FORTINET FORTIGATE DEPLOYMENT GUIDE FOR HIGH AVAILABILITY IN AZURE

DEPLOYMENT GUIDE

OVERVIEW

As a valued security partner for Microsoft's Cloud services, Fortinet has worked diligently to build a complete cloud security solution that extends the Fortinet Security Fabric from the private data center into the cloud, with advanced security orchestration and unified threat protection.

The FortiGate-VM is a key part of this solution and provides more control and visibility by identifying and setting policy by user applications, device specs, IP, and network interfaces. Through these offerings, Fortinet delivers the highly optimized solution for Microsoft Azure where application workloads can be protected beyond native Azure security options.

When it comes to these deployments, high availability (HA) has been one of the biggest challenges for cloud providers to guarantee high service-level agreements. Constructing a highly available security system in the cloud has never been an easy task either. To this end, Fortinet provides end-to-end configuration templates for common cloud practices and makes them available in Fortinet's Azure Marketplace listings. The current marketplace FortiGate HA option in Azure is a highly scalable HA design.

To deploy directly from your Azure portal, click on '+New' and search for 'FortiGate,'then choose "FortiGateNGFW high availability (HA)."

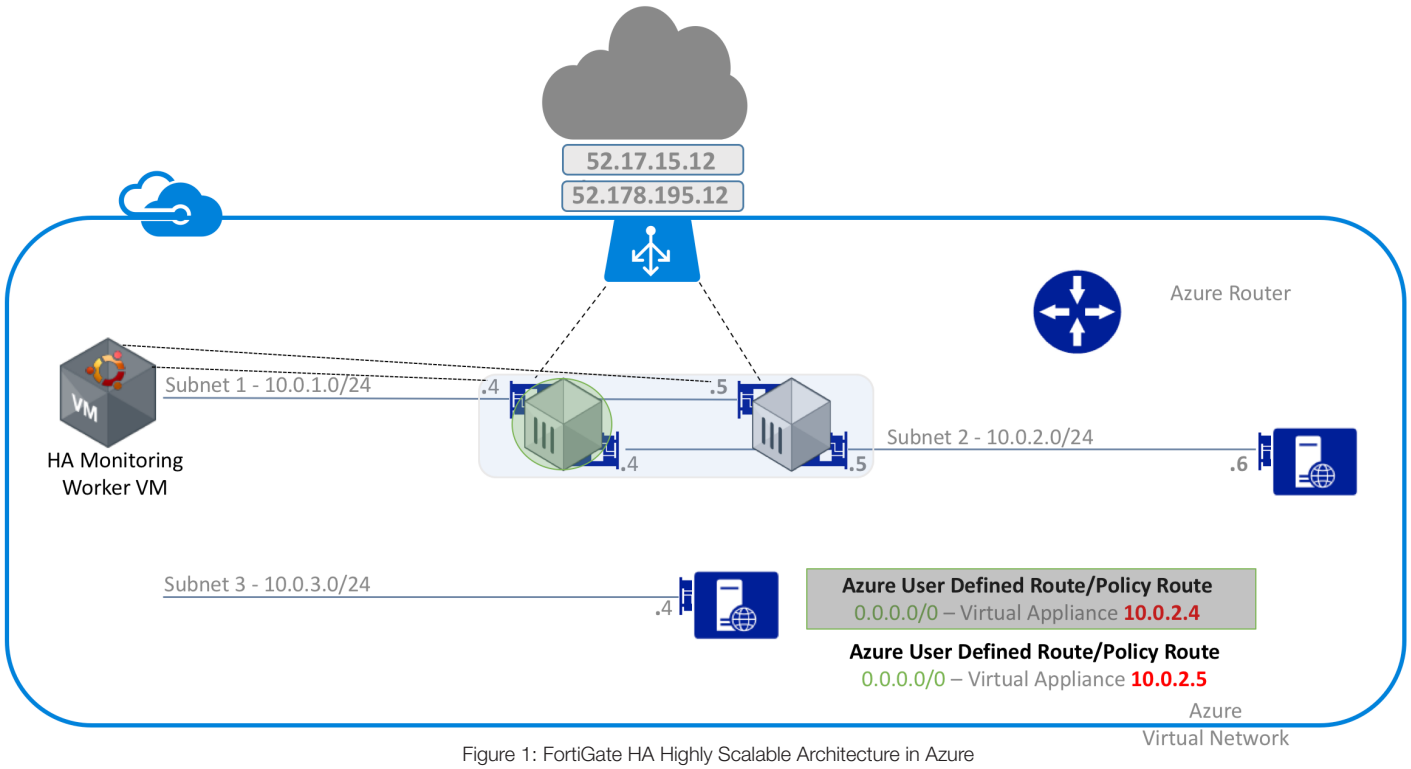

Figure 1: FortiGate HA Highly Scalable Architecture in Azure

In this architecture, inbound traffic comes through the load balancer and the flow of traffic is determined by the load balancer itself (unless a connection is already established, in which case the flow follows the existing path). For inbound traffic coming from the load balancer, both FortiGate appliances are in Active/Active configuration. Source NAT is recommended on the incoming policies in order to maintain path symmetry for return traffic. Fortinet doesn't recommend Active/Passive deployments for this use case. Any manipulation of UDRs or public IPs for Active/Passive solutions takes 30 seconds to be applied after the failover is initiated. Azure load balancers can, however, send probes as often as every 5 seconds and will stop forwarding traffic after two failures. Thus, a failure is detected and mitigated within 6-10 seconds. The only drawback to Active/Active is that it relies heavily on source NAT or FortiGate Session Life Support Protocol (FGSP). FGSP can function, but asymmetric routing will reduce the security effectiveness of IPS and application control.

Outbound flows follow whichever User Defined Route (UDR) is currently installed, and all outbound traffic is initiated through the current active FortiGate. So, for outbound-initiated traffic from Azure Subnets, FortiGate appliances are in Active/Passive mode. We need to rely on Azure software-defined networking (SDN) principles with one or more worker nodes monitoring the Active FortiGate appliance. In case the FortiGate is not reachable, the script will switch to another FortiGate standby appliance.

FortiGate-A starts as active. The script monitors FortiGate-A until it stops responding. Then the route tables (UDRs) are changed to send traffic to FortiGate-B, at which point the script begins monitoring FortiGate-B until such time as FortiGate-B stops responding and the route tables are reverted to send traffic to FortiGate-A (and so on).

The worker nodes that run the monitor script need to be in the public subnet so they can communicate with Azure control to change routing if the primary FortiGate goes offline. We have sample bash scripts that can be tailored to suit the environment. Microsoft has recently developed a similar process using scripts running in a container cluster. Here are the links for that solution: https://channel9.msdn.com/Shows/Azure-Friday/Deploying-Network-Virtual- Appliances-for-High-Availability. The github repo is at https://github.com/mspnp/ha-nva

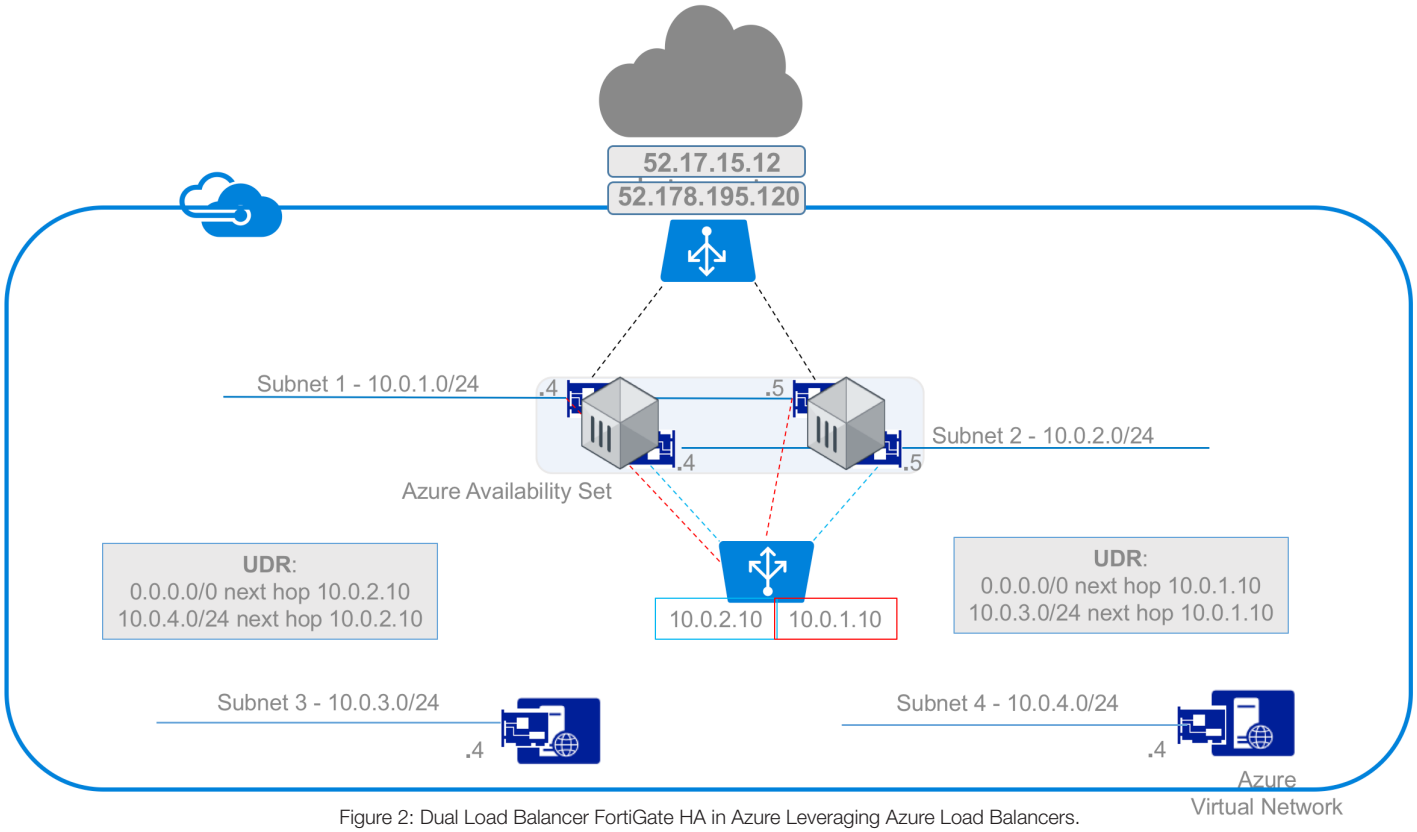

Figure 2: Dual Load Balancer FortiGate HA in Azure Leveraging Azure Load Balancers.
The Internal Azure Load Balancer functions as UDR next hop for internal routes.

DUAL LOAD BALANCER FORTIGATE HA SETUP IN AZURE

Microsoft has updated their internal load balancer so it can be utilized as a next hop for these types of deployments. Fortinet can take advantage of this feature to develop FortiGate HA in Azure.

In this architecture, we leverage dual load balancers (public and internal) in Azure to achieve HA for the FortiGates. This design will remove the need for any sort of SDN scripting. The major difference is that an internal load balancer doesn't have a public IP address. Instead, we associate an internal load balancer with a virtual network subnet and it gets a private IP address. All traffic will be routed to an internally load balanced service via this private IP address. Thus, the internal Azure load balancer functions as the UDR next hop for subnets not directly connected to the FortiGate appliances. To check availability of the FortiGate appliances, it will monitor the FortiGate appliances' (inside/outside) NICs using probes and load balance connections.

For inbound flows from Internet/on-premises to Azure Subnets, the Azure public load balancer will load balance the connections between FortiGate(s) and both FortiGate(s) will be Active/Active, similar to Solution A. For outbound flows as well, with introduction of internal load balancers, this architecture provides Active/Active, similar to inbound flows. It is again recommended to use source NAT on FortiGate(s) for connections initiated outbound from Azure Subnets to maintain path symmetry.

For more information on Azure security deployment guides, please visit www.fortinet.com/azure. For the Fortinet HA solution in the Azure Marketplace, please visit https://azuremarketplace.microsoft.com/en-us/marketplace/apps/fortinet.fortigatengfw-high-availability?tab=Overview. If there are any technical questions, contact azuretech@fortinet.com.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

Copyright © 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

94445-A-0-EN **June 28, 2017**