Migrating to Microsoft Azure with the Barracuda CloudGen WAF

Protecting Web Applications, securing Cloud Services and Data

White Paper

Summary / Abstract

The Internet is a breeding ground for a limitless array of cybercrimes, making a shift to cloud computing seem untenable. Deploying appropriate security measures within your virtual environment can help fill the gap between traditional on-premises protection and the native capabilities in your chosen cloud platform. The Barracuda CloudGen WAF virtual appliance, running in your Microsoft Azure subscription, provides the highest levels of application and data protection with comprehensive application-layer protection backed by security feeds from Barracuda Central, the threat analysis network.

Contents

Introduction

Enterprise cloud services are under greater and more persistent threats than average corporate data centers. This is due in part to the value they contain—not only your data, but the data of millions of other customers just like you—and partly because cloud workloads' highly variable natures makes it more difficult to filter out known-bad traffic. For example, if your high-volume sales application suddenly experiences an activity spike because of a holiday special, how would the platform differentiate between this legitimate traffic and a DDoS attack?.

When you deploy application security or intrusion prevention in an on-premises data center, you can tune it to understand your unique business. Hardware-based application firewalls and intrusion prevention systems can be customized for each application to filter out threats and block exploits of known vulnerabilities. However, since a public cloud environment shares infrastructure across more than one customer on the same physical network, it is not possible to deploy these kinds of security appliances and still tailor each configuration per customer.

The cloud platform can really only protect its own infrastructure; going any deeper would require the service to have a more thorough knowledge of your applications and data, potentially violating your information privacy and integrity mandates.

The question is, "Who is responsible for protecting my data?" The answer is, ultimately, "You are." When you select a cloud provider, you are agreeing to manage specific risks associated with hosting information externally. The applications and data resources that you place in the cloud will be exposed to a constant barrage of attacks, and you must mitigate these threats in a way commensurate with the value of your resources.

Cloud services such as Microsoft Azure deliver technology, operations, and processes that form a secure and compliant foundation for you to build advanced solutions. But while Microsoft bears the responsibility to protect the infrastructure, service offerings (such as Azure Storage or Active Directory), and platform components, customers must take steps to protect their own assets.

The Barracuda CloudGen WAF virtual appliance is an HTTP-aware reverse proxy. It's capable of bi-directional content inspection to provide security from inbound application-layer attacks such as SQL injection, cross-site scripting (XSS) and cross-site request forgery (CSRF), as well as enforcing data leak prevention policies on outbound data.

Data and Application Security

Data security can be thought of like a message in a bottle. The bottle itself can be sturdy and opaque, but if you are able to break it then the message is exposed. To better protect that message, various types of encryption and access control can be applied at points of ingress and egress from the storage environment, as well as protection for data in various states within the infrastructure (specifically, data in-transit, in-use, and at-rest). For example, write the message in a code that only your intended recipient can decipher.

Application security, on the other hand, is a little more like a charcoal filter where various sizes of mesh and carbon particles remove contaminates while the water (data) flows through it unimpeded. If the filter is too dense, the data (and transactions) can't get through efficiently; if it's too loose, and all kinds of unwanted elements come with it. The charcoal functions as an operator that can make the water clean by peaking inside the bottles as they flow by, ensuring that foreign bodies aren't along for the ride.

Exploits

Applications expose more than just a web page to a would-be attacker. Your applications define how your business operates and what kind of information you gather and store; they can divulge sensitive intellectual property that you didn't think was even connected. Just as applications have multiple tiers, so too, do the attacks upon them.

The seven layers of the Open Systems Interconnect (OSI) model can be used to map the range of (volume-based) network stack threats to application attacks. These can range from the common OWASP Top-10 threats to sophisticated, blended attacks coordinated by multiple foreign hosts, as shown in Table 1.

	TYPE	LAYER	NAME	FUNCTIONS	EXAMPLE THREATS
HOST	Data	**7**	Application	User and application access point to network services	Cross-site scripting, HTTP Flood, Slow Post/Get
		6	Presentation	Data formatting and translation	Trojan horses, viruses, Slowloris, XML DTD
		5	Session	Establishes sessions between processes running on different machines	Cookie tampering, hijacking, SSL re-negotiation
	Segments	**4**	Transport	Manages error correction, sequencing	HTTP, TCP exploits
MEDIA	Packet	**3**	Network	Controls subnet operation and physical routing	SYN flooding, ping attacks
	Frame	**2**	Data Link	Data frame transfer between physical nodes	ARP, MAC flooding
	Bit	**1**	Physical	Transmission and reception of raw bit stream	Physical port access

Table 1: Mapping threats to network layers.

These examples don't necessarily represent the many ways by which improperly designed or implemented applications leave their operators open to exploit. Some further examples include poor key security, using unencrypted sessions, and inadequate input validation.

In the cloud, such as Azure, built-in security features include virtual machine and host-level firewalls, anti-malware scanning, virtual network isolation, IP address access control lists (ACLs), and packet filtering that help protect the fundamental physical media connection. Some Layer 4 functionality (such as IPsec and SSL/TLS encryption) is also provided by Azure infrastructure for securing cloud communications and tunneled connections. Azure data centers are protected by network security mechanisms that include intrusion detection and prevention systems.

However, when it comes to specific customer application traffic, Azure does not differentiate between legitimate versus malicious intent; by definition, Azure must not interfere with any customer's unique needs. Thus, it is still possible to deploy an application that is not secure, even if the underlying infrastructure is configured properly. Your applications and data are susceptible to network exploits if proper safeguards are not in place.

Application Security Requirements

The goal in any corporate data center is to design web-facing applications to be secure, resilient, and robust by default. In many companies today, however, development resources are usually stretched thin, time is short, and applications may be deployed before sufficient testing and security hardening has been performed. Because these pressing needs of the business can introduce a higher degree of data risk, many organizations deploy intelligent web security, such as a CloudGen WAF appliance that can detect and remediate HTTP and other threats.

In the rush to Cloud IT, applications may be treated the same way. Hosted web services are deployed, internal applications are migrated to the cloud, and data could be exposed before IT groups thoroughly understand the risks and impacts such a move can have. The added challenge is that the cloud it is not in your data center, so deploying a wire-line security appliance to protect your applications and data is not an option.

To achieve a similar level of security for a physical device, you need to take advantage of one of the cloud's defining characteristics—its ability to run almost any software workload. Security functionality, much like any other software that runs on a general-purpose platform and operating system, can be virtualized for greater deployment flexibility.

Barracuda CloudGen WAF

Barracuda CloudGen WAF provides the dedicated protection that internet-facing applications need, tailored for cloud-deployed applications in Azure Virtual Machines. A WAF Virtual Machine inspects inbound and outbound web traffic to your Azure Virtual Network, and blocks SQL injections, Cross-Site Scripting, malware uploads and application DDoS, or other attacks targeted at your web applications.

Deploying the Barracuda WAF in an Azure Virtual Network protects not only Internet-facing applications, but provides an additional layer of security for back-end application tiers such as data storage (e.g., SQL Server) and middleware. A dedicated WAF VM can be configured in a Virtual Network and positioned in-line with application services to extend the same kind of security you have in your on-premises data center to your cloud environment.

WAF offers strong authentication and user access control capabilities that ensure security and privacy by restricting access to sensitive applications or data to authorized users. Integrated Identity Access and Management capabilities that link to Azure Active Directory pre-authenticates on the VNET perimeter before access is allowed to critical web applications. User Access Control can be offloaded from multiple applications on a single consolidated virtual device, where detailed audit logging provides clear visibility into user activity across all protected applications.

To help protect data stored in the cloud and defend against theft, the Barracuda CloudGen WAF provides Data Loss Prevention (DLP) by inspecting responses from back-end web servers for sensitive data, allowing administrators to either mask or block the information.

For large virtual environments, administrators can deploy multiple WAF VMs to Azure without the elevated costs of additional hardware or network infrastructure. The onboard L4/L7 Load Balancing capabilities enable organizations to quickly add back-end servers to scale deployments as they grow. The WAF's application acceleration capabilities, including SSL Offloading, caching, compression, and connection pooling, ensure faster delivery of web application content.

Case 1—Protecting Web Applications

Websites are vulnerable to modern threats—such as polymorphic and blended attacks—whether or not they are hosted in the cloud. But the ease with which new sites can be created in the cloud (in other words, new rogue servers without concerns for available capacity, support budget, etc.) makes them an even bigger threat to corporate data governance.

Thus, it is critical to keep protection closer to the resources that need it: deploying cloud-based security for applications means you can protect assets in a variety of topologies and locations. The Barracuda WAF makes this possible through easy-to-deploy, pre-configured virtual appliances in the Azure Gallery. Not only can you deploy one or more WAF's at the perimeter of your subscription's Virtual Network to handle varying amounts of application traffic, but any other websites or applications launched within the subscription can also be routed to the same gateway.

If you need an application environment that is more isolated from your main cloud deployment, it is easy to provision another WAF VHD to protect it. Indeed, the range of Internet threats that a web application firewall can deal with makes it a must-have in any deployment:

- Advanced DDoS protection capabilities allow administrators to distinguish real users from botnets through the use of heuristic fingerprinting and IP reputation, thereby allowing them to block, throttle, or challenge suspicious traffic.
- Adaptive profiling enables administrators to build positive security profiles of their applications by sampling web traffic from trusted hosts. Once enabled, the positive security profiles allow administrators to enforce granular whitelist rules on sensitive parts of the application.
- Often the first step of any targeted attack is to probe public-facing applications to find out details about the underlying servers, databases, and operating systems. Cloaking prevents attack reconnaissance of protected applications by suppressing server banners, error messages, HTTP headers, return codes, debug information, or backend IP addresses from leaking to a potential attacker.
- Applications that rely on XML can now be secured with an XML Firewall capability that secures applications against schema and WSDL poisoning, highly-nested elements, recursive parsing, and other XML-based attacks.
- Attacks on a web-based application often start by analyzing and tampering with its URLs. WAF comes with a unique URL Encryption feature that allows administrators to encrypt URLs before they are sent to clients. The original URLs or the directory structure are never exposed externally to prying eyes.
- Barracuda has the ability to integrate with popular scanners including IBM AppScan and Cenzic Hailstorm to automatically configure an application's security template to protect against identified issues.
- The Barracuda CloudGen WAF has a built-in load balancer that can route traffic among backend servers to prevent latency from server congestion. Sophisticated application monitors can detect server issues and remove them from the server pool while redistributing traffic to the remaining servers.

Case 2—Securing Cloud Services and Data

Managing IT and data risk in the cloud is the same as in your corporate datacenter: know who is doing what, where, and when, and enforce controls to prevent either accidental or intentional disclosure of information. So while cloud services offer an easy, scalable solution that alleviates a great deal of the overhead associated with application and infrastructure management, they must still be treated with the same scrutiny—even if the cloud platform itself is secure and compliant.

In particular, when sensitive data is manipulated or stored in the cloud, such as with healthcare or government services, industry regulations such as HIPAA and FISMA require that both cloud providers and customers prove that they can wield such data without loss or compromise. Part of meeting these compliance standards includes rigorous control of application and data access through auditable mechanisms that can be used for reporting on and enforcement of information security policies.

For cloud services, access control extends to granular authentication and content filtering to both prevent unauthorized user access and monitor and log appropriate usage.

- Deployed as a reverse-proxy, the WAF inspects all inbound traffic for attacks and outbound traffic for sensitive data. Content such as credit card numbers, U.S. social security numbers, or any other custom patterns can be identified and either blocked or masked without administrator intervention.
- The WAF fully integrates Active Directory or any other RADIUS or LDAP-compatible authentication services. Combined with the strong access control capabilities, administrators can provide granular control over which users or groups are able to access specific resources.
- The WAF integrates with a number of two-factor authentication technology including client certificates, SMS PASSCODES, and hardware tokens such as RSA SecurID to provide strong user authentication.
- Using client source addresses, organizations can control access to web resources. The Barracuda WAF can control access, based on GeoIP to limit access only to specified regions. It is also integrated with the Barracuda Reputational Database and can identify suspicious IP addresses, bots, TOR networks and other anonymous proxies that are often used by attackers to hide their identity and location.
- The Barracuda WAF maintains a complete set of web firewall, access, audit, and system logs. All logs can be exported to third-party SIEM or log management tools for deep analysis. The Barracuda CloudGen WAF integrates with HP ArcSight, RSA Envision, Splunk, and many other SIEM tools out of the box, providing instant intelligence on an application's security posture.
- The WAF provides alert consolidation and correlation. Custom notifications can be defined using multiple elements such as severity, attack type, application, threshold and frequency (for example, configuring thresholds for SQL Injection frequency on application X and also monitoring forceful browsing for the same application).

Case 3—Migrating to the Cloud

Having the confidence to extend your data center to the cloud means being able to demonstrate not only the security of online systems, but resiliency as well. Additionally, a hybrid-IT environment where applications and data span both physical and virtual infrastructure requires automation of critical maintenance tasks and simplified visibility into configuration details.

Azure is designed to let customers scale their cloud infrastructure to meet changing business needs, and to provide a highly available platform on which to deploy cloud services. The Barracuda WAF syncs and works seamlessly with Azure's native functionality and capabilities.

- Barracuda WAF features security templates that provide the ability to define baseline security settings to use as a model for security policies. By using templates, you can quickly create security policies designed to safeguard a specific application, web-portal, platform, framework or parts thereof.
- Powerful graphical reporting provides immediate insight into compliance, threat activity, web traffic and regulatory compliance. More than 50 different pre-defined reports are available, which can be easily customized further, using numerous filters for attack types, traffic, time range, and more.
- WAF comes with a REST API that enables you to configure and monitor the appliance programmatically. The functionality of the device is exposed in Representational State Transfer compliant interfaces that can be exercised via any programming language of your choice
- The WAF is augmented by an extensive network of more than 150,000 sensors that are deployed worldwide and feed into Barracuda Labs. The sensors provide valuable data used by Barracuda Labs to create the latest threat detection and protection definitions.
- WAF virtual appliances can be clustered in active / passive or active / active pairs with failover to ensure instant recovery. Security configurations and deployments are automatically synchronized between the clusters, providing instant recovery from any outages.

Summary

Enabling data governance in the cloud is a mix of policies, processes, and technologies. Implementing application and data security in a way that extends your existing mechanisms for attack prevention can help streamline not only your ongoing management, but your compliance efforts, as well.

Administrators need to safely manage both corporate and customer information—locally and in the cloud—while addressing privacy and security directives in their industries. By integrating the proven application security and data loss prevention capabilities of Barracuda CloudGen WAF with Microsoft Azure's native security features, administrators are in a superior position to deploy secure, reliable, and resilient cloud services in Azure while meeting any regulatory or compliance needs. To find out more about the Barracuda CloudGen WAF for Microsoft Azure, visit us in the Microsoft Azure gallery, download the WAF on Azure whitepaper or visit the Barracuda TechLibrary.

If your business depends on sharing information with customers and partners, which most online companies do, then protecting that information is a critical component. Web application firewalls in the cloud put protection where it is most relevant—near to the resources being shared.

About Barracuda Networks, Inc.

Barracuda simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications, and data regardless of where they reside. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide, and are delivered in appliance, virtual appliance, cloud, and hybrid configurations. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network security and data protection. For additional information, please visit barracuda.com.

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com