Barracuda Solutions for Microsoft Azure

Barracuda

Microsoft Azure Certified

Securing Your Move to Microsoft Azure

Businesses in diverse industries are moving their computing operations to the cloud at an accelerating pace. According to a recent Gartner report, the bulk of new IT spending by 2016 will be on cloud computing, and by 2017, nearly half of large enterprises will have hybrid cloud deployments using cloud providers such as Microsoft Azure.

Increasingly, organizations are migrating on-premises applications and data to the cloud to achieve agility, efficiency, and cost— effectiveness. But moving applications to the cloud also createsa new attack surface that exposes new vulnerabilities.

With respect to cloud computing, IT managers want to ensure that their virtual networks are secure, that sensitive data is protected, and that compliance requirements are met, particularly because data and applications now reside beyond the reach of customary IT security measures—in data centers not under their direct ownership and control.

In this chapter, we look at some of the new vulnerabilities brought about by moving applications and data to the cloud. Whether public, private, community, or hybrid cloud deployments, the architecture used to deliver cloud services brings additional complexities to network security.

Like on-premises data centers, the cloud-computing environment must be protected from threats. Cloud security solutions must be aware of the evolving threat landscape and how to effectively secure against new attacks. Attackers typically mount broadbased attacks using a threat vector—a pathway, such as email or web application, through which they can gain access to a computer or network server to deliver a malicious payload.

Attackers subvert web applications to circulate infected links, and avoid security defenses through techniques such as proxies, firewall circumventors, infiltration of nonstandard ports, and tunneling. These techniques enable threats to run covertly on

networks and systems, quietly collecting sensitive or personal data, and going undetected as long as possible. This approach enables repeated use of the same exploits and threat vectors, including the ability to cross the security perimeter repeatedly.

Although IT administrators are aware of strategies to mitigate threats to on-premises assets, cloud computing presents a new attack surface along with new vulnerabilities. For example, web applications in the cloud create a new attack surface with multiple attack points, such as transactional interfaces and interfaces with other applications.

Many threats to a physical data center are present in a cloud deployment. Thus, as data and applications move to the cloud, IT administrators must concern themselves with familiar issues such as identity, network and access control, data protection, and endpoint security. As companies move their operations to the public cloud and start using SaaS applications, their attack surfaces change. For example, companies that migrate from an on-site Microsoft Exchange Server to Office 365 have added a new attack surface for threat vectors, including email and web applications.

Administrative and application access by cloud subscribers across the Internet and exposed public interfaces increases the threat of automated attacks. Combined with the new trend of an anytime/anywhere/any device workplace, IT must confront a new magnitude of vulnerabilities to all threat vectors. Mobile Internet is particularly vulnerable to social engineering attacks, and mobile devices that frequently move between secure corporate networks and unsecure home or public networks present another exposed target of malicious exploits. IT administrators must expect that any exposed vectors are subject to attack.

The web application vector is misunderstood by most IT administrators and is often the most exposed. Many companies attempt to secure this threat vector using network firewall technologies that are not adequate. Just as a conventional network firewall is not intended to stop spam, it's also not designed to stop web application attacks. This misunderstanding leaves the threat vector exposed to attack, and leaves the administrator with a false sense of security.

Summary

To effectively secure a cloud environment requires a multi-pronged approach. It requires an understanding of the allowed applications in the cloud environment to reduce the scope of attack, followed by an integrated threat protection system that can address multiple threat vectors to control known and unknown threats.

As they move their operations to the cloud, businesses require a next generation of protection. The following chapters explain how Barracuda Network's security solutions have all the right elements to help protect against both existing and future threats in the cloud environment.

Barracuda

Microsoft Azure Certified

NG

Barracuda
NextGen Firewalls

Securing Microsoft Azure with Barracuda NextGen Firewall

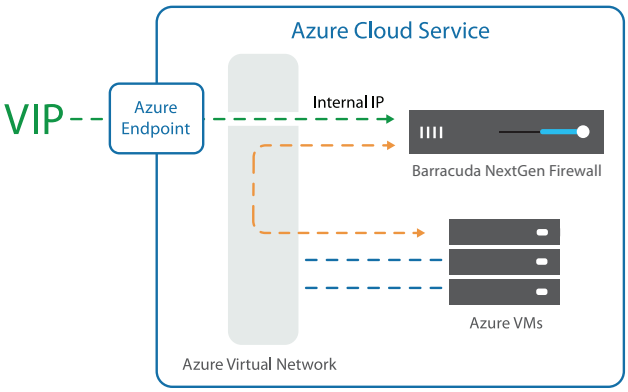
More businesses are deploying applications on cloud platforms in order to take advantage of the economics of scalability, elasticity, and more efficient data storage, backup, and recovery. Hybrid cloud scenarios are increasingly popular. Applications that span both on-premises and the cloud offer organizations the advantages of using secure on-premises infrastructure, while accommodating demand spikes with thev elastic resources and services within the public cloud.

This chapter explains how businesses can deploy the Barracuda NextGen Firewalls—fully functional cloudenables network perimeter firewalls—within the framework of their Microsoft Azure environments. We explain fully functional cloud-enables network perimeter firewalls secure your network perimeter in a hybrid environment.

IT organizations protect their on-premises infrastructure with multiple security layers, the so-called defense-indepth approach. In the cloud, they must strategically supplement the cloud provider's native security features with layered cloud-based security.

The defense-in-depth approach requires using more than one type of security measure in the data path. For example, on-premises servers are protected by anti-malware, antispam, and firewalls. Cloud deployments require comparable security provisions, but protections must be implemented to bridge on-premises systems and the cloud data center.

Deploying the Barracuda NextGen Firewalls in the cloud is very similar to running local network firewalls. It offers common policy enforcement and distributed security management in a hybrid-cloud scenario, and secure remote access to Microsoft Azure. It enables organizations to deploy multi-zone networks in Microsoft Azure, similar to ones deployed in on-premises networks.

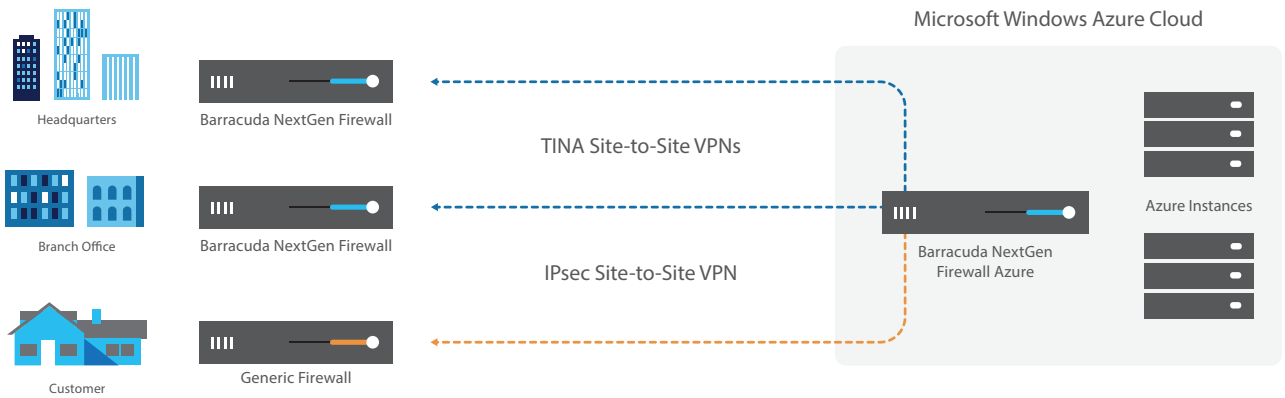


Barracuda NextGen Firewalls go beyond cloud infrastructure security to help implement a defense-in-depth strategy, providing protection where the application and data reside on Microsoft Azure rather than only at the network connection point. By integrating a secure gateway into the Microsoft Azure virtual network, Barracuda NextGen Firewalls create a network security interface where the Azure endpoints meet a customer's virtual machines.

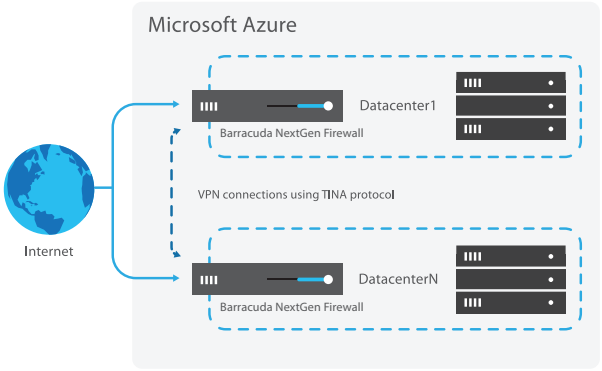
While some organizations are building out greenfield cloud deployments, many businesses are migrating solutions to the cloud from their existing data centers, or supplementing on-premises systems with cloud deployments to take advantage of cloud scalability. These hybrid scenarios require secure connectivity between Microsoft Azure and the on-premises infrastructure. Microsoft Azure provides services for creating secure site-to-site and client-to-site VPN connections. Barracuda NextGen Firewalls offer granular user policies that many IT organizations expect from their hardware-based firewall devices.

Barracuda NextGen Firewalls provide fully integrated VPN capabilities that route traffic securely between virtual and physical sites. By using a proprietary high-performance VPN protocol extension (TINA), Barracuda NextGen Firewalls enable secure high-speed site-to-site and client-to-site connectivity between on-premises networks and virtual networks in Microsoft Azure, enabling better data transfer and WAN optimization in a hybrid cloud scenario.

Barracuda NextGen Firewalls also isolates cloud workloads, separating cloud application users from corporate user accounts if necessary, and distinguishes cloud usage from on-premises policies to enforce cloud resource usage.



Even encrypted content transmitted over VPN—whether by secure sockets layer (SSL) or transport layer security (TLS)—can present a security threat because it's assumed to be safe traffic and is therefore not monitored. Barracuda NextGen Firewalls, however, terminate SSL/TLS sessions and IPsec tunnels so that policy application, malware scanning, confidentiality enforcement, and other firewall protections are applied to all data regardless of the source or destination.



User identity screening is not only essential for access control, but for enforcing a content usage policy. Organizations must implement their own access control measures to maintain the confidentiality of applications and data residing in the cloud.

The Barracuda NextGen Control Center acts as a centralized management point across many different firewalls and remote access users, enabling administrators to configure security and network access policies, control firmware update revisions, and manage user settings.

This intuitive centralized management portal simplifies configuring, updating, and managing multiple cloud deployments from a single location, while also providing comprehensive, real-time network visibility and reporting.

Securing applications and data in Microsoft Azure is more efficient and cost-effective when businesses employ dedicated tools designed for a comprehensive security solution. Barracuda NextGen Firewalls offer secure remote access, cross-premises connectivity, and granular security and policy management, combining on-premises Barracuda NextGen Firewall data center network protection with cloud IT security needs.

Barracuda

Microsoft Azure Certified

WAF

Barracuda
Web Application Firewall

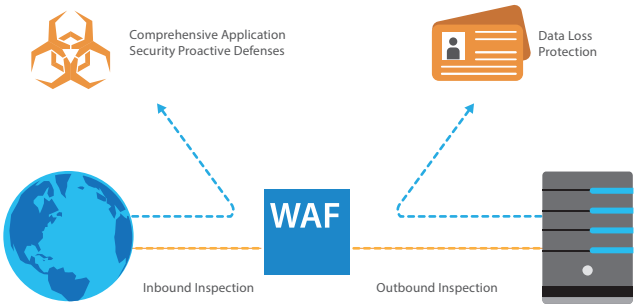
Securing Web Applications in Microsoft Azure with Barracuda Web Application Firewall

Businesses are increasingly relocating on-premises applications to the cloud. But moving applications out from behind the corporate web application firewall raises security concerns. Cloud-based applications offer convenience to end users, but they are also more vulnerable to attackers, who may use them as gateways into corporate networks.

Although moving applications to the cloud offers the benefits of flexibility, cost savings, and scalability, organizations must understand the difference between implementing effective on - premises and cloud-based data security protections. In this chapter, we discuss how the Barracuda Web Application Firewall can help organizations address this issue.

The Barracuda Web Application Firewall for Microsoft Azure is the first integrated, fully scalable virtual security solution available on the Microsoft Azure Marketplace. It monitors inbound and outbound web traffic to the Microsoft Azure Virtual Network. As a reverse-proxy, it inspects all inbound traffic for attacks such as SQL injections, cross-site scripting, malware uploads, and application DDoS to secure your cloud-hosted websites. It also inspects outbound traffic for sensitive data. Content such as credit card numbers, U.S. social security numbers, or any other custom patterns can be identified by the Barracuda Web Application Firewall and either blocked or masked without administrator intervention.

Microsoft Azure offers a new platform to quickly deploy SharePoint server farms and reduce the infrastructure costs associated with onpremises deployments. But moving SharePoint to Microsoft Azure also presents new security vulnerabilities, such as unauthorized access. Barracuda Web Application Firewall provides authentication and user access control that ensures security by restricting



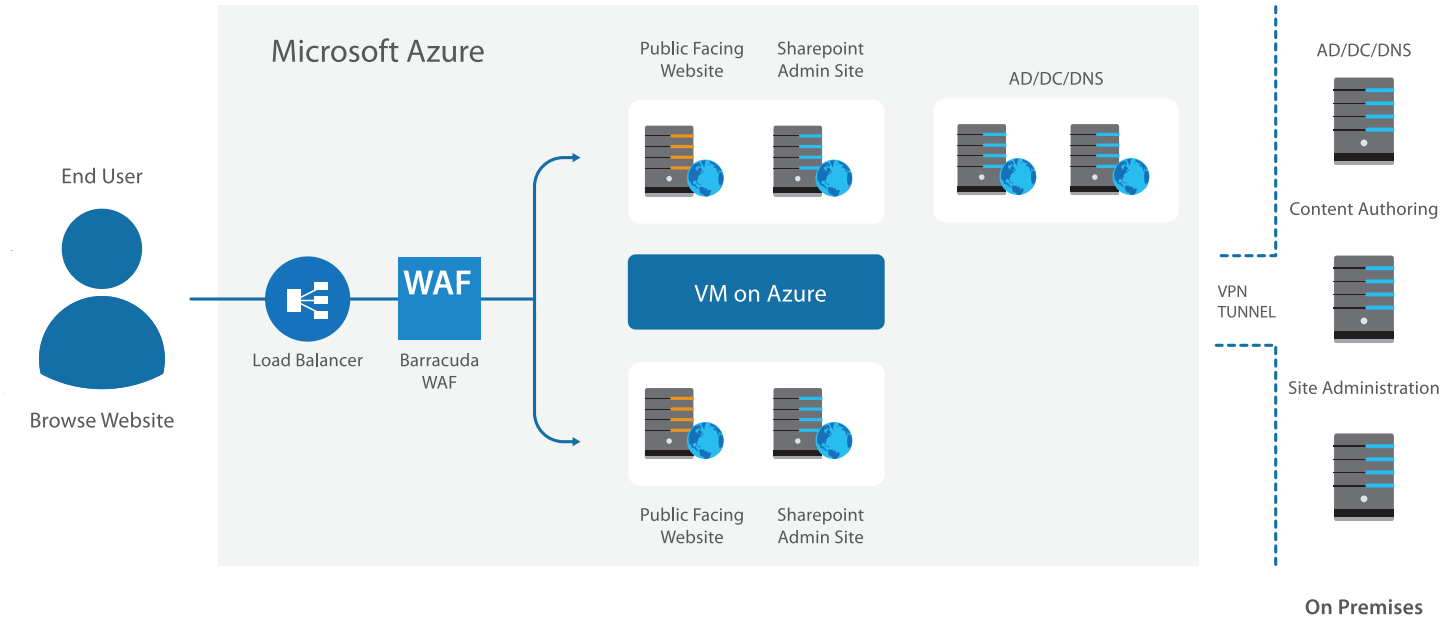
Barracuda Web Application Firewall

SharePoint access to authorized users. Its integrated identity access and management (IAM) functionality pre-authenticates traffic on the virtual network perimeter before allowing access to critical web applications. It can consolidate user access control (UAC) from multiple web applications, and with detailed logging capabilities, can provide visibility into user activity across all protected applications. This gives administrators granular control over the users or groups who are permitted to access specific resources.

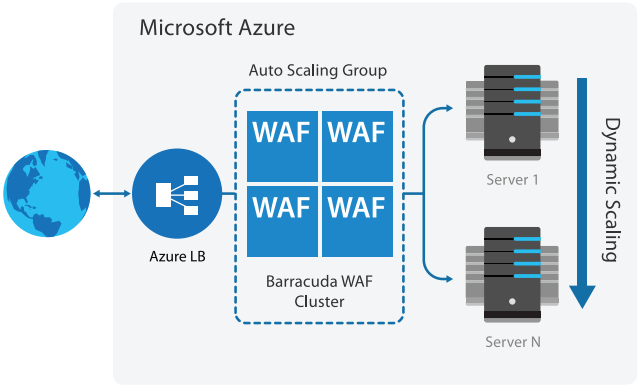
While the Barracuda Web Application Firewall in Microsoft Azure protects Internet-facing applications, it also helps secure middleware and data storage (ex. SQL Server) layers. System administrators can configure a dedicated Barracuda Web Application Firewall and position it in-line with application services to secure their cloud-based web applications.

For large distributed environments, administrators can deploy multiple Barracuda Web Application Firewalls in Microsoft Azure without assuming additional hardware or network infrastructure costs. Barracuda Web Application Firewall L4/L7 load balancing capabilities enable organizations to route traffic among backend servers to prevent latency from server congestion, and add back-end servers to scale deployments as required. Barracuda Web Application Firewall application acceleration capabilities, including SSL offloading, caching, compression, and connection pooling, help speed delivery of web application content.

Proactive system administrators monitor and analyze potential security threats on an ongoing basis. By using the Barracuda Web Application Firewall alert consolidation and correlation capabilities, administrators can define custom notifications by severity, attack type, application, threshold and frequency. This helps ensure that threat activity does not get overlooked, thus lowering your risk profile and operational costs. Administrators also benefit from the management tools that help smooth



deployments into existing environments while providing granular logging, alerting, and reporting for management, compliance, or early warning detection. Pre-built security templates and an intuitive web interface provide immediate security without necessitating time-consuming tuning or learning.



The Barracuda Web Application Firewall running in a Microsoft Azure subscription provides the highest levels of application and data protection with comprehensive application-layer protection backed by security feeds from Barracuda Central. This threat analysis network tracks emerging threats and enables Barracuda Web Application Firewall to block them. Having secured thousands of production applications against more than 11 billion attacks since 2008, the Barracuda Web Application Firewall is the ideal solution for organizations looking to protect web applications from data breaches and defacement.User identity screening is not only essential for access control, but for enforcing a content usage policy. Organizations must implement their own access control measures to maintain the confidentiality of applications and data residing in the cloud. The Barracuda NextGen Control Center acts as a centralized management point across many different firewalls and remote access users, enabling administrators to configure security and network access policies, control firmware update revisions, and manage user settings.

This intuitive centralized management portal simplifies configuring, updating, and managing multiple cloud deployments from a single location, while also providing comprehensive, real-time network visibility and reporting.

Securing applications and data in Microsoft Azure is more efficient and cost-effective when businesses employ dedicated tools designed for a comprehensive security solution. The Barracuda NextGen Firewall offers secure remote access, cross-premises connectivity, and granular security and policy management, combining on-premises data center network protection with cloud IT security needs.

Barracuda

Microsoft Azure Certified

ESG

Barracuda
Email Security Gateway

Securing Email in Microsoft Azure with Barracuda Email Security Gateway

Email remains the most common form of communication in the business world. According to the Radicati Group, a market research firm in Palo Alto, California, worldwide business email traffic will reach 116 billion messages per day in 2015. The same source estimates that of the 88 emails the average business user receives daily, 13% will be spam. Spam is no longer a minor annoyance, it's an ongoing threat that saps worker productivity and depletes business financial resources.

Today, an increasing number of businesses are moving to cloud-based email services, such as Microsoft Office 365. According to the Radicati Group, Microsoft Office 365 will represent 43 percent of business mailboxes by 2018.

Microsoft takes spam control seriously. Each day, Office 365 blocks an average of 10 million spam emails per minute—over 14 billion blocked messages per day. However, even with this level of protection, businesses are still vulnerable to malicious attacks such as spear phishing.

Spear phishing is designed to infiltrate the business networks of a targeted company. Attackers send cleverly crafted emails to specific individuals in an organization. Social engineering tactics can convince recipients to either download a malicious file attachment, or click a link to a malware-infected site, compromising the credentials of the company employee. For example, in 2011, the security firm RSA suffered a breach that began when an employee opened an attachment to a

spear phishing email. That same year, email service provider Epsilon was a victim of a spear phishing attack that caused the organization to lose an estimated four billion U.S. dollars.

As email attacks become more sophisticated and complex, email infrastructure requires advanced protection. In this chapter we look at how the Barracuda Email Security Gateway complements the Office 365 protection service to provide administrators with advanced email security and management for cloud-based email infrastructure.

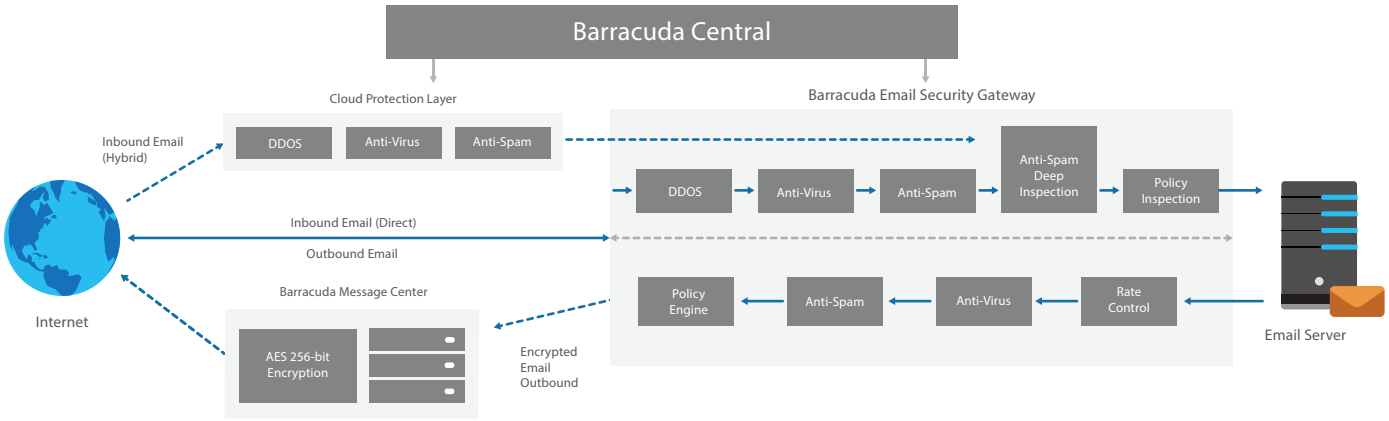
Given the ever-evolving threat landscape, along with the increasing sophistication of attacks, businesses must consider adopting the most advanced and comprehensive email protection
strategy available: the Barracuda Email Security Gateway.

The Barracuda Email Security Gateway provides comprehensive email security, including advanced spam and virus blocking, data protection, DDoS prevention, email continuity, encryption, and policy management. In addition to general email management, the Barracuda Email Security Gateway enables administrators to customize email encryption policies, configure data leak prevention rules, and tailor delivery actions depending on the categories of mail from bulk email senders.

The Barracuda Email Security Gateway also filters outbound emails. Because employees can inadvertently cause internal systems to be hijacked for botnet spam, outbound filtering prevents organizations from being put on spam block lists. Outbound filtering also enables administrators to enforce content polices for data loss prevention and to meet other content standards in outgoing emails. Predefined filters and custom policies can be used to detect sensitive data and block or encrypt emails.

While the Barracuda Web Application Firewall in Microsoft Azure protects Internet-facing applications, it also helps secure middleware and data storage (ex. SQL Server) layers. System administrators can configure a dedicated Barracuda Web Application Firewall and position it in-line with application services to secure their cloud-based web applications.

To secure against zero-hour spam and virus attacks, Barracuda's real-time threat intelligence platform, Barracuda Central, collects and analyzes data worldwide to develop defenses, rules, and signatures. As new threats emerge, Barracuda Central delivers the latest definitions to Barracuda Email Security Gateway through Barracuda Energize Updates. These updates require no administrator intervention and ensure that the Barracuda Email Security Gateway provides comprehensive and accurate protection against the latest Internet threats.



The Barracuda Email Security Gateway is also fully integrated with the Barracuda Message Center, a cloud-based email encryption service.

Emails that match policy or are marked for encryption through the Barracuda Outlook Add-in are securely sent by TLS to the Barracuda Message Center, which uses AES with 25v6-bit keys to encrypt email.

The Barracuda Email Security Gateway integrates with the Cloud Protection Layer, a cloud-based service that prefilters emails before delivery to the Barracuda Email Security Gateway. It enables organizations to scale their email security solution as email volume and attachment sizes increase, and reduce the load on the Office 365 email spam filtering service.

The Cloud Protection Layer is continuously updated with definitions in real time with updates from Barracuda Central. The Cloud Protection Layer also provides email continuity in case of disasters. In the event of service disruptions, emails can be spooled in this cloud layer for up to 96 hours with attempts to resend the spooled messages at preset intervals. The Barracuda Email Security Gateway integrates with the Barracuda Cloud Control (BCC) web-based management portal to leverage Barracuda's global cloud infrastructure and enable organizations to centrally manage all their devices.

Companies that migrate from an on-site Microsoft Exchange Server to Office 365 add a new attack surface. With the increase in automated, sophisticated attacks through email, organizations of all sizes require comprehensive, in-depth protection. Barracuda Email Security Gateway provides advanced threat protection together with enhanced management options with granular controls. It can now be deployed in Microsoft Azure to provide state-of-the-art email security and management.