Securing SharePoint Deployments in Microsoft Azure

with the Barracuda Web Application Firewall

White Paper

The Benefits of Deploying Microsoft SharePoint in the Cloud

Microsoft Azure provides Infrastructure as a Service (IaaS), which enables organizations to host virtual machines on the Azure infrastructure, paying only for actual resources used. SharePoint 2013's architecture typically requires deploying a set of servers in a dedicated server farm topology. Having an on-premises environment is not always easy and requires considerable CPU, RAM, storage, and servers. Microsoft Azure offers a perfect way to host highly scalable development and/or testing environments, labs, and production farms.

Microsoft Azure opens up new opportunities to quickly deploy SharePoint server farms and reduce the total cost of ownership by removing infrastructure related costs. Microsoft Azure makes cloud deployment increasingly attractive for companies with limited IT budgets by the ability to scale up and down based on load while only paying for what is used.

The Importance of Application Security in the Cloud

Businesses increasingly opt to relocate applications to the cloud to reap the benefits of agility, efficiency and cost-effective delivery of services. On the other hand, moving applications out from behind the corporate firewall creates concerns about control and undermines confidence. The accessibility that makes cloud-based applications appealing to users also makes applications more vulnerable to hackers, who may use them as gateways into corporate networks. A single unsecured web application can cause significant danger of data loss and system compromise.

Building confidence in the security of the cloud is an important step in encouraging the adoption of this scalable platform. Microsoft and Barracuda partner to provide a security solution for cloud-hosted, web-based applications. The Barracuda Web Application Firewall for Microsoft Azure deters attempts to penetrate networks and offers organisations a secure, highly reliable defence against threats, with no need to learn, configure, and manage complex technology.

What the Barracuda Web Application Firewall adds to the SharePoint-Azure Solution
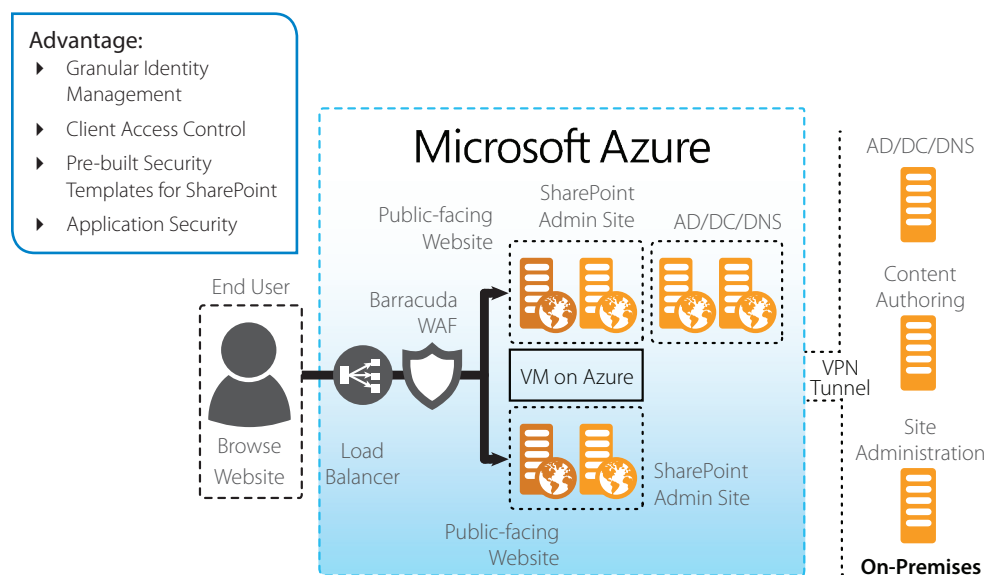
The Barracuda Web Application Firewall offers comprehensive OWASP Top 10 protection. It prevents common attacks including SQL injection, cross-site scripting (XXS) and session tampering, XML-based attacks, brute-force attacks, malware uploads, and more. The Barracuda Energize Updates subscription guarantees that the Barracuda Web Application Firewall receives the latest policy, security and attack definitions automatically. The Barracuda Web Application Firewall also provides strong, identity-based, authentication, and access control that ensures security by restricting SharePoint access to authorized users. Finally, the Barracuda Web Application Firewall offers configurable levels of Logging, Monitoring and Reporting. This way, an administrator is always on top and knows what is going on.

The Barracuda Web Application Firewall sits between the Internet and the web servers hosted in Microsoft Azure and scans inbound traffic to block attacks before they reach the servers and inspects outbound traffic to prevent data leakage.

The Barracuda Web Application Firewall's Application-based DDoS Protection

"Autoscaling", one of the key benefits of the Microsoft Azure platform, enables applications to rapidly scale in the cloud as demand changes. This ensures that the application remains responsive at all times by adding additional instances.

A DDoS attack that is neither identified nor blocked could have a massive impact on the cost of the Microsoft Azure Infrastructure, depending on the settings of "Autoscaling". By using Barracuda's IP Reputation Database, Barracuda Blacklist, Heuristic Fingerprinting, and more, the Barracuda Web Application Firewall provides superior protection against DDoS attacks.

Advantage:
- Granular Identity Management
- Client Access Control
- Pre-built Security Templates for SharePoint
- Application Security

Additional Barracuda Offerings for Microsoft Azure

Barracuda Networks also offers an industry-leading Next Generation Firewall - the Barracuda NG Firewall - which provides advanced network security, connectivity, visibility, and management of the public cloud.

Adding the Barracuda NG Firewall to an Azure SharePoint deployment provides secure and performant connectivity to the cloud. With Barracuda's NG Firewall advanced VPN technology, massive WAN optimization features and comprehensive reporting capabilities find their way into the public cloud. The reporting capabilities include a tightly integrated Revision Control System, real-time monitoring and logging, and creating high-level reports including suggestions on how to improve an organization's application usage policy.

Having state-of-the-art failover and link handling capabilities as an essential part of the Barracuda NG Firewall guarantees business continuity.

Conclusion

The Barracuda Web Application Firewall is an integrated, proven and highly scalable security solution on Microsoft Azure, offering comprehensive protection for web applications and for confidential data hosted in the cloud. This solution ensures that web applications have the same high levels of protection afforded by in-house data centers.

The Barracuda Web Application Firewall for Microsoft Azure is secure, affordable, and easy to use. It combines web application security, access control, and optimization in a single package that is easy and intuitive to set up and administer.

About the Barracuda Web Application Firewall

The Barracuda Web Application Firewall blocks an ever-expanding list of sophisticated web-based intrusions and attacks that target applications hosted on web servers and in the cloud. The Barracuda Web Application Firewall scans all inbound web traffic to block attacks and scans all outbound traffic to provide highly effective Data Loss Prevention (DLP). Available as a physical or virtual appliance, it is deployed in front of the web application servers, on-premises, or in private cloud or public cloud, like Microsoft Azure.

To learn more about the Barracuda Web Application Firewall, please visit: www.barracuda.com/programs/azure.

About Barracuda Networks, Inc. (NYSE: CUDA)

Barracuda provides cloud-connected security and storage solutions that simplify IT. 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 deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda Networks and the Barracuda Networks logo are registered trademarks of Barracuda Networks, Inc. in the United States. All other names are the property of their respective owners.

Barracuda Networks
3175 S. Winchester Boulevard
Campbell, CA 95008
United States
1-408-342-5400
1-888-268-4772 (US & Canada)
www.barracuda.com
info@barracuda.com