VM-Series on 1-arm in Azure

Companion Skillet Guide

Introduction

This guide walks through the design pattern including the Azure setup. The skillet is meant to address loading a configuration snipped that specifically sets up a VM-Series firewall in an existing Azure environment to support a 1-arm mode configuration. The manner in which the environment is brought up matters. The expectation is that an Arm template is use to bring a vanilla environment up, and skillet are loaded to configure the firewall in a particular manner based on the target demonstration the SE is working on.

This guide address details need to understand the why and how behind 1-arm configuration on Azure.

Design Pattern

The is a specific design pattern for environments that require the use of 1-arm VM-Series firewalls.

Overview

The design pattern includes a pair of VM-series firewalls set in between a public load balancer and an internal load balancer. Each firewall uses 3 interfaces, a management, and two datapath interfaces for external and internal facing traffic workloads.

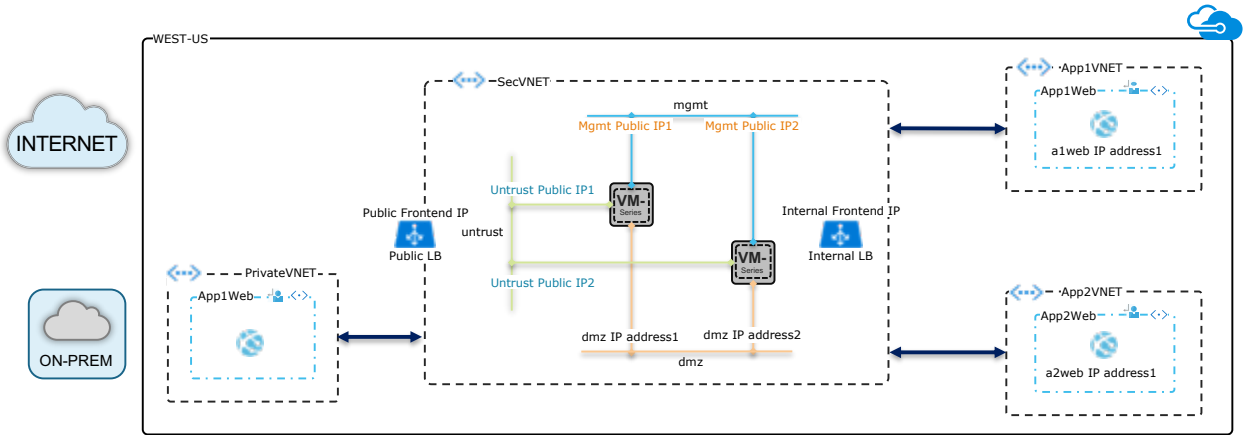


Figure 1. 1-Arm Design Pattern

User Defined Routes (UDRs) are used to control traffic forward on spoke VNET subnets. The UDRs point to the IP address of the internal LB as the next hop.

The Azure infrastructure includes 4 VNETs: the SecVNET which is the hub VNET and houses the VM-Series firewalls, two spoke VNETs App1VNET and App2VNET, and the 4th VNET called PrivateVNET that simulates the on-prem environment.

All spoke VNETs and the PrivateVNET are connected to the hub VNET through VNET peering. Each spoken VNET and the PrivateVNET include a web subnet housing a single server used for testing purposes. Figure 2 shows the networking details.

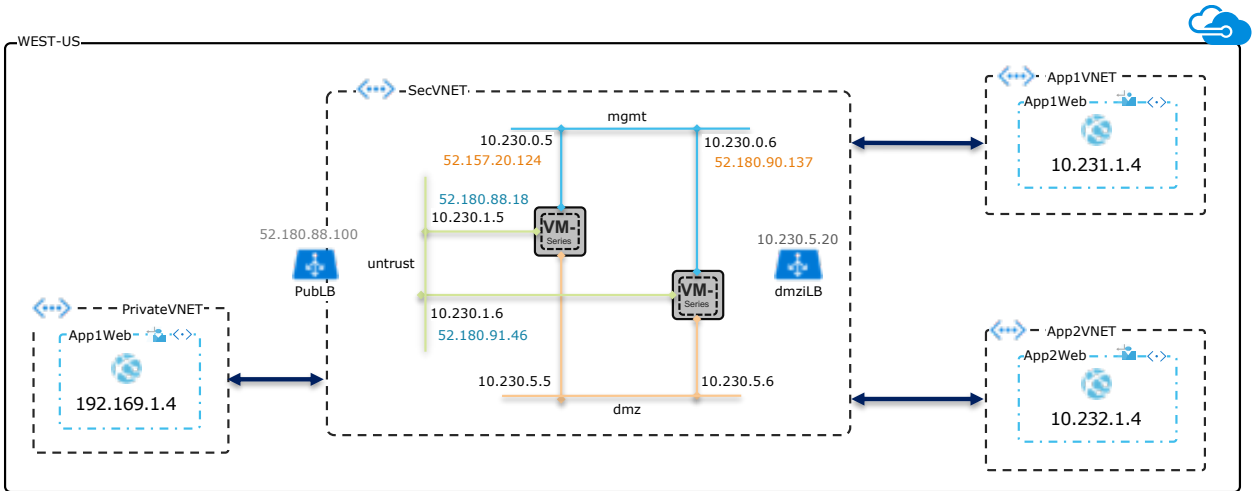


Figure 2. Networking Details

The public load balancer support one or more public ip addresses using frontend IPs. The VM-Series include public IP address on the management interface and also the external datapath interfaces to allow for outbound flows to be NATed without scaling issues.

The internal load balancer uses a single frontend IP which becomes the next hop on any UDR entry in route tables associated with VNET subnets.

The flows supported through the VM-Series are:

- Internet: from any source on the Internet to any destination on a VNET and vice versa
- On-prem: flows from on-prem IP address to public cloud resources and vice versa
- East-West: flows between any two public cloud subnets whether in the same or across VNETs

Figure 3 shows the specific traffic path for each of the supported flows:

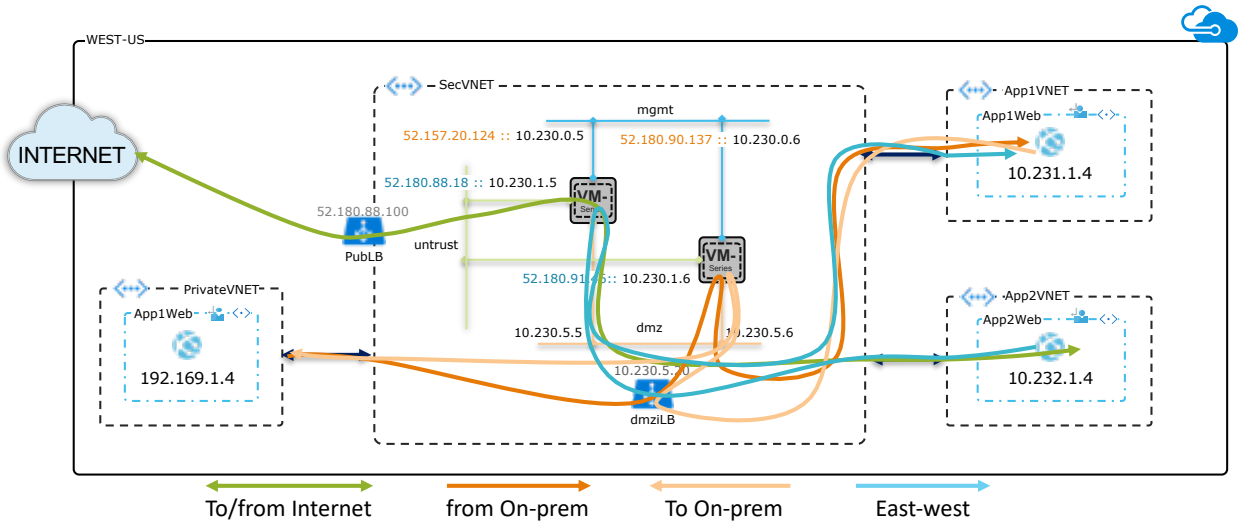


Figure 3. Supported Flows

Networking Details

VNET and Subnets are drawn in the following picture:

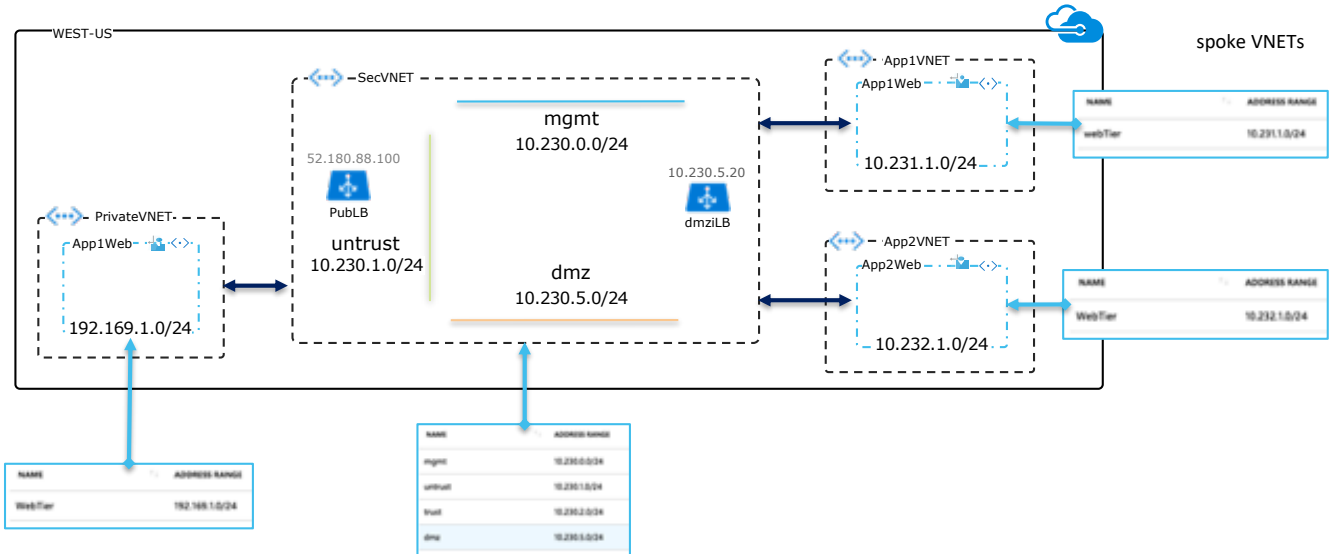


Figure 4. VNETs and Subnets

Each VM-Series uses 3 interfaces. The data path interfaces are place on two different security zones: untrust and dmz.
The untrust interface is placed on a public facing subnet whereas the dmz interface is facing both on-prem and internal VNET subnets. The following diagram shows the interface details:

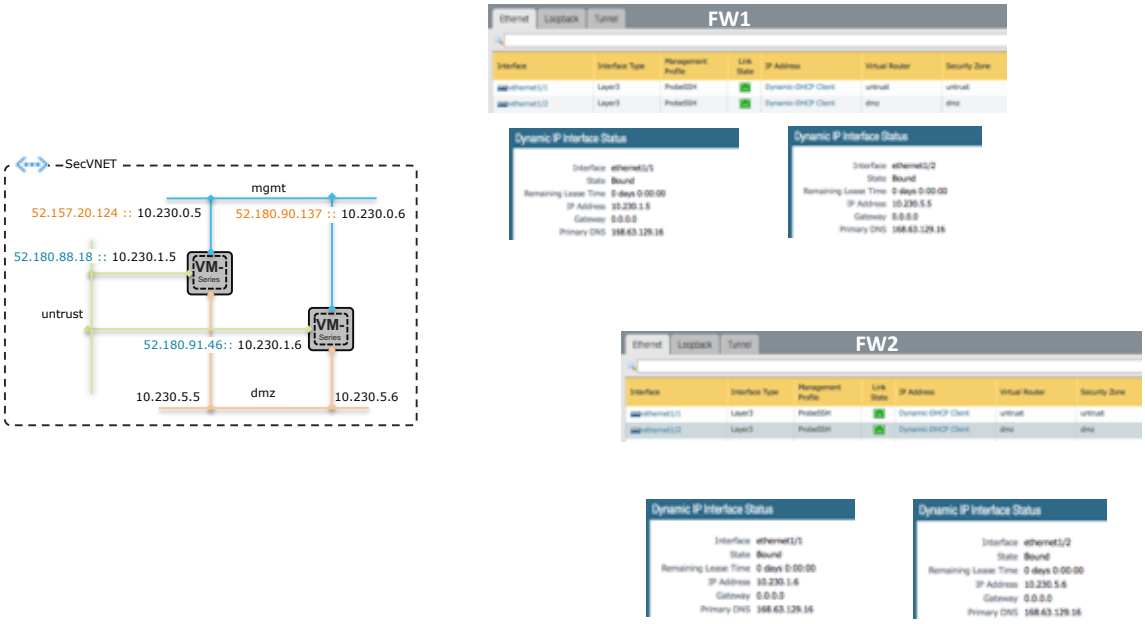


Figure 5. FW Interfaces.

Routing configuration includes both the VM-Series routing tables and the Azure route tables associated with VNET subnets.
The VM-series route tables are dependent on the virtual routers and in environment in which VM-Series re in between load balancers, there is the need to have two different virtual routers. The need is the result of the probes sent by the Azure load balancer using the same source IP address; 168.63.129.16/32.

To be able properly route and or to respond to the probes, two virtual routes are used; one facing the public load balancer and the other one facing the internal load balancer. The following diagram show the VM-Series route tables.

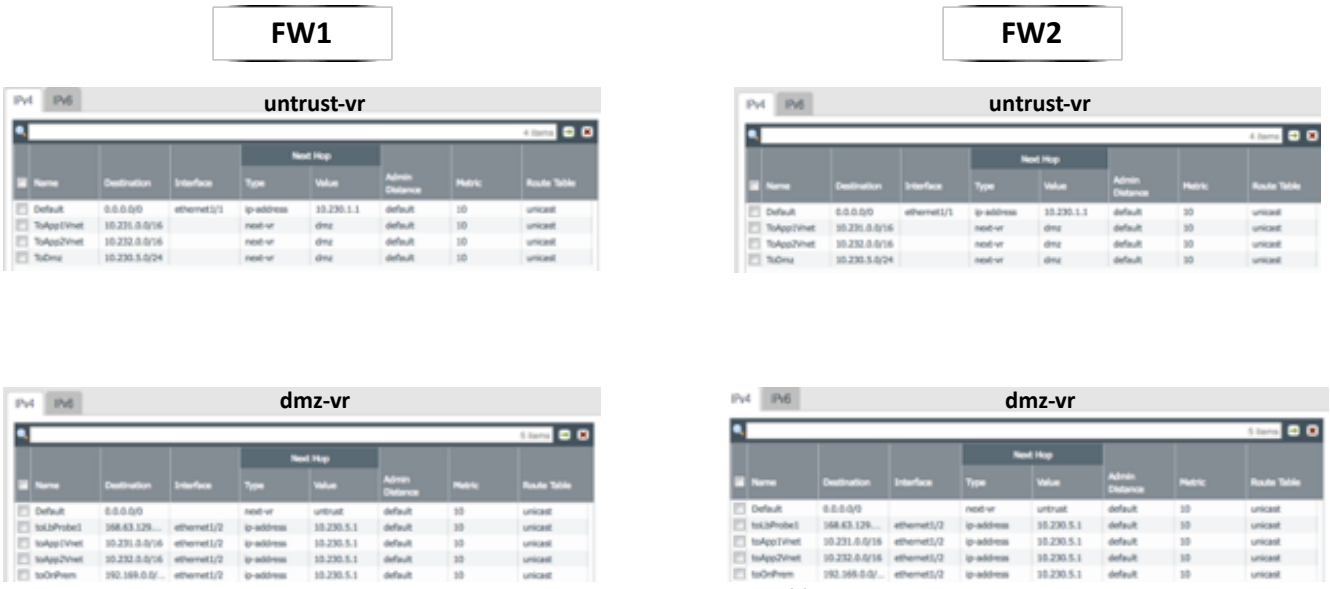


Figure 6. VM-Series Route Tables

The spoke VNET subnet route tables should be identical in that the traffic for any flow is always sent to the internal load balancer front ending the VM-Series pair. The following table show the spoke VNETs route tables.

Figure 7. Spoke VNET web subnets RTs

The Private VNET is a special case since it is a simulated on-prem environment. It essentially needs to know hot o getr to every subnet on any VNAT I wishes to communicate with, and in our case is with the two web subnets under the App1 and App2 VNETs.

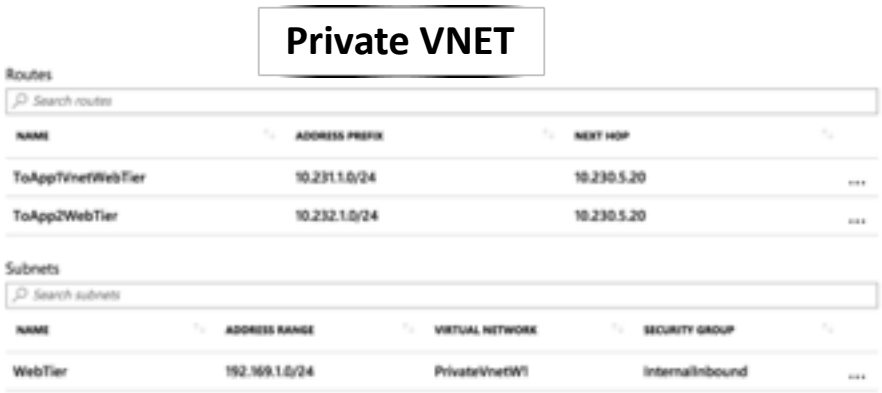
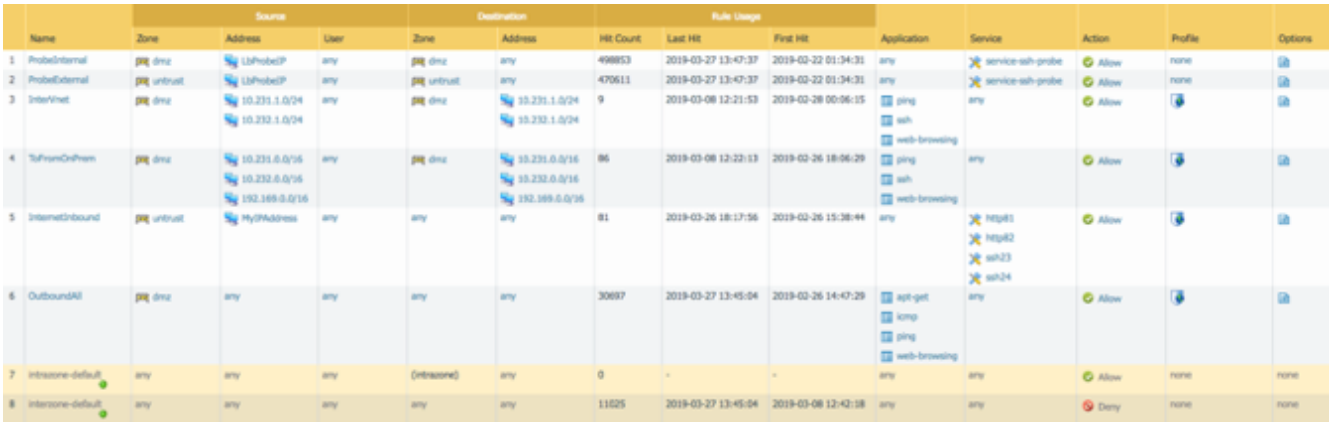


Figure 8. PrivateVNET web subnet RT

Policy Details

The last charts show the security and NAT policies. These are the subjects of the skillet: to automatically configure the VM-Series



	Name	Source			Destination		Rule Usage			Application	Service	Action	Profile	Options
		Zone	Address	User	Zone	Address	Hit Count	Last Hit	First Hit					
1	ProbeInternal	dmz	LbProbeIP	any	dmz	any	498853	2019-03-27 13:47:37	2019-02-22 01:34:31	any	service-ssh-probe	Allow	none	
2	ProbeExternal	untrust	LbProbeIP	any	untrust	any	470611	2019-03-27 13:47:37	2019-02-22 01:34:31	any	service-ssh-probe	Allow	none	
3	InterVnet	dmz	10.231.1.0/24 10.232.1.0/24	any	dmz	10.231.1.0/24 10.232.1.0/24	9	2019-03-08 12:21:53	2019-02-28 00:06:15	ping ssh web-browsing	any	Allow		
4	ToFromOnPrem	dmz	10.231.0.0/16 10.232.0.0/16 192.169.0.0/16	any	dmz	10.231.0.0/16 10.232.0.0/16 192.169.0.0/16	86	2019-03-08 12:22:13	2019-02-26 18:06:29	ping ssh web-browsing	any	Allow		
5	InternetInbound	untrust	MyIPAddress	any	any	any	81	2019-03-26 18:17:56	2019-02-26 15:38:44	any	http81 http82 ssh23 ssh24	Allow		
6	OutboundAll	dmz	any	any	any	any	30697	2019-03-27 13:45:04	2019-02-26 14:47:29	apt-get icmp ping web-browsing	any	Allow		
7	intrazone-default	any	any	any	(intrazone)	any	0	-	-	any	any	Allow	none	none
8	interzone-default	any	any	any	any	any	11025	2019-03-27 13:45:04	2019-03-08 12:42:18	any	any	Deny	none	none

Figure 9. Security Policy

Notice the security policies leverage objects defined in the address object table below:

	Name	Type	Address
	fw1-eth1	IP Netmask	10.230.1.5
	fw1-eth2	IP Netmask	10.230.5.5
	LbProbeIP	IP Netmask	168.63.129.16
	MyIPAddress	IP Netmask	68.15.90.134/32
	PublicLB	IP Netmask	52.180.88.100/32

Figure 10. Address Objects

The security policy include specific entries to deal with probe traffic as well as regular traffic. InterVnet (east-west), on-prem bound and two different policies to deal with Internet inbound and outbound.

	Name	Original Packet						Translated Packet		Rule Usage		
		Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation	Hit Count	Last Hit	First Hit
1	OutboundAll	dmz	untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none	24258	2019-03-27 14:32:57	2019-02-26 14:47:29
2	InboundNATApp1	untrust	untrust	any	any	PublicLB	http81	dynamic-ip-and-port ethernet1/2	destination-translation address: 10.231.1.4 port: 80	30	2019-03-26 18:17:56	2019-02-26 14:54:07
3	InboundNATApp1Ssh	untrust	untrust	any	MyIPAddress	PublicLB	ssh23	dynamic-ip-and-port ethernet1/2	destination-translation address: 10.231.1.4 port: 22	2	2019-03-11 22:12:40	2019-02-26 18:42:33
4	InboundNATApp2	untrust	untrust	any	any	PublicLB	http82	dynamic-ip-and-port ethernet1/2	destination-translation address: 10.232.1.4 port: 80	34	2019-03-26 18:17:53	2019-02-26 15:38:44
5	InboundNATApp2Ssh	untrust	untrust	any	MyIPAddress	PublicLB	ssh24	dynamic-ip-and-port ethernet1/2	destination-translation address: 10.232.1.4 port: 22	1	2019-03-11 22:28:11	2019-03-11 22:28:11
6	NoNATProbeInt	dmz	dmz	any	LbProbeIP	fw1-eth2	any	none	none	419340	2019-03-27 14:33:08	2019-02-26 11:29:30
7	NoNATProbeExt	untrust	untrust	any	LbProbeIP	fw1-eth1	any	none	none	419338	2019-03-27 14:33:08	2019-02-26 11:29:25

Figure 11. NAT Policy

NAT policies include Internet outbound and a few additional ones used for testing purposes to allow traffic from a single source IP to get to the hosts and move around.

The companion guide document also includes logs from the different traffic flows the reader could use to verify their own setup.