



COMMUNITY DAY

TEL AVIV



When the AWS ELB is just not enough...give me MOAR!!!!



Maish Saidel-Keesing | 2018

All things Cloud @CyberArk

@maishsk

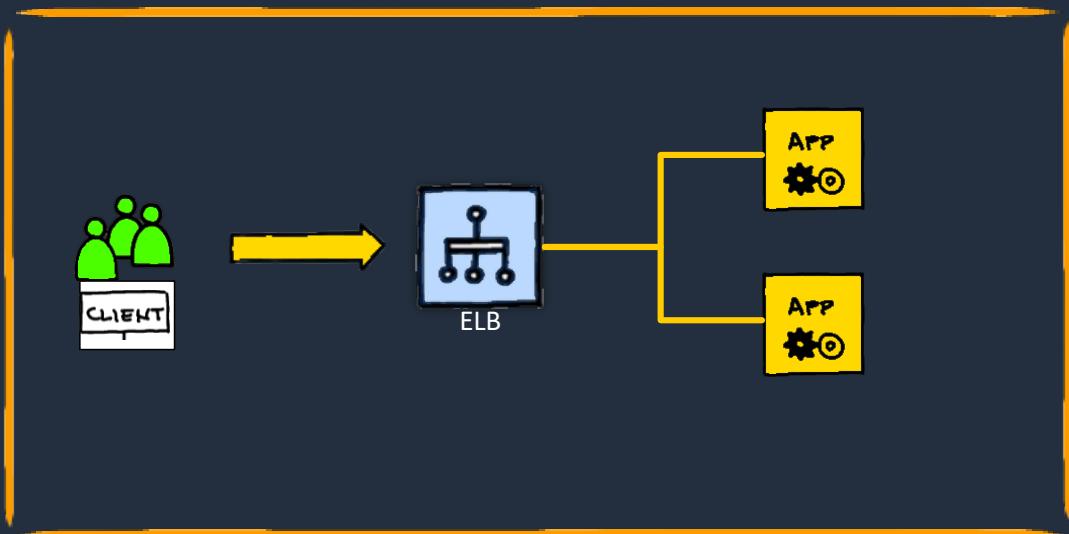


@maishsk



COMMUNITY DAY

Standard Load Balancing Scenario

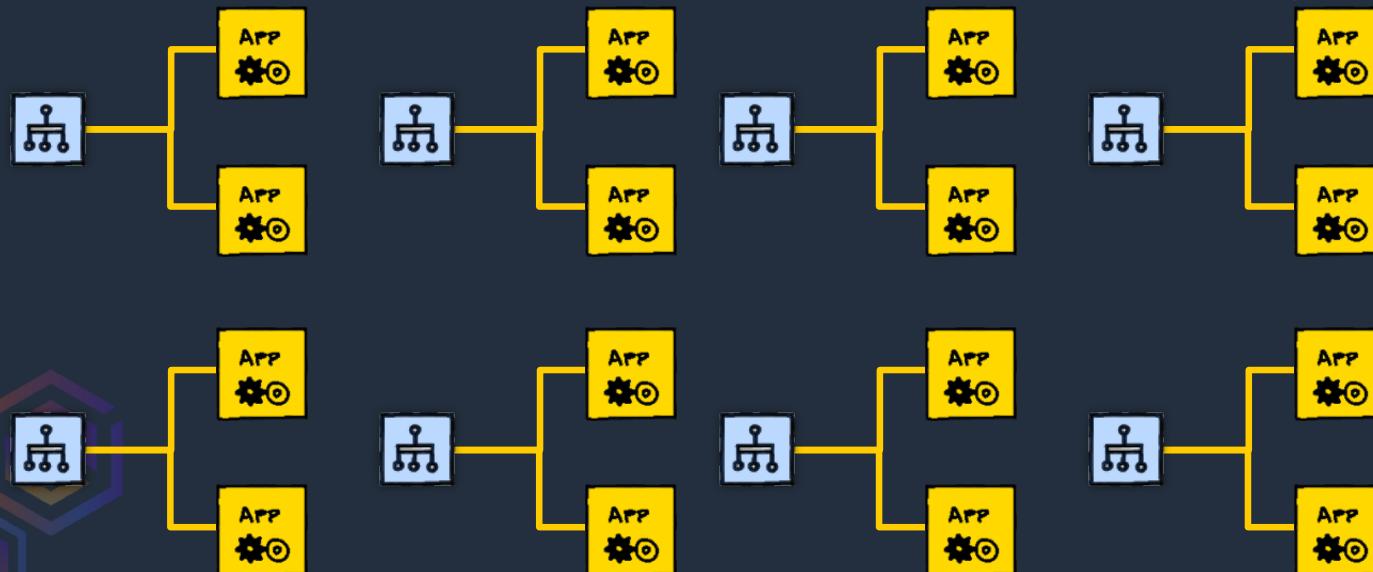


@maishsk



COMMUNITY DAY

All components use a Load Balancer

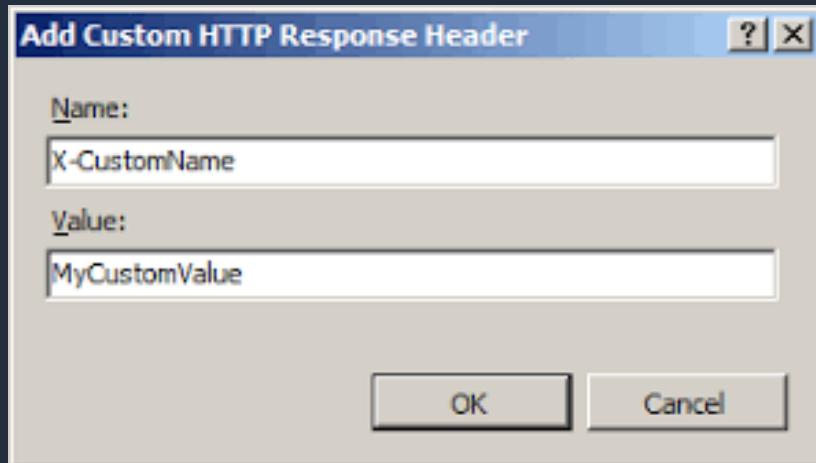


@maishsk



COMMUNITY DAY

Custom HTTP Headers



@maishsk



COMMUNITY DAY

ALB Routing options

maishsk-lb | HTTP:80 (2 rules)

RULE ID	IF (all match)
1 A rule ID (ARN) is generated when you save your rule.	<input type="text" value="Host is..."/> <input type="text" value="Host header"/> + Add condition

Technodrone © 2018

maishsk-lb | HTTP:80 (2 rules)

RULE ID	IF (all match)
1 A rule ID (ARN) is generated when you save your rule.	<input type="text" value="Path is..."/> <input type="text" value="Path"/> + Add condition

Technodrone © 2018



@maishsk



COMMUNITY DAY

Let me Introduce myself

Maish Saidel-Keesing

Cloud & DevOps Architect @CyberArk

Blogger, Author, Speaker

Automator of all things...

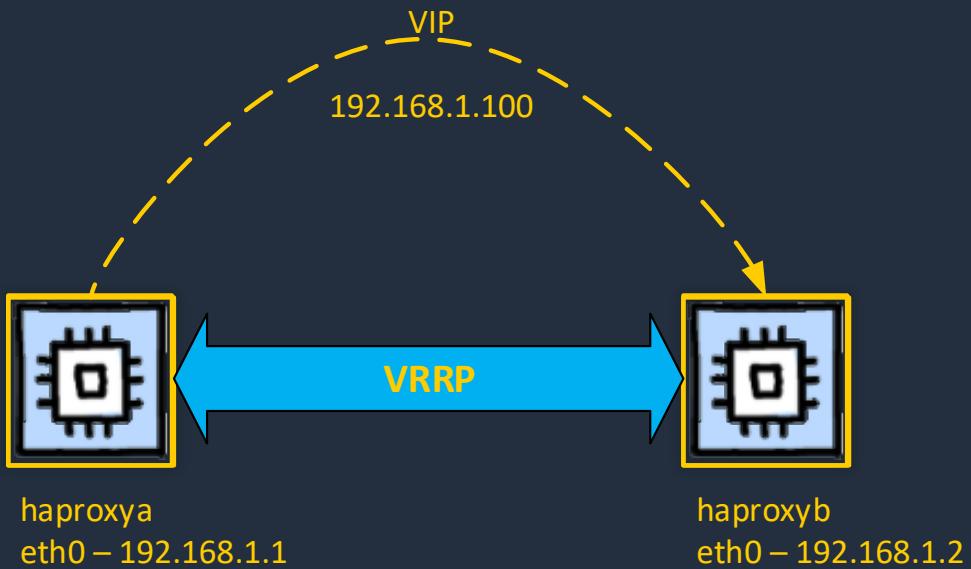


@maishsk



COMMUNITY DAY

Basic haproxy



@maishsk



COMMUNITY DAY

Challenges

- VRRP (Multicast)
 - Simple Use Unicast
- Secondary IP address
 - Add another IP to the interface...
- High Availability across AZ's
 - Not so simple...

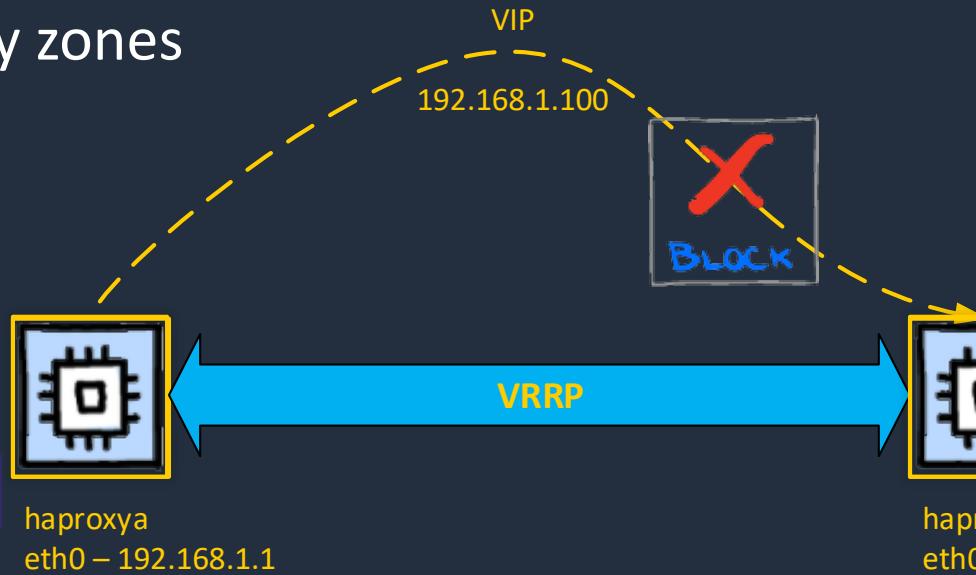


@maishsk



COMMUNITY DAY

haproxy across
availability zones

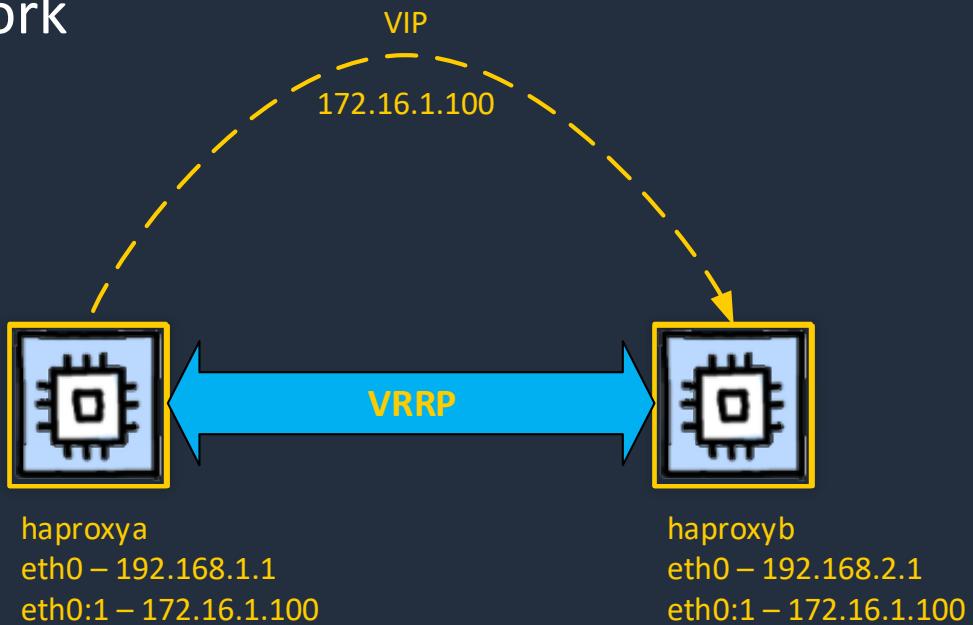


@maishsk



COMMUNITY DAY

Overlay network

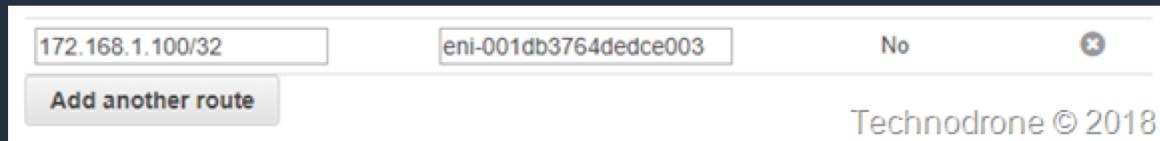


@maishsk



COMMUNITY DAY

Routing to the VIP

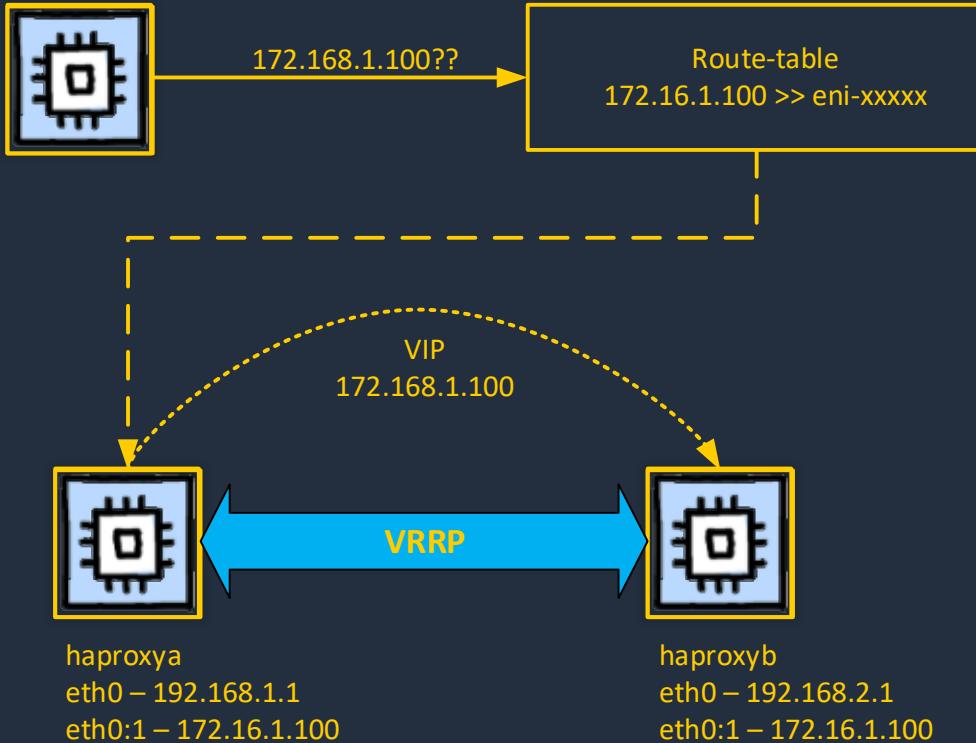


@maishsk



COMMUNITY DAY

Routing Example

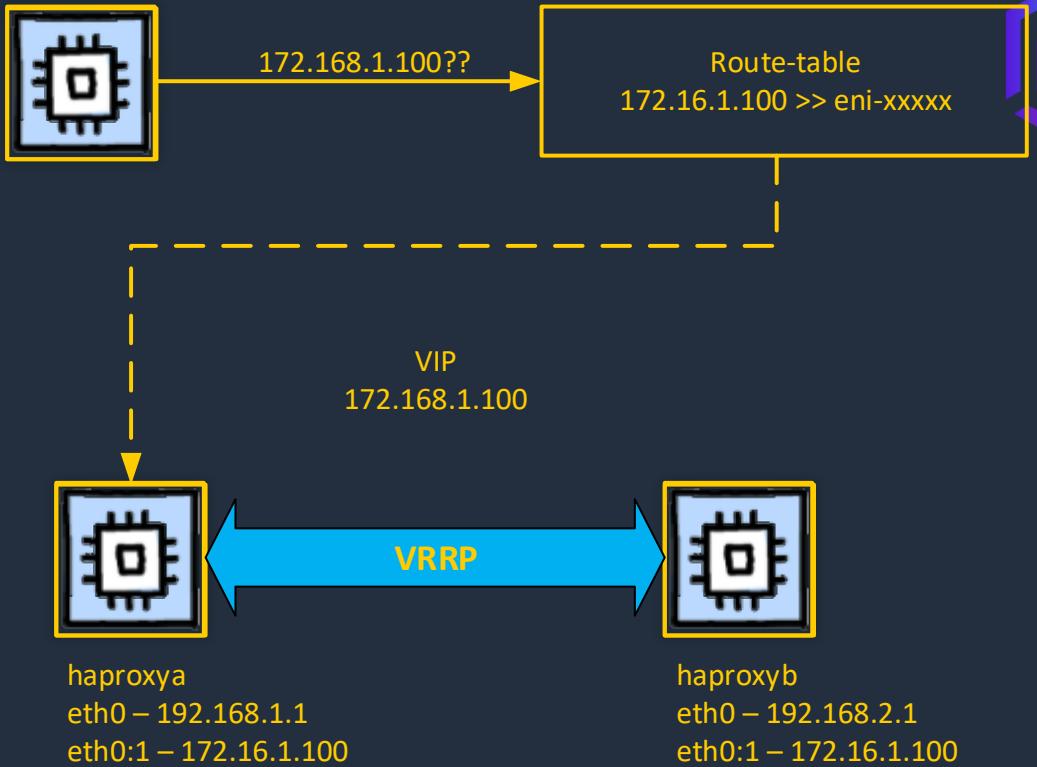


@maishsk



COMMUNITY DAY

All is good

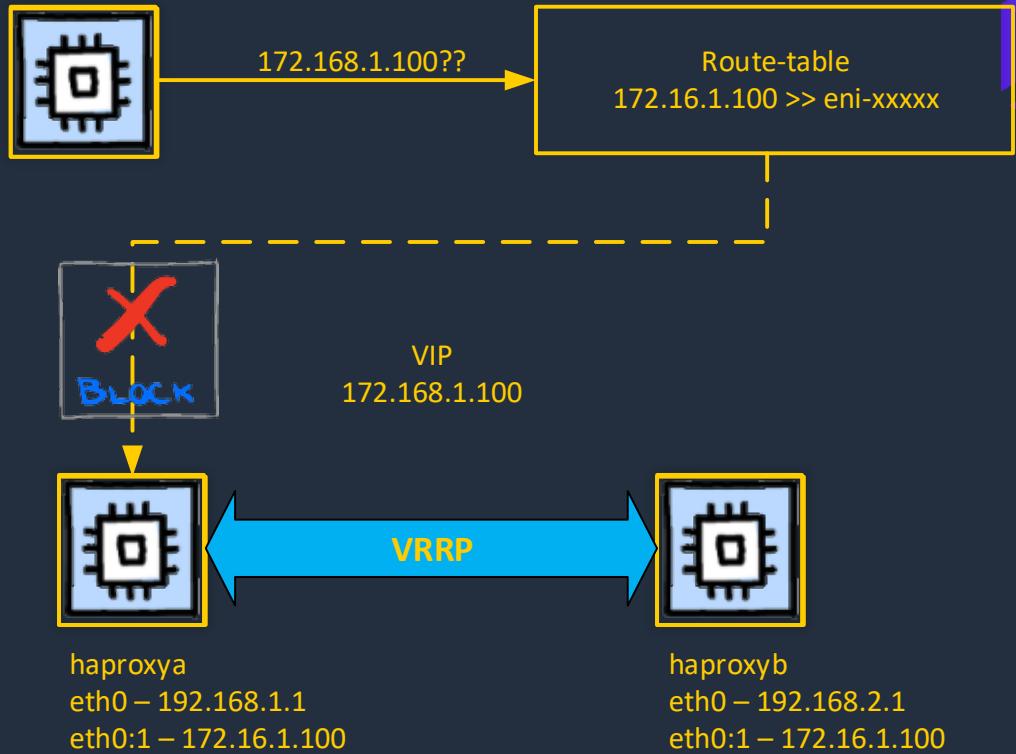


@maishsk



COMMUNITY DAY

AZ1 fails

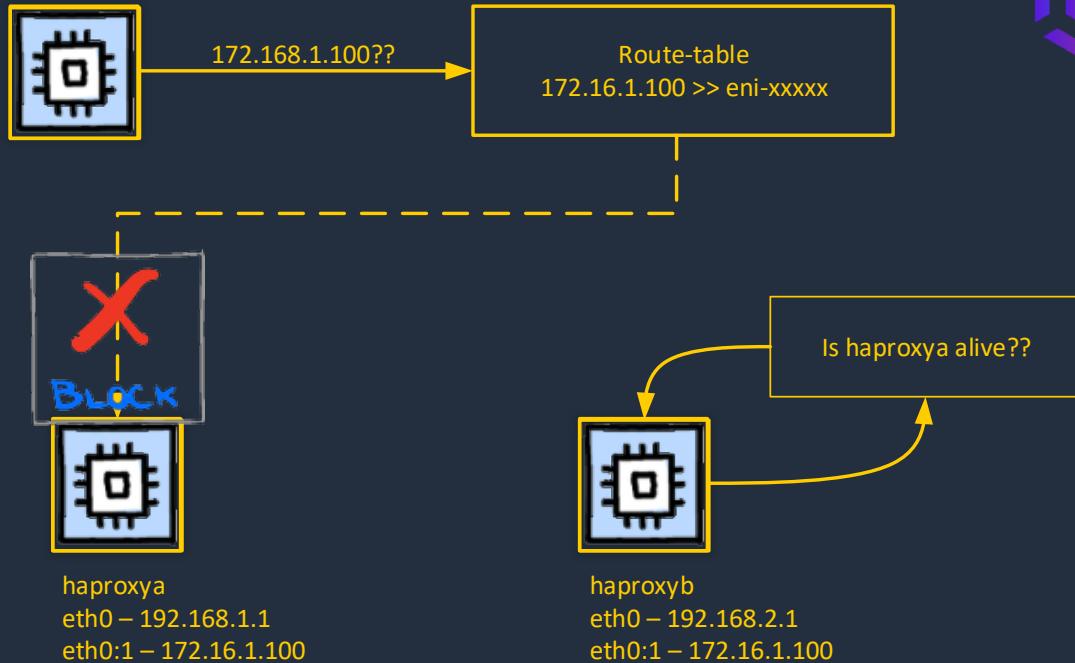


@maishsk



COMMUNITY DAY

haproxyb
awakens

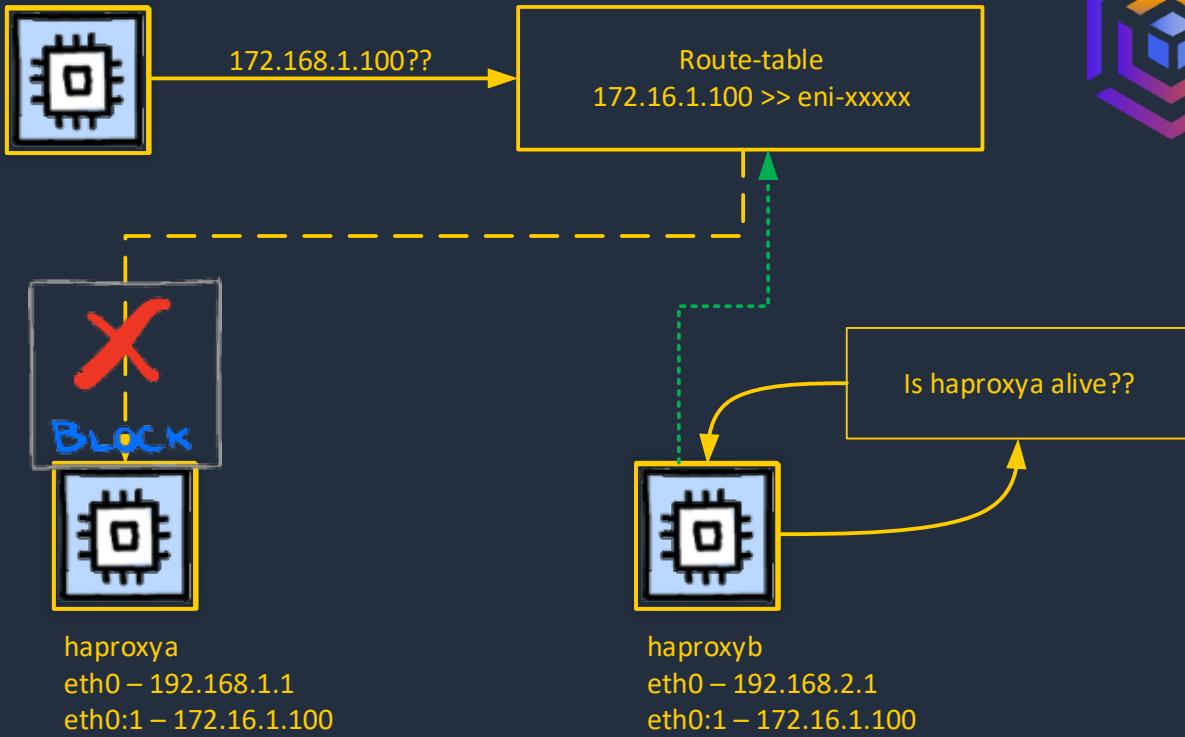


@maishsk



COMMUNITY DAY

Update
route
table

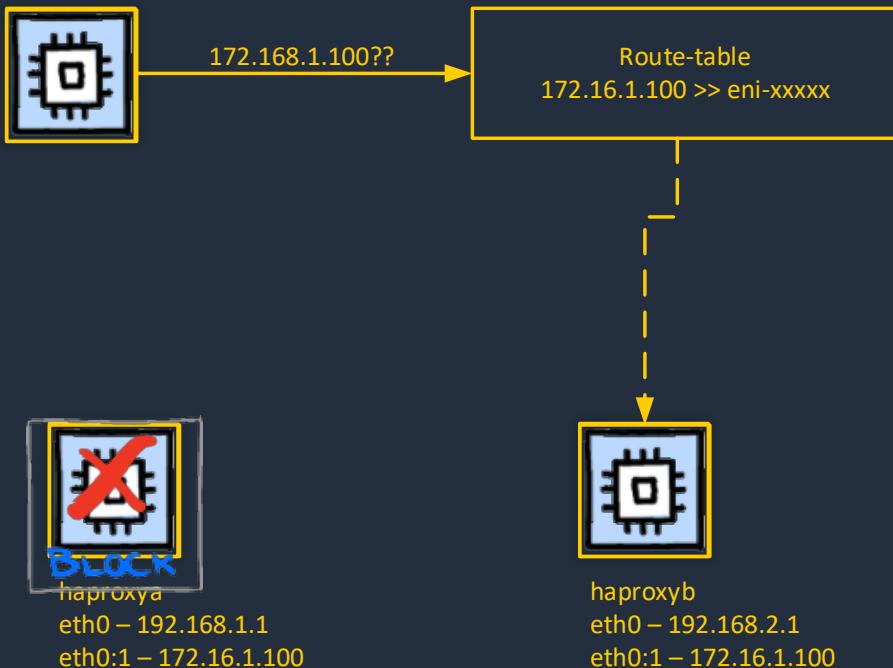


@maishsk



COMMUNITY DAY

Traffic flows



@maishsk



COMMUNITY DAY

Network Deep Dive

rtb-8f98b5e7 | Private-RT

Summary Routes Subnet Associations Route Propagation Tags

Edit

View: All rules

Destination	Target	Status	Propagated
192.168.100.0/24	local	Active	No
0.0.0.0/0	nat-013dd4b467dca7185	Active	No

Technodrone © 2018



@maishsk



COMMUNITY DAY

No Duplicates

Cancel Save A The route identified by 0.0.0.0/0 already exists.

View: All rules

Destination	Target	Status	Propagated	Remove
192.168.100.0/24	local	Active	No	
0.0.0.0/0	nat-013dd4b467dca7185	Active	No	×
10.20.0.0/16	vgw-f6850cc6	Active	No	×
pl-7ba54012	vpce-61e42008	Active	No	
0.0.0.0/0	nat-013dd4b467dca7185	No	Technodrone © 2018	×



@maishsk



COMMUNITY DAY

No Subsets

Cancel Save **A** cannot create a more specific route for 192.168.100.128/26 than CIDR 192.168.100.0/24 associated with the Code: InvalidParameterValue; Request ID: f352daa4-f4d0-4794-984d-6ac82074898d)

View: All rules

Destination	Target	Status
192.168.100.0/24	local	Active
0.0.0.0/0	nat-013dd4b467dca7185	Active
10.20.0.0/16	vgw-f6850cc6	Active
pl-7ba54012	vpce-61e42008	Active
192.168.100.128/26	nat-013dd4b467dca7185	Active

Add another route

Technodrone © 2018



@maishsk



COMMUNITY DAY

Virtual Interface

```
DEVICE="eth0:1"
BOOTPROTO="none"
MTU="1500"
ONBOOT="yes"
TYPE="Ethernet"
NETMASK=255.255.255.0
IPADDR=172.16.1.100
USERCTL=no
```



@maishsk



COMMUNITY DAY

Transferring the VIP

```
vrrp_instance haproxy {  
    [...]  
    notify /etc/keepalived/master.sh  
}
```



@maishsk



COMMUNITY DAY

master.sh script

```
aws ec2 replace-route --route-table-id <ROUTE_TABLE> \  
--destination-cidr-block <CIDR_BLOCK> \  
--instance-id <INSTANCE_ID>
```



@maishsk



COMMUNITY DAY

Automation

- <https://github.com/maishsk/replace-aws-elb>



@maishsk



COMMUNITY DAY

```
vpc_id: vpc-31721b59
keypair: maishsk-keypair
vpc_cidr_block: 192.168.100.0/24
region: us-east-2
virtual_ip: 192.168.55.100
instance_count: 2
instance_type: t2.large
use_public_ip: "no"
source_dest_check_enabled: "no"
iam_role: vrrp_Role
volume_type: gp2
root_disk_size: 50
component_name: haproxy
image_id: ami-0b59bfac6be064b78
policy_file: "./files/vrrp_policy.json"
trust_policy: "./files/trust_policy.json"
```

```
policyDescription: "Policy to allow HAProxy
to manage routes for high availability"
role_description: "Role to allow HAProxy
instances to manage routes for high
availability"
```

```
#### Security group rules for the component
component_rules:
```

- proto: tcp
from_port: 1
to_port: 65535
cidr_ip: "{{ vpc_cidr_block }}"



@maishsk



COMMUNITY DAY



@maishsk



COMMUNITY DAY

Closing thoughts

- Was it worth it?
- What was the hardest part of the solution?
- Was this all you were doing with haproxy?
- Did you save money?
- Does this scale?
- Other benefits?
- External facing load balancers?
- Why not use an EIP in the first place?



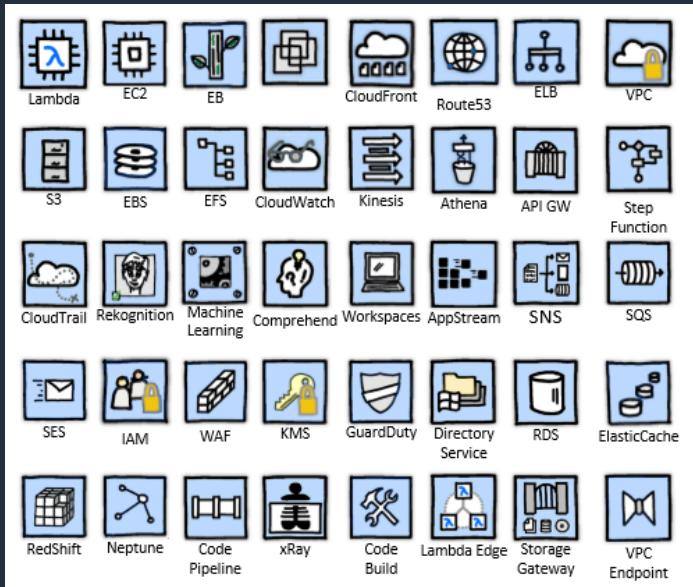
@maishsk



COMMUNITY DAY

- AWS Community Stencils

https://bit.ly/aws_visio



@maishsk