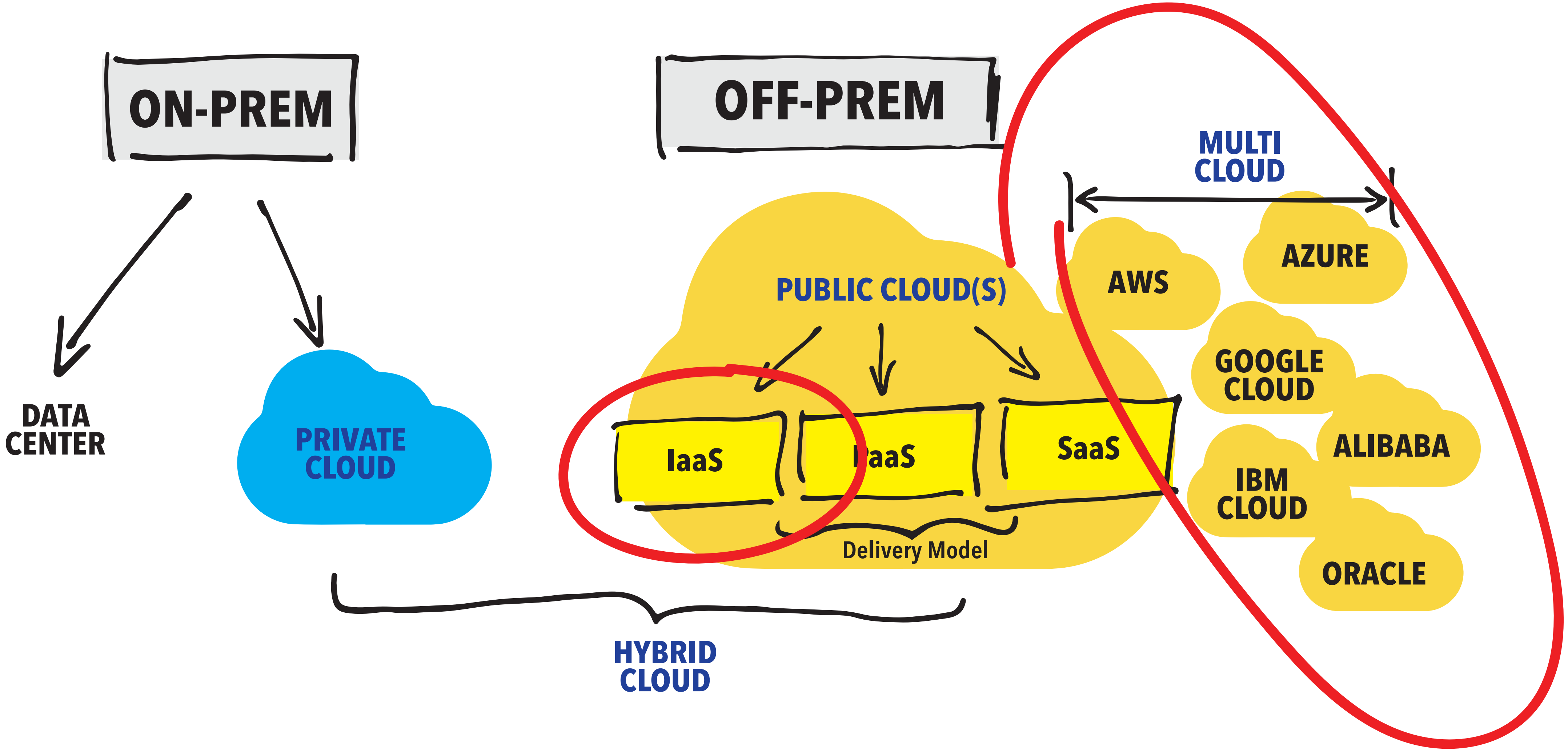
IaaS Security & Workload Protection

Tobias Balschun

AVANTEC
Competence. Security. Trust.



ON-PREM

DATA
CENTER

PRIVATE
CLOUD

OFF-PREM

PUBLIC CLOUD(S)

IaaS

PaaS

SaaS

Delivery Model

HYBRID
CLOUD

MULTI
CLOUD

AWS

AZURE

GOOGLE
CLOUD

ALIBABA

IBM
CLOUD

ORACLE

How TecBite Industries looks like, so far…

TECBITE INDUSTRIES

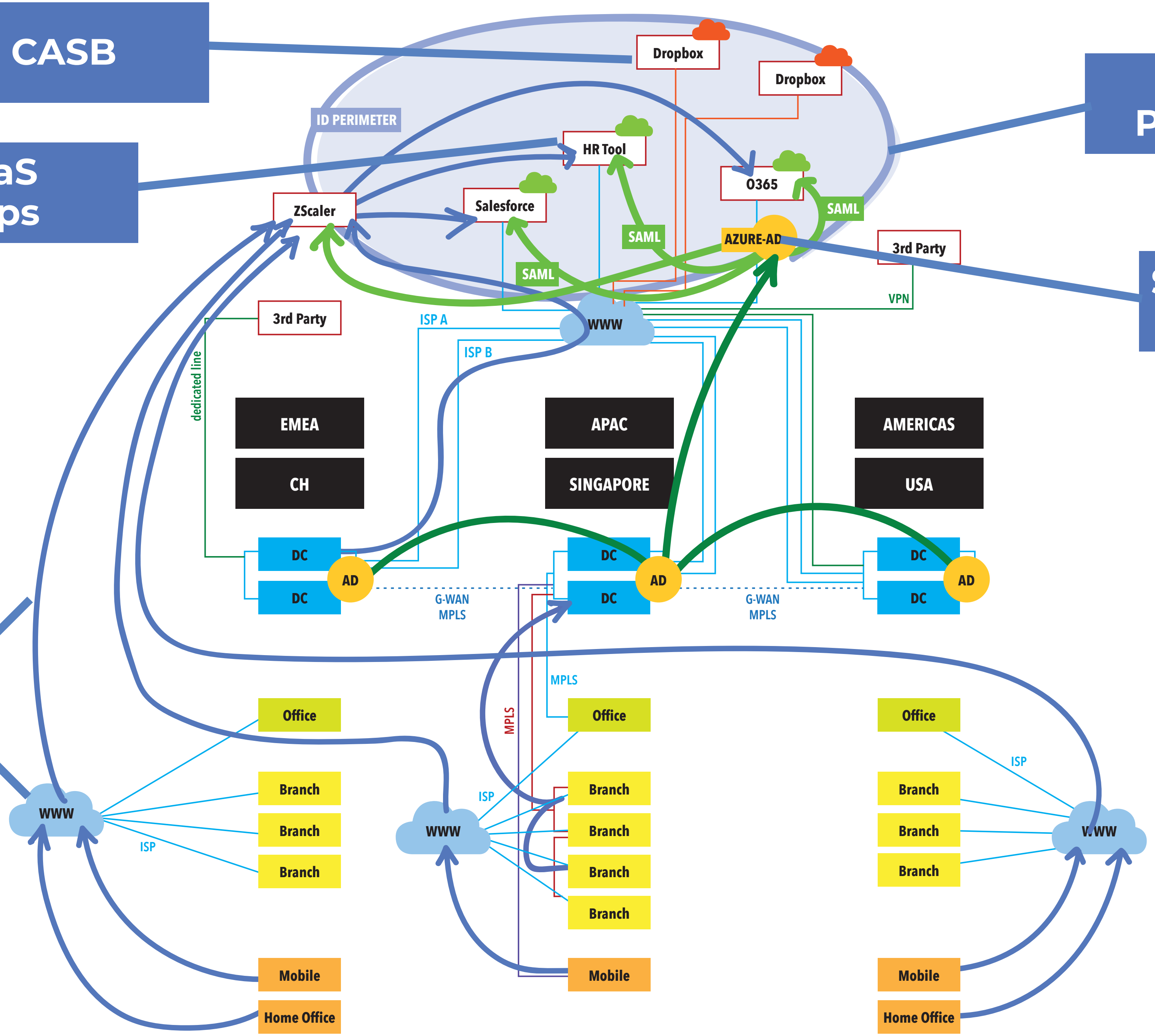
CASB

SaaS Apps

Identity Perimeter

Single sign on SSO

No more MPLS

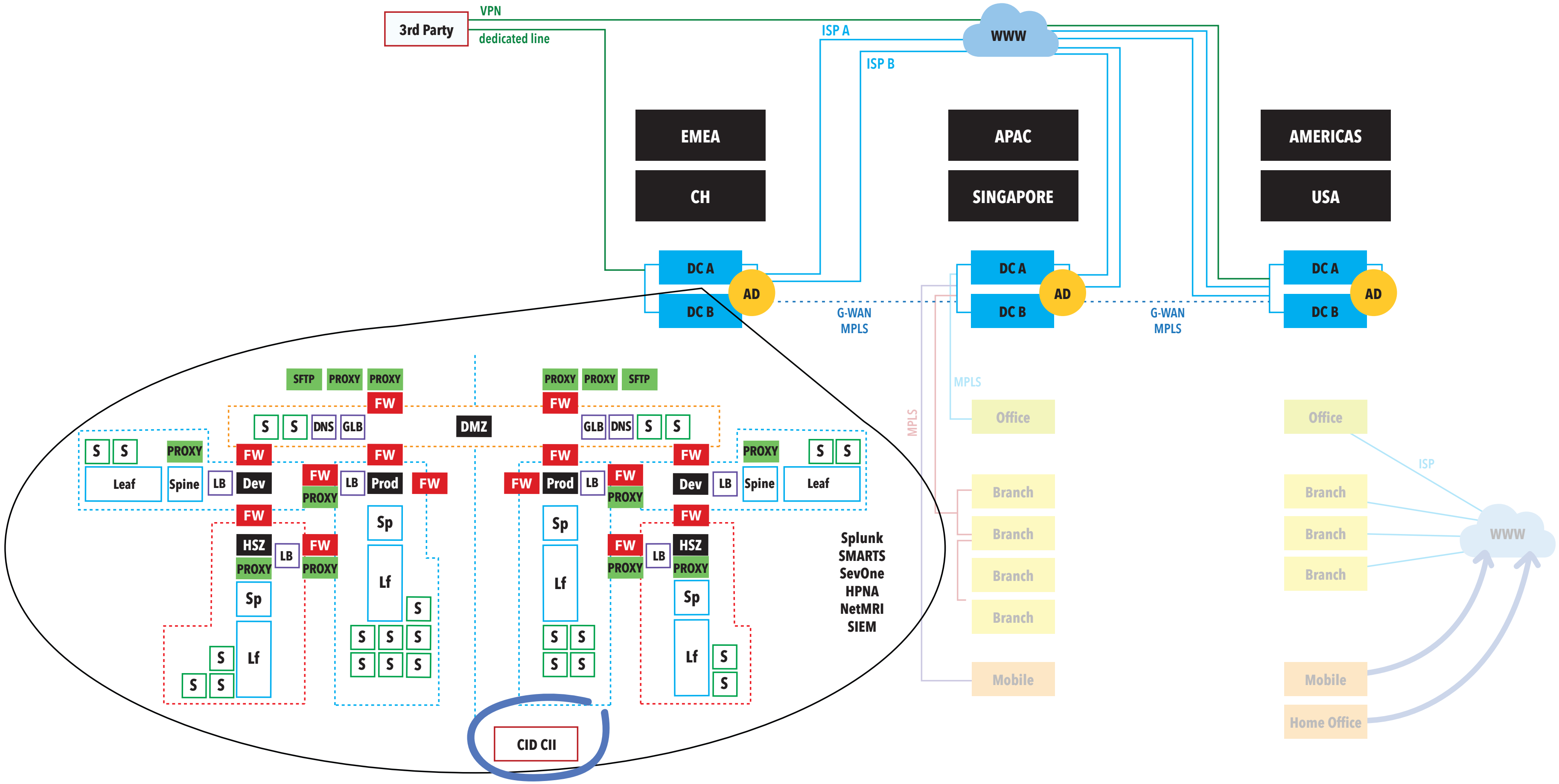


AVANTEC

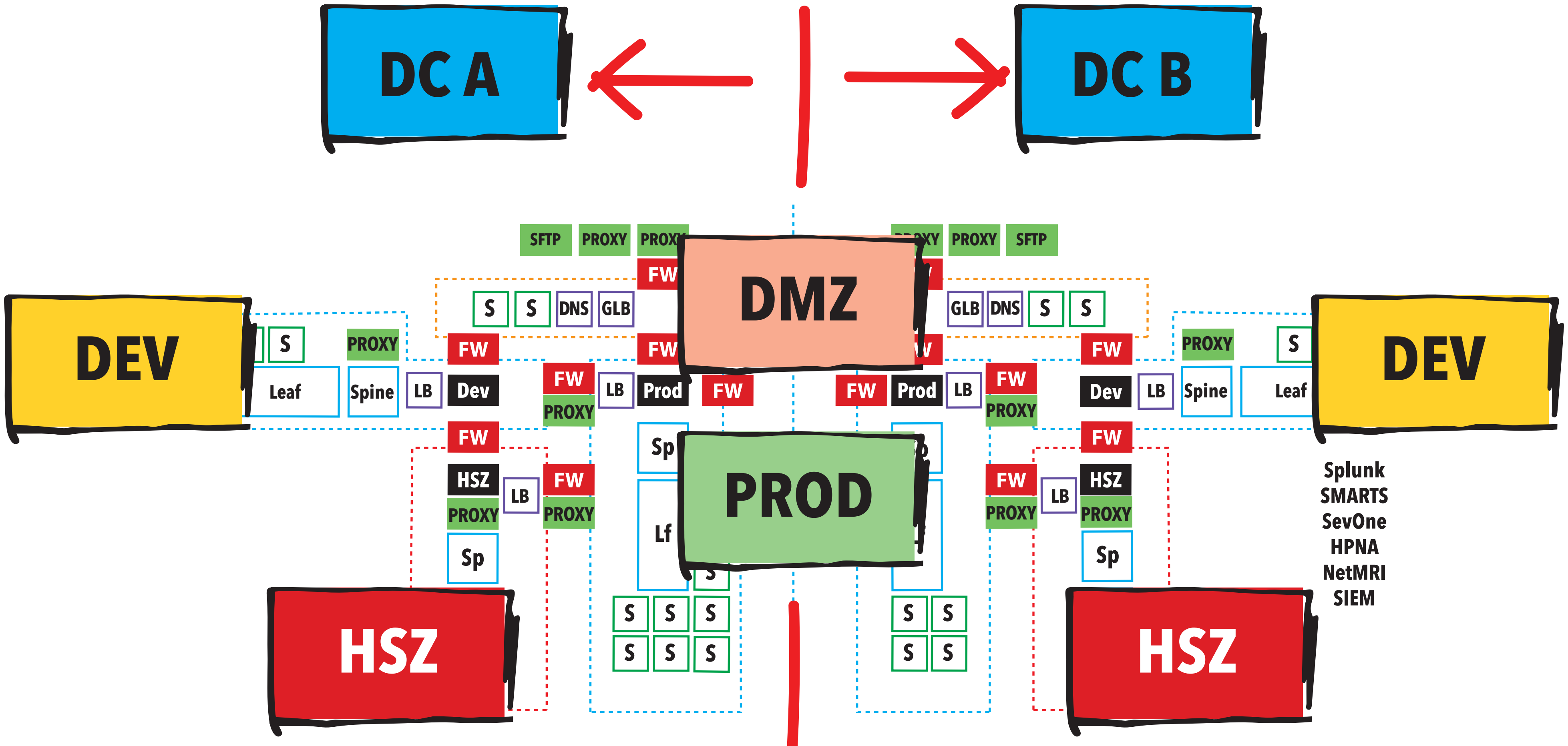
Competence. Security. Trust.

TECBITE INDUSTRIES

Now let’s look at their Data Centers



AVANTEC
Competence. Security. Trust.



Splunk
SMARTS
SevOne
HPNA
NetMRI
SIEM

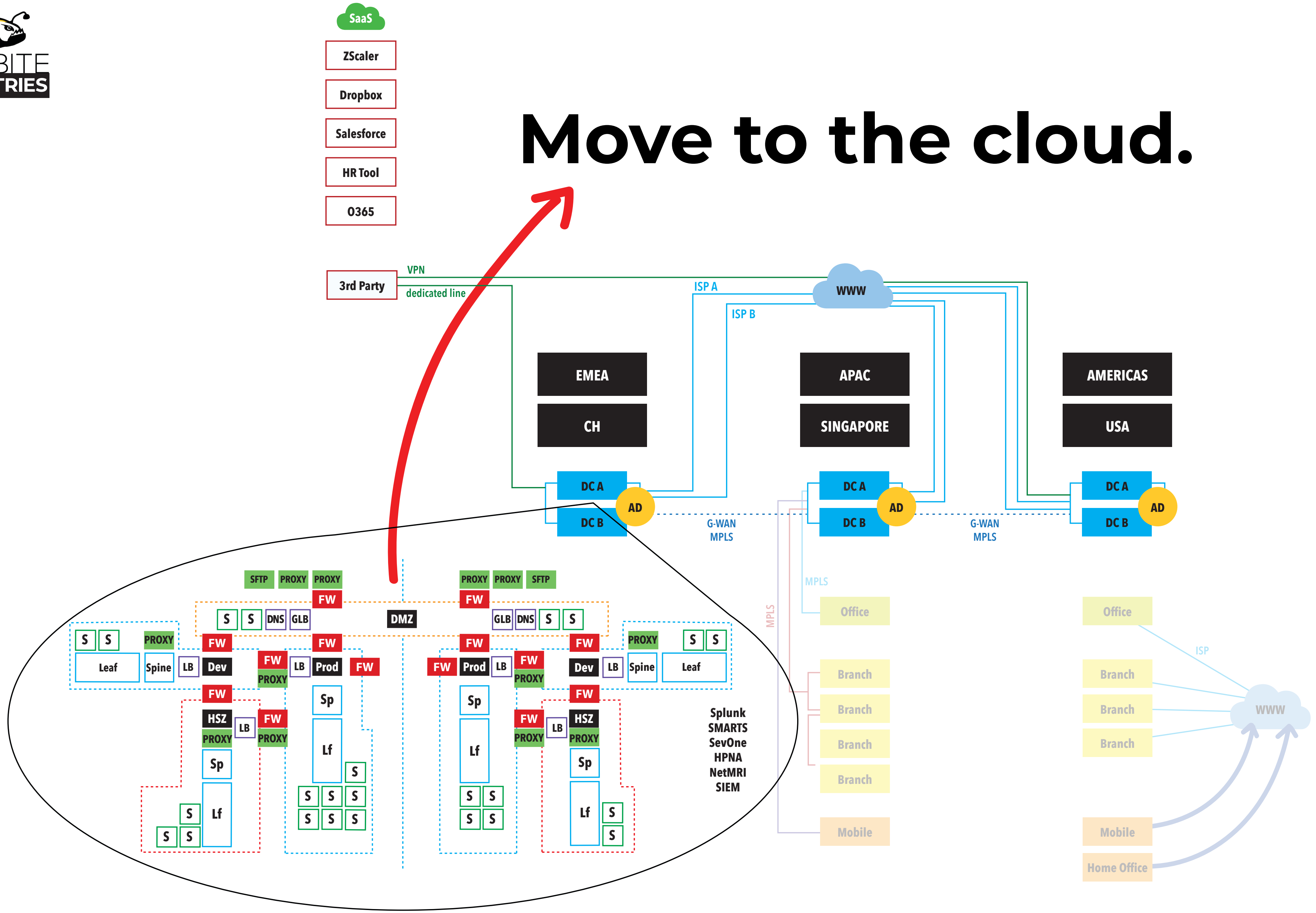
High Security Zone

High Security Zone

AVANTEC
Competence. Security. Trust.

TECBITE INDUSTRIES

Move to the cloud.

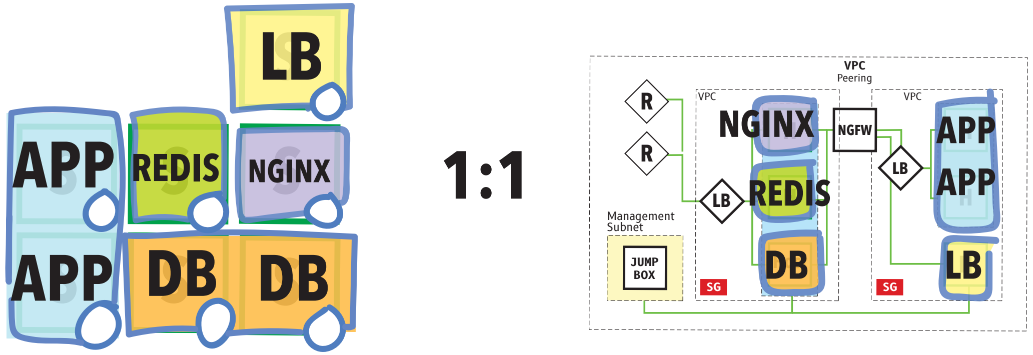


AVANTEC
Competence. Security. Trust.

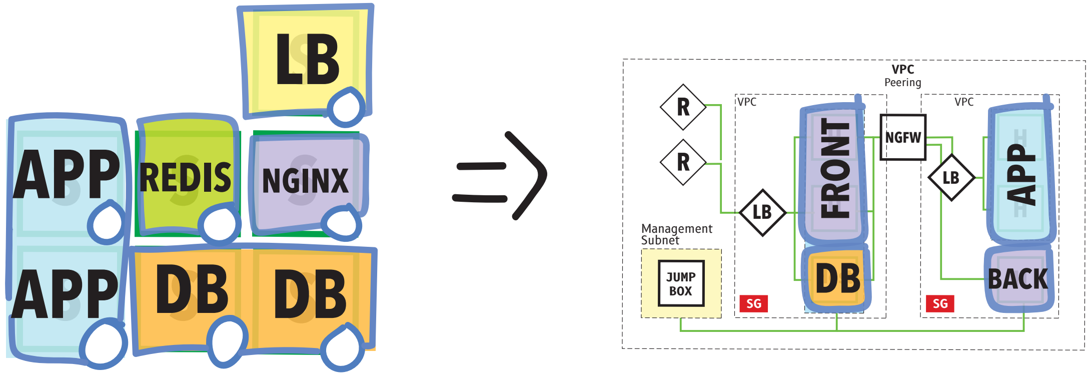
How to move to the cloud:

Lift and shift
Replatform
Refactor

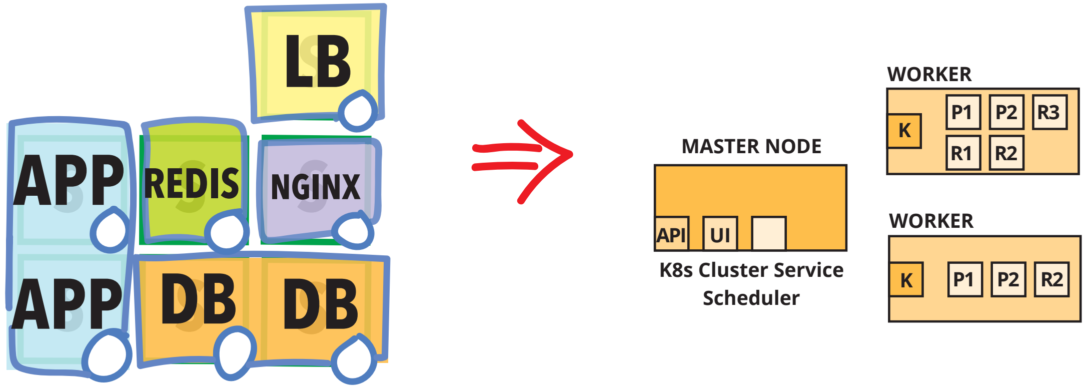
Lift and shift



Replatform



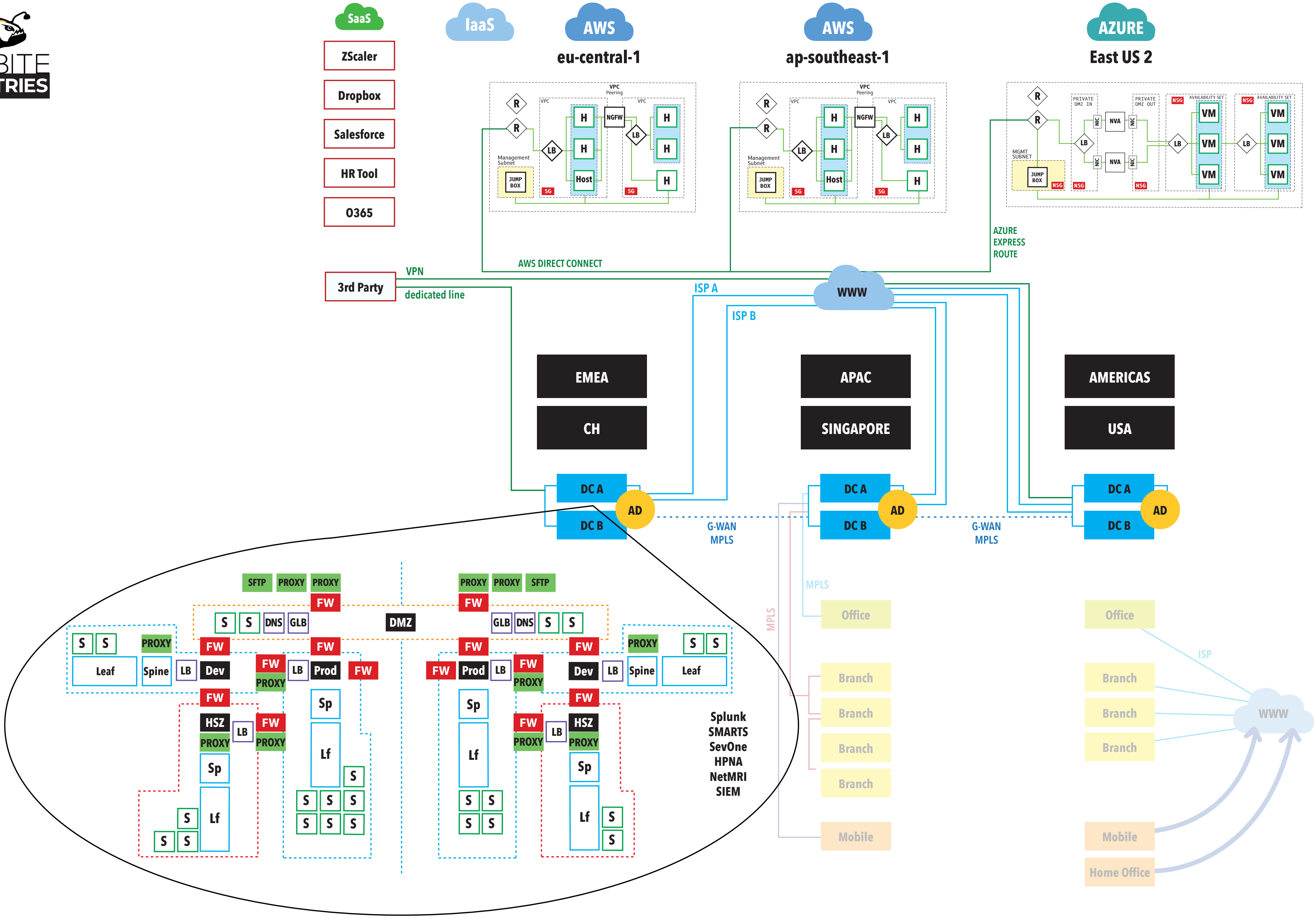
Refactor



Other approaches

Green-field
Cloud-bursting
Move workloads
IoT

TECBITE INDUSTRIES



SaaS
ZScaler
Dropbox
Salesforce
HR Tool
O365

IaaS

AWS
eu-central-1
VPC Peering
VPC
VPC
R
R
LB
H
H
Host
NGFW
LB
H
H
H
Management Subnet
JUMP BOX
SG
SG

AWS
ap-southeast-1
VPC Peering
VPC
VPC
R
R
LB
H
H
Host
NGFW
LB
H
H
H
Management Subnet
JUMP BOX
SG
SG

AZURE
East US 2
R
R
PRIVATE DMZ IN
PRIVATE DMZ OUT
NIC
NVA
NIC
NIC
NVA
NIC
LB
NSG
AVAILABILITY SET
NSG
AVAILABILITY SET
LB
VM
VM
VM
LB
VM
VM
VM
MGMT SUBNET
JUMP BOX
NSG
NSG
NSG

AZURE EXPRESS ROUTE
AWS DIRECT CONNECT
3rd Party
VPN
dedicated line
ISP A
ISP B
WWW

EMEA
CH
DC A
DC B
AD

APAC
SINGAPORE
DC A
DC B
AD

AMERICAS
USA
DC A
DC B
AD

G-WAN MPLS
G-WAN MPLS
MPLS
MPLS

Office
Branch
Branch
Branch
Branch
Mobile

Office
ISP
Branch
Branch
Branch
WWW
Mobile
Home Office

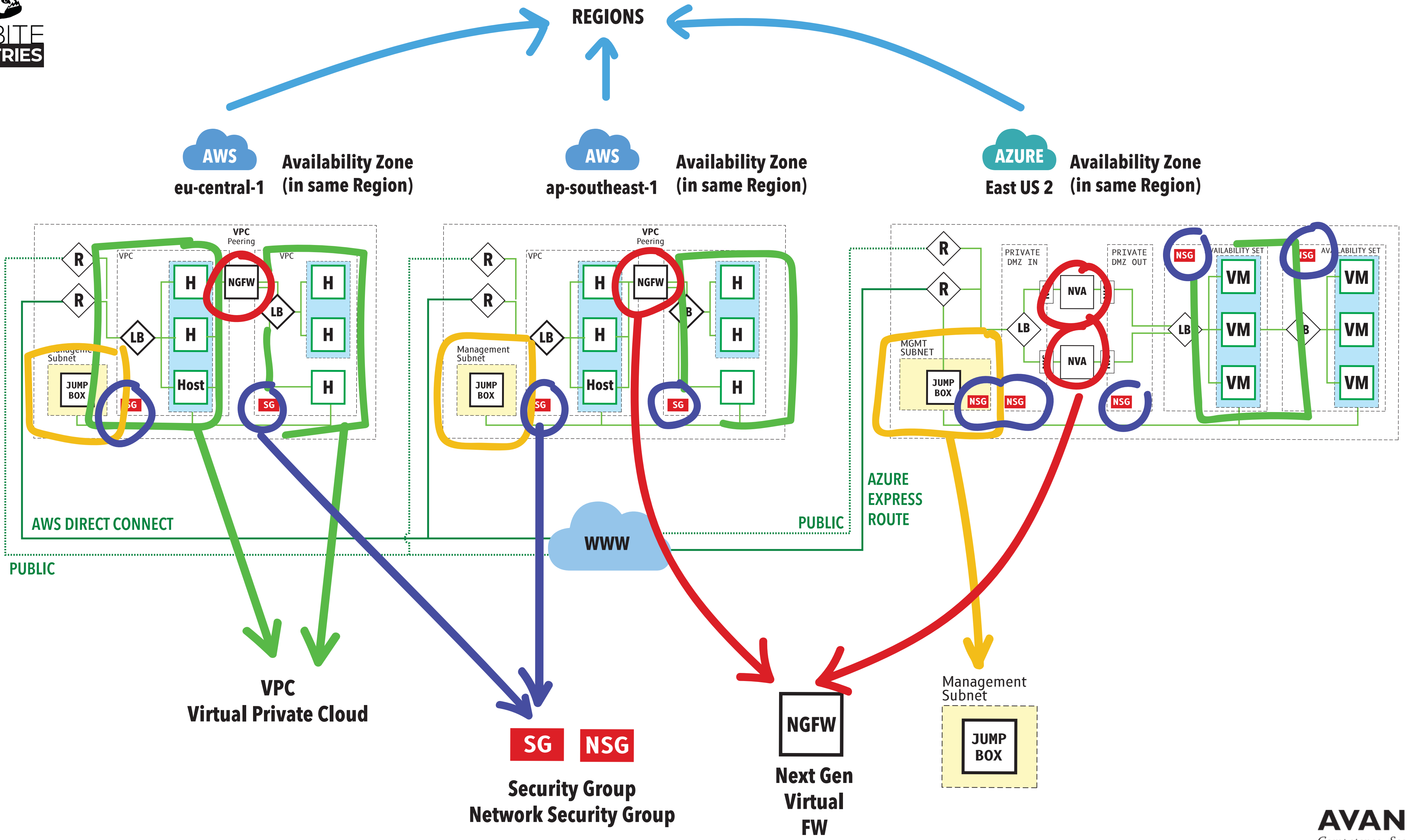
SFTP
PROXY
PROXY
FW
S
S
DNS
GLB
DMZ
PROXY
PROXY
SFTP
FW
GLB
DNS
S
S

S
S
PROXY
Leaf
Spine
LB
Dev
FW
FW
PROXY
LB
Prod
FW
FW
FW
HSZ
LB
PROXY
FW
PROXY
Sp
Lf
S
S
S
Sp
Lf
S
S
S
S
S
S
S

FW
Prod
LB
FW
PROXY
FW
Dev
LB
Spine
Leaf
PROXY
S
S
FW
Sp
Lf
S
S
S
S
FW
PROXY
LB
HSZ
PROXY
Sp
Lf
S
S

Splunk
SMARTS
SevOne
HPNA
NetMRI
SIEM

AVANTEC
Competence. Security. Trust.



REGIONS

AWS
eu-central-1
Availability Zone
(in same Region)

AWS
ap-southeast-1
Availability Zone
(in same Region)

AZURE
East US 2
Availability Zone
(in same Region)

VPC
Virtual Private Cloud

SG NSG
Security Group
Network Security Group

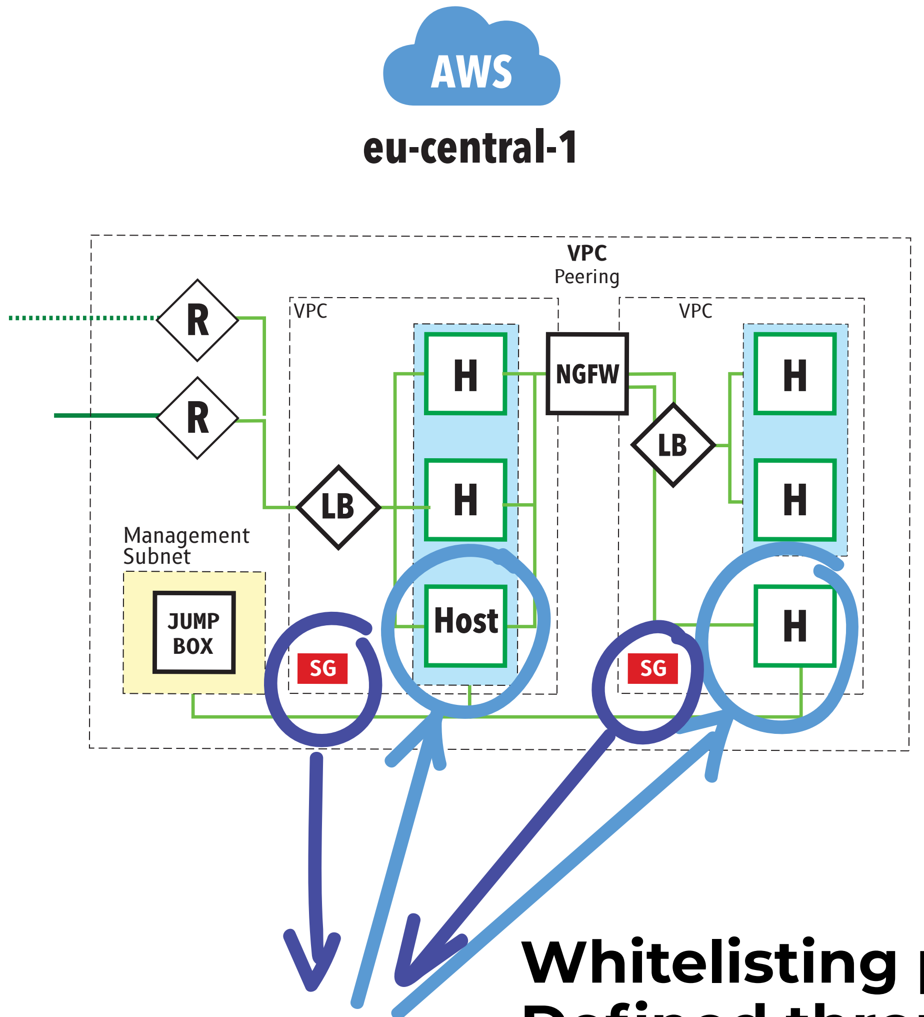
NGFW
Next Gen
Virtual
FW

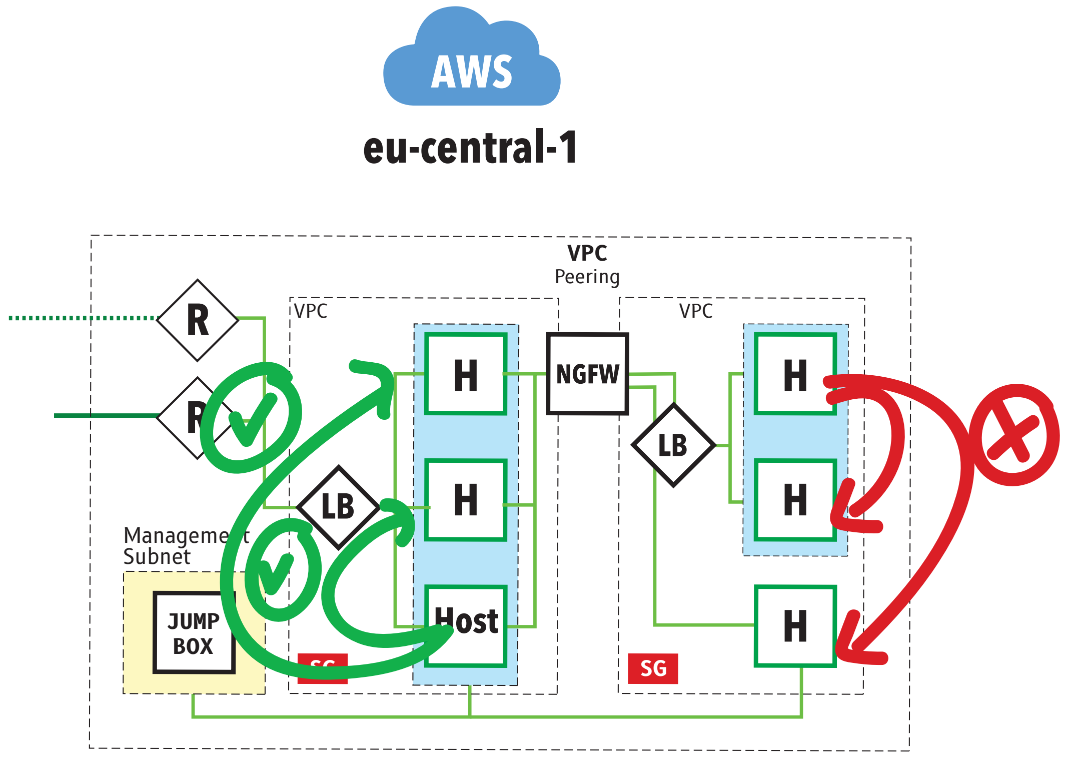
Management
Subnet
JUMP
BOX

AVANTEC
Competence. Security. Trust.

Cloud native

A short explanation

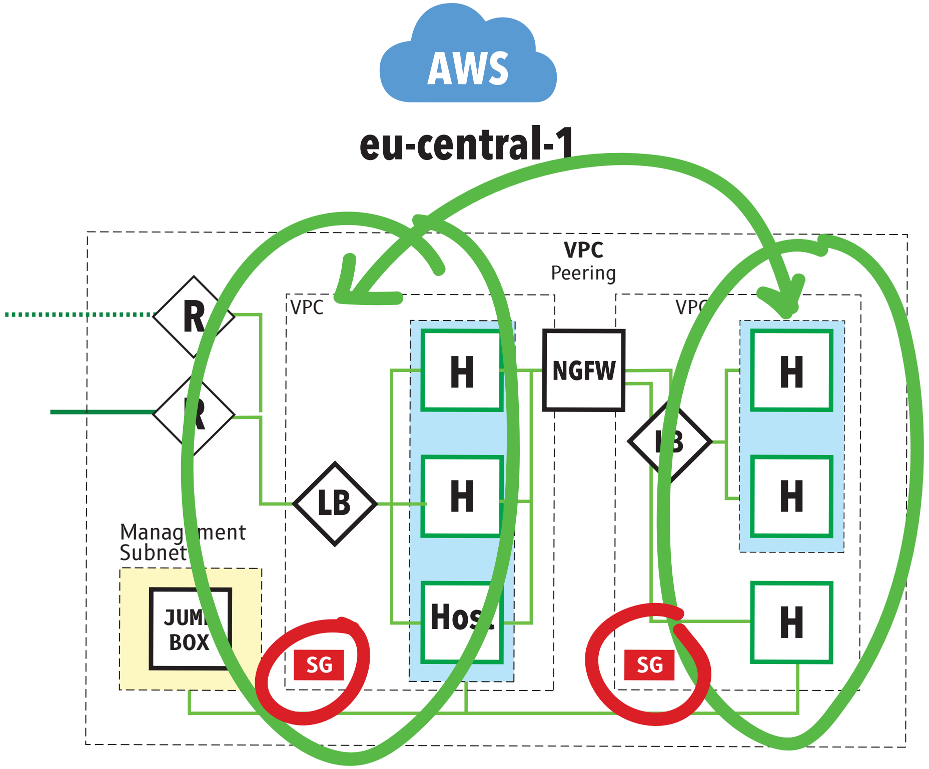




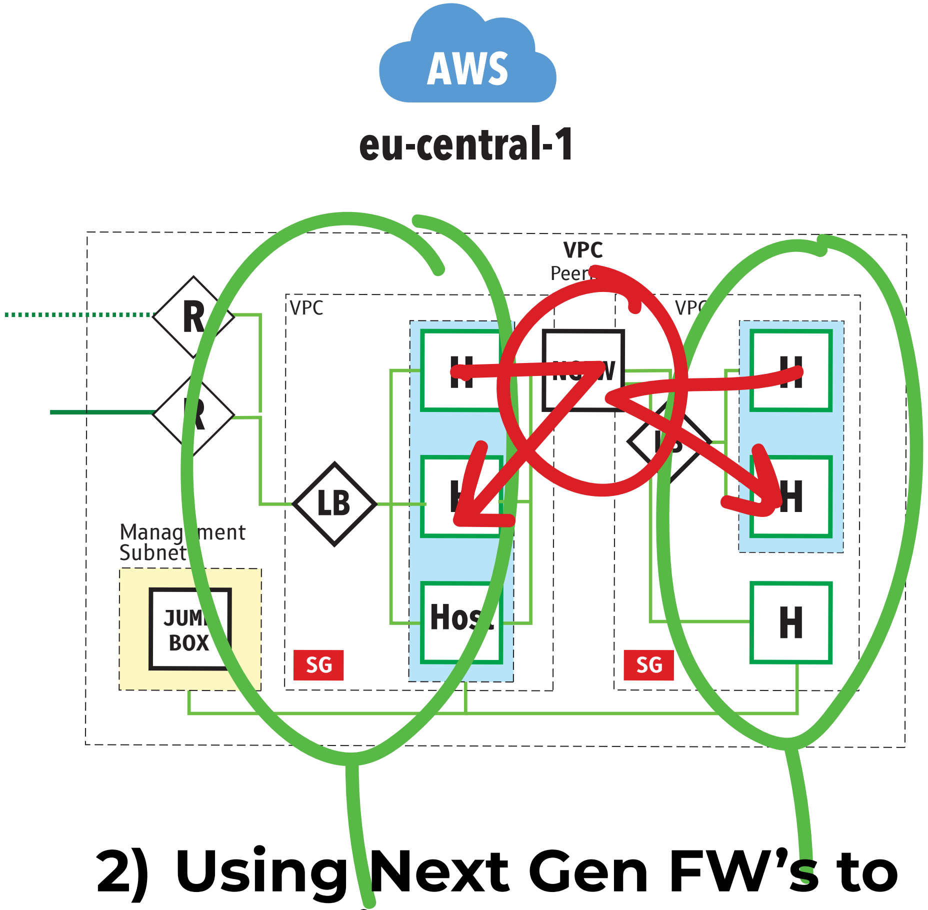
Whitelisting policy for micro segmentation
Defined through the security group (SG)

Cloud native & NGFW

Two different approaches

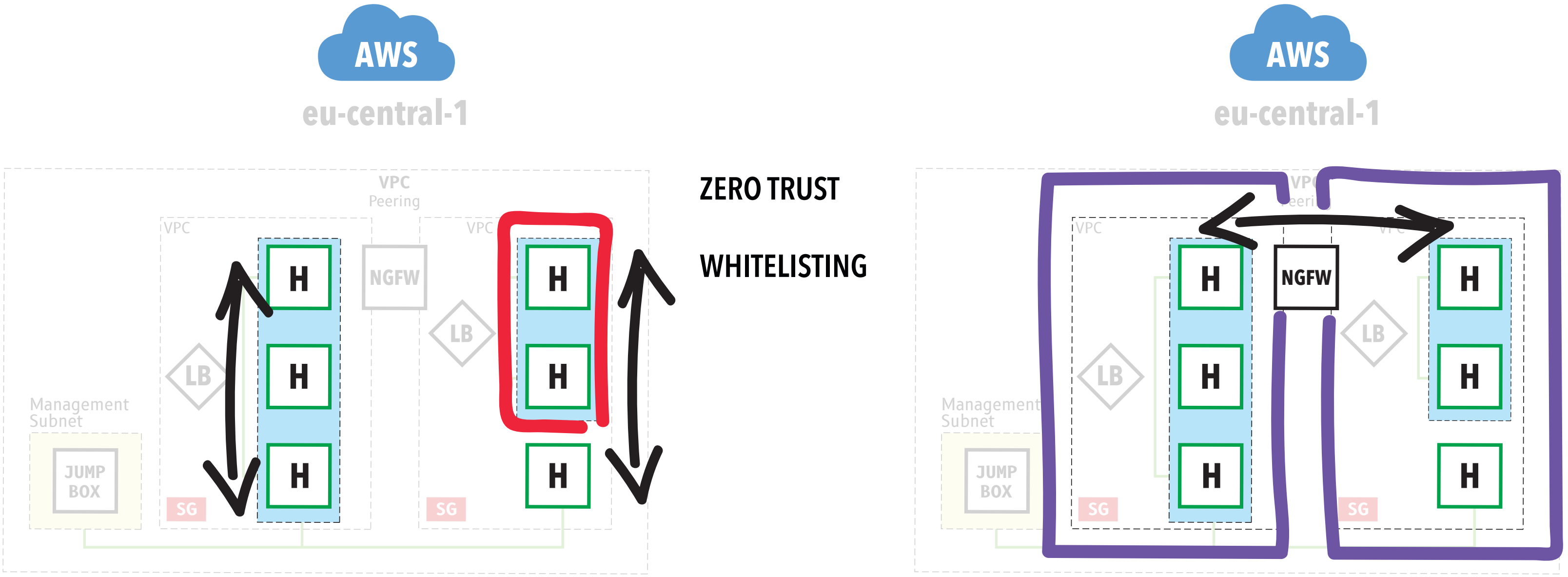


1) Everything is controlled through cloud native mechanisms



2) Using Next Gen FW's to route intra-VPC and inter-VPC traffic

Competence. Security. Trust.



ZERO TRUST

WHITELISTING

NGFW

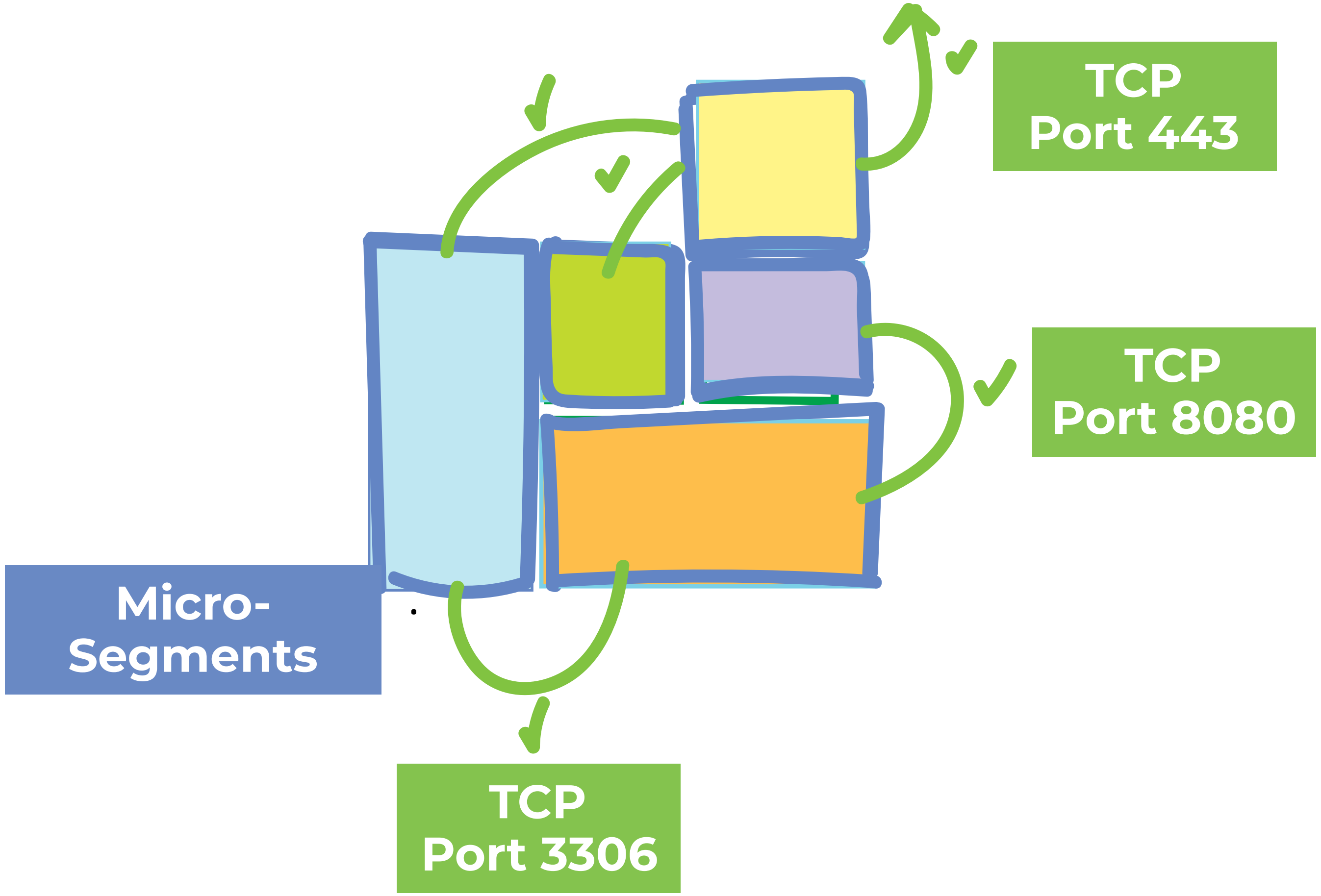
L3-L7
TRANSIT

3) Mixed approach. Using cloud native functionality for intra-VPC connectivity (whitelisting and microseg), while using NGFWs for inter-VPC traffic (including transitive routing)

Microsegmentation

A very short explanation

Microsegmentation



TCP Port 443

TCP Port 8080

Micro-Segments

TCP Port 3306

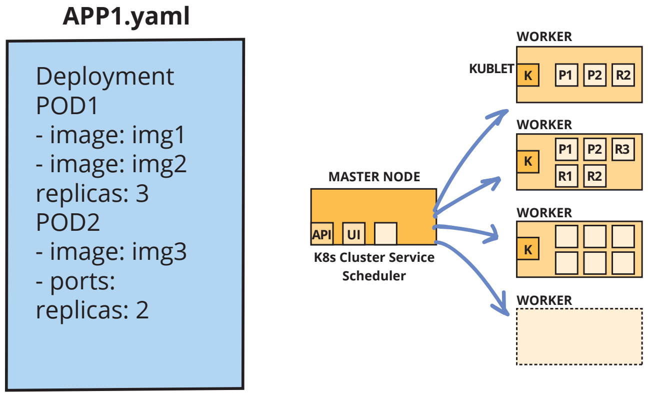
Infrastructure as Code

A very short explanation

Infrastructure as Code

From a developers perspective, the state of an infrastructure should be defined programmatically.
Defined by Code.

Infra by YAML.



APP1.yaml

```
Deployment
POD1
- image: img1
- image: img2
replicas: 3
POD2
- image: img3
- ports:
replicas: 2
```

AVANTEC
Competence. Security. Trust.

Infrastructure as Code

Any kind of change in this state, should be achieved by changing the underlying code.

Adding a host? Code
Elasticity? Code

Infrastructure as Code

This makes automation much easier.

If traffic increases, add more hosts.

When traffic decreases under a threshold, reduce those hosts again.

Infrastructure as Code

Which means that the next big challenge for security is to be part of this.

Security as code

Security as Code

AVANTEC
Competence. Security. Trust.

Thank you