Overview

Welcome to the SonicWall® Web Application Firewall MS Azure Deployment Guide. This Deployment Guide contains installation procedures and configuration guidelines for deploying the SonicWall Web Application Firewall (WAF) in your MS Azure cloud network.

SonicWall WAF provides the following benefits:

- **Security**
  - WAF enforces a defense-in-depth strategy to protect a suite of backend web applications, thereby significantly reducing the development cost and effort involved in protecting individual web applications.
  - WAF provides an optimized, non-tamperable architecture.
- **Scalability and Redundancy**
  - Multiple virtual machines can be deployed as a single system, enabling specialization, scalability, and redundancy.
- **Operational Ease**
  - You can virtualize your entire environment and deploy multiple machines within a single server or across multiple servers.
- **Product Versatility**
  - WAF is compatible with other SonicWall platforms as a stand-alone (All-in-One) unit.

The award-winning SonicWall Web Application Firewall service enforces defense-in-depth strategy to protect your web applications running in Azure from most common threats using a high performance real-time intrusion scanning engine. It offers businesses a complete, affordable, out-of-box compliance solution for web applications that is easy to manage and deploy.

WAF supports OWASP Top Ten and PCI DSS compliance, providing protection against malicious injection and cross-site scripting attacks, credit card and Social Security Number theft, cookie tampering and cross-site request forgery. Dynamic signature updates and Application Profiling that leverages an active learning algorithm protect against known and zero-day vulnerabilities. Virtual Patching using Custom Rules allows customers to instantly address a vulnerability and avoid attacks that happen while waiting for a security hotfix. SonicWall WAF supports IP Reputation services and Rate Limiting features to block automated and brute-force attacks. Stacked authentication including 2-factor authentication, one-time passwords and SSL client certificate authentication combined with access policies provides granular access control to the web applications.

**Highlights:**

- Secures web applications against advanced web attacks including OWASP Top Ten
- Layer 7 Load Balancing and Health Monitoring features provides accelerated application delivery and high availability of your applications
- Geo-IP based visualization and policies help block potential attacks from high risk locations or countries
- Denial of service (DoS) protection, Rate Limiting and Botnet protection with Remediation blocks automated brute-force attacks
- Includes advanced statistics and reporting options for compliance