traditional firewalls. While on-premises firewalls offer low latency for other on-premises devices, this advantage dwindles for organizations with users, devices, and workloads that are transient or mobile. Cloud services are ideally positioned for supporting remote users and edge computing, performing security inspections closer to the endpoint, and thus providing lower latency. Cloud firewall vendors are working to expand their edge to support all users, devices, and workloads regardless of location. Ultimately, latency is becoming less of a restraint and more of a differentiator between cloud providers. IT buyers should consider the strength of a vendor's cloud infrastructure when considering cloud firewalls.

Considering Non-Zero for Zero Trust

While enterprises are looking to adopt zero trust, ongoing education is necessary. Unfortunately, mixed marketing messages abound. For clarification, traditional firewalls should not be positioned as "zero trust." Legacy firewalls are useful for establishing a network perimeter.

However, this model allows excessive privileges and lateral movement. Lacking behavior monitoring capabilities, legacy firewalls are also prone to evasion and escalation tactics. By comparison, cloud firewalls support businesses on their zero trust journey, aligning with key principles of least privilege access, strong authentication practices, and continuous monitoring.

Cloud firewalls support businesses on their zero trust journey, aligning with key principles of least privilege access, strong authentication practices, and continuous monitoring.

Navigating Artificial Barriers

Cloud firewalls must justify their existence in the presence of existing security investments. Sunk costs in legacy firewall approaches, including virtual form factors, may increase the difficulty to establish a business case for firewall as a service. However, numerous factors must be considered for a complete assessment:

- **Ability to maximize value from existing firewalls.** Cloud firewalls shift security inspection to the cloud. This strategy reduces the load on existing firewalls, especially for compute-intensive functions such as SSL inspection. As a result, cloud firewalls can help in extending or ending firewall refresh cycles.
- **Reduced risk of digital transformation.** A gradual migration to cloud offers a stair-step approach to security modernization that reduces project risk. Businesses can adopt a plan for eventual phaseouts of legacy firewalls including hardware and maintenance costs.
- **Ability to reduce or eliminate technical debt.** Cloud firewalls provide a consistent security posture through centralized administration and universal coverage. The cloud migration is necessary to eliminate security complexity that leads to costly data breaches and ransomware.

The State of Firewalls Today

The following conditions characterize the challenges facing legacy firewalls:

- **Security is complex.** Enterprise security architectures feature many firewalls, some of which are designed for specialized environments. Firewall heterogeneity may result from other situations, such as mergers and acquisitions, incomplete migrations, and vendor changes. The result is a security architecture that is complex and ineffective and that includes hundreds of rules, across dozens of firewalls, and multiple brands. This is a burden for anyone to manage and inevitably will lead to policy conflicts or gaps.

- **Manual processes do not scale.** IT networks have changed drastically over the past decade, now featuring diverse and distributed devices, users, and workloads. The legacy approach to firewalls, with manual approval processes and static rules, presents a practical limitation, if not a technical one.
- **Encryption works both ways.** Encryption protects sensitive data from prying eyes. Cybermiscreants have recognized this fact and are using encryption to cover their exploits. Now that most network traffic is encrypted, firewalls must make difficult decisions between security and performance. Encrypted traffic requires extra computing power to decrypt and inspect. This results in a potential performance bottleneck or a glaring security gap if organizations choose to bypass encrypted traffic.

Conclusion

Cloud firewalls are the future, but legacy hurdles remain. Practical, real-world, and artificial limitations can be overcome, however, to achieve a modern enterprise security posture.

About the Analyst

Christopher Rodriguez, Research Director, Security and Trust

Christopher Rodriguez is a Research Director in IDC's Security and Trust research practice focused on the products designed to protect critical enterprise applications and network infrastructure.

MESSAGE FROM THE SPONSOR

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at www.zscaler.com or follow us on Twitter @zscaler.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.