FORTIGATE VM - NEXT GENERATION FIREWALL ON AZURE

By Achilleas Eleftheriou – Senior Systems Engineer

Nowadays, cloud is the way to go, no matter the size of a company and/or organization. More enterprises are migrating their resources Microsoft Azure to extend their data centers and take advantage of the elasticity and high-availability of the public cloud. While Microsoft secures the infrastructure, you are responsible to protect the data that you place in Microsoft Azure/Cloud. As FortiNet explains in their website, Fortinet Security Fabric provides Azure and Office 365 users the broad protection, native integration and automated management enabling customers with consistent enforcement and visibility across their multi-cloud infrastructure. The Fortinet Security Fabric offers deep multi-layer-security protection and operational benefits for securing web applications, mail applications, preventing zero day threats and managing global security infrastructures from the cloud.

A good way to connect on-premises infrastructure to Windows Azure through Site to Site VPNs without using Azure Gateway is to use FortiGate Next -Generation Firewall which can be deployed as a virtual appliance in Microsoft Azure cloud (IaaS).

As Microsoft states in Azure website FortiGate Next-Generation Firewall technology combines a comprehensive suite of powerful security features. Application control, firewall, antivirus, IPS, Web filtering and VPN along with advanced features such as an extreme threat database, vulnerability management and flow-based inspection work in concert to identify and mitigate the latest complex security threats. The security-hardened FortiOS operating system is purpose-built for inspection and identification of malware.

The FortiGate-VM on Azure delivers next generation firewall capabilities for organizations of all sizes, with the flexibility to be deployed with role of firewall and/or VPN gateway, in basic words a virtual infrastructure will be under the security and monitoring of a next generation firewall.

FortiGate-VM for Microsoft Azure supports both bring-your-own-license (BYOL) and on-demand pay-as-you-go (PAYG) licensing models.

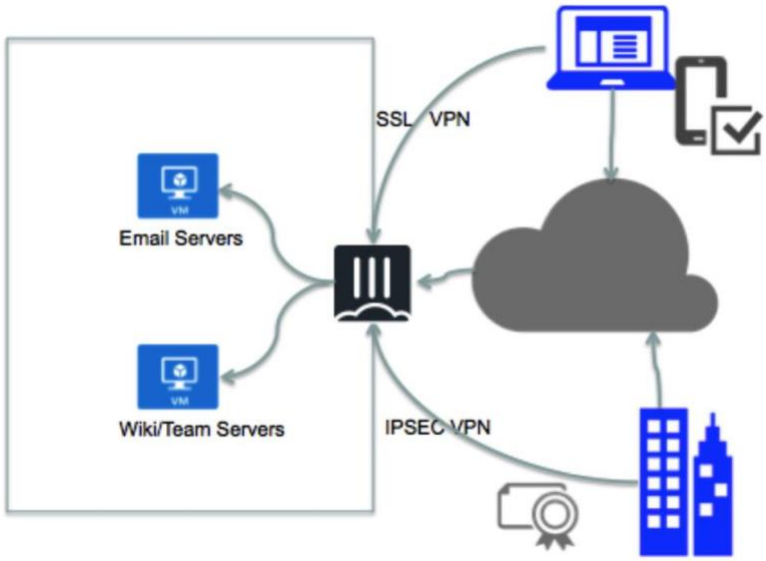
This next generation firewall on cloud can be deployed for protecting following use cases:

- Internet Gateway for ingress/egress security protection.
- Multi-cloud or multi-site connectivity.
- Inter-subnet among app-web-db tiered security within a VNET.
- Intra-VNETs classic VPN deployment.
- End-to-end protection for remote access.

Below are some of the main features of FortiGate-VM on Azure

- Networking
  - Delivers extensive routing, switching, firewall policies, and VPN capabilities to consolidate networking and security functionality
- Security
  - Protects against knows exploits and malware using continuous threat intelligence provided by FortiGuard Labs security services.
  - Application Control
  - Web Filtering
  - Protects against unknown attacks using dynamic analysis

The following diagram demonstrates the functionality of FortiGate VM on Azure and the communication paths. It is clear from the below diagram that FortiGate on Azuere operates with very similar way like the local FortiGate devices but with on high availability (using Azure functionality) and less operational costs.



In addition, FortiGate on Azure supports active/passive high availability (HA) configuration, that means when FortiGate detects a failure, the passive firewall instance becomes active using Azure AP calls to its interfaces/ports. Also, FortiGate on Azure delivers complete IPS technology which is responsible to protect against current and emerging network -level threats, signature-based threat detection, performing anomaly-based detection which alerts users to any traffic that matches attack behaviour profiles.

Achilleas Eleftheriou is working with IBSCY LTD for the last 7 years. During his employment with IBSCY, he had several roles starting from junior positions. Currently, he is one of our Senior Systems Consultants. His background is mostly on networking, but he has also vast experience on systems implementations with Windows Server, local and in the cloud. He is the head of our technical implementations team and holds a BSc in Computer Science from Frederick University plus several certifications from FortiNet and Microsoft.