VM-Series on 1-arm mode

Companion Skillet Guide

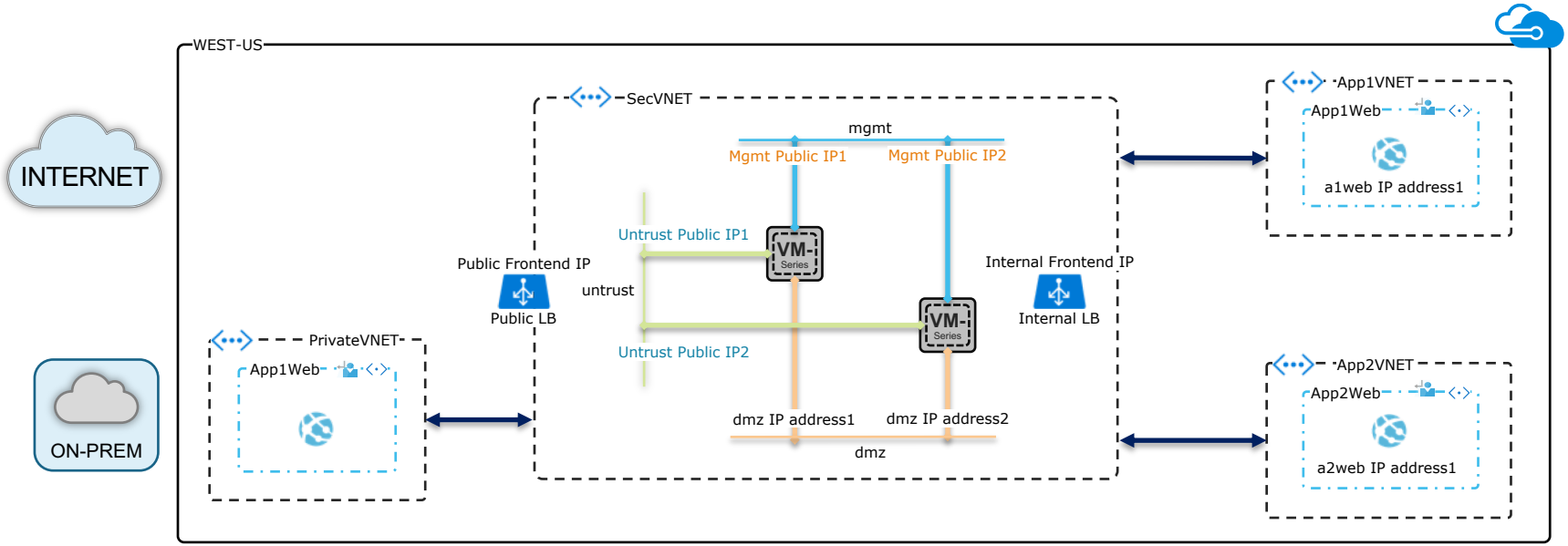
Mauricio Arregoces

Cloud Consulting Engineer

AGENDA

- Design Pattern
- Azure Configuration
- VM-Series Configuration
- Testing
- Checking logs
- Conclusion

Azure Environment



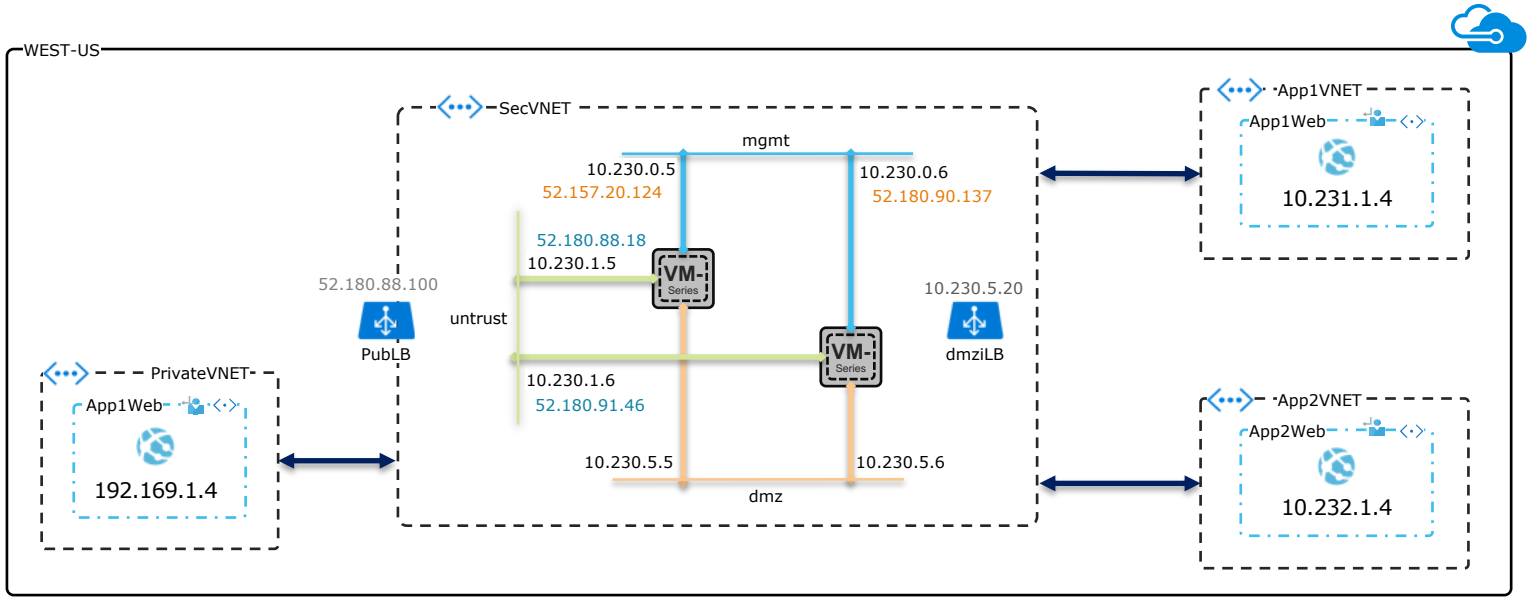
VM-Series

- Firewall pair between load balancers
- 3-Interfaces: Mgmt, Untrust & DMZ
- UDRs to route to virtual appliances

Flows

- East-West: VNET to VNET
- On-prem: to / from on-prem CIDRs
- Internet: to / from Internet hosts

Azure Environment :: Networking Details



Load Balancers

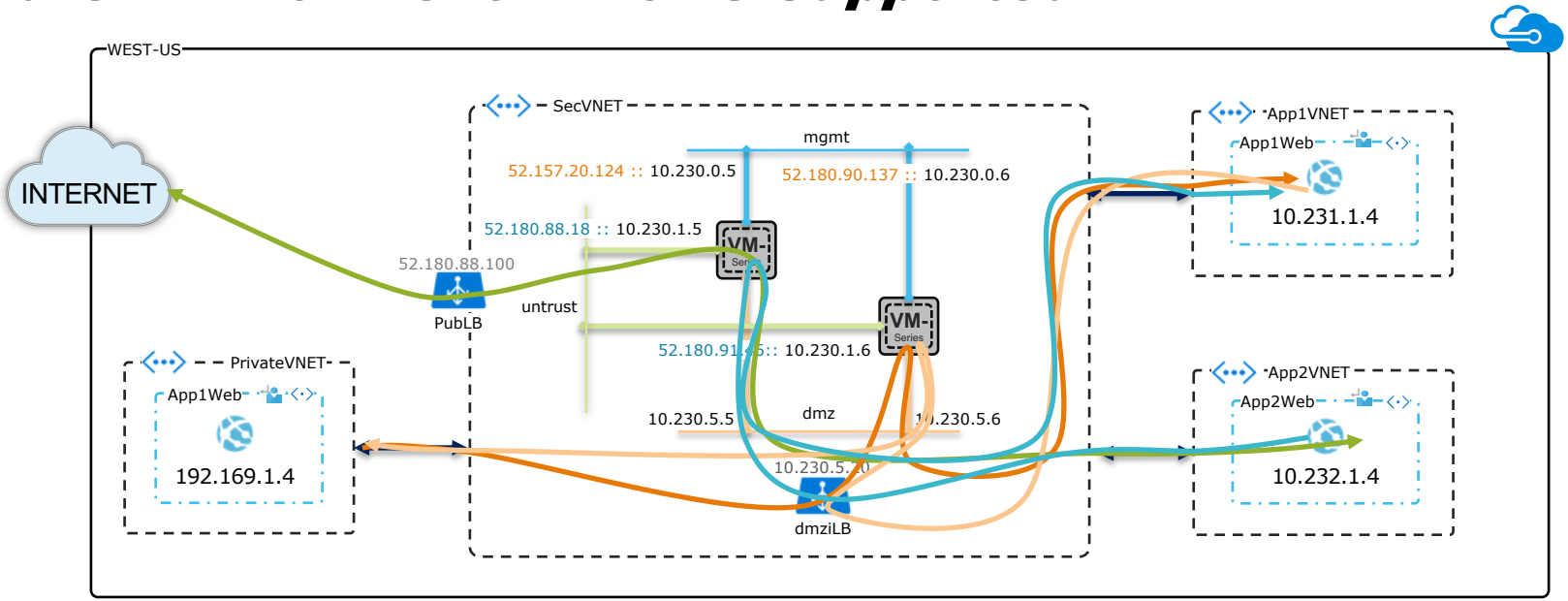
- Standard LB: leverage HA ports & hash calc for symmetric traffic
- Public :: FEIP per app :: multiple ports (UDP or TCP)
- Internal :: single FEIP :: next hope for "all UDRs"

Route Tables

- Subnet RT: Single route entry using iLB FEIP as next hop
- VM-Series RT: control routing traffic between zones and subnets
- On-prem & east-west traffic is intrazone – single interface

To/from Internet from On-prem To On-prem East-west

Azure Environment :: Flows Supported



Highlights

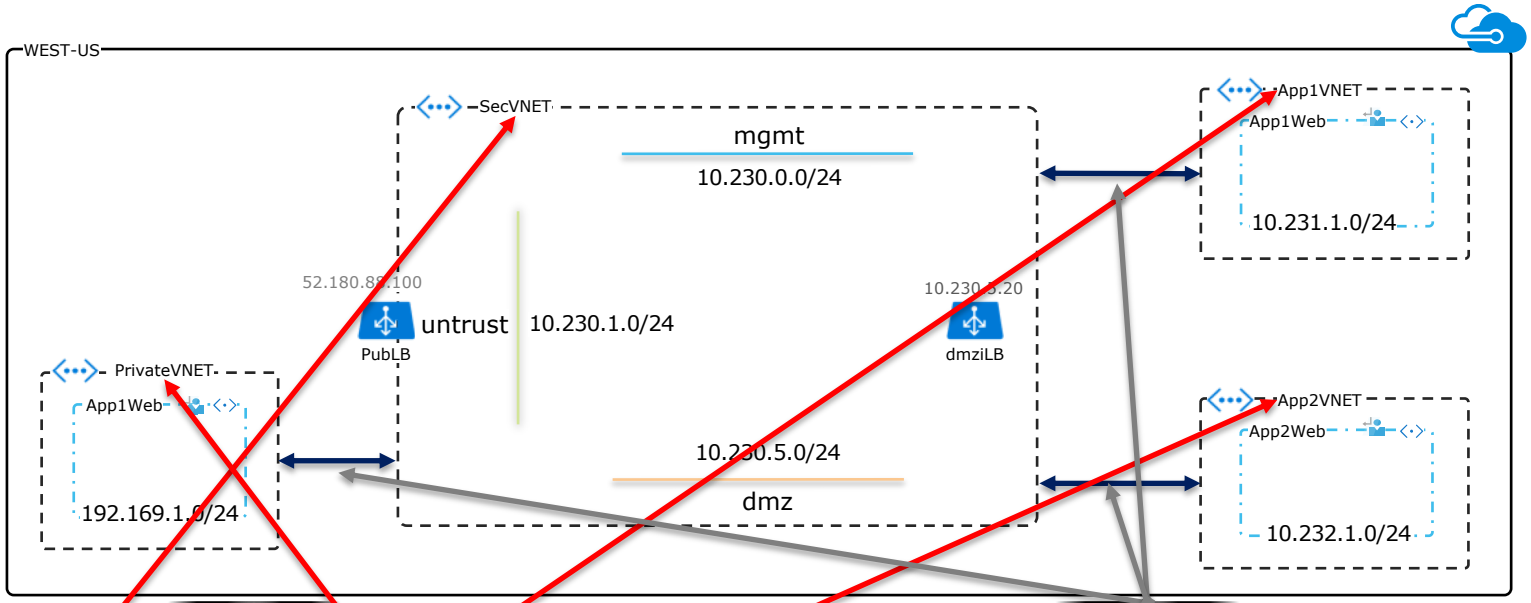
- On-Prem is simulated through a peered VNET
- Internet Flows are always SNATed
- On-prem and East-West are not NATted

NAT

- NAT Avoidance :: leverage Standard iLB to stitch traffic together
- VM-Series :: Apply NAT to Internet flows only
- Using floating IP on both publicLB and iLB in front of FWs

To/from Internet | from On-prem | To On-prem | East-west

Azure Environment :: VNET Details



SUBNETS

NAME	ADDRESS RANGE
mgmt	10.230.0.0/24
untrust	10.230.1.0/24
trust	10.230.2.0/24
dmz	10.230.5.0/24

SecVNET

NAME	ADDRESS RANGE
webTier	10.231.1.0/24

NAME	ADDRESS RANGE
WebTier	10.232.1.0/24

NAME	ADDRESS RANGE
WebTier	192.169.1.0/24

spoke VNETs

PEERINGS

PEERING STATUS	PEER	GATEWAY TRANSIT
Connected	PrivateVnetW1	Enabled
Connected	App1Vnet	Enabled
Connected	App2Vnet	Enabled

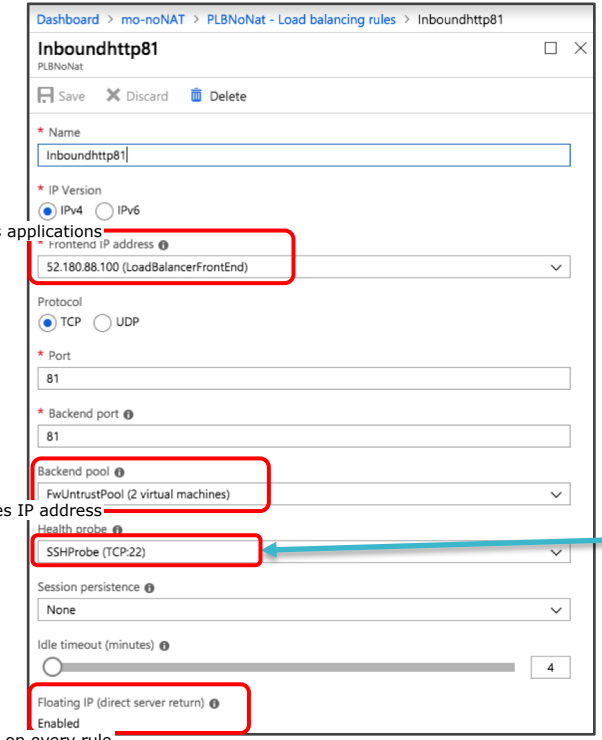
SecVNET

spoke VNETs

PEERING STATUS	PEER	GATEWAY TRANSIT
Connected	SecVNET	Disabled

Azure Environment :: Load Balancer Rules

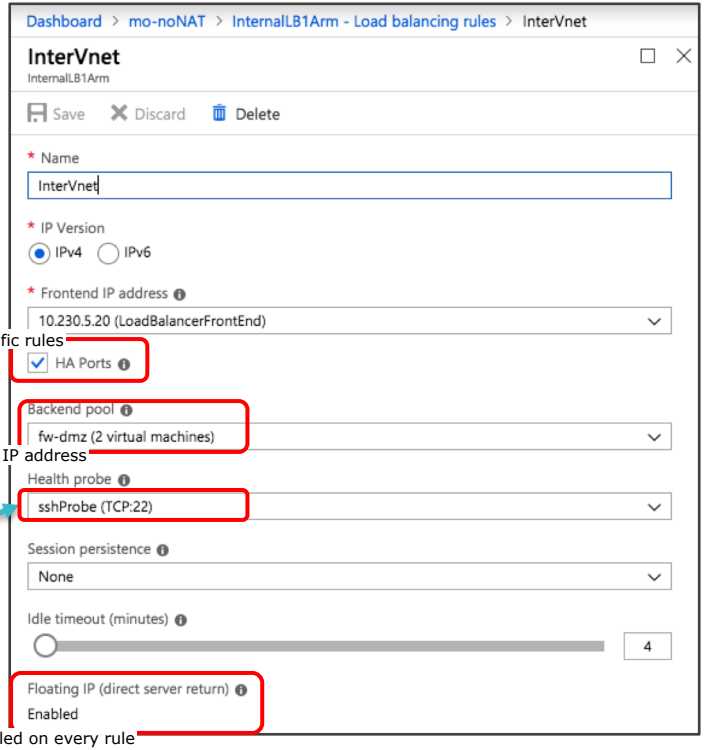
PUBLIC LB RULE



- Public IP to access applications
- Untrust interfaces IP address
- Floating IP enabled on every rule
- Conserves the src IP

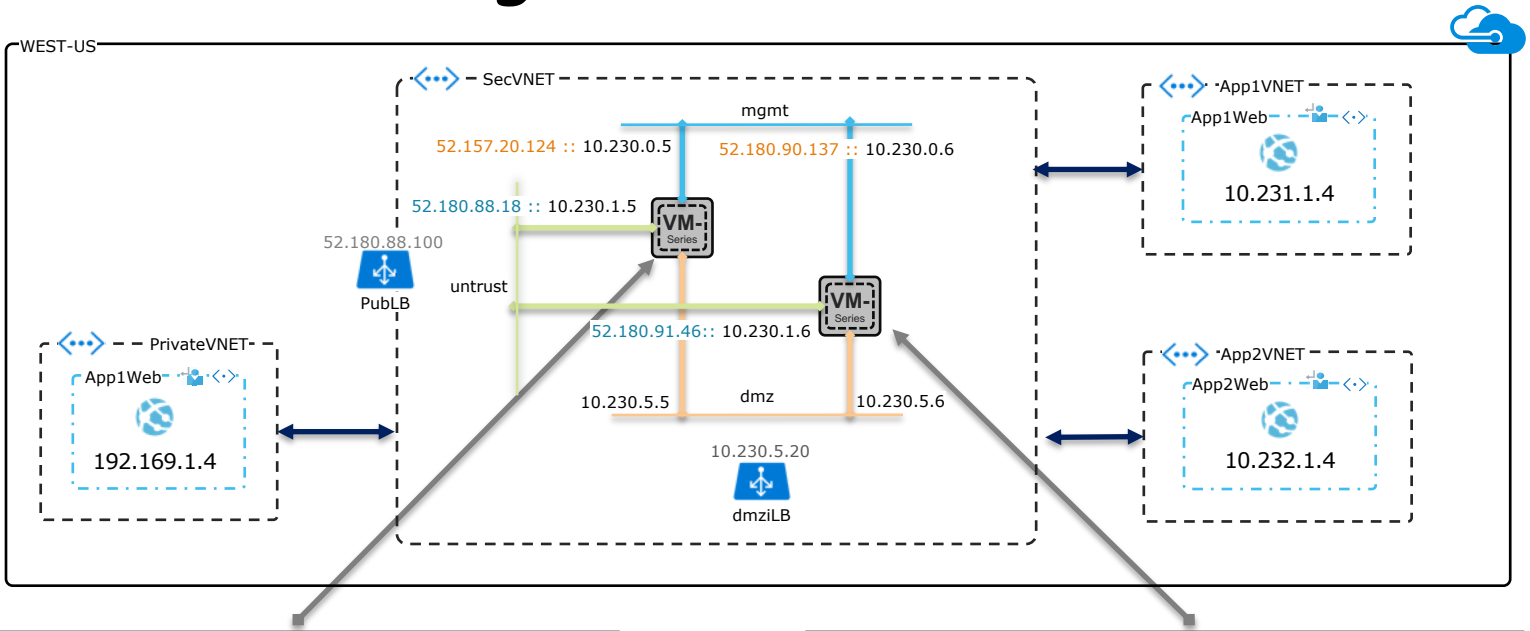
VM-series respond to probe traffic

INTERNAL LB RULE



- HA ports to avoid specific rules
- dmz interfaces IP address
- Floating IP enabled on every rule

VM-Series Networking :: Interfaces



FW1

Ethernet | Loopback | Tunnel

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Security Zone
ethernet1/1	Layer3	ProbeSSH		Dynamic-DHCP Client	untrust	untrust
ethernet1/2	Layer3	ProbeSSH		Dynamic-DHCP Client	dmz	dmz

Dynamic IP Interface Status

Interface	ethernet1/1
State	Bound
Remaining Lease Time	0 days 0:00:00
IP Address	10.230.1.5
Gateway	0.0.0.0
Primary DNS	168.63.129.16

Dynamic IP Interface Status

Interface	ethernet1/2
State	Bound
Remaining Lease Time	0 days 0:00:00
IP Address	10.230.5.5
Gateway	0.0.0.0
Primary DNS	168.63.129.16

FW2

Ethernet | Loopback | Tunnel

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Security Zone
ethernet1/1	Layer3	ProbeSSH		Dynamic-DHCP Client	untrust	untrust
ethernet1/2	Layer3	ProbeSSH		Dynamic-DHCP Client	dmz	dmz

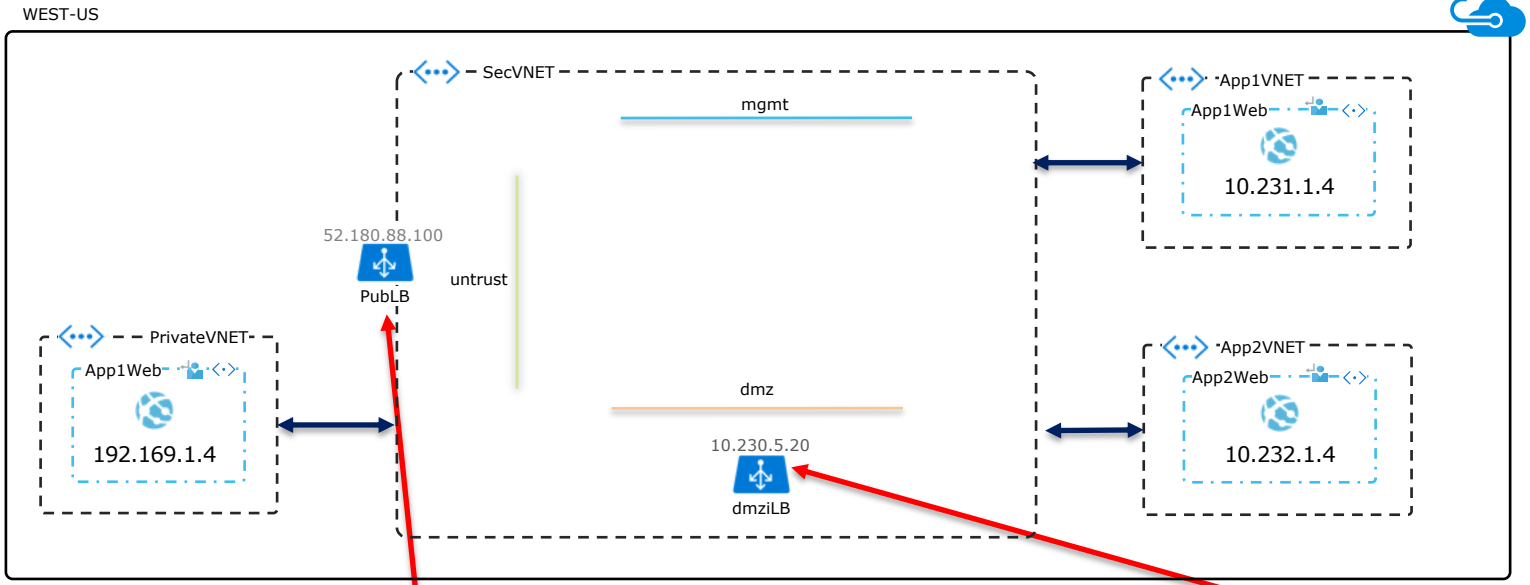
Dynamic IP Interface Status

Interface	ethernet1/1
State	Bound
Remaining Lease Time	0 days 0:00:00
IP Address	10.230.1.6
Gateway	0.0.0.0
Primary DNS	168.63.129.16

Dynamic IP Interface Status

Interface	ethernet1/2
State	Bound
Remaining Lease Time	0 days 0:00:00
IP Address	10.230.5.6
Gateway	0.0.0.0
Primary DNS	168.63.129.16

Azure Environment :: Load Balancer Details



PUBLIC LB

LoadBalancerFrontEnd	52.180.88.100 (publbip)

SSHProbe	TCP	22

FwUntrustPool (2 virtual machines)

fw1	Running	fw1-eth1	10.230.1.5
fw2	Running	fw2-eth1	10.230.1.6

Inboundhttp81	Inboundhttp81 (TCP/81)	FwUntrustPool	SSHProbe
InboundHttp82	InboundHttp82 (TCP/82)	FwUntrustPool	SSHProbe
InboundSsh23	InboundSsh23 (TCP/23)	FwUntrustPool	SSHProbe
InboundSsh24	InboundSsh24 (TCP/24)	FwUntrustPool	SSHProbe

INTERNAL LB

LoadBalancerFrontEnd	10.230.5.20

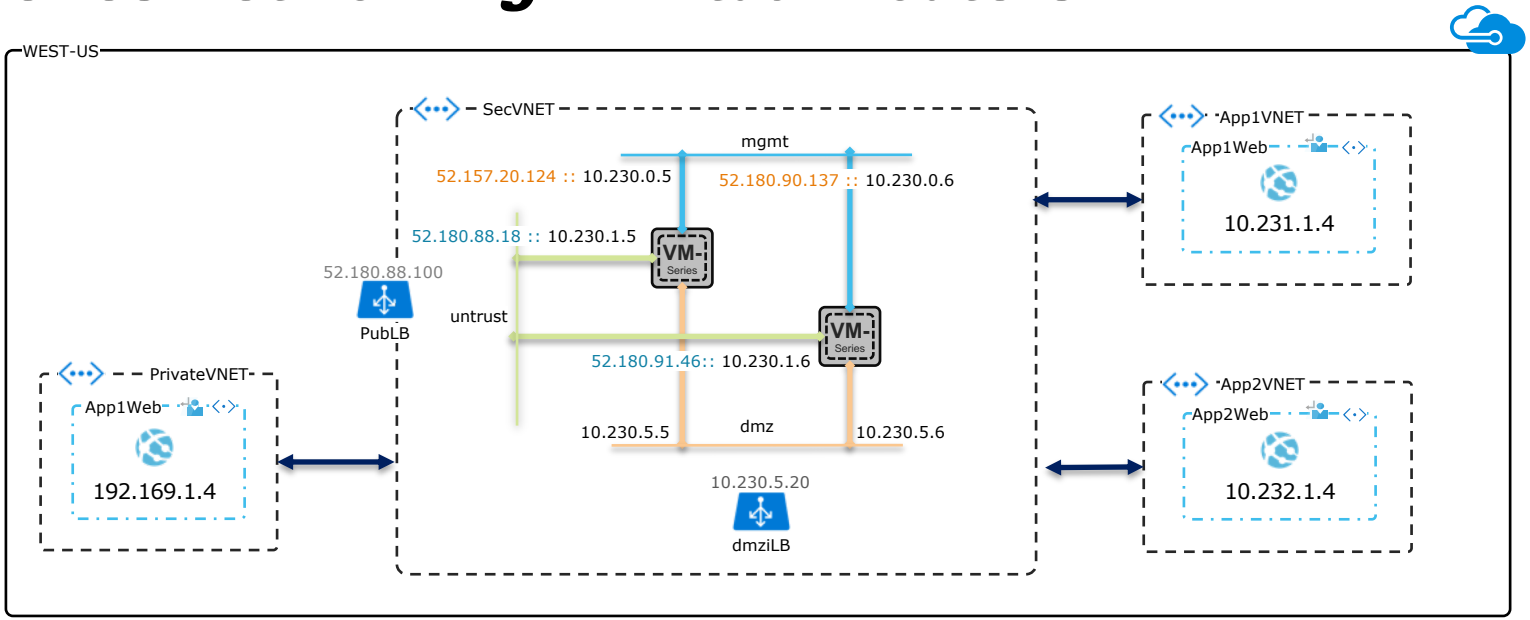
fw-dmz (2 virtual machines)

fw1	Running	fw1-eth2	10.230.5.5
fw2	Running	fw2-eth2	10.230.5.6

sshProbe	TCP	22

InterVnet	InterVnet (All/0)	fw-dmz	sshProbe

VM-Series Networking :: Virtual Routers



FW1

Name	Interfaces	Configuration	Runtime Stats
dmz	ethernet1/2	Static Routes: 5 ECMP status: Enabled	More Runtime Stats
untrust	ethernet1/1	Static Routes: 4 ECMP status: Disabled	More Runtime Stats

FW2

Name	Interfaces	Configuration	Runtime Stats
dmz	ethernet1/2	Static Routes: 5 ECMP status: Enabled	More Runtime Stats
untrust	ethernet1/1	Static Routes: 4 ECMP status: Disabled	More Runtime Stats

- A virtual router is required per data path interface when there are multiple load balancers
- Every load balancer sends probes using the same src IP address: 168.63.129.16

VM-Series Virtual Routers :: Static Routes

FW1

IPv4 | IPv6

untrust

4 items

Name	Destination	Interface	Next Hop Type	Next Hop Value	Admin Distance	Metric	Route Table
Default	0.0.0.0/0	ethernet1/1	ip-address	10.230.1.1	default	10	unicast
ToApp1Vnet	10.231.0.0/16		next-vr	dmz	default	10	unicast
ToApp2Vnet	10.232.0.0/16		next-vr	dmz	default	10	unicast
ToDmz	10.230.5.0/24		next-vr	dmz	default	10	unicast

IPv4 | IPv6

dmz

5 items

Name	Destination	Interface	Next Hop Type	Next Hop Value	Admin Distance	Metric	Route Table
Default	0.0.0.0/0		next-vr	untrust	default	10	unicast
toLbProbe1	168.63.129....	ethernet1/2	ip-address	10.230.5.1	default	10	unicast
toApp1Vnet	10.231.0.0/16	ethernet1/2	ip-address	10.230.5.1	default	10	unicast
toApp2Vnet	10.232.0.0/16	ethernet1/2	ip-address	10.230.5.1	default	10	unicast
toOnPrem	192.169.0.0/...	ethernet1/2	ip-address	10.230.5.1	default	10	unicast

FW2

IPv4 | IPv6

untrust

4 items

Name	Destination	Interface	Next Hop Type	Next Hop Value	Admin Distance	Metric	Route Table
Default	0.0.0.0/0	ethernet1/1	ip-address	10.230.1.1	default	10	unicast
ToApp1Vnet	10.231.0.0/16		next-vr	dmz	default	10	unicast
ToApp2Vnet	10.232.0.0/16		next-vr	dmz	default	10	unicast
ToDmz	10.230.5.0/24		next-vr	dmz	default	10	unicast

IPv4 | IPv6

dmz

5 items

Name	Destination	Interface	Next Hop Type	Next Hop Value	Admin Distance	Metric	Route Table
Default	0.0.0.0/0		next-vr	untrust	default	10	unicast
toLbProbe1	168.63.129....	ethernet1/2	ip-address	10.230.5.1	default	10	unicast
toApp1Vnet	10.231.0.0/16	ethernet1/2	ip-address	10.230.5.1	default	10	unicast
toApp2Vnet	10.232.0.0/16	ethernet1/2	ip-address	10.230.5.1	default	10	unicast
toOnPrem	192.169.0.0/...	ethernet1/2	ip-address	10.230.5.1	default	10	unicast

Azure Route Tables

App1VNET

Routes

Search routes

NAME	ADDRESS PREFIX	NEXT HOP	
DefaultRoute	0.0.0.0/0	10.230.5.20	...

Subnets

Search subnets

NAME	ADDRESS RANGE	VIRTUAL NETWORK	SECURITY GROUP	
webTier	10.231.1.0/24	App1Vnet	InternalInbound	...

App2VNET

Routes

Search routes

NAME	ADDRESS PREFIX	NEXT HOP	
default	0.0.0.0/0	10.230.5.20	...

Subnets

Search subnets

NAME	ADDRESS RANGE	VIRTUAL NETWORK	SECURITY GROUP	
WebTier	10.232.1.0/24	App2Vnet	InternalInbound	...

Private VNET

Routes

Search routes

NAME	ADDRESS PREFIX	NEXT HOP	
ToApp1VnetWebTier	10.231.1.0/24	10.230.5.20	...
ToApp2WebTier	10.232.1.0/24	10.230.5.20	...

Subnets

Search subnets

NAME	ADDRESS RANGE	VIRTUAL NETWORK	SECURITY GROUP	
WebTier	192.169.1.0/24	PrivateVnetW1	InternalInbound	...

FW1 Security Policies

	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

Address Objects

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

FW2 Security Policies

		Source				Destination		Rule Usage							
	Name	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action	Profile	Options
1	ProbeInternal	dmz	LbProbeIP	any	any	dmz	any	427275	2019-03-27 14:13:37	2019-02-25 22:03:03	any	service-ssh-p...	Allow	none	
2	ProbeExternal	untrust	LbProbeIP	any	any	untrust	any	427230	2019-03-27 14:13:37	2019-02-25 22:08:06	any	service-ssh-p...	Allow	none	
3	InterVnet	dmz	10.231.1.0/24 10.232.1.0/24	any	any	dmz	10.231.1.0/24 10.232.1.0/24	444	2019-03-26 20:12:29	2019-02-26 14:47:49	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	any	dmz	10.231.0.0/16 10.232.0.0/16 192.169.0.0/16	58	2019-03-26 20:12:57	2019-02-26 15:38:55	ping ssh web-browsing	any	Allow		
5	InternetInbound	untrust	MyIPAddress	any	any	any	any	64	2019-03-26 18:17:44	2019-02-26 15:38:42	any	http81 http82 ssh23 ssh24	Allow		
6	OutboundAll	dmz	any	any	any	any	any	32383	2019-03-27 14:11:12	2019-02-26 14:43:01	apt-get icmp ping web-browsing	any	Allow		
7	intrazone-default	any	any	any	any	(intrazone)	any	0	-	-	any	any	Allow	none	none
8	interzone-default	any	any	any	any	any	any	10051	2019-03-27 14:11:12	2019-03-10 00:16:03	any	any	Deny	none	none

Address Objects

Name	Type	Address
fw1-eth1	IP Netmask	10.230.1.6
fw1-eth2	IP Netmask	10.230.5.6
LbProbeIP	IP Netmask	168.63.129.16
MyIPAddress	IP Netmask	68.15.90.134/32
PublicLB	IP Netmask	52.180.88.100/32

FW1 NAT Policies

		Original Packet						Translated Packet		Rule Usage		
	Name	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

Address Objects

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

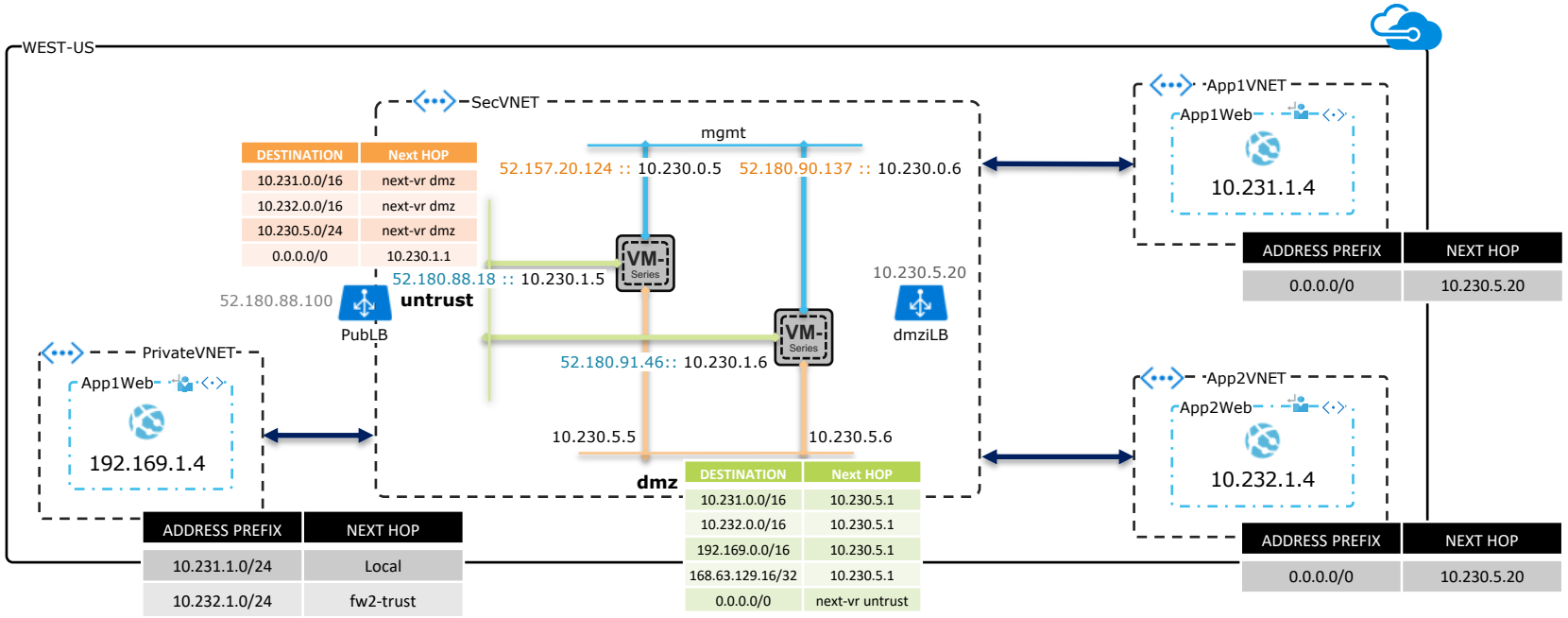
FW2 NAT Policies

		Original Packet						Translated Packet		Rule Usage		
	Name	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	26015	2019-03-27 14:30:58	2019-02-26 14:43:01
2	InboundNATApp1	untrust	untrust	any	any	PublicLB	http81	dynamic-ip-and-port ethernet1/2	destination-translation address: 10.231.1.4 port: 80	39	2019-03-26 18:17:44	2019-02-26 14:39:49
3	InboundNATApp1Ssh	untrust	untrust	any	MyIPAddress	PublicLB	ssh23	dynamic-ip-and-port ethernet1/2	destination-translation address: 10.231.1.4 port: 22	1	2019-02-26 16:47:25	2019-02-26 16:47:25
4	InboundNATApp2	untrust	untrust	any	any	PublicLB	http82	dynamic-ip-and-port ethernet1/2	destination-translation address: 10.232.1.4 port: 80	27	2019-03-20 10:09:03	2019-02-26 16:34:16
5	InboundNATApp2Ssh	untrust	untrust	any	MyIPAddress	PublicLB	ssh24	dynamic-ip-and-port ethernet1/2	destination-translation address: 10.232.1.4 port: 22	0	-	-
6	NoNATProbeInt	dmz	dmz	any	LbProbeIP	fw1-eth2	any	none	none	419343	2019-03-27 14:33:01	2019-02-26 11:29:14
7	NoNATProbeExt	untrust	untrust	any	LbProbeIP	fw1-eth1	any	none	none	419340	2019-03-27 14:33:01	2019-02-26 11:29:11

Address Objects

Name	Type	Address
fw1-eth1	IP Netmask	10.230.1.6
fw1-eth2	IP Netmask	10.230.5.6
LbProbeIP	IP Netmask	168.63.129.16
MyIPAddress	IP Netmask	68.15.90.134/32
PublicLB	IP Netmask	52.180.88.100/32

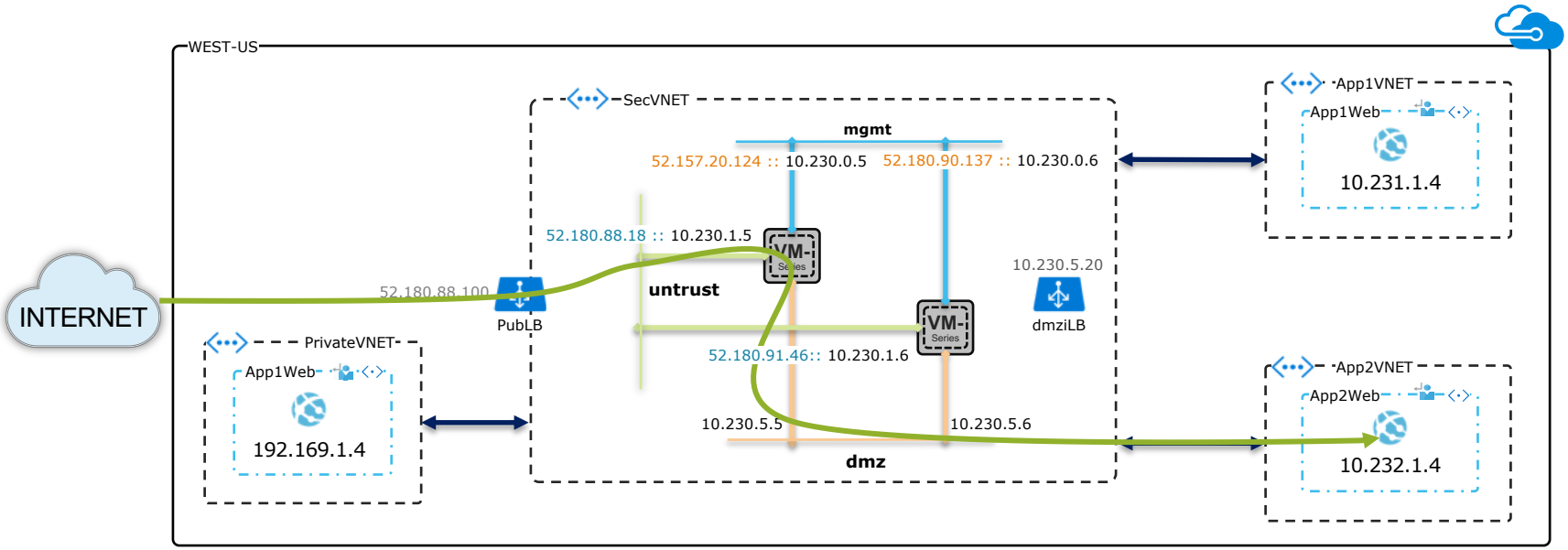
Testing the environment

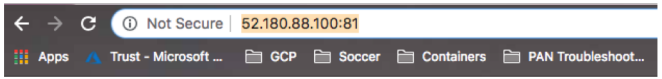


Testing flows

- Inbound ssh to web servers
- http to web servers
- Security zones do not apply to east-west and on-prem flows
- Flows are not bound to security zones – single interface/zone

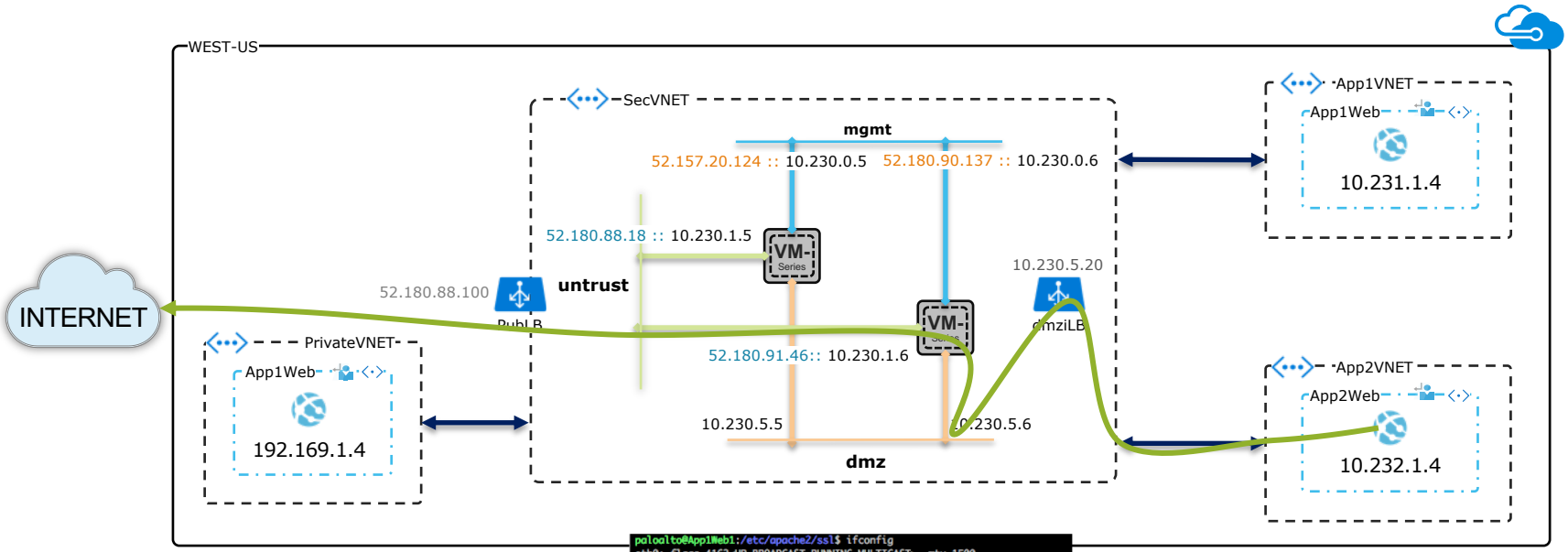
Inbound Flow





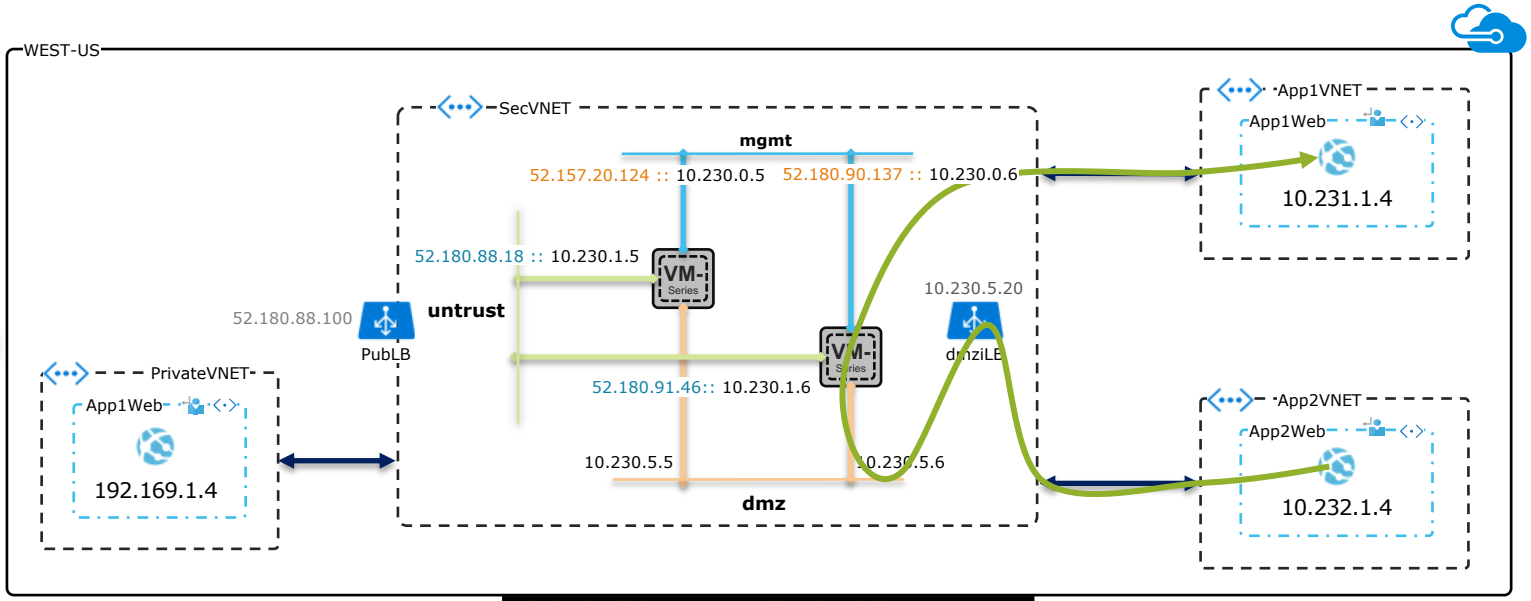
Success! testapp1 virtual host is working!

Outbound Flow



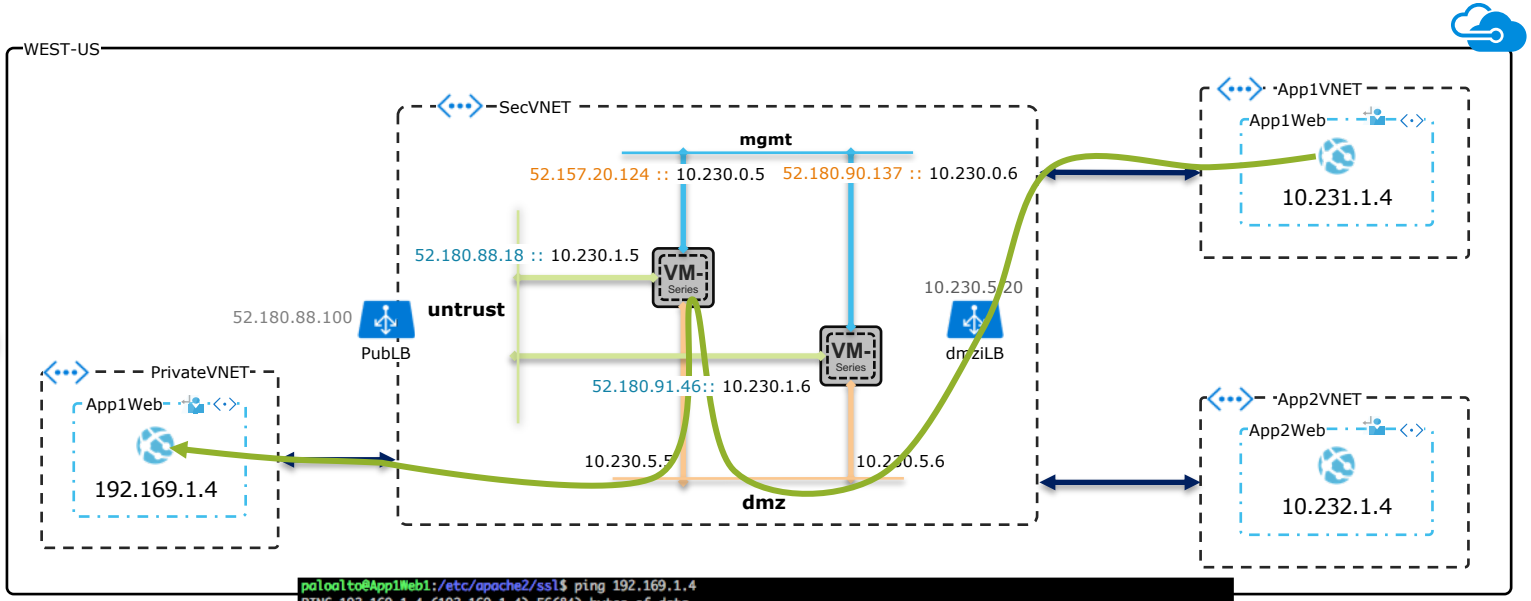

```
paloalto@App1Web1:/etc/apache2/ssl$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.231.1.4  netmask 255.255.255.0  broadcast 10.231.1.255
        inet6 fe80::20d:3aff:fe36:96f0  prefixlen 64  scopeid 0x20<link>
        ether 00:0d:3a:36:96:f0  txqueuelen 1000  (Ethernet)
        RX packets 84011055  bytes 88668564639 (88.6 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44295391  bytes 9612804429 (9.6 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1678745  bytes 212773391 (212.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1678745  bytes 212773391 (212.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

paloalto@App1Web1:/etc/apache2/ssl$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=3.40 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=3.21 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=3.39 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=3.34 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=115 time=3.08 ms
```


East-West Flow




```
paloalto@App2Web1:/etc/apache2$ curl  10.231.1.4
<html>
  <head>
    <title>Welcome to testapp1.com!</title>
  </head>
  <body>
    <h1>Success!  testapp1  virtual host is working!</h1>
  </body>
</html>
paloalto@App2Web1:/etc/apache2$ ping 10.231.1.4
PING 10.231.1.4 (10.231.1.4) 56(84) bytes of data.
64 bytes from 10.231.1.4: icmp_seq=1 ttl=63 time=3.78 ms
64 bytes from 10.231.1.4: icmp_seq=2 ttl=63 time=2.37 ms
64 bytes from 10.231.1.4: icmp_seq=3 ttl=63 time=2.16 ms
64 bytes from 10.231.1.4: icmp_seq=4 ttl=63 time=2.18 ms
64 bytes from 10.231.1.4: icmp_seq=5 ttl=63 time=2.01 ms
64 bytes from 10.231.1.4: icmp_seq=6 ttl=63 time=2.37 ms
64 bytes from 10.231.1.4: icmp_seq=7 ttl=63 time=2.28 ms
64 bytes from 10.231.1.4: icmp_seq=8 ttl=63 time=2.26 ms
```


On-prem Flow




```
paloalto@App1Web1:/etc/apache2/ssl$ ping 192.169.1.4
PING 192.169.1.4 (192.169.1.4) 56(84) bytes of data.
64 bytes from 192.169.1.4: icmp_seq=1 ttl=63 time=3.60 ms
64 bytes from 192.169.1.4: icmp_seq=2 ttl=63 time=2.76 ms
64 bytes from 192.169.1.4: icmp_seq=3 ttl=63 time=2.24 ms
64 bytes from 192.169.1.4: icmp_seq=4 ttl=63 time=2.55 ms
64 bytes from 192.169.1.4: icmp_seq=5 ttl=63 time=2.59 ms
^C
--- 192.169.1.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.242/2.753/3.606/0.460 ms
paloalto@App1Web1:/etc/apache2/ssl$ curl 192.169.1.4 | more
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2016-11-16
    See: https://launchpad.net/bugs/1288690
  -->
```


FW1 & FW2 probe traffic logs

Dashboard | ACC | Monitor | Policies | Objects | Network | Device

Commit

(addr.src in 168.63.129.16)

	Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Egress I/F	Ingress I/F	NAT Source Port	NAT Source IP	NAT Destination Port	NAT Dest IP	Application	IP Protocol	From Port	Action	Rule	Session End Reason	Bytes
	03/27 14:47:47	end	dmz	dmz	168.63.129.16	10.230.5.5	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	53388	allow	ProbeInternal	tcp-rst-from-client	370
	03/27 14:47:47	end	untrust	untrust	168.63.129.16	10.230.1.5	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	53389	allow	ProbeExternal	tcp-rst-from-client	370
	03/27 14:47:45	start	dmz	dmz	168.63.129.16	10.230.5.5	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	53493	allow	ProbeInternal	n/a	262
	03/27 14:47:45	start	untrust	untrust	168.63.129.16	10.230.1.5	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	53494	allow	ProbeExternal	n/a	262
	03/27 14:47:41	end	dmz	dmz	168.63.129.16	10.230.5.5	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	53355	allow	ProbeInternal	tcp-rst-from-client	370
	03/27 14:47:41	end	untrust	untrust	168.63.129.16	10.230.1.5	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	53356	allow	ProbeExternal	tcp-rst-from-client	370
	03/27 14:47:39	start	dmz	dmz	168.63.129.16	10.230.5.5	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	53462	allow	ProbeInternal	n/a	262
	03/27 14:47:39	start	untrust	untrust	168.63.129.16	10.230.1.5	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	53461	allow	ProbeExternal	n/a	262
	03/27 14:47:35	end	dmz	dmz	168.63.129.16	10.230.5.5	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	53326	allow	ProbeInternal	tcp-rst-from-client	370
	03/27 14:47:35	end	untrust	untrust	168.63.129.16	10.230.1.5	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	53327	allow	ProbeExternal	tcp-rst-from-client	370
	03/27 14:47:33	start	untrust	untrust	168.63.129.16	10.230.1.5	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	53424	allow	ProbeExternal	n/a	262
	03/27 14:47:33	start	dmz	dmz	168.63.129.16	10.230.5.5	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	53425	allow	ProbeInternal	n/a	262
	03/27 14:47:29	end	dmz	dmz	168.63.129.16	10.230.5.5	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	53286	allow	ProbeInternal	tcp-rst-from-client	370
	03/27 14:47:29	end	untrust	untrust	168.63.129.16	10.230.1.5	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	53287	allow	ProbeExternal	tcp-rst-from-client	370
	03/27 14:47:27	start	untrust	untrust	168.63.129.16	10.230.1.5	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	53389	allow	ProbeExternal	n/a	262
	03/27 14:47:27	start	dmz	dmz	168.63.129.16	10.230.5.5	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	53388	allow	ProbeInternal	n/a	262
	03/27 14:47:23	end	dmz	dmz	168.63.129.16	10														
	03/27 14:47:23	end	untrust	untrust	168.63.129.16	10														
	03/27 14:47:21	start	dmz	dmz	168.63.129.16	10														

Dashboard | ACC | Monitor | Policies | Objects | Network | Device

Commit | Config

Manual

(addr.src in 168.63.129.16)

	Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Ingress I/F	Egress I/F	NAT Source Port	NAT Source IP	NAT Destination Port	NAT Dest IP	Application	IP Protocol	From Port	Action	Rule	Session End Reason	Bytes
	03/27 14:50:34	end	dmz	dmz	168.63.129.16	10.230.5.6	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	51322	allow	ProbeInternal	tcp-rst-from-client	370
	03/27 14:50:34	end	untrust	untrust	168.63.129.16	10.230.1.6	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	51321	allow	ProbeExternal	tcp-rst-from-client	370
	03/27 14:50:32	start	untrust	untrust	168.63.129.16	10.230.1.6	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	51434	allow	ProbeExternal	n/a	262
	03/27 14:50:32	start	dmz	dmz	168.63.129.16	10.230.5.6	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	51435	allow	ProbeInternal	n/a	262
	03/27 14:50:28	end	dmz	dmz	168.63.129.16	10.230.5.6	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	51267	allow	ProbeInternal	tcp-rst-from-client	370
	03/27 14:50:28	end	untrust	untrust	168.63.129.16	10.230.1.6	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	51268	allow	ProbeExternal	tcp-rst-from-client	370
	03/27 14:50:26	start	untrust	untrust	168.63.129.16	10.230.1.6	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	51387	allow	ProbeExternal	n/a	262
	03/27 14:50:26	start	dmz	dmz	168.63.129.16	10.230.5.6	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	51388	allow	ProbeInternal	n/a	262
	03/27 14:50:22	end	untrust	untrust	168.63.129.16	10.230.1.6	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	51234	allow	ProbeExternal	tcp-rst-from-client	370
	03/27 14:50:22	end	dmz	dmz	168.63.129.16	10.230.5.6	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	51233	allow	ProbeInternal	tcp-rst-from-client	370
	03/27 14:50:20	start	dmz	dmz	168.63.129.16	10.230.5.6	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	51353	allow	ProbeInternal	n/a	262
	03/27 14:50:20	start	untrust	untrust	168.63.129.16	10.230.1.6	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	51352	allow	ProbeExternal	n/a	262
	03/27 14:50:16	end	dmz	dmz	168.63.129.16	10.230.5.6	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	51211	allow	ProbeInternal	tcp-rst-from-client	370
	03/27 14:50:16	end	untrust	untrust	168.63.129.16	10.230.1.6	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	51210	allow	ProbeExternal	tcp-rst-from-client	370
	03/27 14:50:14	start	dmz	dmz	168.63.129.16	10.230.5.6	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	51322	allow	ProbeInternal	n/a	262
	03/27 14:50:14	start	untrust	untrust	168.63.129.16	10.230.1.6	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	51321	allow	ProbeExternal	n/a	262
	03/27 14:50:10	end	dmz	dmz	168.63.129.16	10.230.5.6	22	ethernet1/2	ethernet1/2	0		0		ssh	tcp	51183	allow	ProbeInternal	tcp-rst-from-client	370
	03/27 14:50:10	end	untrust	untrust	168.63.129.16	10.230.1.6	22	ethernet1/1	ethernet1/1	0		0		ssh	tcp	51182	allow	ProbeExternal	tcp-rst-from-client	370

FW1 & FW2 outbound traffic logs

Dashboard | ACC | Monitor | Policies | Objects | Network | Device

Commit

(port.dst eq 80)

Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Egress I/F	Ingress I/F	NAT Source Port	NAT Source IP	NAT Destination Port	NAT Dest IP	Application	IP Protocol	From Port	Action	Rule	Session End Reason	Bytes
03/27 15:31:25	end	dmz	untrust	10.231.1.4	91.189.91.26	80	ethernet1/1	ethernet1/2	31663	10.230.1.5	80	91.189.91.26	apt-get	tcp	53090	allow	OutboundAll	tcp-fin	96.9k
03/27 15:31:10	start	dmz	untrust	10.231.1.4	91.189.91.26	80	ethernet1/1	ethernet1/2	31663	10.230.1.5	80	91.189.91.26	apt-get	tcp	53090	allow	OutboundAll	n/a	496
03/27 15:31:10	start	dmz	untrust	10.231.1.4	91.189.91.26	80	ethernet1/1	ethernet1/2	31663	10.230.1.5	80	91.189.91.26	web-browsing	tcp	53090	allow	OutboundAll	n/a	496
03/27 15:10:53	end	dmz	untrust	10.232.1.4	13.91.129.249	80	ethernet1/1	ethernet1/2	49515	10.230.1.5	80	13.91.129.249	apt-get	tcp	60868	allow	OutboundAll	tcp-fin	174.0k
03/27 15:10:38	start	dmz	untrust	10.232.1.4	13.91.129.249	80	ethernet1/1	ethernet1/2	49515	10.230.1.5	80	13.91.129.249	apt-get	tcp	60868	allow	OutboundAll	n/a	492
03/27 15:10:38	start	dmz	untrust	10.232.1.4	13.91.129.249	80	ethernet1/1	ethernet1/2	49515	10.230.1.5	80	13.91.129.249	web-browsing	tcp	60868	allow	OutboundAll	n/a	492
03/27 15:07:24	end	dmz	untrust	10.231.1.4	91.189.88.149	80	ethernet1/1	ethernet1/2	64100	10.230.1.5	80	91.189.88.149	apt-get	tcp	53506	allow	OutboundAll	tcp-fin	96.9k
03/27 15:07:08	start	dmz	untrust	10.231.1.4	91.189.88.149	80	ethernet1/1	ethernet1/2	64100	10.230.1.5	80	91.189.88.149	apt-get	tcp	53506	allow	OutboundAll	n/a	496
03/27 15:07:08	start	dmz	untrust	10.231.1.4	91.189.88.149	80	ethernet1/1	ethernet1/2	64100	10.230.1.5	80	91.189.88.149	web-browsing	tcp	53506	allow	OutboundAll	n/a	496
03/27 14:46:52	end	dmz	untrust	10.232.1.4	91.189.88.149	80	ethernet1/1	ethernet1/2	35599	10.230.1.5	80	91.189.88.149	apt-get	tcp	36902	allow	OutboundAll	tcp-fin	96.9k
03/27 14:46:36	start	dmz	untrust	10.232.1.4	91.189.88.149	80	ethernet1/1	ethernet1/2	35599	10.230.1.5	80	91.189.88.149	apt-get	tcp	36902	allow	OutboundAll	n/a	496
03/27 14:46:36	start	dmz	untrust	10.232.1.4	91.189.88.149	80	ethernet1/1	ethernet1/2	35599	10.230.1.5	80	91.189.88.149	web-browsing	tcp	36902	allow	OutboundAll	n/a	496
03/27 14:43:22	end	dmz	untrust	10.231.1.4	91.189.88.162	80	ethernet1/1	ethernet1/2	58123	10.230.1.5	80	91.189.88.162	apt-get	tcp	33318	allow	OutboundAll	tcp-fin	96.9k

Dashboard | ACC | Monitor | Policies | Objects | Network | Device

Commit | Config

Manual

(port.dst eq 80)

Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Ingress I/F	Egress I/F	NAT Source Port	NAT Source IP	NAT Destination Port	NAT Dest IP	Application	IP Protocol	From Port	Action	Rule	Session End Reason	Bytes
03/27 15:31:24	end	dmz	untrust	10.231.1.4	13.91.129.249	80	ethernet1/2	ethernet1/1	44655	10.230.1.6	80	13.91.129.249	apt-get	tcp	56592	allow	OutboundAll	tcp-fin	174.5k
03/27 15:31:09	start	dmz	untrust	10.231.1.4	13.91.129.249	80	ethernet1/2	ethernet1/1	44655	10.230.1.6	80	13.91.129.249	apt-get	tcp	56592	allow	OutboundAll	n/a	492
03/27 15:31:09	start	dmz	untrust	10.231.1.4	13.91.129.249	80	ethernet1/2	ethernet1/1	44655	10.230.1.6	80	13.91.129.249	web-browsing	tcp	56592	allow	OutboundAll	n/a	492
03/27 15:10:53	end	dmz	untrust	10.232.1.4	91.189.88.149	80	ethernet1/2	ethernet1/1	50306	10.230.1.6	80	91.189.88.149	apt-get	tcp	42970	allow	OutboundAll	tcp-fin	96.3k
03/27 15:10:37	start	dmz	untrust	10.232.1.4	91.189.88.149	80	ethernet1/2	ethernet1/1	50306	10.230.1.6	80	91.189.88.149	apt-get	tcp	42970	allow	OutboundAll	n/a	496
03/27 15:10:37	start	dmz	untrust	10.232.1.4	91.189.88.149	80	ethernet1/2	ethernet1/1	50306	10.230.1.6	80	91.189.88.149	web-browsing	tcp	42970	allow	OutboundAll	n/a	496
03/27 15:07:24	end	dmz	untrust	10.231.1.4	13.91.129.249	80	ethernet1/2	ethernet1/1	3178	10.230.1.6	80	13.91.129.249	apt-get	tcp	50516	allow	OutboundAll	tcp-fin	174.5k
03/27 15:07:08	start	dmz	untrust	10.231.1.4	13.91.129.249	80	ethernet1/2	ethernet1/1	3178	10.230.1.6	80	13.91.129.249	apt-get	tcp	50516	allow	OutboundAll	n/a	492
03/27 15:07:08	start	dmz	untrust	10.231.1.4	13.91.129.249	80	ethernet1/2	ethernet1/1	3178	10.230.1.6	80	13.91.129.249	web-browsing	tcp	50516	allow	OutboundAll	n/a	492
03/27 14:46:52	end	dmz	untrust	10.232.1.4	13.91.129.249	80	ethernet1/2	ethernet1/1	2037	10.230.1.6	80	13.91.129.249	apt-get	tcp	54800	allow	OutboundAll	tcp-fin	174.3k
03/27 14:46:36	start	dmz	untrust	10.232.1.4	13.91.129.249	80	ethernet1/2	ethernet1/1	2037	10.230.1.6	80	13.91.129.249	apt-get	tcp	54800	allow	OutboundAll	n/a	492
03/27 14:46:36	start	dmz	untrust	10.232.1.4	13.91.129.249	80	ethernet1/2	ethernet1/1	2037	10.230.1.6	80	13.91.129.249	web-browsing	tcp	54800	allow	OutboundAll	n/a	492

FW1 & FW2 inbound traffic logs

Dashboard | ACC | Monitor | Policies | Objects | Network | Device

Commit

(zone.src eq untrust) and (zone.dst eq dmz) and (app eq web-browsing)

Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Egress I/F	Ingress I/F	NAT Source Port	NAT Source IP	NAT Destination Port	NAT Dest IP	Application	IP Protocol	From Port	Action	Rule	Session End Reason	Bytes
03/27 16:35:25	end	untrust	dmz	68.15.90.134	52.180.88.100	81	ethernet1/2	ethernet1/1	62354	10.230.5.5	80	10.231.1.4	web-browsing	tcp	36012	allow	InternetInbound	tcp-rst-from-client	7.4k
03/27 16:34:59	start	untrust	dmz	68.15.90.134	52.180.88.100	81	ethernet1/2	ethernet1/1	62354	10.230.5.5	80	10.231.1.4	web-browsing	tcp	36012	allow	InternetInbound	n/a	741
03/27 16:10:02	end	untrust	dmz	68.15.90.134	52.180.88.100	81	ethernet1/2	ethernet1/1	54255	10.230.5.5	80	10.231.1.4	web-browsing	tcp	39789	allow	InternetInbound	tcp-fin	5.0k
03/27 16:09:48	end	untrust	dmz	68.15.90.134	52.180.88.100	82	ethernet1/2	ethernet1/1	33672	10.230.5.5	80	10.232.1.4	web-browsing	tcp	34326	allow	InternetInbound	tcp-fin	2.9k
03/27 16:09:40	start	untrust	dmz	68.15.90.134	52.180.88.100	81	ethernet1/2	ethernet1/1	54255	10.230.5.5	80	10.231.1.4	web-browsing	tcp	39789	allow	InternetInbound	n/a	741
03/27 16:09:38	end	untrust	dmz	68.15.90.134	52.180.88.100	82	ethernet1/2	ethernet1/1	7919	10.230.5.5	80	10.232.1.4	web-browsing	tcp	46102	allow	InternetInbound	tcp-fin	2.3k
03/27 16:09:26	start	untrust	dmz	68.15.90.134	52.180.88.100	82	ethernet1/2	ethernet1/1	33672	10.230.5.5	80	10.232.1.4	web-browsing	tcp	34326	allow	InternetInbound	n/a	703
03/27 16:09:14	start	untrust	dmz	68.15.90.134	52.180.88.100	82	ethernet1/2	ethernet1/1	7919	10.230.5.5	80	10.232.1.4	web-browsing	tcp	46102	allow	InternetInbound	n/a	703
03/27 16:09:08	end	untrust	dmz	68.15.90.134	52.180.88.100	81	ethernet1/2	ethernet1/1	48300	10.230.5.5	80	10.231.1.4	web-browsing	tcp	46264	allow	InternetInbound	tcp-fin	3.9k
03/27 16:09:03	end	untrust	dmz	68.15.90.134	52.180.88.100	81	ethernet1/2	ethernet1/1	39724	10.230.5.5	80	10.231.1.4	web-browsing	tcp	48214	allow	InternetInbound	tcp-rst-from-server	1.7k
03/27 16:08:59	end	untrust	dmz	68.15.90.134	52.180.88.100	81	ethernet1/2	ethernet1/1	21501	10.230.5.5	80	10.231.1.4	web-browsing	tcp	38502	allow	InternetInbound	tcp-fin	2.6k
03/27 16:08:46	start																		

Dashboard | ACC | Monitor | Policies | Objects | Network | Device

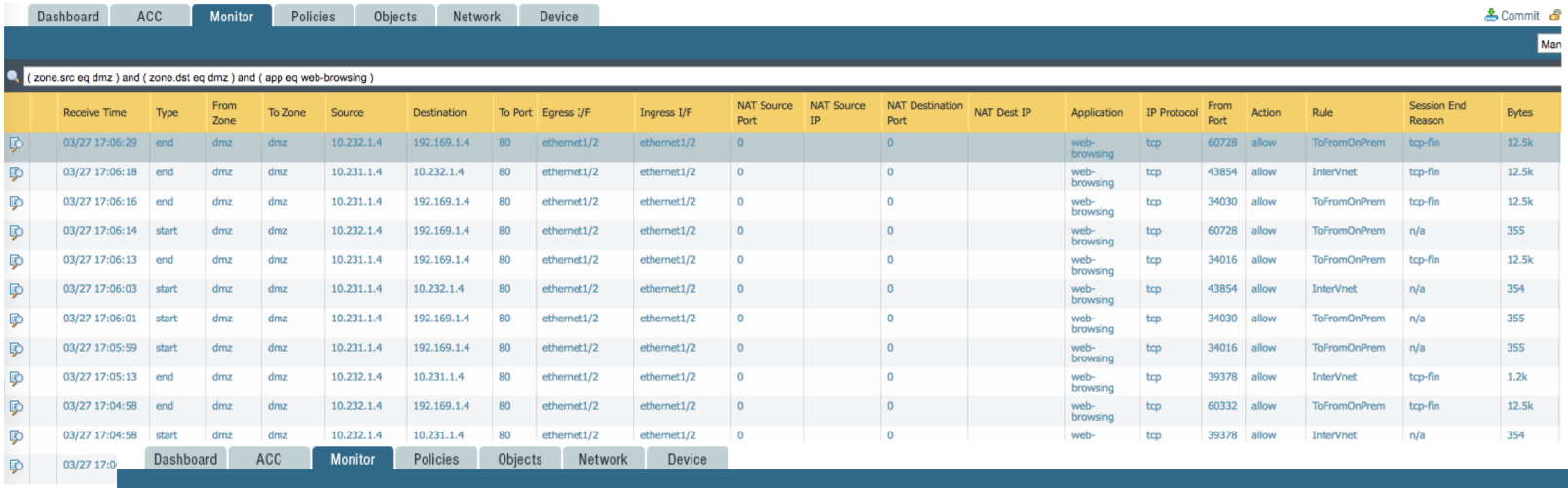
Commit | Config

Manual

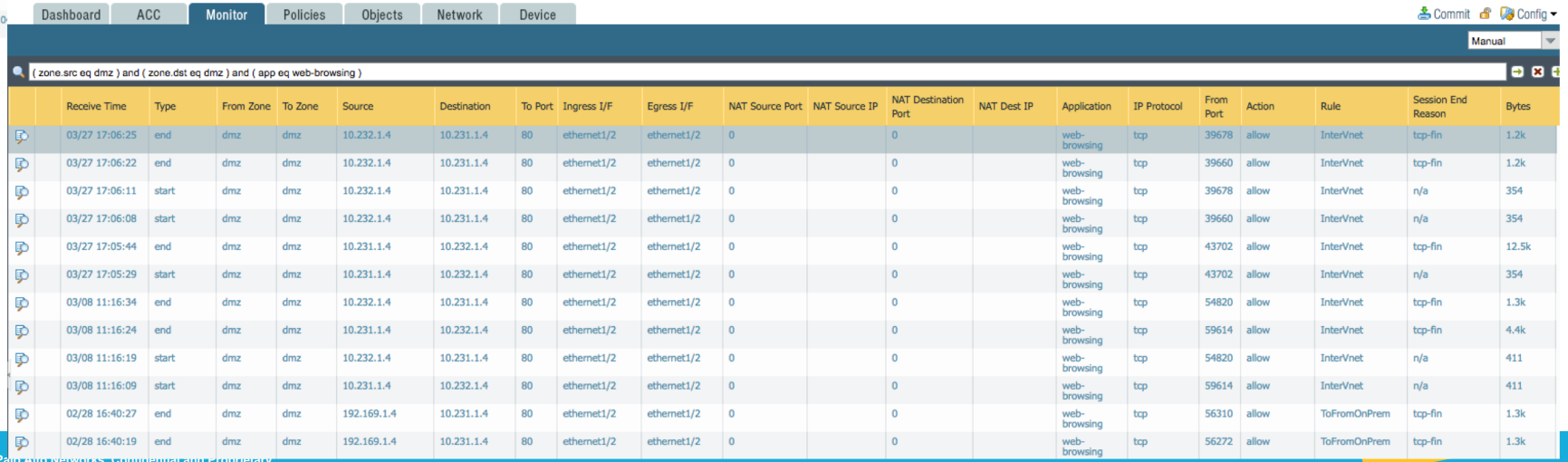
(zone.src eq untrust) and (zone.dst eq dmz) and (app eq web-browsing)

Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Ingress I/F	Egress I/F	NAT Source Port	NAT Source IP	NAT Destination Port	NAT Dest IP	Application	IP Protocol	From Port	Action	Rule	Session End Reason	Bytes
03/27 16:38:02	end	untrust	dmz	68.15.90.134	52.180.88.100	81	ethernet1/1	ethernet1/2	21408	10.230.5.6	80	10.231.1.4	web-browsing	tcp	36595	allow	InternetInbound	tcp-fin	8.4k
03/27 16:37:46	end	untrust	dmz	68.15.90.134	52.180.88.100	82	ethernet1/1	ethernet1/2	46661	10.230.5.6	80	10.232.1.4	web-browsing	tcp	41571	allow	InternetInbound	tcp-fin	30.5k
03/27 16:37:46	end	untrust	dmz	68.15.90.134	52.180.88.100	82	ethernet1/1	ethernet1/2	2125	10.230.5.6	80	10.232.1.4	web-browsing	tcp	46167	allow	InternetInbound	tcp-fin	6.1k
03/27 16:37:37	start	untrust	dmz	68.15.90.134	52.180.88.100	81	ethernet1/1	ethernet1/2	21408	10.230.5.6	80	10.231.1.4	web-browsing	tcp	36595	allow	InternetInbound	n/a	741
03/27 16:37:23	start	untrust	dmz	68.15.90.134	52.180.88.100	82	ethernet1/1	ethernet1/2	2125	10.230.5.6	80	10.232.1.4	web-browsing	tcp	46167	allow	InternetInbound	n/a	703
03/27 16:37:23	start	untrust	dmz	68.15.90.134	52.180.88.100	82	ethernet1/1	ethernet1/2	46661	10.230.5.6	80	10.232.1.4	web-browsing	tcp	41571	allow	InternetInbound	n/a	743
03/27 16:35:41	end	untrust	dmz	68.15.90.134	52.180.88.100	82	ethernet1/1	ethernet1/2	6553	10.230.5.6	80	10.232.1.4	web-browsing	tcp	38985	allow	InternetInbound	tcp-fin	7.8k
03/27 16:35:38	end	untrust	dmz	68.15.90.134	52.180.88.100	82	ethernet1/1	ethernet1/2	16481	10.230.5.6	80	10.232.1.4	web-browsing	tcp	34907	allow	InternetInbound	tcp-fin	39.2k
03/27 16:35:11	start	untrust	dmz	68.15.90.134	52.180.88.100	82	ethernet1/1	ethernet1/2	6553	10.230.5.6	80	10.232.1.4	web-browsing	tcp	38985	allow	InternetInbound	n/a	703
03/27 16:35:11	start	untrust	dmz	68.15.90.134	52.180.88.100	82	ethernet1/1	ethernet1/2	16481	10.230.5.6	80	10.232.1.4	web-browsing	tcp	34907	allow	InternetInbound	n/a	743
03/27 16:09:49	end	untrust	dmz	68.15.90.134	52.180.88.100	82	ethernet1/1	ethernet1/2	5825	10.230.5.6	80	10.232.1.4	web-browsing	tcp	36344	allow	InternetInbound	tcp-fin	13.5k
03/27 16:09:39	end	untrust	dmz	68.15.90.134	52.180.88.100	82	ethernet1/1	ethernet1/2	37196	10.230.5.6	80	10.232.1.4	web-browsing	tcp	40523	allow	InternetInbound	tcp-fin	19.4k

FW1 & FW2 east-west / on-prem traffic logs



Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Egress I/F	Ingress I/F	NAT Source Port	NAT Source IP	NAT Destination Port	NAT Dest IP	Application	IP Protocol	From Port	Action	Rule	Session End Reason	Bytes
03/27 17:06:29	end	dmz	dmz	10.232.1.4	192.169.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	60728	allow	ToFromOnPrem	tcp-fin	12.5k
03/27 17:06:18	end	dmz	dmz	10.231.1.4	10.232.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	43854	allow	InterVnet	tcp-fin	12.5k
03/27 17:06:16	end	dmz	dmz	10.231.1.4	192.169.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	34030	allow	ToFromOnPrem	tcp-fin	12.5k
03/27 17:06:14	start	dmz	dmz	10.232.1.4	192.169.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	60728	allow	ToFromOnPrem	n/a	355
03/27 17:06:13	end	dmz	dmz	10.231.1.4	192.169.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	34016	allow	ToFromOnPrem	tcp-fin	12.5k
03/27 17:06:03	start	dmz	dmz	10.231.1.4	10.232.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	43854	allow	InterVnet	n/a	354
03/27 17:06:01	start	dmz	dmz	10.231.1.4	192.169.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	34030	allow	ToFromOnPrem	n/a	355
03/27 17:05:59	start	dmz	dmz	10.231.1.4	192.169.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	34016	allow	ToFromOnPrem	n/a	355
03/27 17:05:13	end	dmz	dmz	10.232.1.4	10.231.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	39378	allow	InterVnet	tcp-fin	1.2k
03/27 17:04:58	end	dmz	dmz	10.232.1.4	192.169.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	60332	allow	ToFromOnPrem	tcp-fin	12.5k
03/27 17:04:58	start	dmz	dmz	10.232.1.4	10.231.1.4	80	ethernet1/2	ethernet1/2	0		0		web-	tcp	39378	allow	InterVnet	n/a	354
03/27 17:0																			



Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Ingress I/F	Egress I/F	NAT Source Port	NAT Source IP	NAT Destination Port	NAT Dest IP	Application	IP Protocol	From Port	Action	Rule	Session End Reason	Bytes
03/27 17:06:25	end	dmz	dmz	10.232.1.4	10.231.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	39678	allow	InterVnet	tcp-fin	1.2k
03/27 17:06:22	end	dmz	dmz	10.232.1.4	10.231.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	39660	allow	InterVnet	tcp-fin	1.2k
03/27 17:06:11	start	dmz	dmz	10.232.1.4	10.231.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	39678	allow	InterVnet	n/a	354
03/27 17:06:08	start	dmz	dmz	10.232.1.4	10.231.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	39660	allow	InterVnet	n/a	354
03/27 17:05:44	end	dmz	dmz	10.231.1.4	10.232.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	43702	allow	InterVnet	tcp-fin	12.5k
03/27 17:05:29	start	dmz	dmz	10.231.1.4	10.232.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	43702	allow	InterVnet	n/a	354
03/08 11:16:34	end	dmz	dmz	10.232.1.4	10.231.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	54820	allow	InterVnet	tcp-fin	1.3k
03/08 11:16:24	end	dmz	dmz	10.231.1.4	10.232.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	59614	allow	InterVnet	tcp-fin	4.4k
03/08 11:16:19	start	dmz	dmz	10.232.1.4	10.231.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	54820	allow	InterVnet	n/a	411
03/08 11:16:09	start	dmz	dmz	10.231.1.4	10.232.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	59614	allow	InterVnet	n/a	411
02/28 16:40:27	end	dmz	dmz	192.169.1.4	10.231.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	56310	allow	ToFromOnPrem	tcp-fin	1.3k
02/28 16:40:19	end	dmz	dmz	192.169.1.4	10.231.1.4	80	ethernet1/2	ethernet1/2	0		0		web-browsing	tcp	56272	allow	ToFromOnPrem	tcp-fin	1.3k

Conclusion

- Consider the flavor of load balancer in use both public and internal
- Decide between the step by step and the end to end probing
- Be aware of the cloud provider probe specifics
- Ensure proper VM-Series configuration

Thank You!