SANS Institute

Sponsored by:

aws marketplace

Cloud-Based Firewalls Best Practices in AWS

Compiled from works completed by
Brian Russell | **Kevin Garvey**
with an introduction by **John Pescatore**

December 2019

Analyst Program

Table of Contents

Long before the internet (actually, long before electricity), businesses faced two major threats: (1) thieves breaking into their stores and warehouses and stealing the goods and (2) fire sweeping through business districts of the wooden buildings that housed most businesses. Thieves would generally hit one business at a time and rattle the doorknobs to find a business that hadn't locked its doors, often not even needing to break down a door or pick a lock. Fire was different, as many large cities learned. A fire that started to burn in one building could spread rapidly to nearby connected structures and often decimate entire neighborhoods and business districts.

This danger led to the development of the original "fire wall:" a fireproof barrier that could keep the dangerous stuff (fire) away from the valuable stuff (people and products). In the 1600s, fire walls implemented the original "DenyAll" rules, while locked doors provided "Allow only those explicitly permitted" policies to be applied.

Flash-forward to the late 1980s, and the internet was just starting to become the conduit for criminals and the cyber equivalent of fire—the DoS attack. In 1988, the Morris worm took down 10% of internet servers,[1] with an estimated 30% of internet traffic impacted. Innovative network engineers at AT&T and Digital Equipment Corp. (DEC) began to develop network-based firewalls, putting in place the TCP/IP version of perimeter security policy of "Deny all except what is explicitly allowed" at the port and protocol level. As threats matured, firewalls evolved, adding stateful filtering, deep packet inspection, application-level security policies and other advanced capabilities.

> **"Firewall services are a key component in protecting cloud-based business services, both at the perimeter and between internal processing segments."**

As businesses moved to embrace hybrid and public cloud computing, the definition of the perimeter has changed, but the need for perimeter security has not disappeared. A firewall at the edge is the most cost-effective way to assure DoS attacks (fires) don't spread into and across your organization. Perimeter security is also the only place to protect misconfigured or rogue hosts on the network from attackers. Finally, firewalls provide the detailed and hard-to-corrupt logs of all traffic crossing network and system boundaries—often critical in investigating threats and incidents, much the way video surveillance cameras are used by law enforcement.

Today, firewall services are a key component in protecting cloud-based business services, both at the perimeter and between internal processing segments. The papers that follow describe best practices and techniques for securing cloud-based firewalls in Amazon Web Services (AWS):

- ***JumpStart Guide for Cloud-Based Firewalls in AWS***, written by Brian Russell, provides a tutorial on firewall terminology and deployment options. This whitepaper presents a methodology that details the business, technical and operational considerations involved in architecting the optimal firewall architecture for protecting your organization's AWS services.
- ***How to Protect Enterprise Systems with Cloud-Based Firewalls***, by Kevin Garvey, drills down deeper into firewall-based security controls and policies and provides guidance on how to effectively and efficiently deploy and manage firewalls across cloud and hybrid environments.

Take advantage of cloud-based resources, such as cloud-based firewalls, to improve your security program and stay one step ahead of would-be attackers.

[1] "The Morris Worm," https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

A SANS Whitepaper

JumpStart Guide for Cloud-Based Firewalls in AWS

Written by **Brian Russell**

July 2019

Sponsored by:

AWS Marketplace
in conjunction with
Optiv

Webcast

You can access the associated webcast at:
https://pages.awscloud.com/optiv-aws-cloud-based-firewalls.html

Introduction

Firewalls have evolved from providing simple packet filtering based on port and protocol combinations. Today's cloud-based firewalls are virtualized in the cloud and provide rich features such as application-based filtering, microsegmentation, encrypted traffic inspection and DNS security. Cloud-based firewalls are becoming true security platforms that incorporate intrusion prevention and detection features and threat prevention services that allow organizations to stay protected against both known and unknown malware.

This guide examines options for implementing firewalls within Amazon Web Services (AWS). It examines the needs and capabilities associated with today's firewall and threat prevention services and details general, technical and operational considerations when choosing these products. The guide concludes by examining AWS-specific considerations and recommending a plan of action for organizations considering the purchase of cloud-based firewalls. Before we begin, Table 1 provides definitions of key firewall-related terms.

Table 1. Key Terminology in This Guide

Terms	Descriptions
Network Firewall	Network security device used to monitor incoming traffic and block unauthorized traffic. Commonly, a set of rules is defined for ingress and egress traffic. Only authorized traffic is allowed into and out of the network. Rules are typically set up based on IP address and port combinations.
Web Application Firewall	An HTTP application-specific firewall used to protect an application's back-end servers from attacks such as cross-site scripting and SQL injection. A set of rules governing the format and content of HTTP messages is defined. HTTP messages are then evaluated to ensure the criteria set forth by the rules are enforced.
Next-Generation Firewall	Next-generation firewalls build upon traditional firewalls to include additional protection mechanisms. Functionalities may include intrusion prevention, application firewalling, TLS/SSL-encrypted traffic inspection and more.
Cloud-Based Firewall	Firewalls that operate within the cloud on a variety of licensing terms and provide cloud-tailored features such as application control, dynamic addressing and microsegmentation. They can scale to meet the demands of the cloud.
Threat Prevention	Threat prevention services are add-on features to firewall product offerings. The services are designed to enhance firewall capabilities by adding features such as zero-day malware prevention, IDS/IPS, antivirus, DDoS protection and URL filtering. Subscription-based services can keep threat data up to date and include blacklisted IP addresses, URLS or domains.

The considerations in this guide are designed to inform a systematic evaluation strategy for choosing the optimal firewall for your requirements. An evaluation strategy should be based on an organization's specific needs and implementation requirements. The evaluation should consider the capabilities of the native AWS firewall offerings and then incorporate a review and comparison of AWS Marketplace offerings. Finally, following the simple "Analysis of Alternatives" detailed in the "Making the Choice" section of this paper will assist you in making the right decision for your organization.[1]

[1] "Analysis of Alternatives," https://en.wikipedia.org/wiki/Analysis_of_Alternatives

Implementation Options in AWS

Security engineers have many options when choosing firewalls to deploy within AWS. AWS offers a native firewall solution that provides packet filtering and is integrated directly into the AWS environment. Third-party vendor solutions often offer additional features and are available from AWS Marketplace.

Customers can also engage through Consulting Partner Private Offers (CPPO) to work directly with trusted advisors to select and configure firewall solutions from AWS Marketplace. As organizations build out their cloud and cloud security strategy and plan, they may want to consider working with partners to accelerate their efforts or fill any gaps in knowledge or resources that are identified. All consulting partners may extend AWS Marketplace third-party solutions directly to customers through CPPO.[2] Not every organization will be able to find resources with deep cloud experience, and even experienced cloud technologists may have experience only in specific industries or with certain cloud vendors.

More information on each approach is detailed in Table 2.

Table 2. Options for Choosing the Right Firewall Vendor for Use Within AWS

Terms	Descriptions
Bring Your Own License (BYOL)	For businesses that already own firewall licenses, BYOL provides a flexible deployment option. A BYOL approach allows an organization to reassign its licenses. This approach can be ideal because the license is not tied to a specific subscription. BYOL requires that licenses be tracked. Firewalls available within AWS Marketplace may be available for use directly with AWS accounts.
Managed Firewall/ Firewall-as-a-Service	Traditionally, firewalls are a separate physical device. Managed firewalls and firewall-as-a-service offer a cloud-based rather than a device-based solution. In AWS, firewall-as-a-service offers immediate protection and, in some ways, may be more cost-effective for smaller companies that may not be able to purchase and maintain the firewall infrastructure.
Virtual Firewall Appliances	Virtual firewall appliances are installed and operate directly within the cloud. Virtual firewalls can be deployed quickly and many options are available from AWS Marketplace.
Trusted Advisors	Trusted advisors are experts in an area and can be used on a consulting basis to support selection and configuration of the optimal firewall products based on specified requirements. You can view a listing of AWS Security Competency Partners here: https://aws.amazon.com/security/partner-solutions

Needs and Capabilities: The Business Case for Firewalls and Threat Prevention in the Cloud

The perimeter is no more. But even though networks are no longer defined by their perimeters, firewall products still fill a critical role in an organization's security architecture. Firewalls have evolved from simple filtering based on IP addresses and ports. To protect today's organization, they allow security administrators to filter based on specific applications and even application functions. Firewalls support nested policies and can be used to securely connect the data center and the cloud. Firewalls are becoming even more important as the network perimeter changes and the capabilities of attackers increase.

[2] Consulting Partner Private Offers, https://aws.amazon.com/marketplace/features/cpprivateoffers

This section and Figure 1 detail the reasons for deploying firewalls and threat prevention services in the cloud.

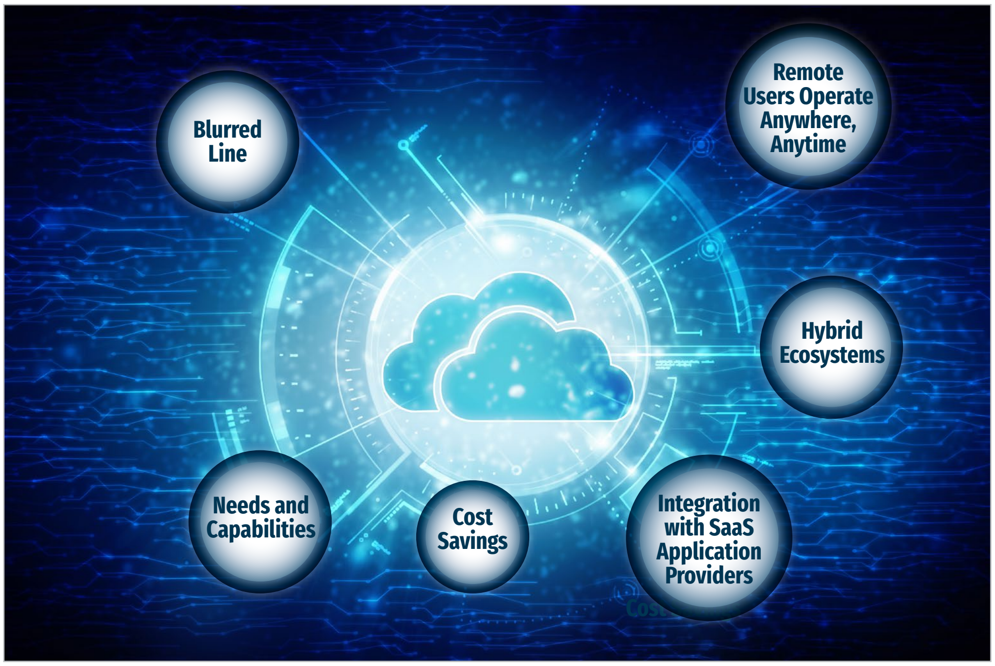
Blurred Line
Remote Users Operate Anywhere, Anytime
Hybrid Ecosystems
Needs and Capabilities
Cost Savings
Integration with SaaS Application Providers

Figure 1. Reasons to Deploy Firewalls and Threat Prevention Techniques in the Cloud

Blurred Line

A network perimeter is what separates the private side of a company's network from its public side. The private side is usually managed by the company, and the public network is typically managed by the provider of the network. However, with the growing popularity of mobile devices, cloud solutions and social networks, the line between private and public is increasingly blurred, making protecting the network using traditional firewalls more challenging. Mobile devices must be able to operate on networks outside the corporate firewall. Firewalls and threat prevention techniques in the cloud allow for flexibility to reconfigure according to new challenges, scalability to accommodate influxes of devices and widespread coverage beyond the physical network.

Remote Users Operate Anywhere, Anytime

Related to the disappearance of the network perimeter, more and more employees are working remotely and accessing applications that can be hosted anywhere geographically. Traditional firewalls do not allow secure and fast connection from anywhere in the world or any time of the day. Cloud-based firewall solutions are scalable for securely tunneling all user traffic and support multifactor authentication, allowing remote users to connect via secure tunneling so that no matter where they are, their connection is secured.

Hybrid Ecosystems

As companies expand, they are turning toward hybrid ecosystems, where resources are both on premises and in the cloud. Such ecosystems reduce capital investment in physical infrastructure. Cloud-based firewalls enable hybrid ecosystems by instantiating and enforcing virtual private networks (VPNs) between the data center and the cloud. These cloud-based firewalls can be configured to scale to meet the demands of today's enterprises and can even be configured to augment the capacity of firewalls installed on premises. These cloud-based firewalls can be quickly deployed within AWS using CloudFormation templates.

Integration with SaaS Application Providers

Assuring the security of mission-critical SaaS applications can be a challenge. Cloud-based firewalls can be configured to protect against malicious attacks on these applications, and they offer features above and beyond traditional firewalls such as deep packet inspection, application-based access controls, threat prevention and zero-day malware detection.

Cost Savings

Cloud-based firewalls can be procured with flexible subscriptions. Cost models are shifting from requiring large up-front capital expenditures to monthly expenses. Cost savings can be realized through the unique licensing options available within AWS; a combination of monthly and hourly pricing supports lower-cost handling of peak demand. Additionally, when firewalls are deployed to the cloud, fewer instances may be required compared to data center installations, further reducing overall cost. Administrative costs can be lowered through automation using firewall management APIs.

Needs and Capabilities

Cloud-based firewalls provide security around the cloud implementation and support network segmentation. They enhance threat prevention capabilities.

Cloud-Based Firewalls

The need: Firewalls allow organizations to filter and log unauthorized or suspicious connections based on rules and/or behaviors. Firewalls also support network segmentation and can be used to ensure that only authorized applications or application types are run within an organization. They can also require multifactor authentication for all remote connections and can be used to detect and prevent intrusion attempts.

Capabilities

- Allow administrators to define and load policies that filter on IP addresses, ports, protocols, application types, groups and users. This capability ensures that only authorized users, communications and applications are allowed to interact with or access organizational assets, or even to limit functions within an application for some users.
- Allow administrators to segment their networks and isolate both north-south and east-west traffic. This functionality provides dynamic security across cloud/data center implementations as well as throughout the application service stack.
- Provide dynamic addressing support such as network address translation (NAT) that enables seamless integration across the cloud and data center. This support allows IP traffic across the entire ecosystem even when IP addresses change.
- Inspect encrypted traffic flowing through Transport Layer Security (TLS) tunnels. This capability mitigates the threat of an adversary passing malicious data into the network within an encrypted tunnel.
- Reduce administrative burden by providing automated policy management using well-defined APIs or providing AWS CloudFormation templates. This capability may also support touchless deployment, which significantly reduces the time needed to begin use.

Threat Prevention

The need: Threat prevention adds to a cloud-based firewall by providing advanced logging, alerting and prevention of both known and unknown threats. This feature includes services that keep firewall policy up to date with the latest threats and protects against both known and unknown malware.

Capabilities

- Provides advanced intrusion prevention capabilities that analyze, prevent and report on suspicious behavior within the system.
- Provides antivirus protections that identify and remediate malicious content based on known signatures.
- Logs events and alerts on suspicious behavior and may also support correlation across multiple firewall/threat prevention instances.
- Maintains a continually and dynamically updated threat database that includes known malware and known malicious sites and IP addresses.
- Protects the infrastructure from malware and provides advanced functionality such as DNS sinkholing.

General Cloud-Based Firewall and Threat Prevention Considerations

Business Considerations

	Consideration	Details
$	On-demand access	Today's users operate globally and 24/7. Users require secure access to their applications and data spread across the data center and the cloud.
$	Hybrid ecosystems	Today's organizations use multiple infrastructures in support of their missions. Organizations spread data and applications across the data center and multiple SaaS providers. Data must be securely passed among these environments.
$	Regulatory compliance mandates	Regulations mandate compliance with security and privacy requirements. Firewalls support this compliance by enforcing technical security policies that enable the confidentiality of information.
$	Speed to market and agile capabilities	Organizations rely on elastic cloud services to quickly introduce new capabilities or to scale to meet demand. Cloud-based firewalls enable organizations to move quickly to meet demand and demonstrate new agile capabilities securely.
$	Cost	The pay-as-you-go model enables organizations to procure cloud-based firewalls using operational dollars instead of capital expenditure (CapEx) funds. Combining hourly and annual subscriptions supports cost-effective dynamic scaling. Costs can also be saved using managed updates.
$	Dynamic threat environment	Security teams are often overworked and have trouble maintaining situational awareness of the latest threats. Threat prevention services keep security teams updated on the latest in attack methods and automatically update firewall rules to guard against these new threats.

Technical Considerations

	Consideration	Details
	Application-layer support	Network communications are no longer bound to discrete service ports that can be easily filtered by a firewall. Today, most communication happens over ports 80 and 443 in the form of web traffic, leaving traditional firewalls unable to perform their functions of filtering defined IP address/port ranges. Identifying applications at Layer 7 becomes more important to safely enable the use of an application as well as reduce the attack surface.
	HTTP(S) inspection	TLS-encrypted traffic streams provide attackers with a method of gaining access to systems. Firewalls must be able to peer inside this encrypted traffic to perform filtering functions that identify the underlying application as well as any potential threats.
	Dynamic addressing	Cloud-based firewalls must be able to support environments where virtual network address ranges change on a regular basis. Dynamic addressing allows you to create policy that automatically adapts to changes—adds, moves or deletions of servers.
	Network isolation and microsegmentation	Firewalls must be able to provide network segmentation and filter traffic between trusted and untrusted environments.
	Automated policy management	Firewalls installed within the cloud must be able to be managed efficiently. APIs can support the automated management of firewall policies and enable coordination of firewall enforcement across multiple instances.
	Threat prevention	Threats change quickly, with new exploits and attack methods constantly being developed. Vendors must be able to update firewalls quickly with new information on malicious content, sites and addresses to protect the enterprise.
	Granular policy definition and enforcement	Cloud-based firewalls should be able to support policies at multiple layers of the ecosystem, including applications, application types and functions, users, networks, ports and protocols.
	Situational awareness	Firewall instances might be installed across cloud regions and within several data centers. They must be able to share logging information in standardized formats to enable situational awareness across the organization's infrastructure.
	Single-view visibility and management	Single-view visibility makes it easier for system administrators to manage deployed firewall instances using a single management application.
	East-west traffic security	Firewalls should support the isolation of networks and security across different environments, including east-west security.
	File blocking and analysis	Threat prevention systems can block known-malicious files and analyze suspicious files before allowing them into the network. This function can keep an organization safe from the insertion of malware into the network.
	DNS monitoring	Threat prevention systems can monitor for outgoing communications to known-bad URLs and can be configured to send traffic destined to these URLs to an administrator-owned site for analysis.

Operational Considerations

	Consideration	Details
	Costs	Cloud-based firewalls can help organizations better manage their security infrastructure costs. Automated management, ease of deployment and managed updates all reduce labor costs associated with system administrators. Shifting funds from CapEx to operational budgets introduces flexibility. Combining annual subscriptions with hourly costs allows economical scalability as needed.
	Incident response	Incident response requires access to log data for situational awareness. Organizations should update incident response plans to include analysis of cloud-based firewall log information.
	Data exfiltration security	As the perimeter of the network changes and the focus shifts to data security, ensuring that data cannot be exfiltrated from the organization's network becomes critical. Threat prevention solutions flag and alert on data being sent to known-malicious sites.
	Intrusion prevention	Intrusions are blocked after evaluating traffic based on both behavior and known signatures.
	Multifactor authentication	Multifactor authentication provides an extra layer of security to VPN logins, requiring all users to use two or more forms of authentication.
	Proxy	Firewalls can act as proxies between networks, hiding the details of the private network from the outside world.

AWS Implementation Considerations

The general considerations discussed so far can help security leaders make the case for obtaining funding for the procurement of cloud-based firewalls and threat prevention services. The next section examines specific considerations for operating cloud-based firewalls within AWS. Use this section to differentiate between solutions available in AWS Marketplace.

Cloud-Based Firewalls

Firewalls have been a staple of security architectures for decades now and there are many to choose from. Determining the right firewall solution for your organization requires an analysis of your specific requirements. This section provides a set of considerations that can help when selecting cloud-based firewalls for use within AWS.

	Consideration	Details
	Level of AWS integration	The native AWS firewall is directly integrated with AWS services. You should ensure that AWS Marketplace firewalls have a high degree of integration with the AWS services that you use and evaluate the options for automation of deployment and update. **Evaluate:** • Does the firewall provide support for both virtual private cloud (VPC) and EC2 instances? • Does the firewall integrate with AWS security services such as AWS Firewall Manager, AWS Security Hub, AWS Transit Gateway and AWS GuardDuty? • Does the firewall seamlessly support high availability across multiple AWS regions? • Does the firewall offer CloudFormation templates that can reduce time to deployment?
	Policy management	Cloud-based firewalls should enable granular and automated policy management features. **Evaluate:** • Does the firewall support nested policies within security groups? • Does the firewall enable automated configuration of security policies? • Does the firewall support risk-based policy definitions?
	Hybrid environment support	Firewalls implement IPsec VPNs to securely network across multiple VPCs, enterprise sites and SaaS providers. **Evaluate:** • Does the firewall support dynamic addressing that allows you to create policy that automatically adapts to changes—adds, moves or deletions of servers? • Does the firewall support networking across multiple VPCs?
	Logging	Logs provide a vital resource for incident response and forensics. All firewalls should provide logging features. **Evaluate:** • Does the firewall offer a solution that allows for aggregation of logs across multiple firewall instances? • Does the firewall integrate with AWS logging mechanisms?

Cloud-Based Firewalls (continued)

	Consideration	Details
	Hybrid environment support	Firewalls implement IPsec VPNs to securely network across multiple VPCs, enterprise sites and SaaS providers. **Evaluate:** • Does the firewall support dynamic addressing that allows you to create policy that automatically adapts to changes—adds, moves or deletions of servers? • Does the firewall support networking across multiple VPCs?
	Logging	Logs provide a vital resource for incident response and forensics. All firewalls should provide logging features. **Evaluate:** • Does the firewall offer a solution that allows for aggregation of logs across multiple firewall instances? • Does the firewall integrate with AWS logging mechanisms?
	Separation of trusted and untrusted zones	Firewalls must be able to segregate both north-south and east-west traffic. This segregation allows untrusted zones (such as development) to interact with trusted zones (such as production), and supports processes such as DevOps. **Evaluate:** • Does the firewall filter across trusted and untrusted zones? • Does the firewall support micro-segmentation and isolation of subnetworks?
	Management of multiple firewall instances	Many firewall vendors provide software that allows for the seamless management of multiple firewall instances. **Evaluate:** • Does the firewall include software that can manage all of the firewall instances in the cloud? • Does the firewall management software allow you to push policies and perform updates to device configurations?
	Scalability	Cloud-based firewalls should support elastic expansion, allowing them to scale automatically to meet the demands of users. **Evaluate:** • Does the firewall scale automatically? • Can you use the firewall to augment data center installations to support peak demand (e.g., cloudbursting)?
	Dynamic reporting	Reporting provides administrators with insight into trends as events occur across the network. Cloud-based firewalls should provide insightful reporting features. **Evaluate:** • Does the firewall provide reporting that allows for analysis of incoming requests? • Does the firewall provide reporting that tracking of trends in violations?

The above considerations are based on integration of firewall capabilities within an AWS environment. Organizations may not need all of the capabilities discussed here, but they can review these considerations and determine what is needed based on their specific requirements. A critical consideration, however, is the capability to seamlessly integrate with AWS services. Any solution selected from AWS Marketplace should provide this baseline capability.

Threat Prevention

Threat prevention is critical to keep organizations ahead of the dynamically changing threat landscape. Threat prevention techniques incorporate the latest threat intelligence data and dynamically update policies to guard against the latest attack methods and malicious sites. Threat prevention services can provide file-blocking features, keep data from leaving the network, and identify and prevent intrusions.

	Consideration	Details
🛡	Cloud context support	Threat prevention is based heavily on the ability to acquire relevant information on the latest threats, threat actors and their capabilities. Ensure that the threat prevention services you procure within AWS are supported by top-quality threat intelligence feeds. **Evaluate:** • Is the threat intelligence data timely? • Is the threat intelligence data relevant to your organization's mission?
🛡	Performance and efficiency	Threat prevention services should keep customers up to date on the latest threats to their systems. **Evaluate:** • Does the threat prevention service provide a listing of known-bad addresses and sites? • Does the threat prevention service automatically update new malware signatures? • Does the threat prevention service automatically update firewall rules based on known malicious activity? • Does the threat prevention service have the ability to perform DNS sinkholing or DNS security?
🛡	Deployment	Firewalls incorporating threat prevention should be capable of creating a baseline of behavior and alerting on anomalies. **Evaluate:** • Does the threat prevention service analyze logs, correlate events and block/alert on suspicious activity? • Does the threat prevention service support behavioral analysis? • Does the threat prevention service scan all traffic, including applications, users and content?
🛡		Threat prevention services should incorporate antivirus support that includes maintaining an updated list of signatures. **Evaluate:** • Does the threat prevention service incorporate network antivirus features? • Does the threat prevention service provide file-blocking and analysis capabilities?
🛡		Threat prevention services should provide features that keep data from leaving the network. **Evaluate:** • Does the threat prevention service support DNS monitoring and redirection to an administrator-specified site? • Does the threat prevention service flag on traffic destined to known malicious domains?

The above should be taken into consideration when choosing threat prevention services to add on to your firewall platform procurement within AWS.

Making the Choice

A simple Analysis of Alternatives (AoA) will allow your organization to objectively compare the products available in AWS Marketplace against one another and against the native AWS firewall service. An AoA consists of multiple steps that include:

1. Review this guide and identify your organization's specific requirements.
2. Weigh the requirements according to the importance to your organization. For example, weigh critical requirements as "high" and desired requirements as "low." Cost should also be considered as a factor in the evaluation.
3. Review the capabilities of the native AWS firewall.
4. Compile a list of vendor firewall/threat prevention offerings from AWS Marketplace.
5. Evaluate each firewall/threat prevention offering against selected requirements.
6. Score each of the products against each requirement.
7. Calculate the sum score for each offering and select the product with the highest score.

Organizations can also opt to contract through AWS Marketplace CPPO to perform this analysis of alternatives. Choosing this approach is often optimal based on the level of expertise available through these partner organizations.

Conclusion

Options for cloud-based firewalls for use in an AWS deployment include native AWS offerings and third-party products offered in AWS Marketplace. An analysis of the available options based on the considerations in this paper will allow for the selection of a firewall that meets the unique requirements of any organization. Critical considerations when choosing firewall and threat prevention capabilities include the abilities to separate trusted and untrusted zones, evaluate encrypted traffic, perform behavioral analysis, operate across hybrid environments and integrate directly with AWS services. To perform this analysis, identify firewall and threat prevention options available today in AWS Marketplace and evaluate each against the criteria in this paper.

Performing a formal analysis of alternatives will support an objective determination of the best technology solution. Alternatively, organizations can reach out to trusted third-party Consulting Partners to customize a firewall and threat prevention approach for security within the cloud. Visit the AWS Security Competency Partners page[3] for more information.

About the Author

Brian Russell is the Chair of the Cloud Security Alliance (CSA) Internet of Things (IoT) Working Group and founder at TrustThink, LLC where he leads security engineering for autonomous vehicles and smart devices. He was previously Chief Engineer for Cyber Security Solutions at Leidos - a Fortune 500 Government Contractor. In that role he led Research and Development (R&D) for secure cloud systems, permissioned blockchain networks, and cryptographic key management. Brian is an adjunct professor with the University of San Diego (USD) in the graduate Cyber Security Operations and Leadership Program and co-author of the book Practical Internet of Things Security.

Sponsor

SANS would like to thank this paper's sponsor:

aws marketplace

in conjunction with

OPTIV

About Optiv

Optiv is a market-leading provider of end-to-end cybersecurity solutions. Optiv helps clients plan, build and run successful cybersecurity programs that achieve business objectives through our depth and breadth of cybersecurity offerings, extensive capabilities and proven expertise in cybersecurity strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers.

RETURN TO THE
TABLE OF CONTENTS

A SANS Whitepaper

How to Protect Enterprise Systems with Cloud-Based Firewalls

Written by **Kevin Garvey**

July 2019

Sponsored by:

AWS Marketplace

Webcast

You can access the associated webcast at:
https://pages.awscloud.com/Enterprise_Cloud-Based_Firewalls.html

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.

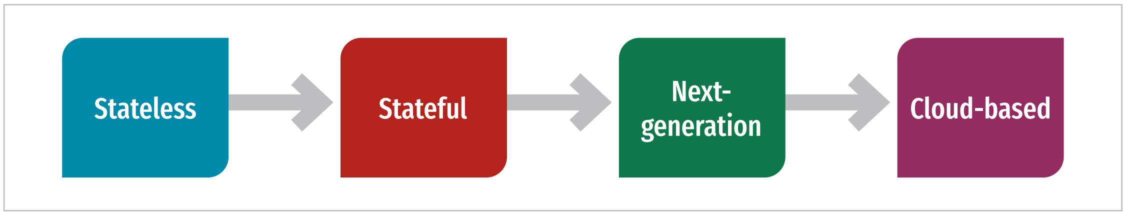

Figure 1. Evolution of Firewalls

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.

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.

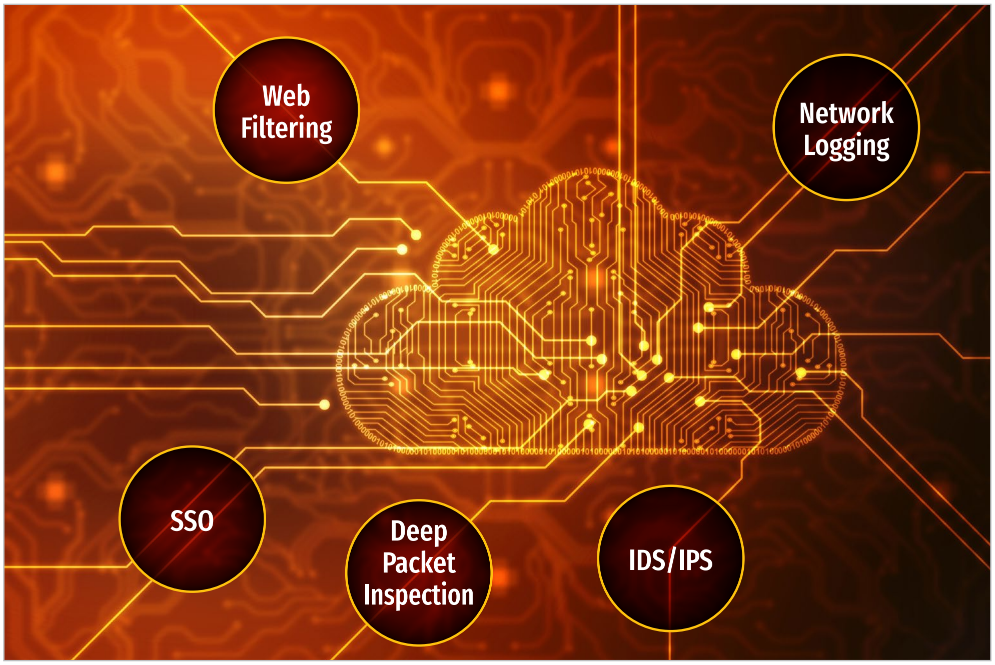

Figure 2. Features of Cloud-Based Firewalls

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.

> *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.*

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.

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.

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

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.

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.

Deep Packet Inspection

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.

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.

[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.

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.

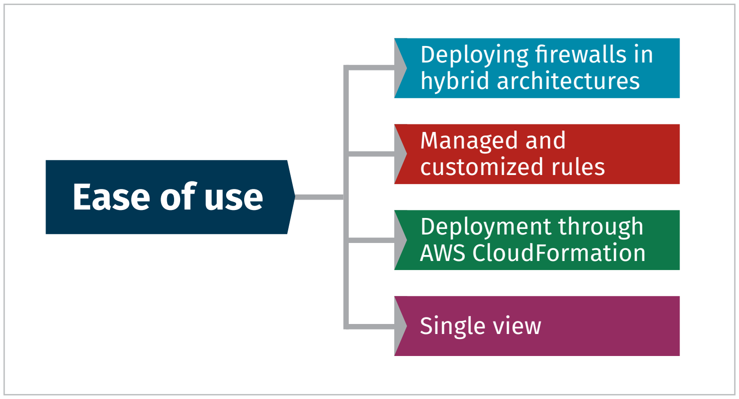
Ease of use
Deploying firewalls in hybrid architectures
Managed and customized rules
Deployment through AWS CloudFormation
Single view

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.

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.

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 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

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:

aws marketplace

RETURN TO THE
TABLE OF CONTENTS

Next Steps

By applying the guidelines in the preceding whitepapers, you have been able to:

- Justify the need for firewall services to protect cloud-based applications
- Understand the different types of firewalls and their capabilities
- Document the key considerations that drive the overall perimeter security architecture and selection of firewall products and services
- Deploy an integrated and manageable network of firewalls

The capabilities of infrastructure-as-a-service (IaaS) have enabled businesses and development organizations to move applications and services to market faster. Attackers are also using the same power of the cloud to morph their assaults faster. Security organizations need to also take advantage of the strengths of cloud computing to move at the same speed and to make advances in raising the bar against increasingly sophisticated attacks.

Your cloud-based firewall strategy needs to evolve as well:

- Movement to DevOps and CI/CD pipeline approaches will drive the need for more frequent firewall policy assessment, but can also enable the integration to have firewall policies embedded in standard workloads and cloud infrastructure configurations.
- More advanced behavioral-based rules can be added to increase the level of protection by both blocking more and more quickly identifying potential anomalous behavior.
- Firewall management tools that work across cloud-based and on-premises firewalls should be investigated to reduce the time required to assess requested changes, as well as reduce administrative requirements of managing large numbers of firewall implementations.

A "crunchy exterior" is never the final security solution, but it is always a necessary component. An aggressive and well-managed cloud-based firewall architecture can enable digital business while greatly reducing the risk of business downtime.

RETURN TO THE
TABLE OF CONTENTS