SANS

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

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

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.

of action for organizations considering the purchase of cloud-based firewalls. Before we begin, Table 1 provides definitions of key firewall-related terms.

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]

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

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

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

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.

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

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.

Technical Considerations (continued)

	Consideration	Details
	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.

Cloud-Based Firewalls (continued)

	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?
	AWS security competency approval	AWS security competencies for infrastructure security products provide a degree of confidence that the firewall meets minimum security standards for operation within AWS. **Evaluate:** • Does the firewall have AWS security competency approval? • Does the firewall meet other security standards and best practices?
	Application control	Firewalls should provide administrators with the capability to set policy based on the organization's specific needs. This capability includes filtering on approved applications and nesting policy within security groups. **Evaluate:** • Does the firewall support filtering based on app ID to permit only approved applications within the network? • Does the firewall support dynamic application filters and application groups that restrict the types of applications authorized on the network? • Does the firewall support dynamic profiling, allowing the firewall to learn the typical behavior of the application over time?

Cloud-Based Firewalls (continued)

	Consideration	Details
	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.

Threat Prevention (continued)

	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.

[3] AWS Security Competency Partners, https://aws.amazon.com/security/partner-solutions

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.