SANS

A SANS Whitepaper

# How to Protect Enterprise Systems with Cloud-Based Firewalls

Written by **Kevin Garvey**

July 2019

*Sponsored by:*

**AWS Marketplace**

## Introduction

On-premises perimeter security has been a cornerstone of information security programs since the advent of the firewall. Numerous on-premises guidelines and requirements have been drafted to help information security professionals assess their capabilities against best-of-breed compliance certifications. Now, as more organizations realize the rising demand for, and full potential of, migrating their infrastructure and workloads to the cloud, world-class security is no less essential.

Organizations have been meeting the growing demands for securing on-premises networks and data by utilizing the latest generation of firewalls while employing defense-in-depth solutions throughout the enterprise. As cloud migrations have been ramping up over the last few years, the views on network security devices such as web application firewalls (WAFs) and cloud-based firewalls have evolved as well. Gone are the days of deploying network security devices using on-premises equipment only. Organizations can now virtually deploy WAFs and firewalls in cloud environments. In many cases, the deployment is as quick as pushing a few buttons, reducing the initial setup time from hours to minutes. Organizational focus can now shift from maintenance of the technology—firmware upgrades, patching requirements and physical replacements—to key security initiatives.

The requirements that apply to securing on-premises networks also apply to securing networks that have migrated to cloud environments—but the cloud provides a fresh approach to the security strategy and changes day-to-day expectations.

In this paper, we review how you can rethink on-premises security capabilities and technologies so that your deployments for cloud environments will be familiar and yet improved. We also look at an example of how an organization can successfully implement cloud-based firewalls.

## Cloud-Based Firewalls Provide Familiar Features

Since their inception, firewalls have been critical in securing an organization's perimeter. They are the first line of defense against incoming traffic, and the last line of defense for outbound traffic destined for the internet. For years, stateful firewalls that relied solely on port- or protocol-based filtering were sufficient for most organizations. But because bad actors were able to circumvent this simple firewall setup, firewall admins had to look beyond the blocking techniques of traditional firewalls. As the technology matured, firewall engineers and other security practitioners had the responsibility of implementing firewall rules, investigating firewall security alerts and troubleshooting connectivity issues when normal network traffic was disrupted. The latest generation of on-premises firewalls have highly advanced features, and firewall practitioners will find that these capabilities translate very well to a new generation of firewalls: cloud-based firewalls. Figure 1 shows the evolution of firewalls.

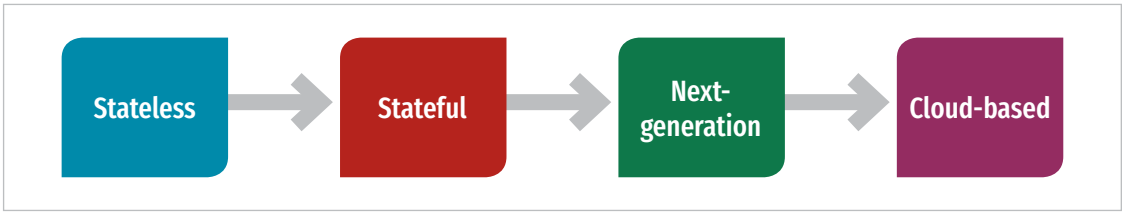


*Figure 1. Evolution of Firewalls*

Cloud-based firewalls fill an important role. With the increase in cloud implementations, the perimeter has taken on a different meaning and is not as easily defined. Cloud-based firewalls provide the same type of protection as on-premises firewalls, but they protect cloud-based resources and data. These firewalls allow organizations to extend their security controls to various environments in the cloud, including cloud-to-cloud traffic. They solve the problem of capturing traffic from all ingress and egress points, not only those in on-premises environments, but also cloud-connected traffic. All the new capabilities of cloud-based firewalls, coupled with the transfer of operational responsibility out of the end user's hands, has made cloud-based firewalls part of the forward-looking strategic discussions within IT departments.

## Firewall Features

While firewalls have developed to include functions that address the ever-changing threat landscape hitting an organization's perimeters, many of these features translate well to cloud-based deployments. In particular, features that allow organizations to gather data and inspect multiple on-premises and cloud perimeters help both security practitioners and operations groups make intelligent decisions. The features shown in

Figure 2 and detailed in the following sections are important considerations when deploying cloud-based firewalls.

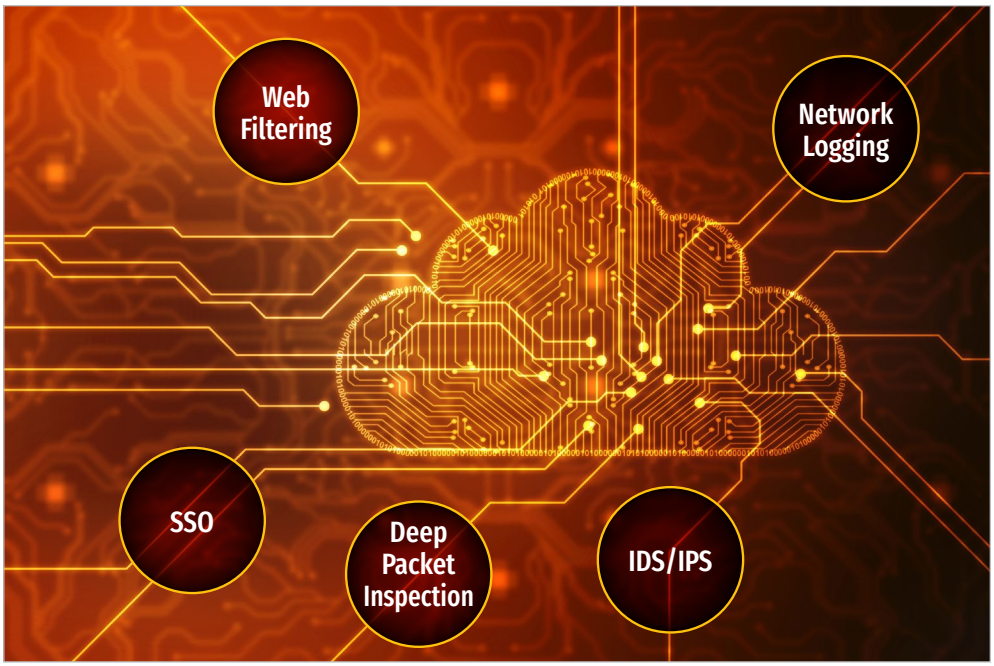


*Figure 2. Features of Cloud-Based Firewalls*

## Web Filtering

Web filtering allows organizations to mitigate against the risk of user activity that does not align with their acceptable-use policies. Many organizations have deployed web filtering to monitor user internet traffic and block websites that they deem a threat to the organization's risk posture. Such blocking can be done organization-wide, or a more granular approach can allow specified users or departments to bypass the filtering policies for defined websites. Many users are accustomed to web filtering, particularly if they have mistakenly tried to visit a website that is in violation of company policy.

Cloud web filtering is a new iteration of web filtering that allows organizations to enforce web content policies regardless of users' locations. Organizations can set policies based on whether the user is on or off premises. This type of web filtering affords organizations the flexibility to allow users access to the resources they need to be successful while mitigating against activity outside of the company's risk profile. Cloud-based web filtering can also reduce the need for on-premises web filtering equipment.

*Cloud web filtering affords organizations the flexibility to allow users access to the resources they need to be successful while mitigating against activity outside of the company's risk profile.*

## Network Logging

Traditional firewall configurations can produce network metrics on anything visible to them. Firewalls can give an IT group valuable data points on the activity on the network, from blocked and allowed websites to ports being utilized and the duration of network connections. This data allows network administrators and security practitioners to establish a baseline of what "normal" looks like, so that they can identify when the network is in need of troubleshooting or detect anomalous traffic on the network.

Cloud-based firewalls extend an organization's monitoring capabilities into the cloud. This lets administrators track cloud-based traffic to and from the on-premises environment, allowing security practitioners to establish a baseline for normal cloud network traffic patterns and to identify incongruous patterns. For example, if a rogue vulnerability scanner were running within the cloud environment, changes from the baseline cloud-based network would be detected, and security practitioners would be alerted so that they could investigate.

## IDS/IPS

IDS/IPS is a natural addition to any firewall setup. Both an IDS and an IPS watch for questionable network activity by using signature-based rules that search for predetermined patterns in network activity or by analyzing network traffic to identify deviations from the baseline. An IDS is able to identify anomalous traffic but does not block the traffic, while an IPS blocks traffic based upon a predefined set of rules.

IDS/IPS in the cloud works similarly to an on-premises device. Many IDS/IPS vendors offer cloud-based solutions that security teams can deploy easily to protect against cloud-based traffic. Some vendors allow organizations to connect their cloud IDS/IPS deployment to their on-premises solution so that users have a single, comprehensive view.

*Cloud-based firewalls extend an organization's monitoring capabilities into the cloud. This lets administrators track cloud-based traffic to and from the on-premises environment, allowing security practitioners to establish a baseline for normal cloud network traffic patterns and to identify incongruous patterns.*

## SSO/Authentication Support

Firewalls in the past were siloed from directory stores, forcing firewall admins to administer firewall rules and user roles separately. Cloud-based firewalls have the capability to seamlessly integrate with identity and access management (IAM) technologies such as SSO to make the process of administering user roles as simple as possible.

Because cloud-based firewalls can integrate with existing directory stores, admins have fine-grained control of firewall features through existing SSO technologies. This integration also helps eliminate the security risk of stale login accounts on the firewall. Making sure that IAM policies on a firewall stay fresh as users change roles or leave the organization helps to maintain a strong security posture. Cloud-based firewalls make analyzing and correlating SaaS-based application and other cloud-based architecture network traffic easier by showing admins a more complete picture.

*Many IDS/IPS vendors offer cloud-based solutions that security teams can deploy easily to protect against cloud-based traffic.*

The integration of directory services allows network administrators to transfer the responsibility of reassessing users' access from firewall administrators to the appropriate IAM teams. When deploying cloud-based firewalls, an integration with an organization's directory service offers the same features as an on-premises firewall, eliminating the need to audit IAM concerns in cloud-based firewall deployments.

If an organization has not connected its directory store to AWS, it can utilize AWS Directory Service[1] to reduce the burden of maintaining separate accounts in each firewall cloud deployment.

*Cloud-based firewalls make analyzing and correlating SaaS-based application and other cloud-based architecture network traffic easier by showing admins a more complete picture.*

[1] This paper mentions product names to provide real-life examples of how firewall tools can be used. The use of these examples is not an endorsement of any product.

## Deep Packet Inspection

Deep packet inspection (DPI) has been included in firewall deployments for years. DPI investigates network packet headers and data to determine whether a packet contains a malicious payload. If the firewall deems the packet to be malicious, the firewall deals with it by following either built-in rules or custom rules developed by the firewall administrator. The most common use case is to drop or block the packet from proceeding to the next hop. Now that firewalls are commonly built with much more processing power, the worry about DPI introducing significant network latency has fallen away, and DPI has become commonplace.

DPI of cloud traffic is just as important as it is for on-premises traffic. Cloud-based firewalls detect malicious traffic not only as it enters the cloud environment, but also as it traverses the cloud infrastructure. This key component allows AWS users, for example, to use VPC Traffic Mirroring in a multi-account AWS environment, capturing traffic from virtual private clouds (VPCs) spread across many AWS accounts and then routing it to a central VPC for inspection.

# Ease of Management of Firewalls and Firewall Features in AWS

Many cloud-based firewalls allow network and security teams to expand their current, on-premises firewall capabilities to protect their cloud infrastructure. The beauty of the extension is how seamless it is to integrate these new firewalls into day-to-day operations with little operational upkeep by the admin. The following sections point out some of the key features (see Figure 3) that simplify cloud-based firewall deployments.

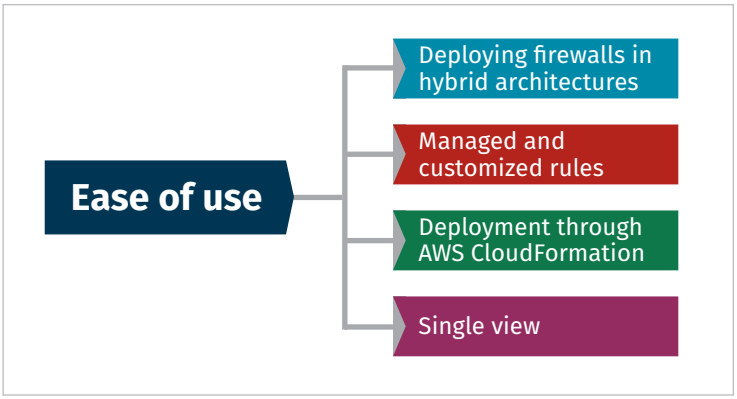


*Figure 3. Seamless Integration of Cloud-Based Firewalls with Operations*

## Managing All Firewalls in a Single, Comprehensive View

Firewall administrators in the past had to log into firewalls one by one to deploy changes throughout their perimeters. This process created an enormous amount of administrative work for network administrators and security practitioners. More recently, many firewall vendors have provided a single, comprehensive view, allowing teams to save time by making changes on multiple on-premises firewalls at once. Not only has this change been positive for administrators, but it has allowed teams to analyze traffic patterns from a group of firewalls in one console. It also enables richer search results and faster mean time to resolution for security alerts and network outages. Firewall administrators can take comfort in knowing that they can add many of their cloud-based firewall deployments into existing comprehensive views, allowing for easy data correlation between on-premises and cloud-based network traffic.

## Deployment Through AWS CloudFormation

AWS CloudFormation provides a common language for describing and provisioning all the infrastructure resources in your cloud environment. With AWS CloudFormation, you can use a simple text file to model and provision—in an automated and secure manner—all the resources needed for your applications across all regions and accounts. For example, using AWS CloudFormation is helpful for cloud-based WAF deployments and ensures all of them are deployed in a consistent manner, making management of each WAF simpler. With the assistance of a master template, AWS CloudFormation is able to launch WAF solutions for web applications. The default configuration deploys an AWS WAF web access control list (ACL) with eight preconfigured rules, but you can also customize the template based on your specific needs.

## Advantages of Using a Third-Party WAF/Firewall in AWS

While AWS offers strong in-house-developed firewalls for each customer to deploy, some customers may find it easier to continue their deployment with their existing vendor ecosystem. This allows the customer to enjoy a comprehensive view of their on-premises and cloud-based firewall, and have a simpler license model with their vendor.

## Deploying Firewalls in Hybrid Architectures

Many organizations have operational and security requirements in their on-premises environments that they think cannot be properly met in the cloud. Some of them have decided to pursue an intermediate approach, setting up a private cloud, which co-exists with on-premises and public cloud strategies.

Private clouds require the same oversight as public clouds and on-premises networks. In addition, the network security requirements in private clouds are very similar. Just as in a public cloud, cloud-based firewalls are a necessity in a private cloud, and deployment is similar. But all firewalls—whether on premises, public cloud and private cloud—should report to a single location to streamline log aggregation and correlation.

## Managed and Customized Rules

While several "... as-a-service" offerings have hit the market over the last few years, many organizations are finding firewall-as-a-service (FWaaS) to be an attractive option. The reason is that FWaaS takes all the administrative burden—patching and management of the firewall platforms—out of the hands of administrators and establishes a unified policy among all deployed firewalls in an organization.

Vendors offer FWaaS as a solution to merge and unify rules and logs from disparate firewalls while the customer enjoys a "hands-off" experience. It might seem as if deploying firewalls on-premises, in a private cloud and in a public cloud would cause administrative headaches, but in fact, FWaaS can remove unnecessary administrative burdens and requirements. This type of service allows administrators to push through policies for all the firewalls in their purview.

# Advanced Features

Like many security technologies, firewalls have matured since their inception, including the introduction of enhanced security in so-called next-generation firewalls (NGFWs). As firewalls continue to develop, newer security features, such as behavioral threat detection and analytics, are being incorporated to make organizations even more secure.

## Behavioral Threat Detection

Many cloud-based firewalls have started using more advanced features in recent years and continue to build upon the other features each year. Given the amount of data that modern firewalls collect, it only makes sense to put some of that data into action.

Behavioral firewalls convert those data points already present in firewalls into predictions of deviations from the normalized baseline. Identifying what users are doing outside of their typical tasks is a great first start to detecting insider threats. Cloud-based firewalls extend behavioral threat detection into the cloud, giving insight into what is happening outside of the organization's on-premises environment. An additional benefit is that insider threats can be contained more swiftly if organizations can link on-premises behaviors to anomalous cloud-based activity.

## Next-Generation Analytics

Cloud-based firewalls let organizations see, through aggregated sets of metrics and data points, the effectiveness of their security posture. For example, security administrators can easily find out the number of DDoS attacks their cloud and on-premises firewalls have prevented. Cloud-based firewalls also allow security personnel to see the external traffic hitting their cloud space and the network traffic traversing that cloud space. This visibility helps security teams recognize threats not yet written into an alert.

## Support for AWS Services

When deploying cloud-based firewalls in an AWS account, where the logs of the cloud-based firewall and WAF ultimately go is a decision any organization can make. For example, to receive a history of all AWS WAF API calls made on your account, you simply turn on AWS CloudTrail in the AWS Management Console.

# Use Case: Deploying a Cloud-Based Firewall

When deploying a whole new cloud infrastructure, integrating cloud-based firewalls within a new VPC will both reinforce the security-first mindset and ensure long-term measurement and growth of the VPC. And of course, having protection against the latest threats hitting cloud environments is critical. Let's examine the approach "Acme Corp.," a fictional company, used to deploy its cloud-based firewall.

After testing the waters of cloud computing by moving nonessential company infrastructure into the cloud over the last few years, Acme started a migration of its critical assets to the cloud. Firewall administrators noticed that they did not have good visibility into the traffic going in and out of some of the VPCs that were being stood up by Acme. More importantly, Acme was blind to the traffic flowing between VPCs. While Acme's on-premises firewalls were deployed with attention to security best practices and were well maintained, cloud-based firewalls were not being provisioned in a similar fashion. Many cloud-based firewalls did not follow the security requirements of the on-premises firewall setup, nor were they reporting to a centralized console for each network, which was an important provision for its security teams. Acme's move to the cloud enabled the organization to realize all of the operational benefits of a cloud-based environment. Acme was excited to accelerate the migration of its existing on-premises assets to the cloud and wanted to make sure the security and administration of its new assets matched the world-class quality it had in its on-premises environment.

Acme wanted to add the logs from all of the provisioned cloud-based firewalls into its log aggregator. While it was technically possible to connect all of the log sources into the log aggregator and create correlations and alerts on the new cloud-based log sources, Acme knew that cloud-based firewalls would facilitate a much easier method of moving forward with the requirement. What Acme found was that by deploying a cloud-based firewall, it could go beyond that, because the cloud-based firewall allowed for a single, comprehensive view into both its on-premises and cloud traffic. That meant it would take less time to investigate firewall alerts from various environments.

Acme also wanted a better understanding of traffic in its cloud. To do that, it needed first to determine the baseline network traffic in the cloud and then to detect anomalies from the baseline and identify network segmentation requirements. In the cloud, detection of anomalies cannot be port-based, so using some of the newest cloud-based firewall features, such as behavioral analytics and behavioral threat detection, meets the requirements for Acme's new firewall deployments.

Another goal for Acme was the capability to quickly see whether any anomalous activity in the cloud was connected to alerts in its on-premises architecture. To accomplish that, Acme needed a solution that would put everything under one management console, which would reduce investigation time for both security practitioners and network analysts.

In the end, Acme felt comfortable that deploying the new features in its cloud-based firewalls would satisfy its security requirements. See Table 1, which summarizes the requirements and challenges Acme had to address.

**Table 1. Requirements and Challenges**

| Requirements of Cloud-Based Firewalls | Challenges |
|---|---|
| Behavioral analytics | Not seeing all traffic moving from on premises to cloud |
| Comprehensive view | Missing cloud-to-cloud traffic<br>Having to log into multiple management consoles to manage firewall alerts |
| Next-generation analytics | Needing to have top-of-the-line, cloud-based firewall technology options |

Acme deployed the metered F5 Big-IP Local Traffic Manager (LTM) + Advanced Firewall Manager. Not only did it provide NGFW capabilities such as comprehensive threat protection, granular control and visibility into Acme's cloud environment, but it also allowed Acme to deploy secure office-to-cloud connectivity and cloud network segmentation.

## Summary

Whenever organizations add new network segments, their compatibility with firewalls and other network security equipment is a top concern. Cloud security migrations are the next-generation leap many companies have been looking forward to for years. As a result, organizations need to look at cloud-based firewalls that are able to work in concert with traditional firewalls to secure the organization and the applications and assets it has migrated to the cloud.

Using cloud-based firewalls enables businesses to focus on what makes them great while moving the heavy lifting of infrastructure and hardware support to the cloud. Cloud-based firewalls free up network administrators and security practitioners to focus on their key job requirements by relying on the cloud to take over many of the tasks they had to take on for so many years.

Today's cloud-based firewalls have brought the best of what security practitioners and network administrators love about NGFWs to the cloud, while also expanding the capability to aggregate cloud data points. This data is used smartly in DPI, next-generation data analysis and behavioral analysis. Cloud-based firewalls are no longer just a requirement for network security; they are an integral part of network- and security-based decisions in a cloud deployment.

## About the Author

**Kevin Garvey** is a SANS instructor-in-training for MGT512 and security operations manager at an international bank based in New York City. He has been a cybersecurity aficionado ever since he became interested in computers, but formalized his passion by moving from a career in IT to become a cyber professional in 2013. Kevin has worked at the New York Power Authority, JP Morgan and Time Warner, contributing and leading efforts to grow new and existing cyber initiatives. He holds a CISSP, GCIH, GLEG, GCFA, GCFE and GSLC.

## Sponsor

**SANS would like to thank this paper's sponsor:**