aws

COMMUNITY DAY

TEL AVIV

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

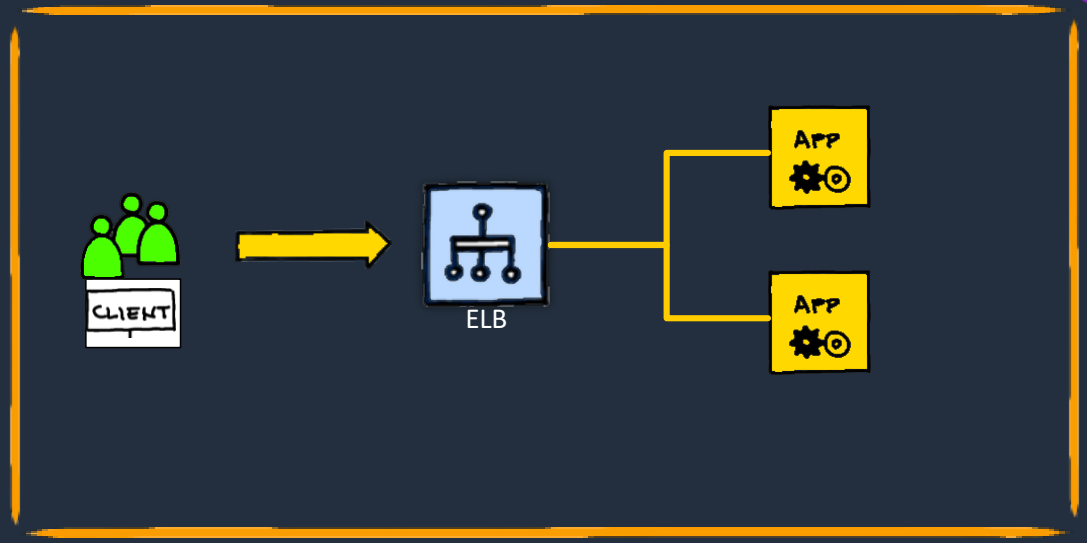
Maish Saidel-Keesing | 2018
All things Cloud @CyberArk
@maishsk

@maishsk

aws

COMMUNITY DAY

Standard Load Balancing Scenario

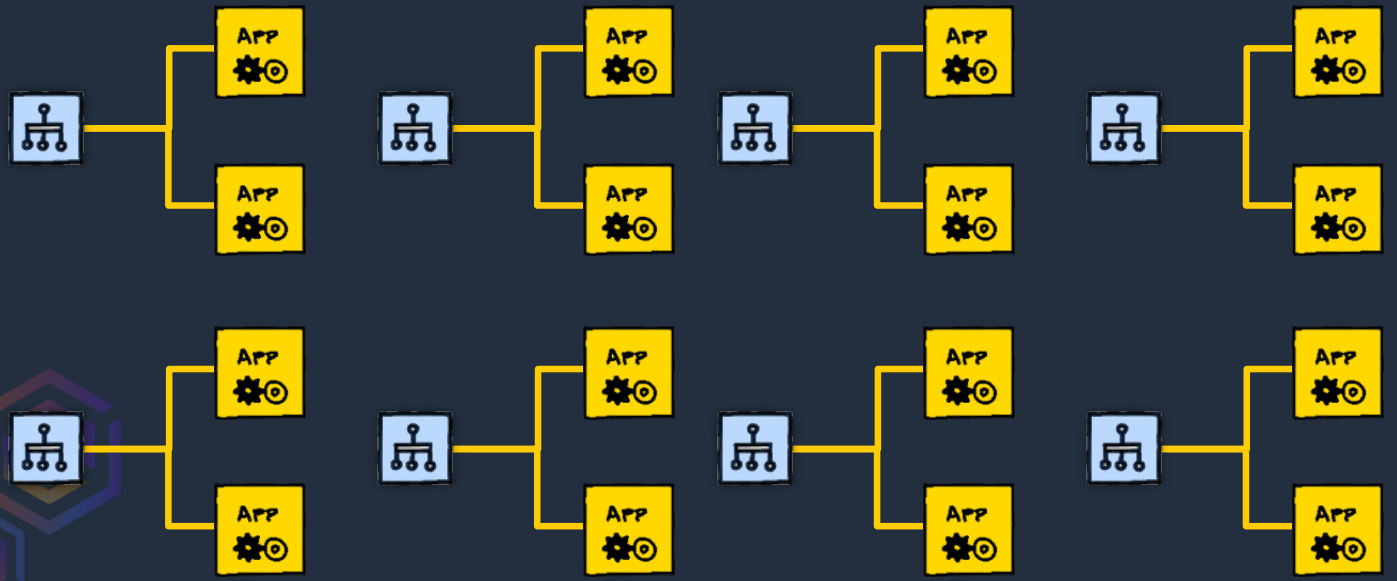


@maishsk

aws

COMMUNITY DAY

All components use a Load Balancer

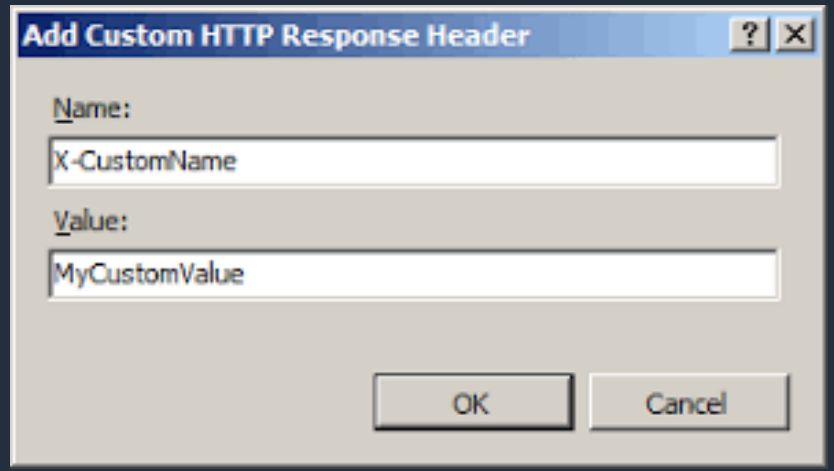


@maishsk

aws

COMMUNITY DAY

Custom HTTP Headers

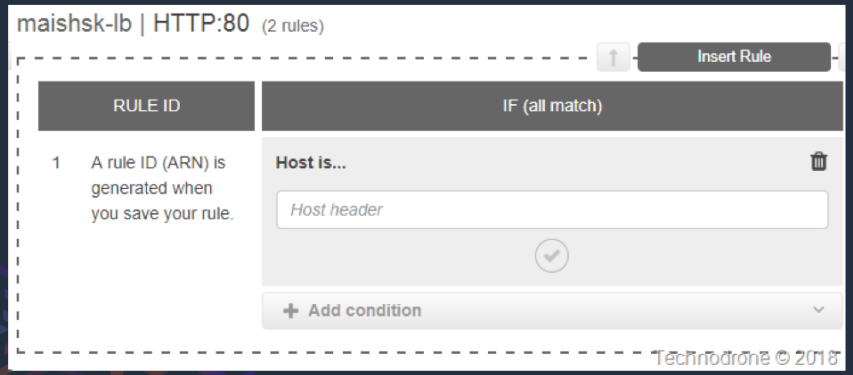


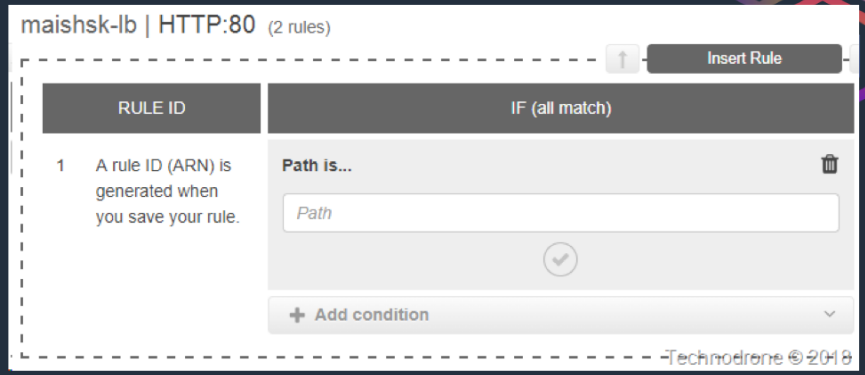
@maishsk

aws

COMMUNITY DAY

ALB Routing options





@maishsk

aws

COMMUNITY DAY

Let me Introduce myself

Maish Saidel-Keesing

Cloud & DevOps Architect @CyberArk

Blogger, Author, Speaker

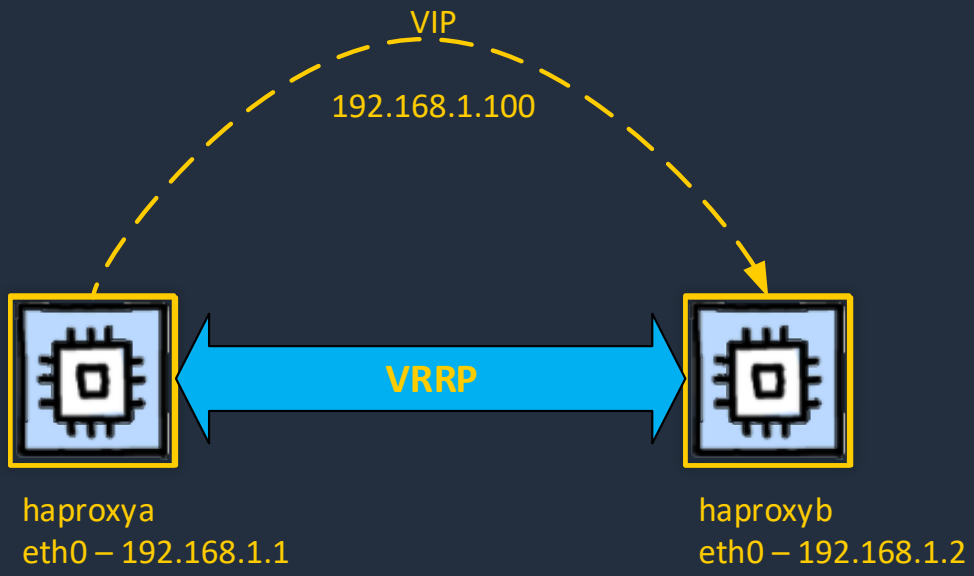
Automator of all things…

@maishsk

aws

COMMUNITY DAY

Basic haproxy



@maishsk

aws

COMMUNITY DAY

Challenges

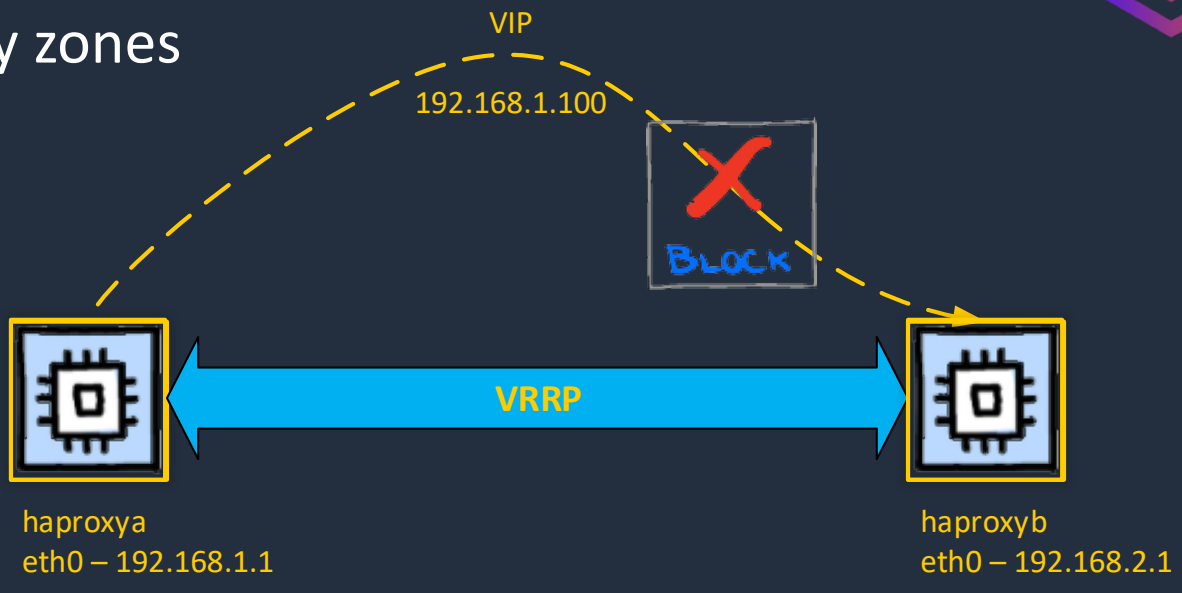
- VRRP (Multicast)
  - Simple …. Use Unicast
- Secondary IP address
  - Add another IP to the interface…
- High Availability across AZ's
  - Not so simple… 

@maishsk

aws

COMMUNITY DAY

haproxy across availability zones

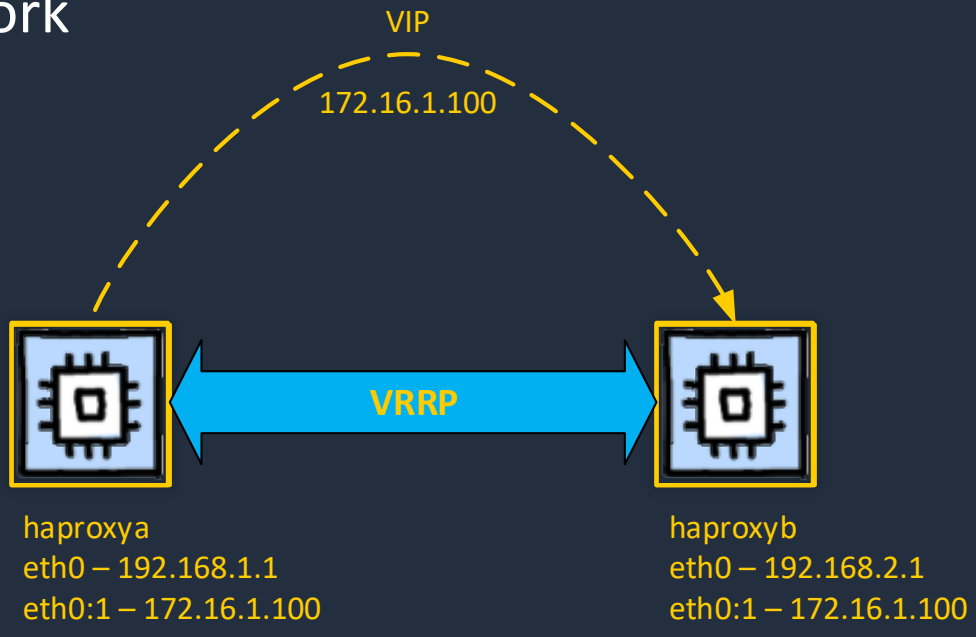


@maishsk

aws

COMMUNITY DAY

Overlay network



aws

COMMUNITY DAY

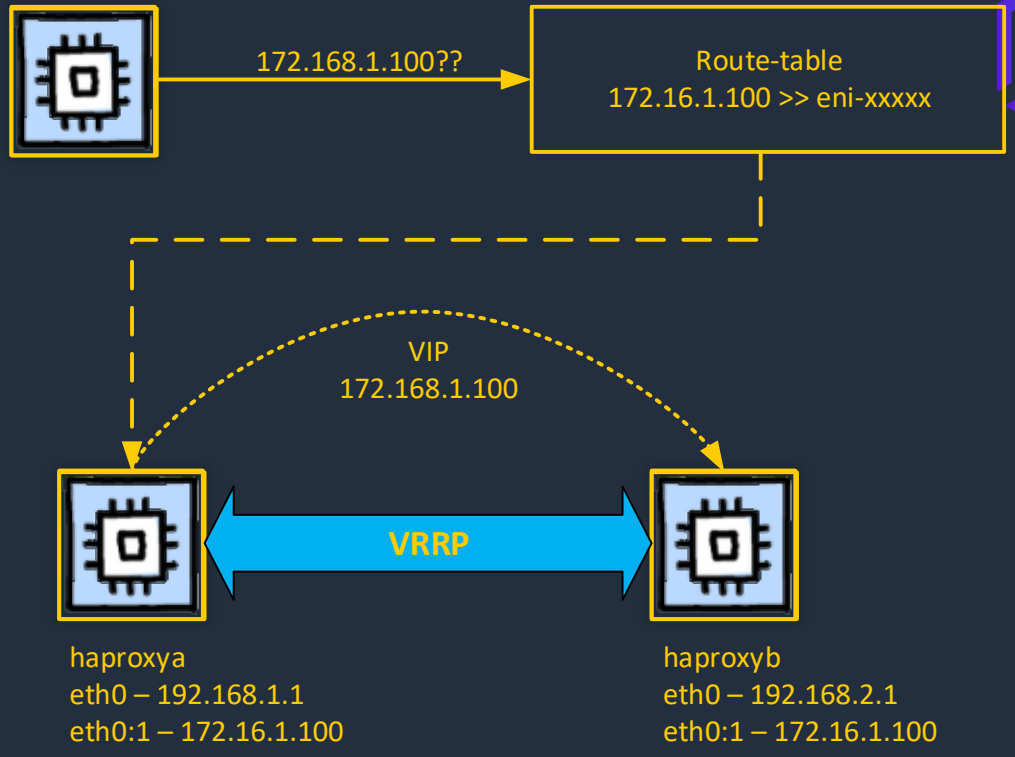
Routing to the VIP

@maishsk

aws

COMMUNITY DAY

Routing Example

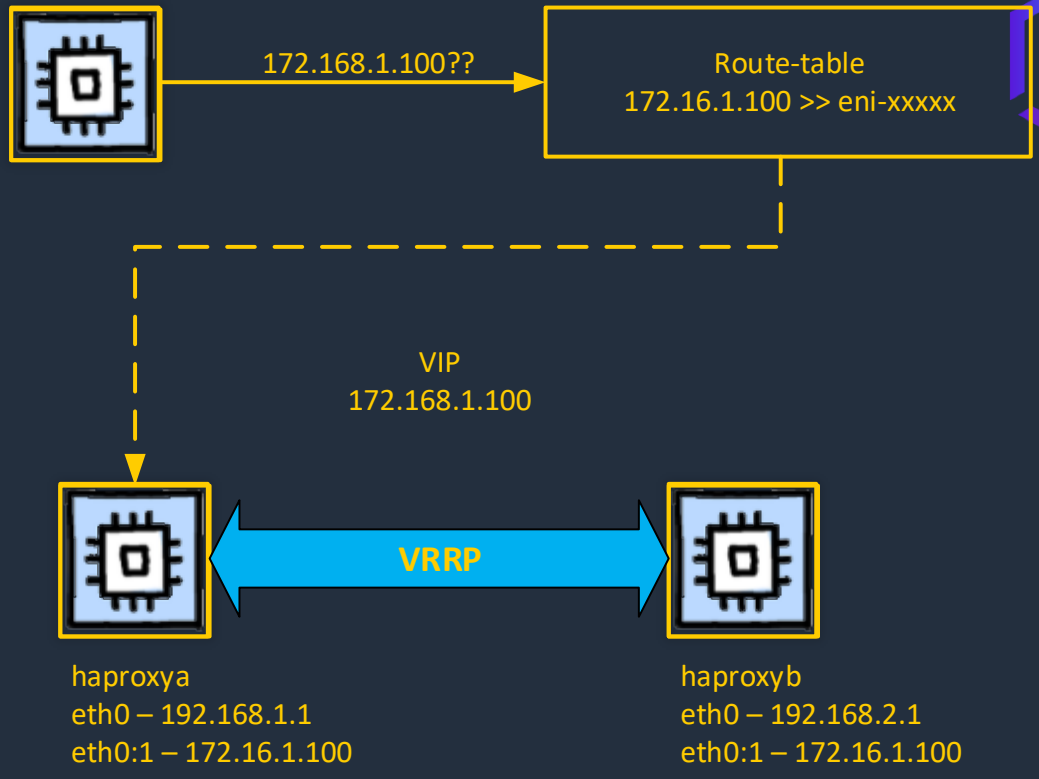


@maishsk

aws

COMMUNITY DAY

All is good

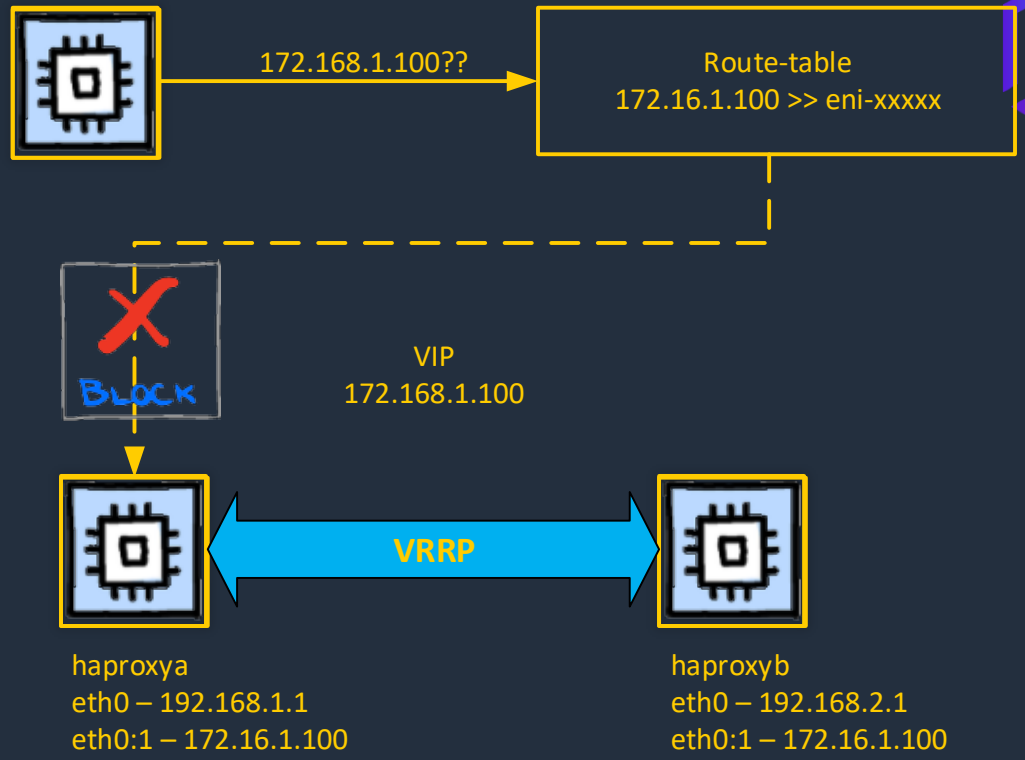


@maishsk

aws

COMMUNITY DAY

AZ1 fails

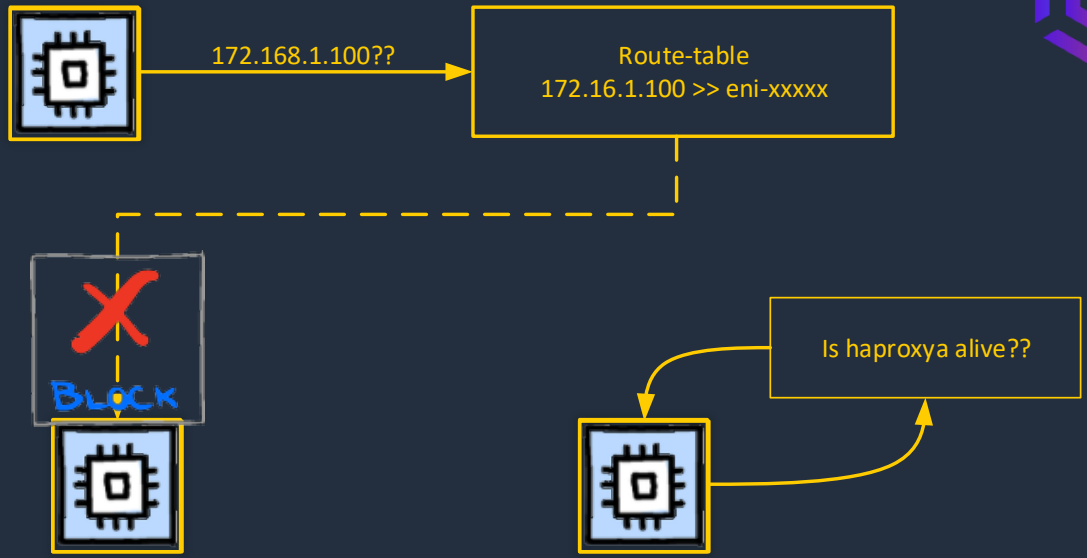


@maishsk

aws

COMMUNITY DAY

haproxyb awakens

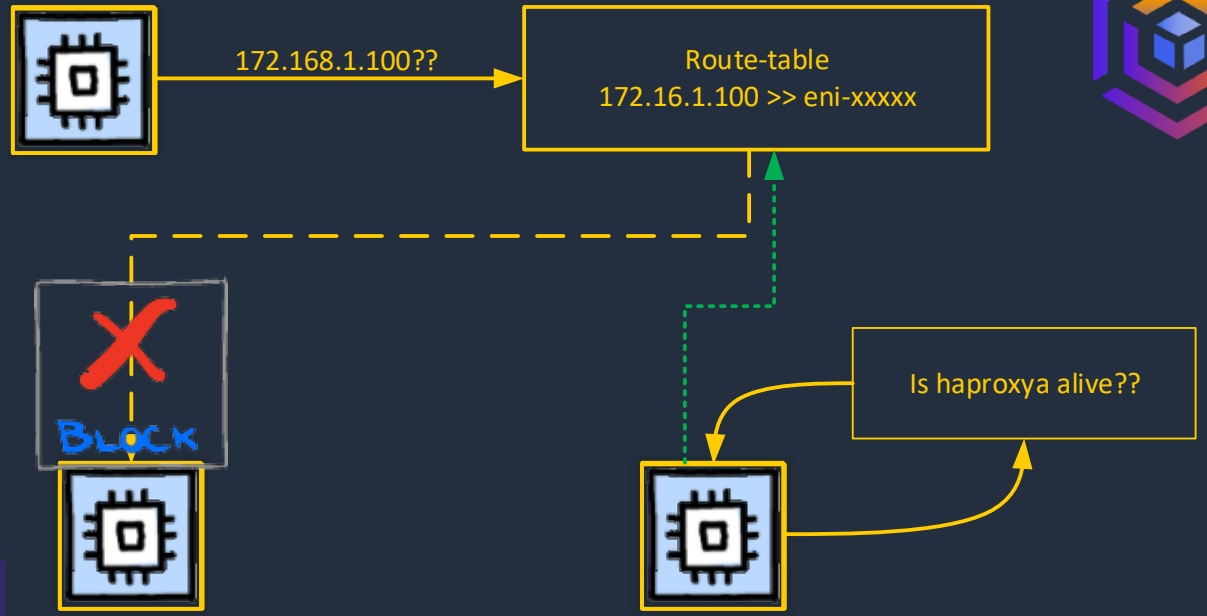


@maishsk

aws

COMMUNITY DAY

Update route table

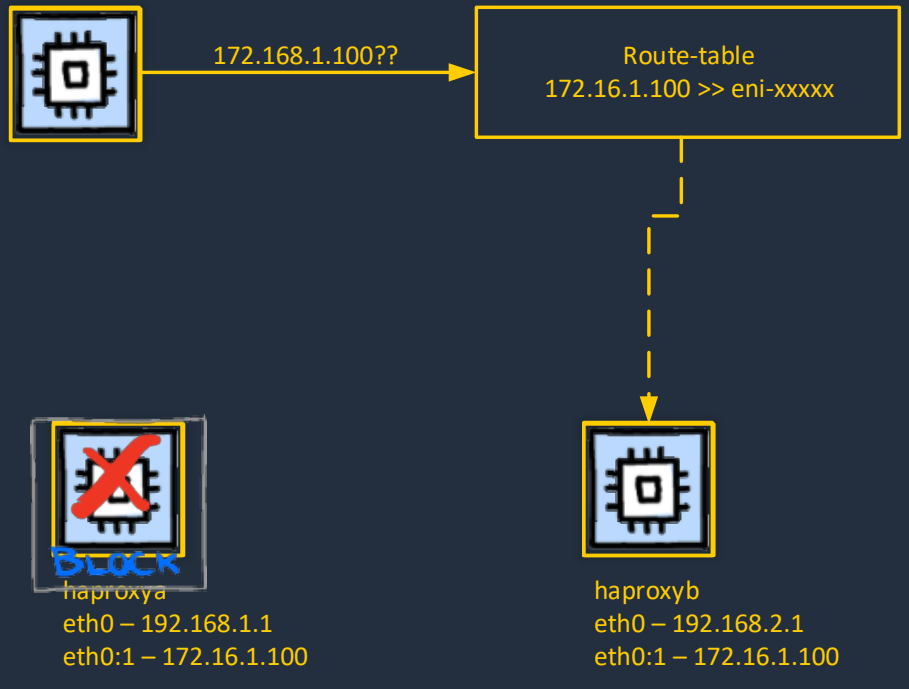


@maishsk

aws

COMMUNITY DAY

Traffic flows

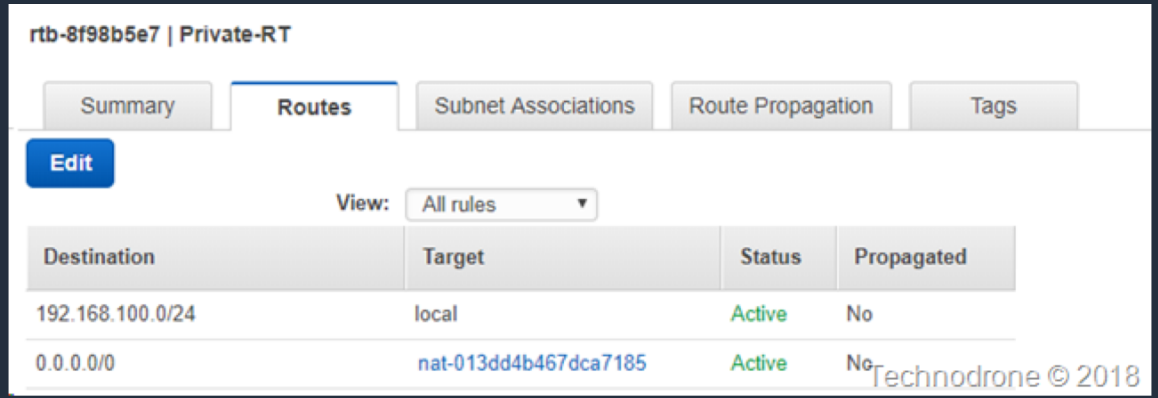


@maishsk

aws

COMMUNITY DAY

Network Deep Dive

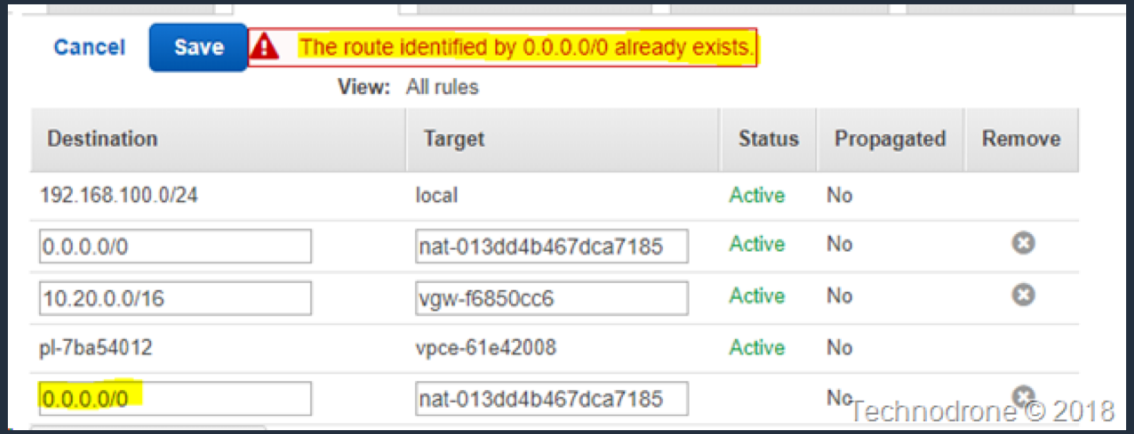


@maishsk

aws

COMMUNITY DAY

No Duplicates

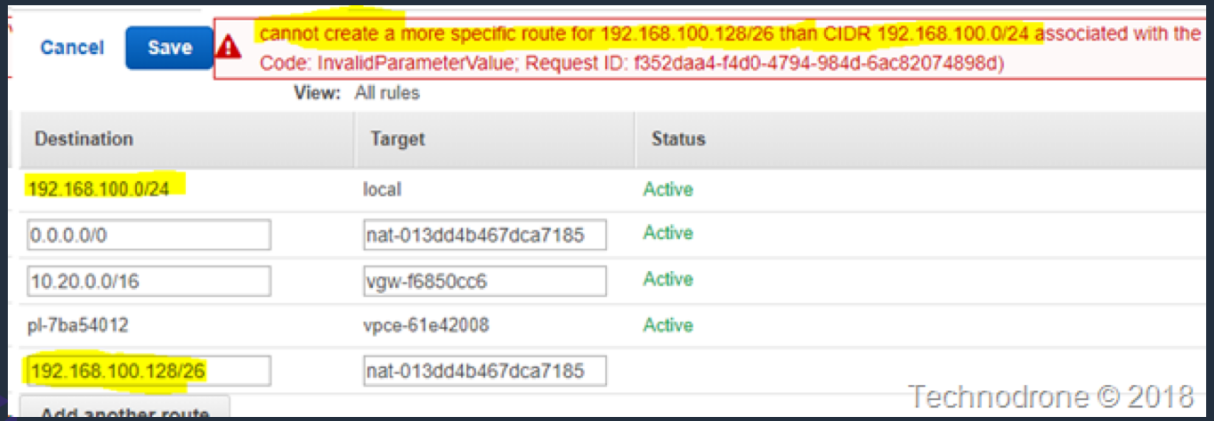


@maishsk

aws

COMMUNITY DAY

No Subsets



@maishsk

aws

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
```

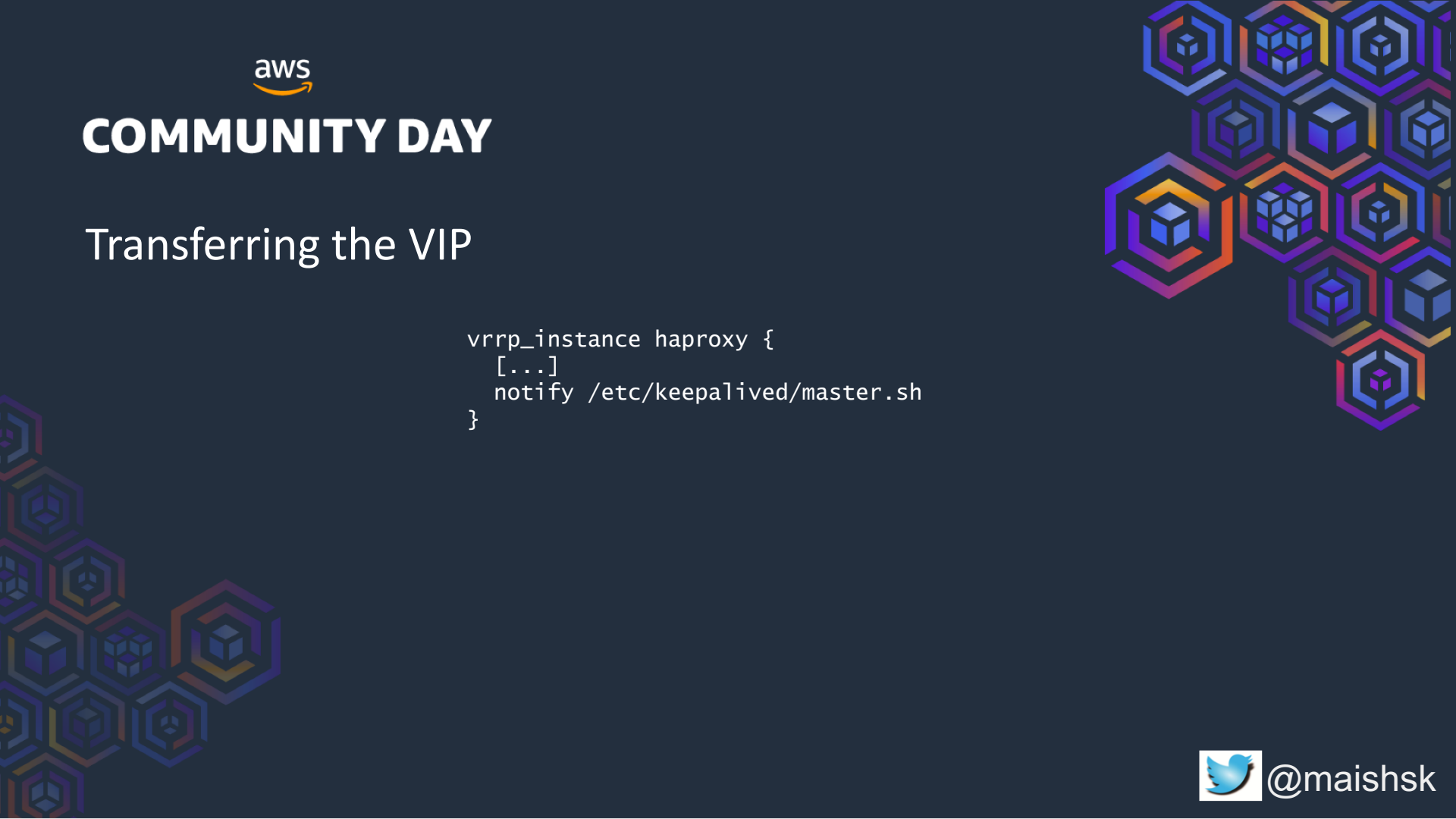
@maishsk

aws

COMMUNITY DAY

Transferring the VIP

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



aws

COMMUNITY DAY

master.sh script

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

@maishsk

aws

COMMUNITY DAY

Automation

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

@maishsk

aws

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

aws

COMMUNITY DAY

@maishsk

aws

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?

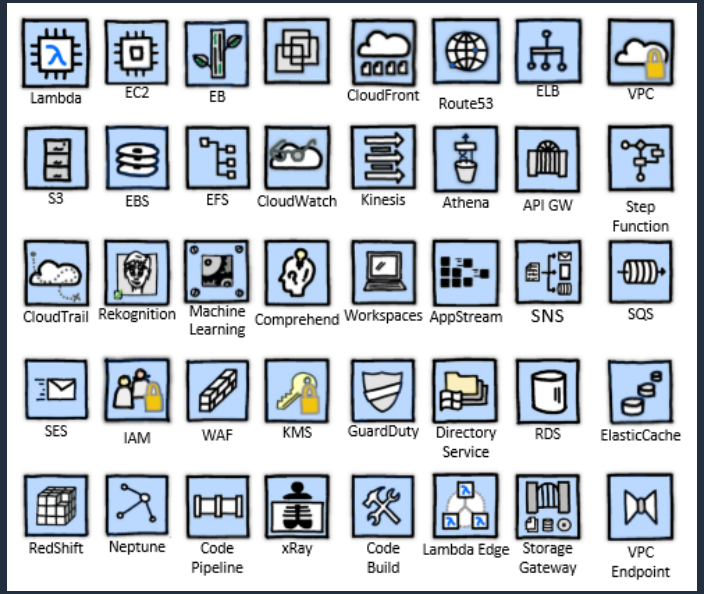
@maishsk

aws

COMMUNITY DAY

- AWS Community Stencils

  https://bit.ly/aws_visio



@maishsk