LONDON
INTERNATIONAL
SOFTWARE DEVELOPMENT
CONFERENCE 2015

goto; conference

Rugged Reperimeterisation

Chris Swan

@cpswan

goto; conference

Click ‘engage’ to rate session.

Rate **12** sessions to get the supercool GOTO reward

Join the conversation #gotoldn

Google moves its corporate apps to the Internet!!!

Google Inc., taking a new approach to enterprise security, is moving its corporate applications to the Internet. In doing so, the Internet giant is flipping common corporate security practice on its head, shifting away from the idea of a trusted internal corporate network secured by perimeter devices such as firewalls, in favor of a model where corporate data can be accessed from anywhere with the right device and user credentials.

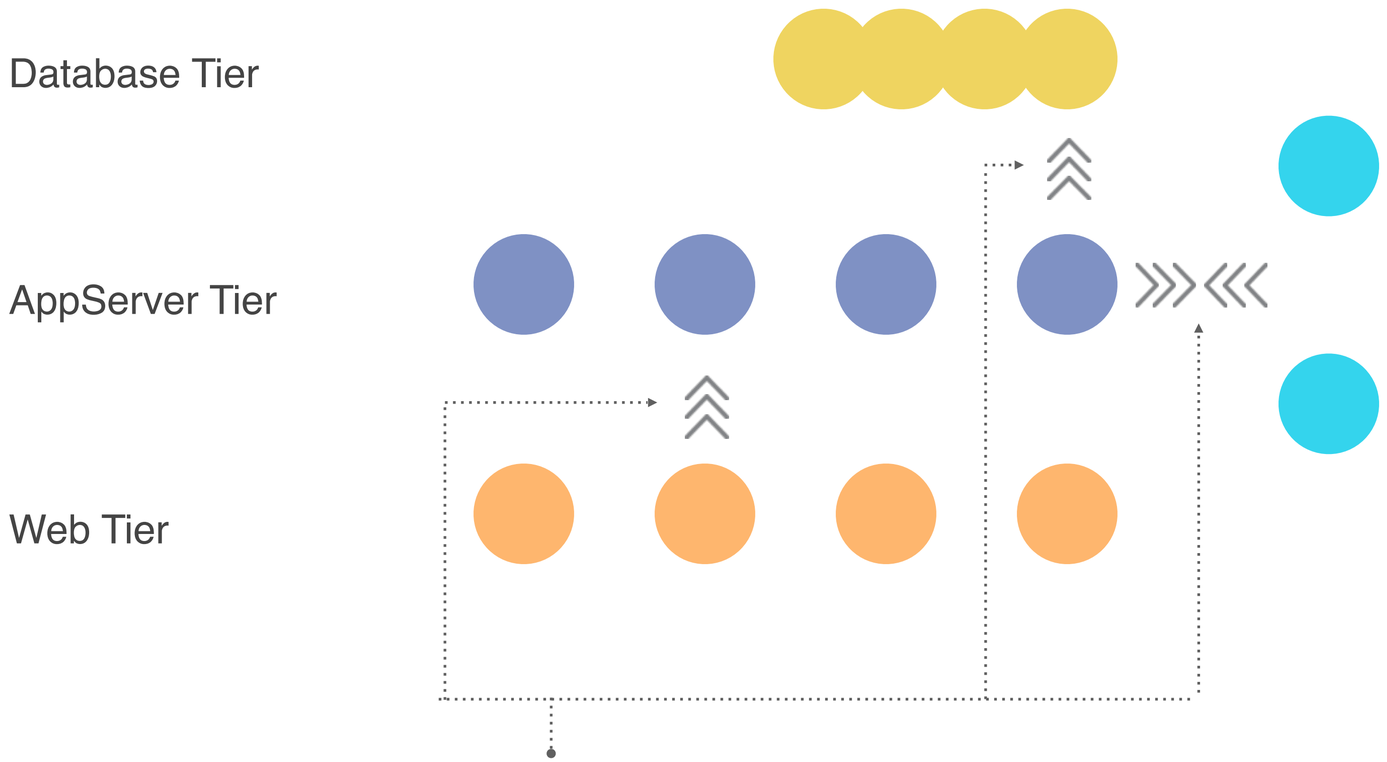
The new model — called the BeyondCorp initiative — assumes that the internal network is as dangerous as the Internet.

(Wall Street Journal l “Google Moves Its Corporate Applications to the Internet” l May 11, 2015)

Setting the scene

Traditional apps

Business applications are **collections** of (virtual) servers

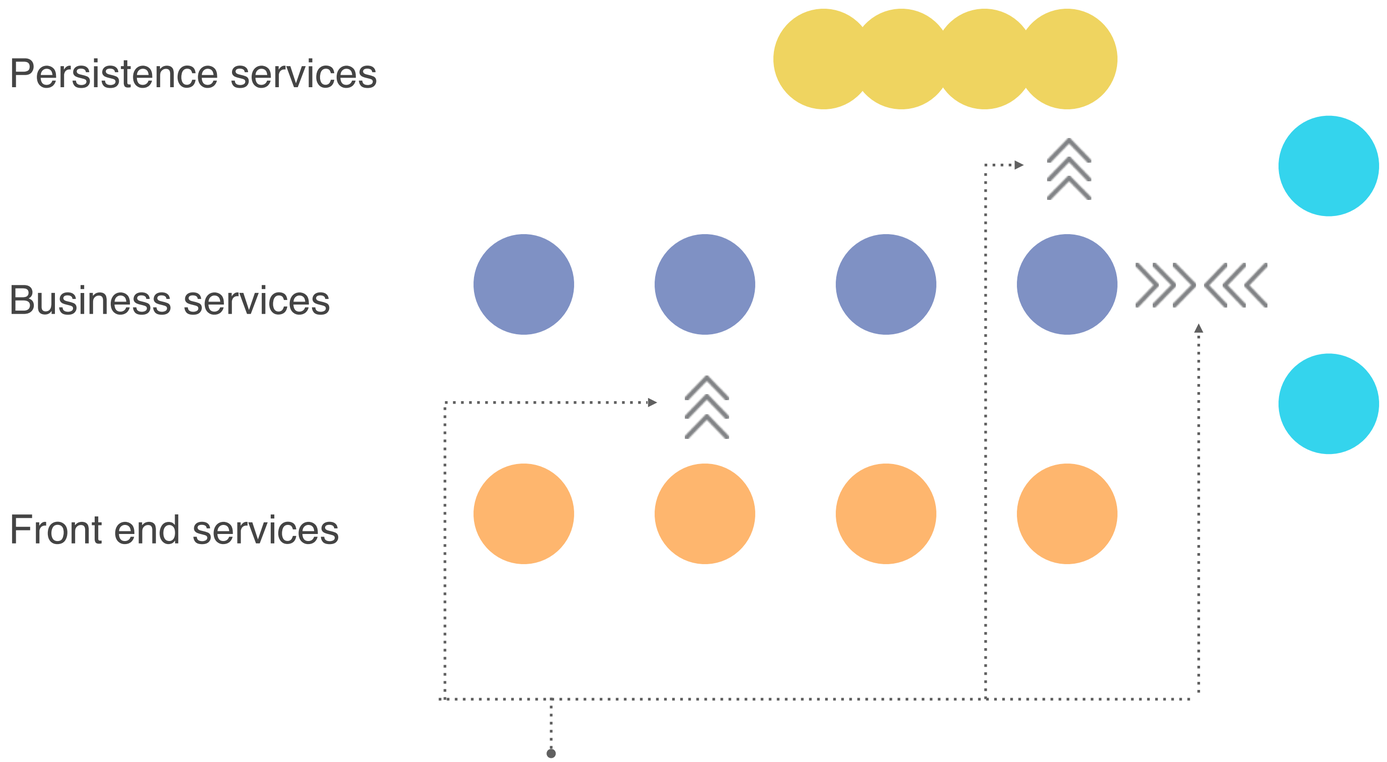


= type of server

Is the "**right**" traffic going to/from our servers?

Modern architectures don’t change things that much

Micro services based applications are **collections** of services



= type of server

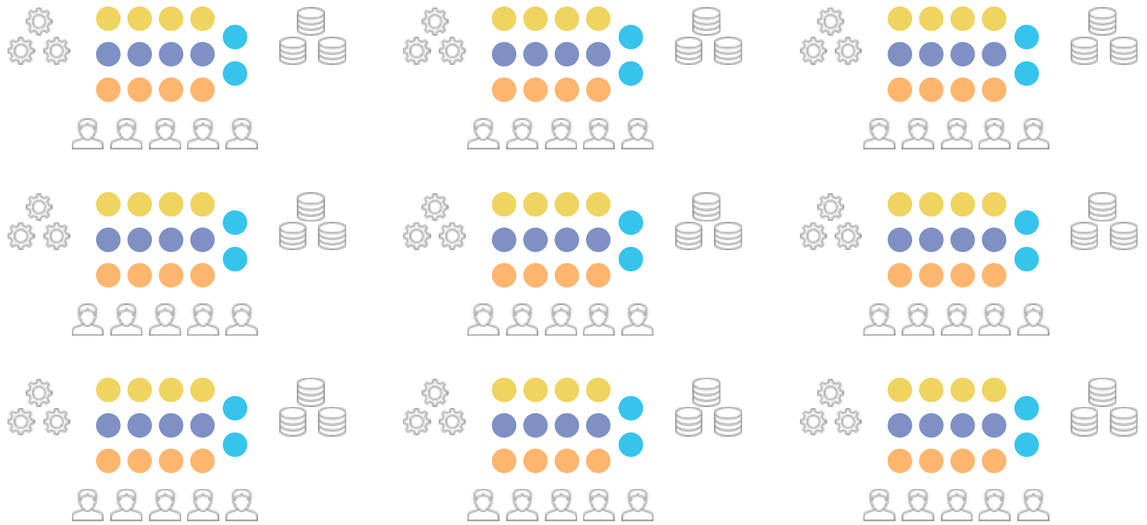
Is the “**right**” traffic going to/from our services?

Enterprise data center

Enterprise data centers are **filled with these applications**, often left **insecure by lack of focus** on interior network paths.

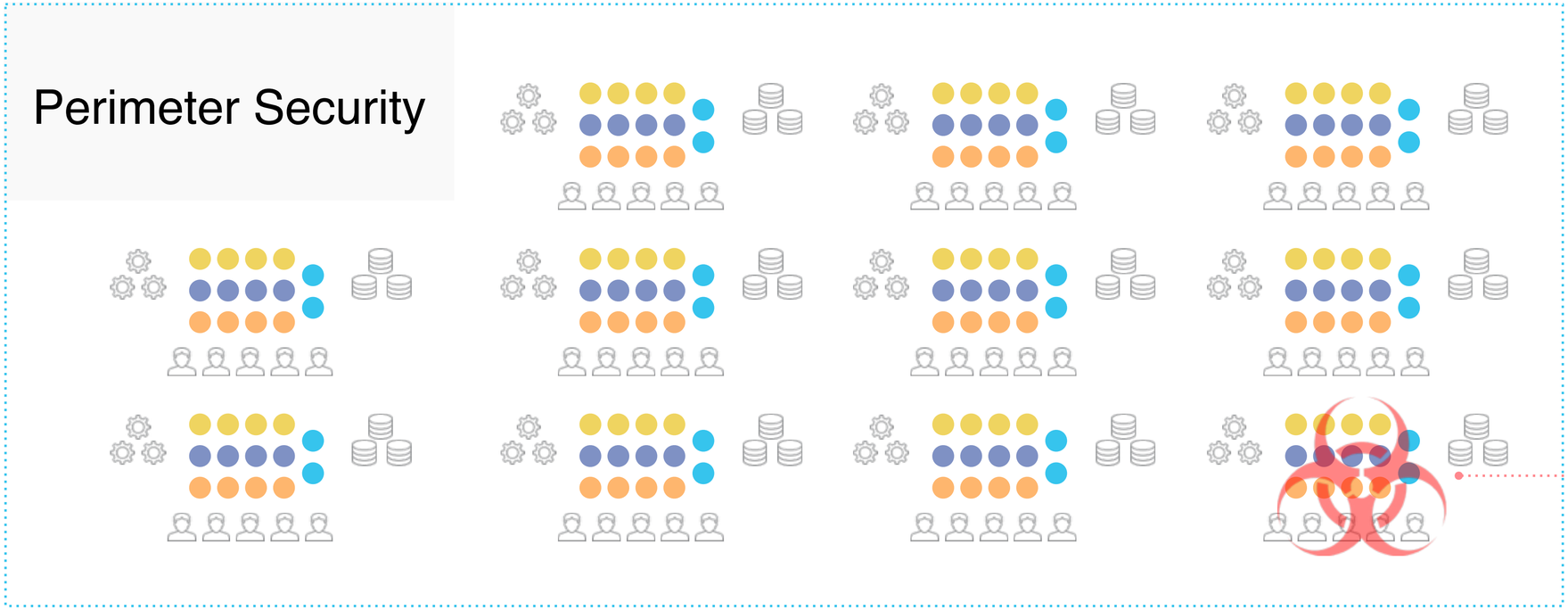
Perimeter Security

20% of Security Spend is on “interior”, yet 80% of the network traffic.

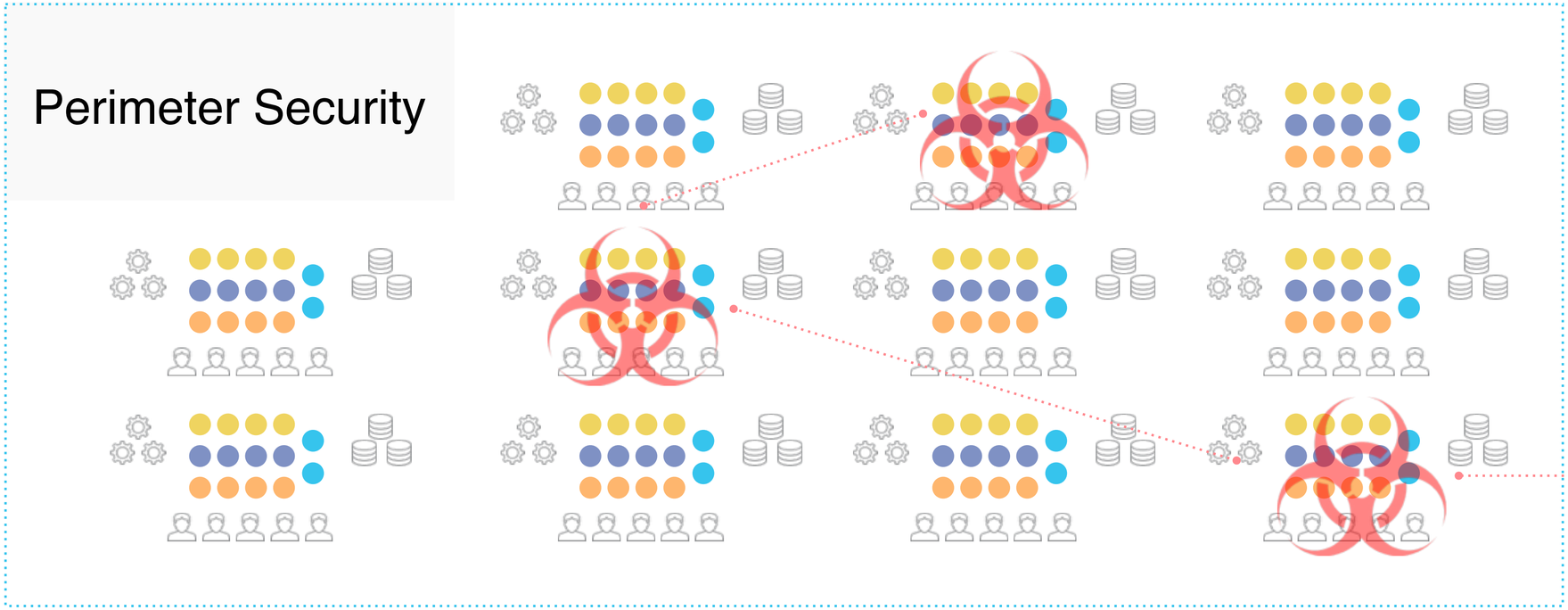


80% of Security Spend is on perimeter, 20% of traffic.

Hard on the outside, soft on the inside

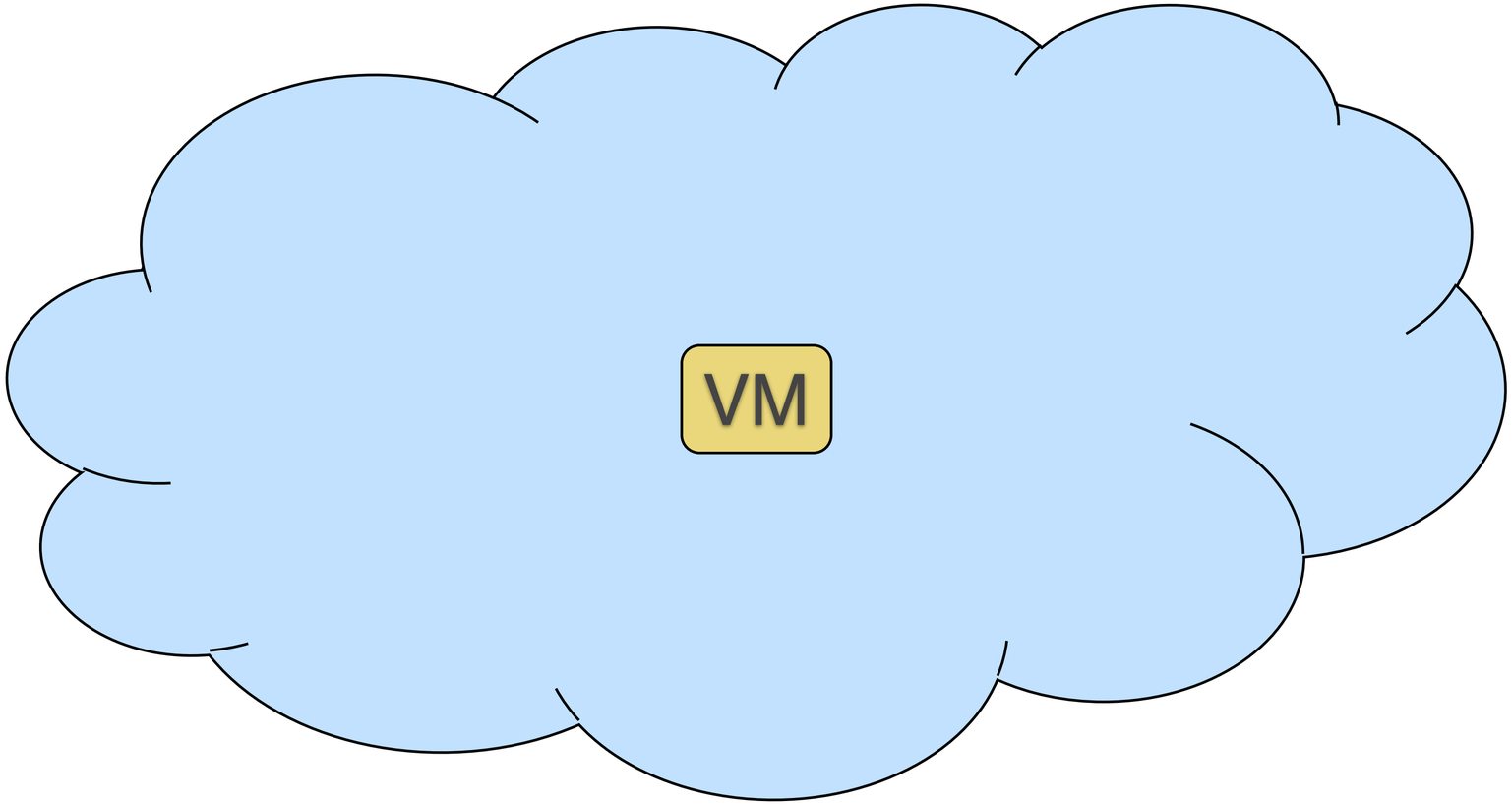


One penetration creates major “East-West” exposure

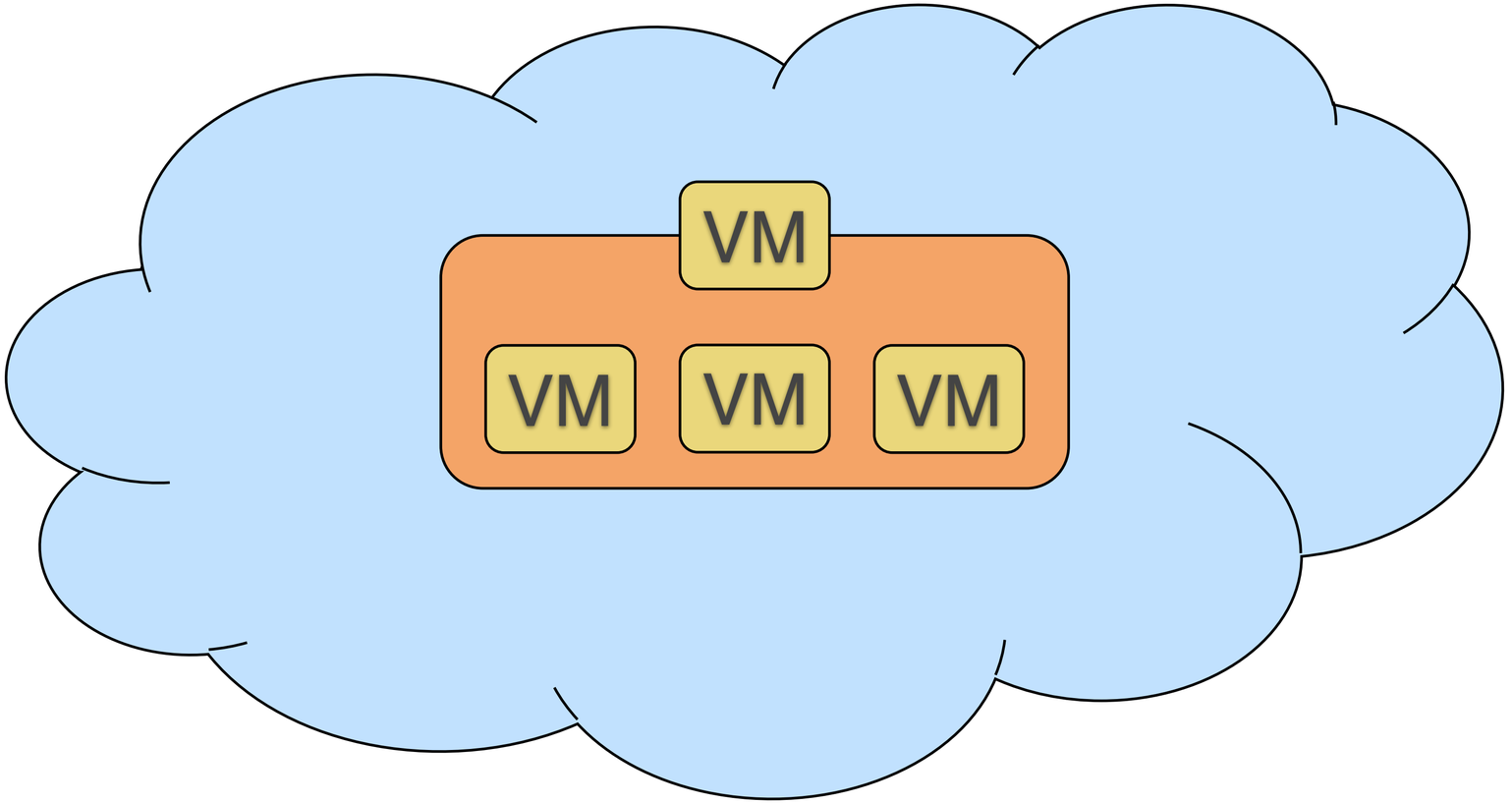


Cloud architectures have been different

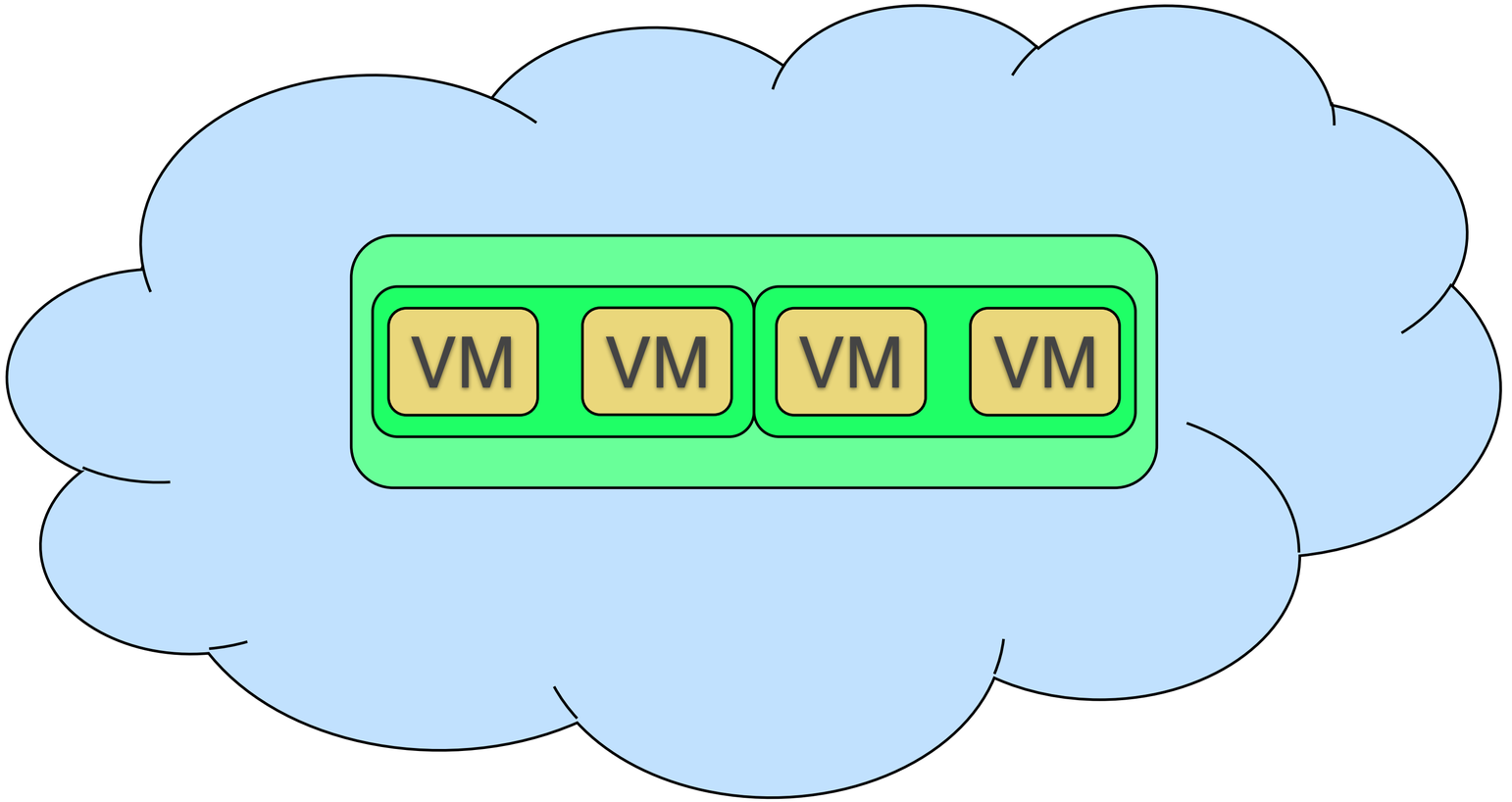
2006 – The lonely (and exposed) VM



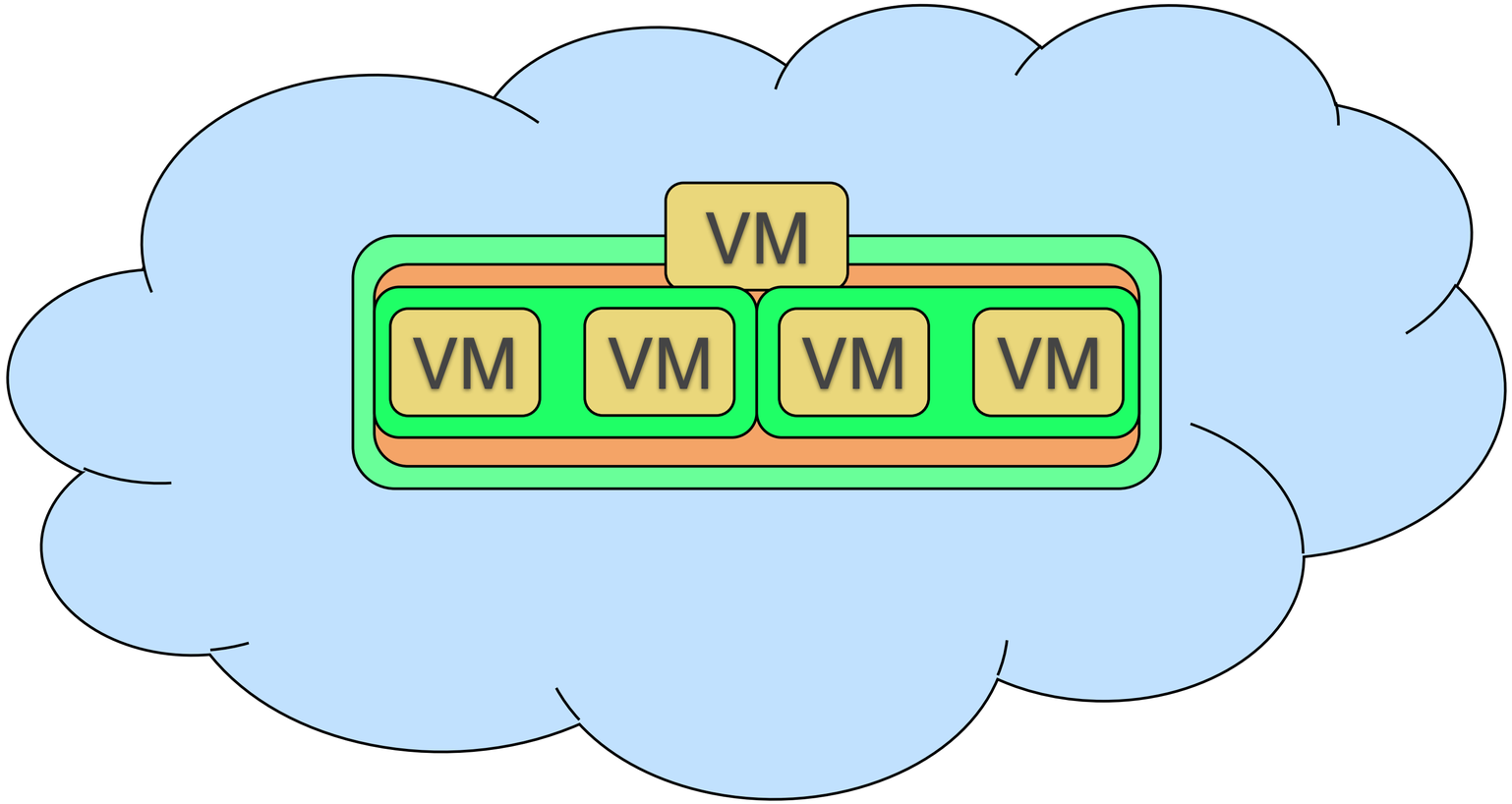
2008 - Overlays



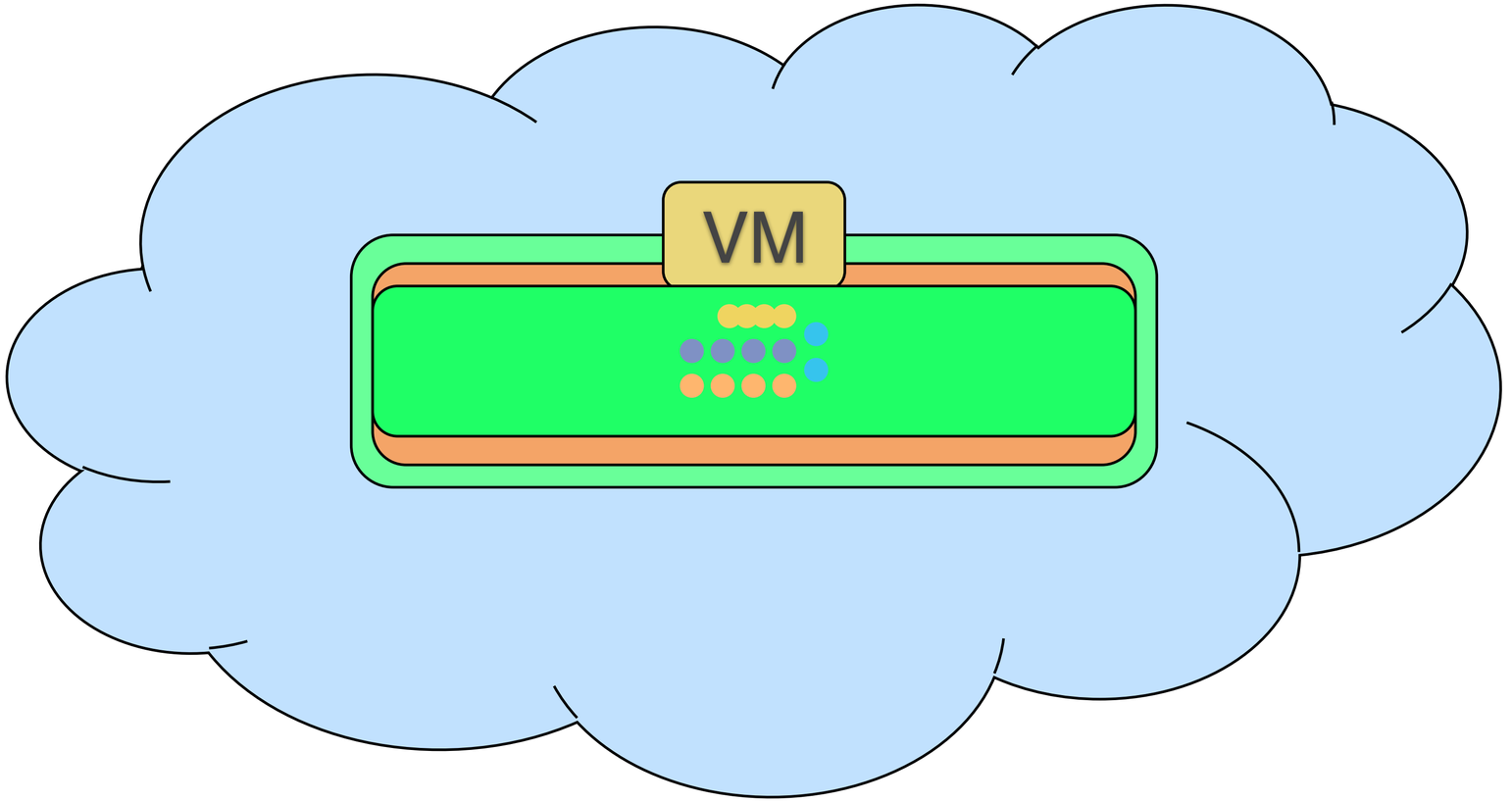
2009 - VPCs



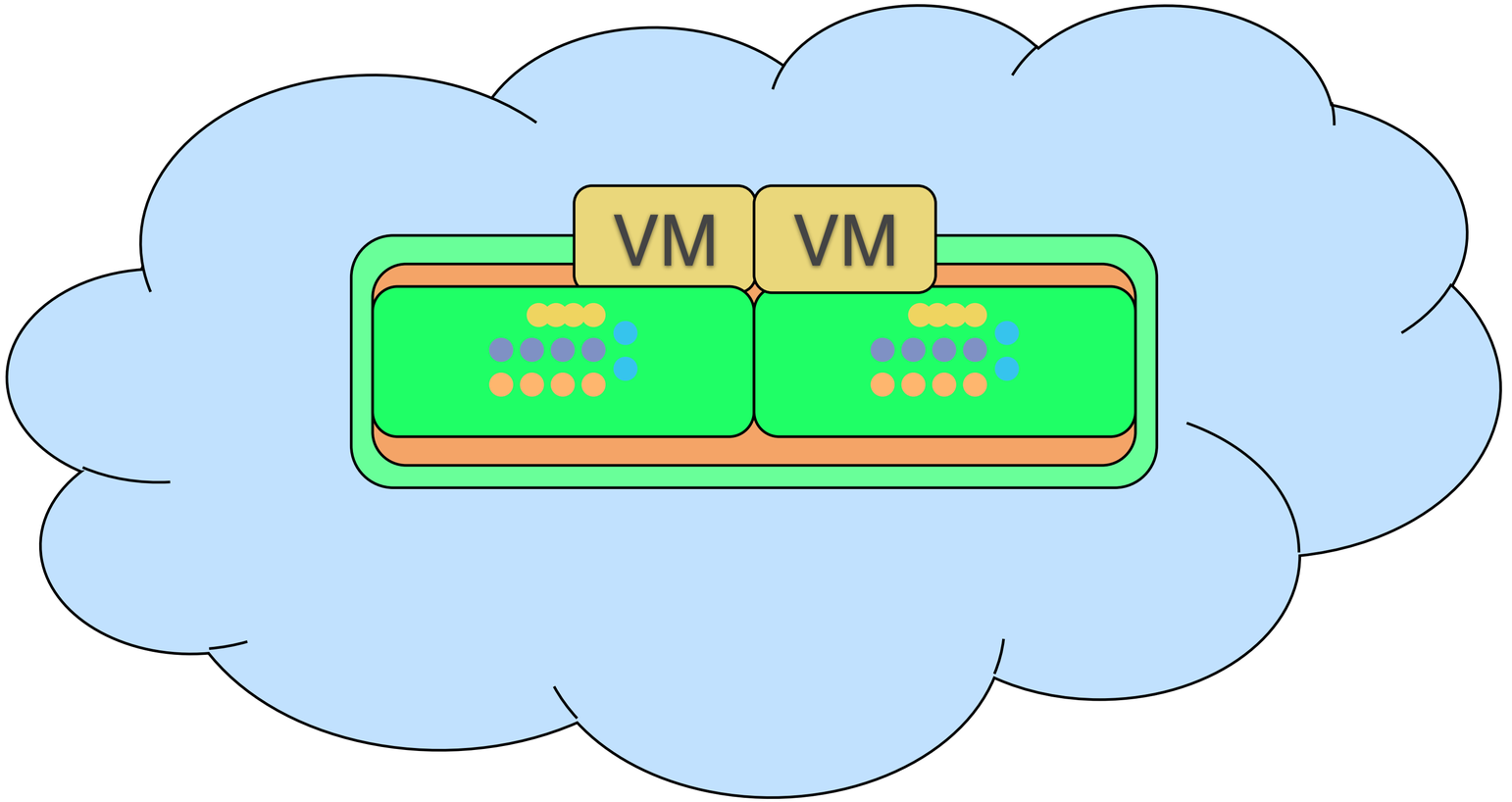
Containment often not enough – overlays stayed



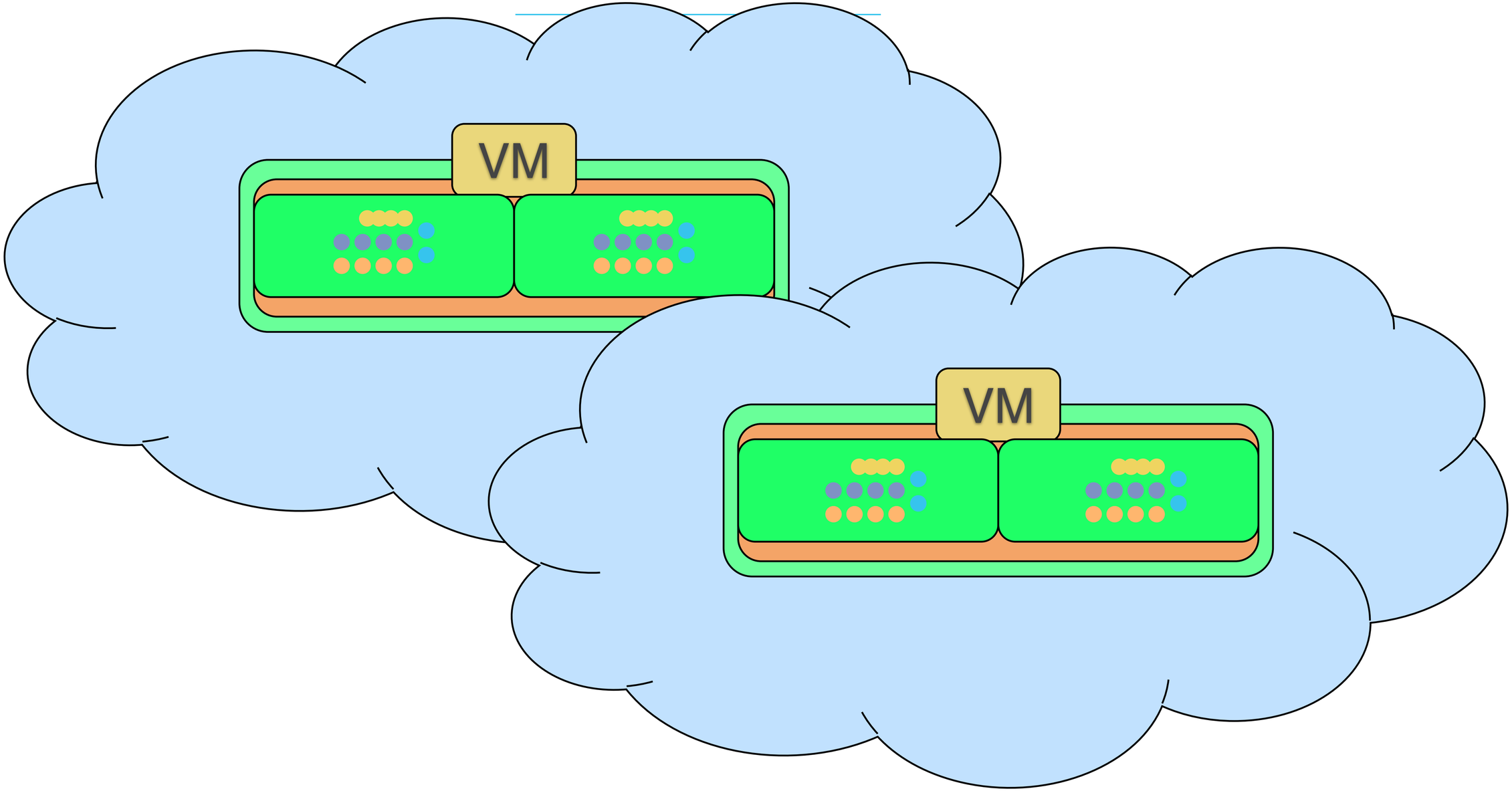
Lots of people did something like this



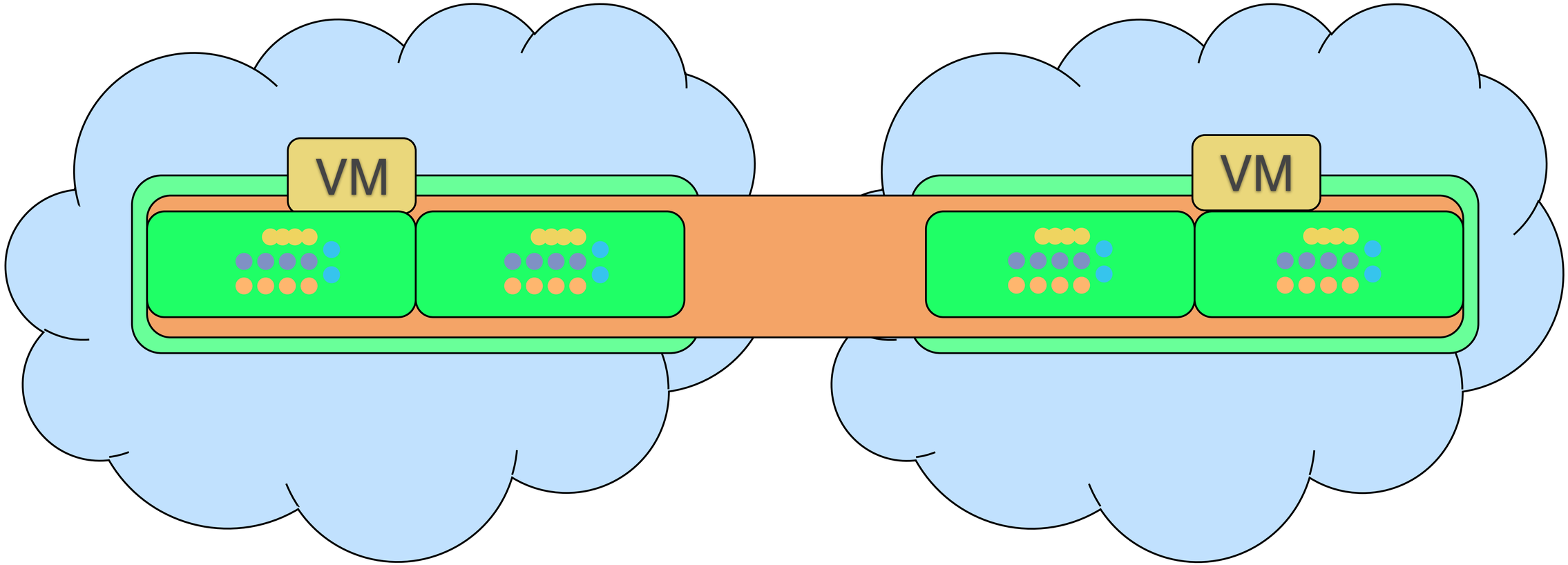
Some even did something like this



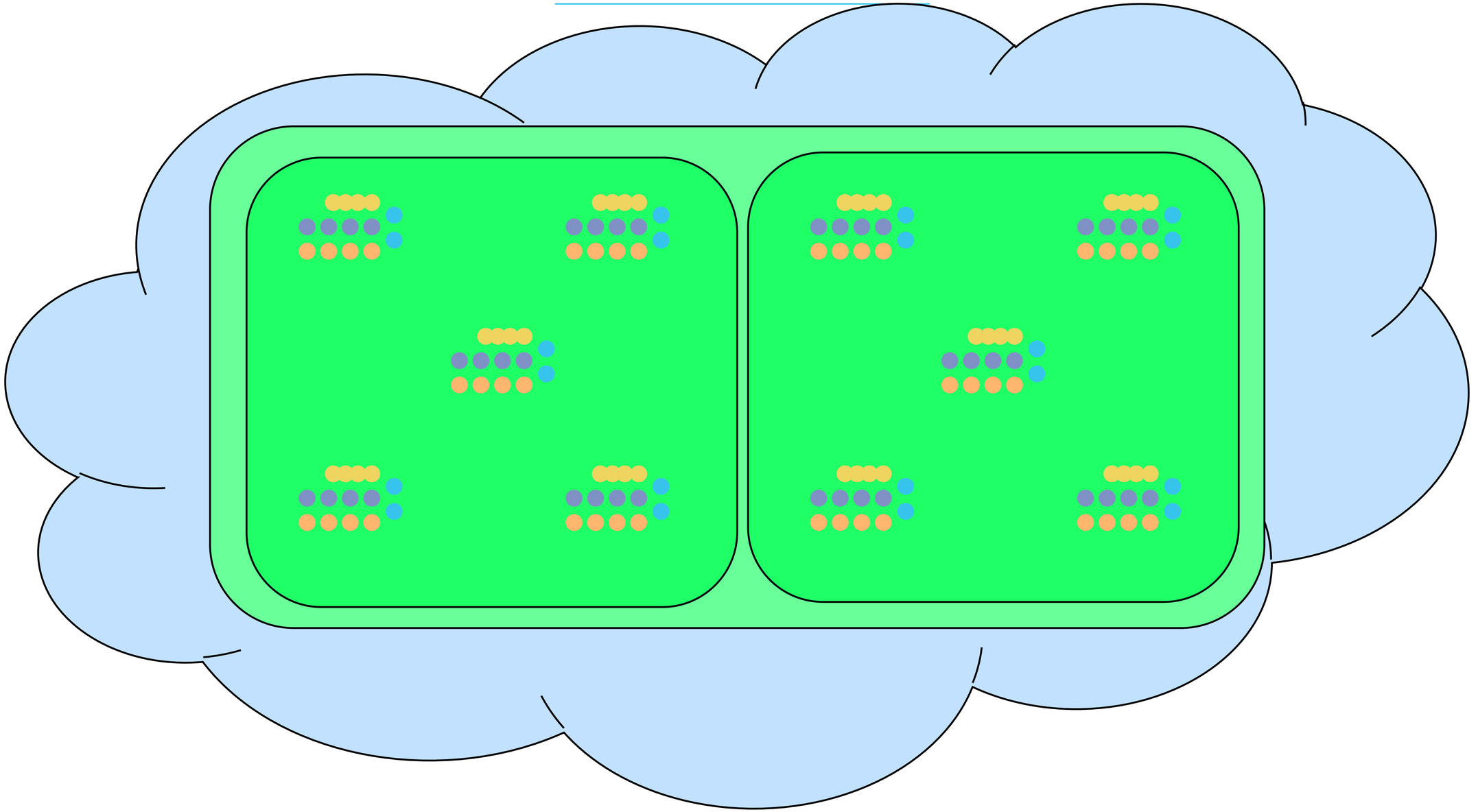
And the really large (or paranoid) might do this



Or even this



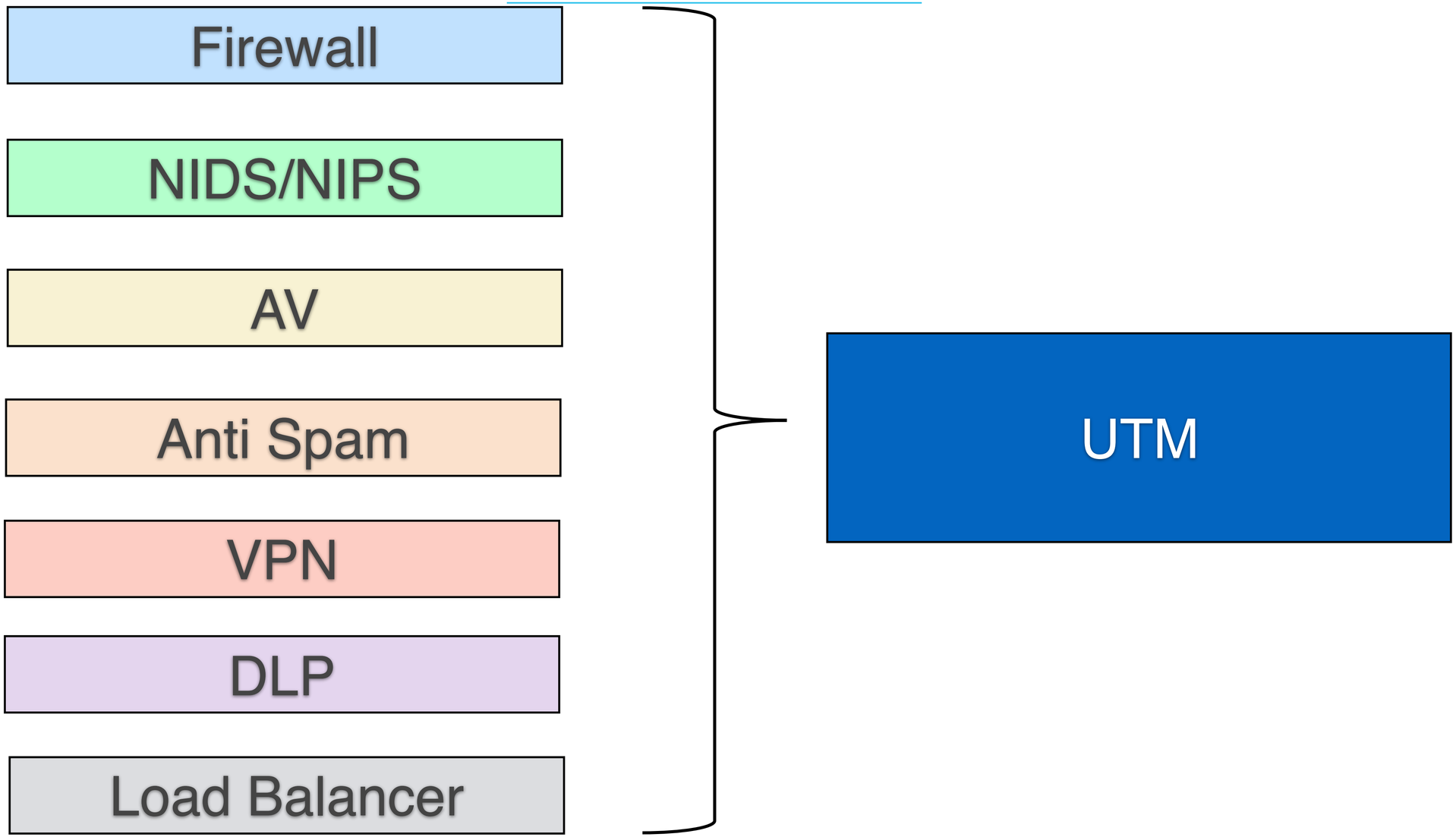
Thankfully almost nobody tries to do this



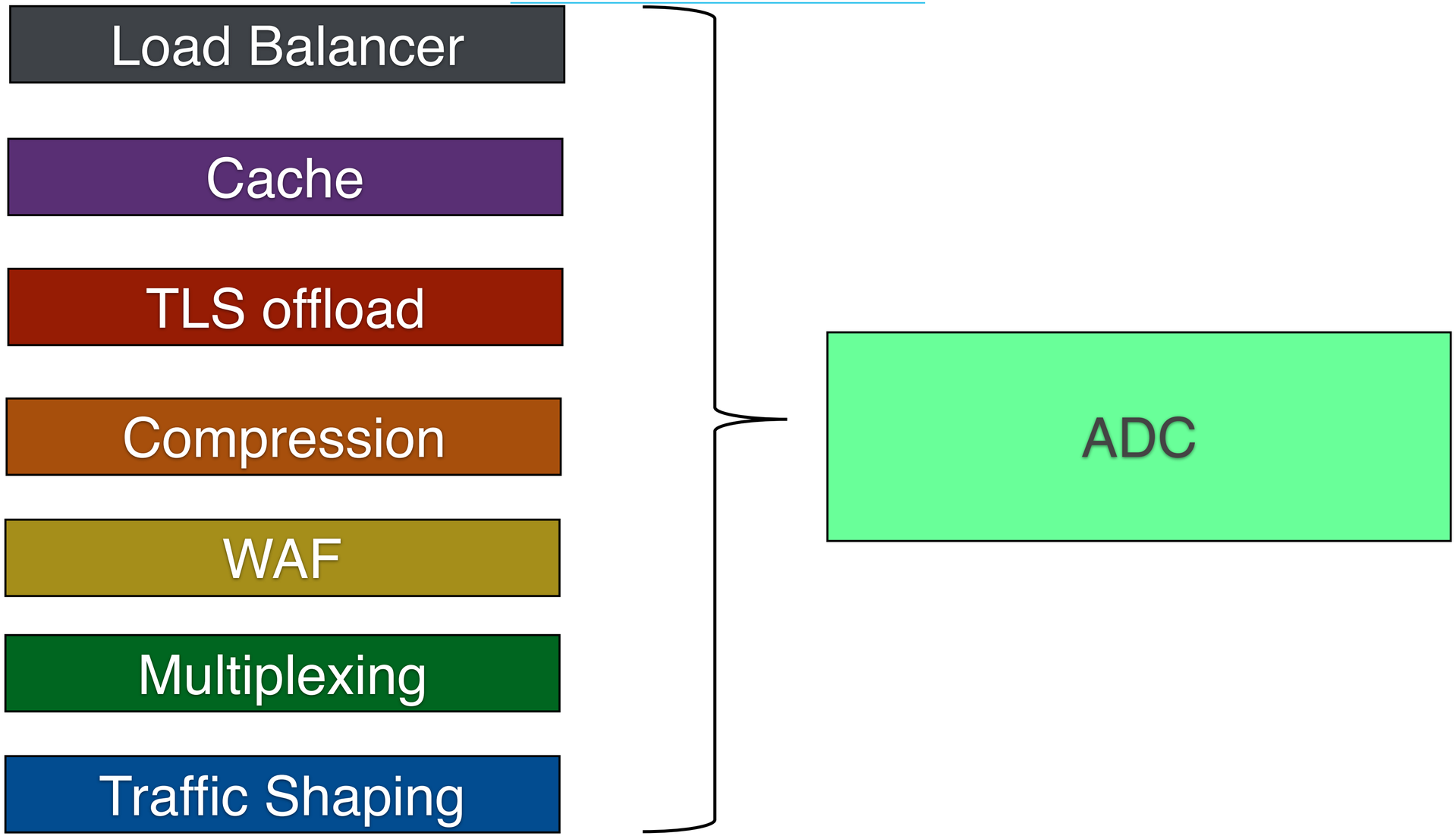
What was that perimeter made of?

A quick detour to the worlds of:

Unified Threat Management



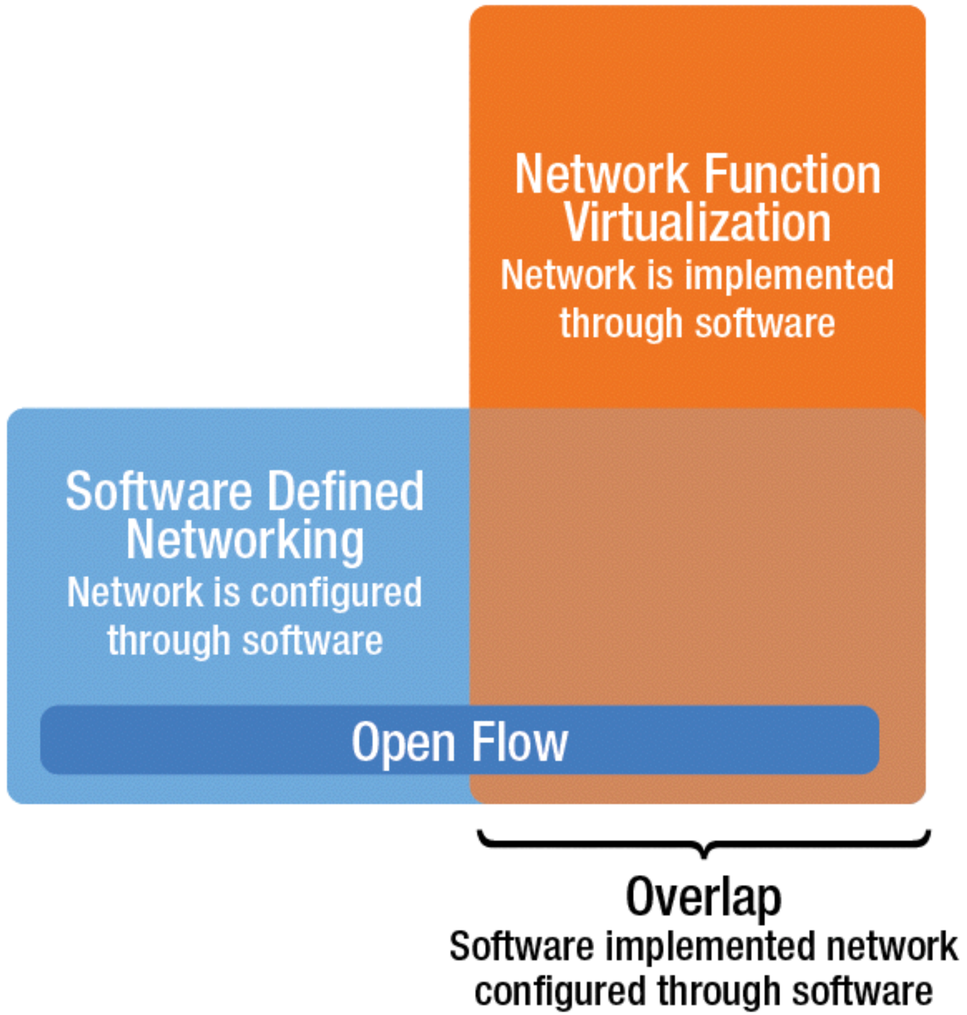
Application Delivery Controllers



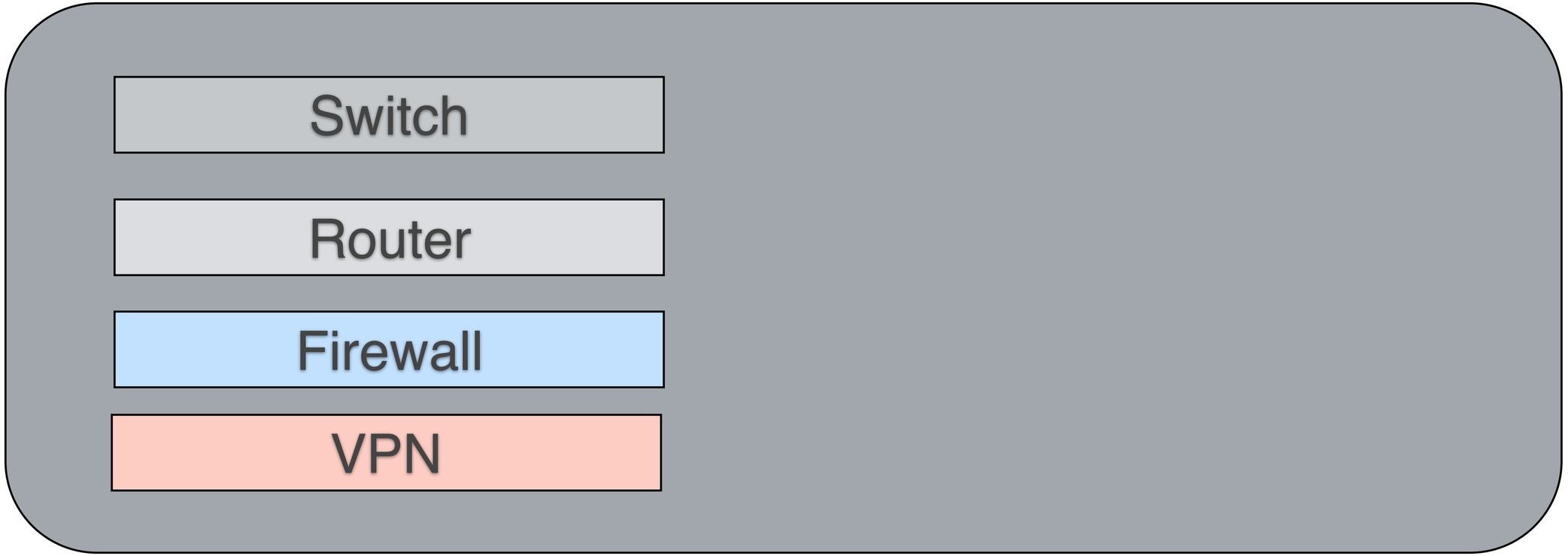
The UTM & ADC delivery model

SDN and NFV

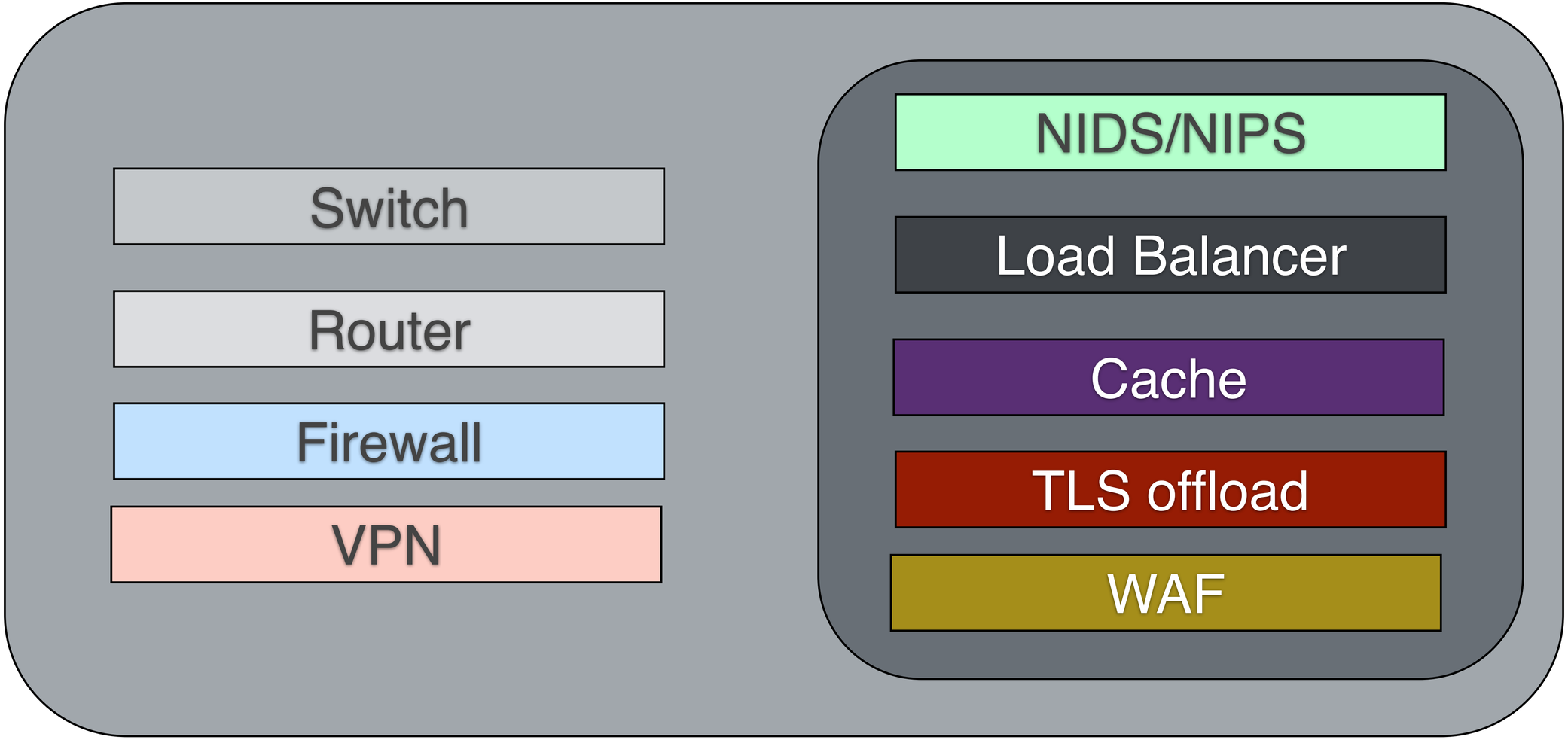
Networks made from and configured by software



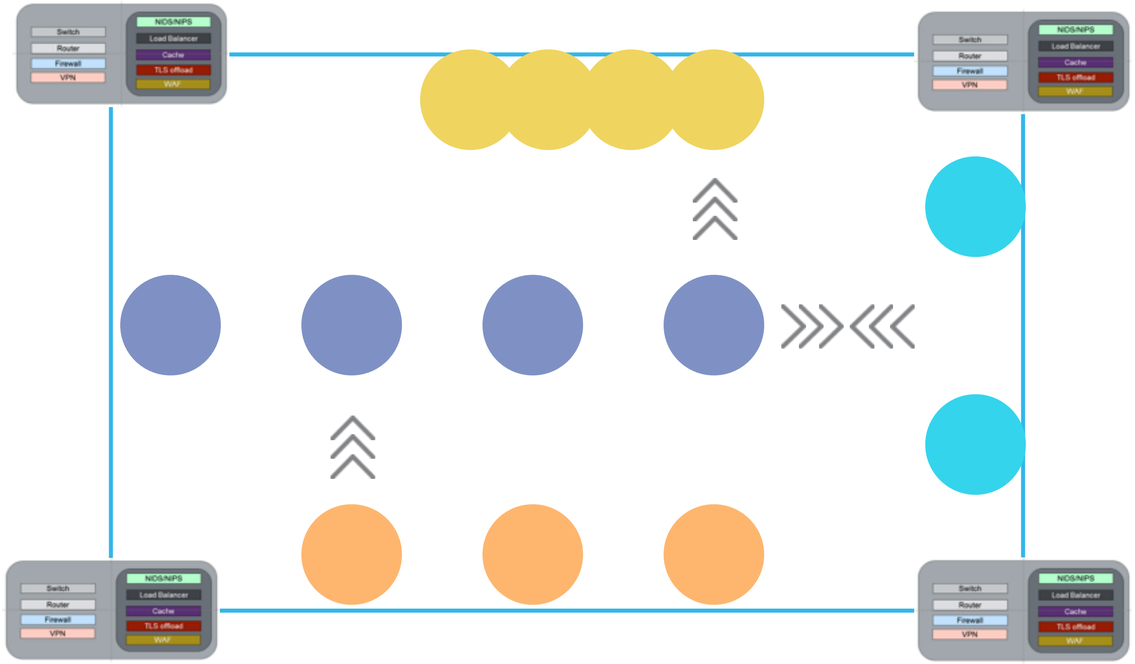
We can put a bunch of ‘network’ onto a VM



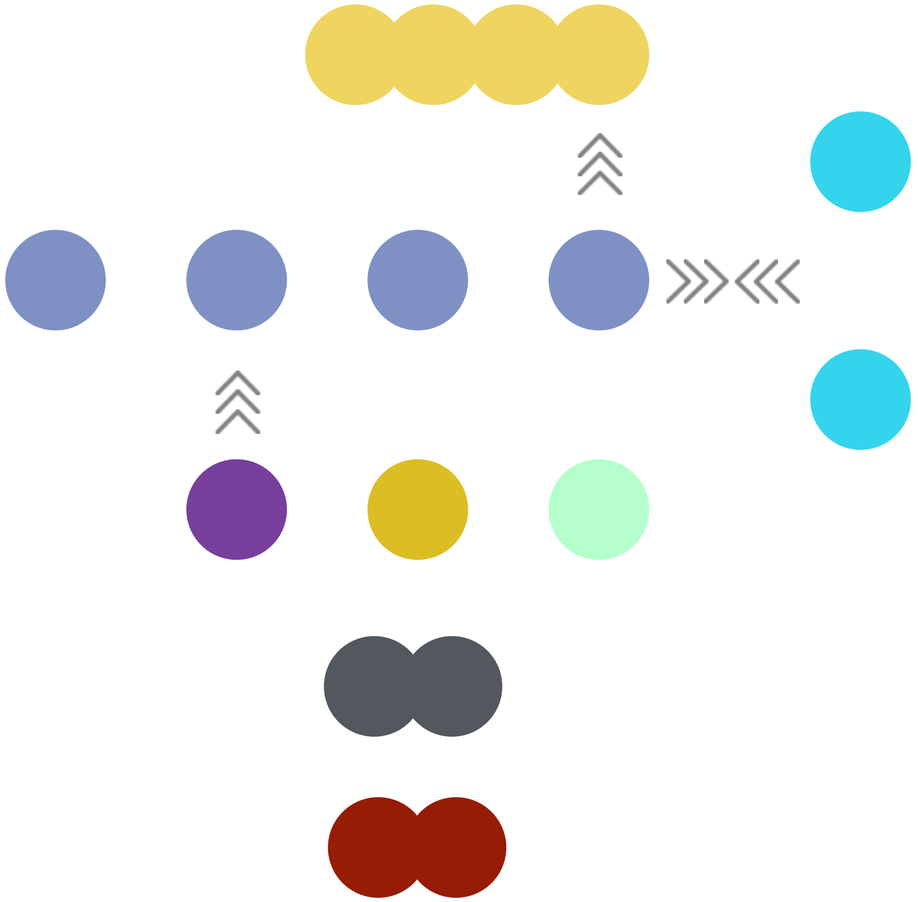
And add more functions into containers



This could be thought of as an app centric perimeter



But it refactors very readily into microservices

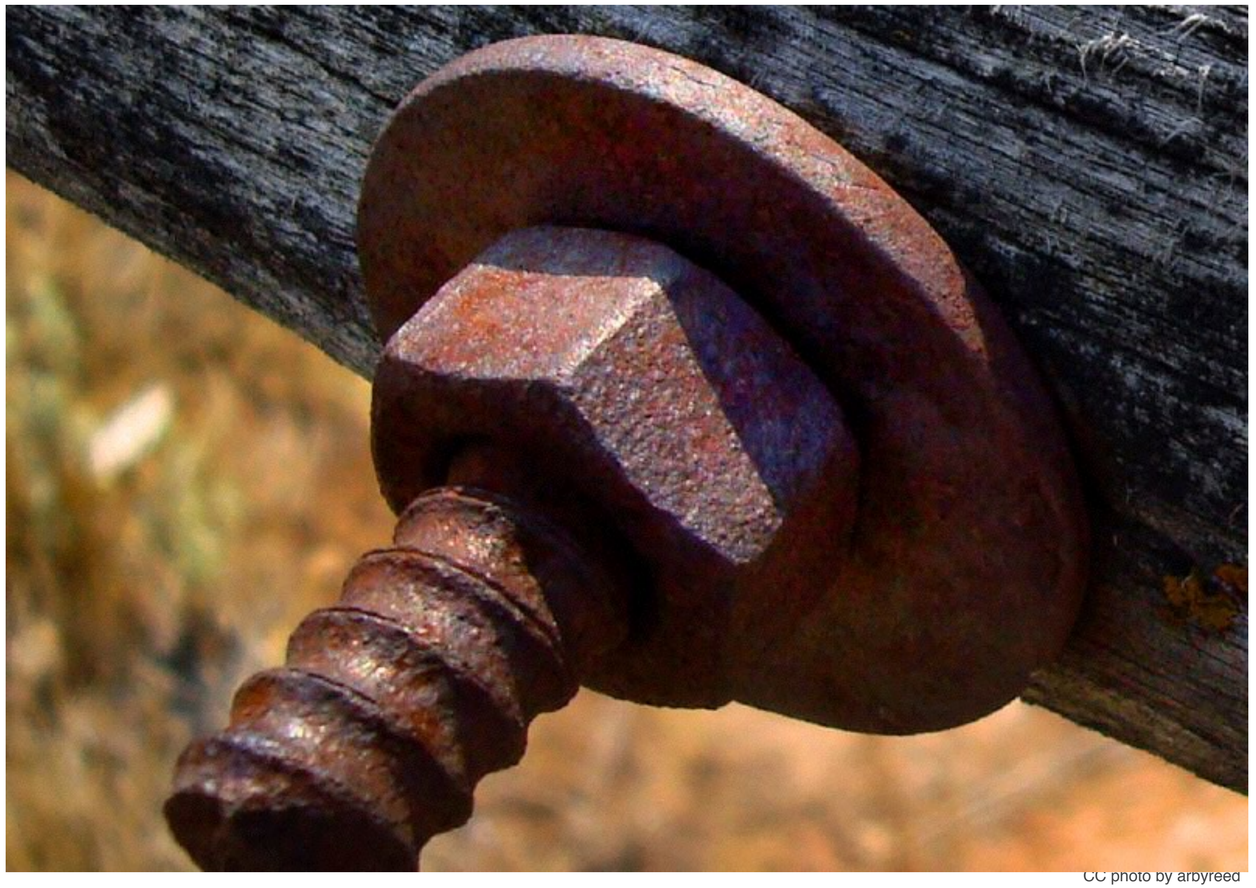


The audit paradox

Building in

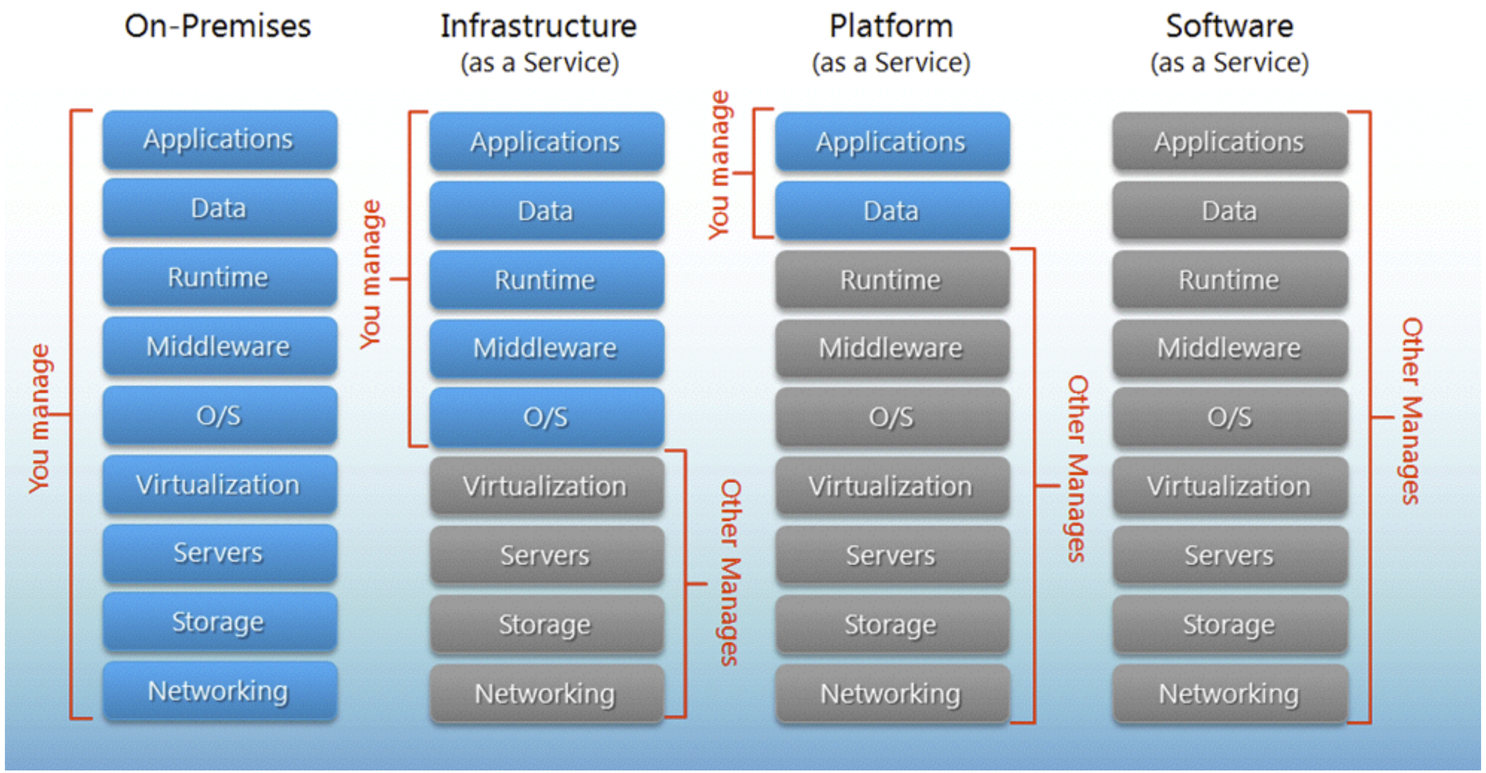
CC photo by WorldSkills

Bolting on

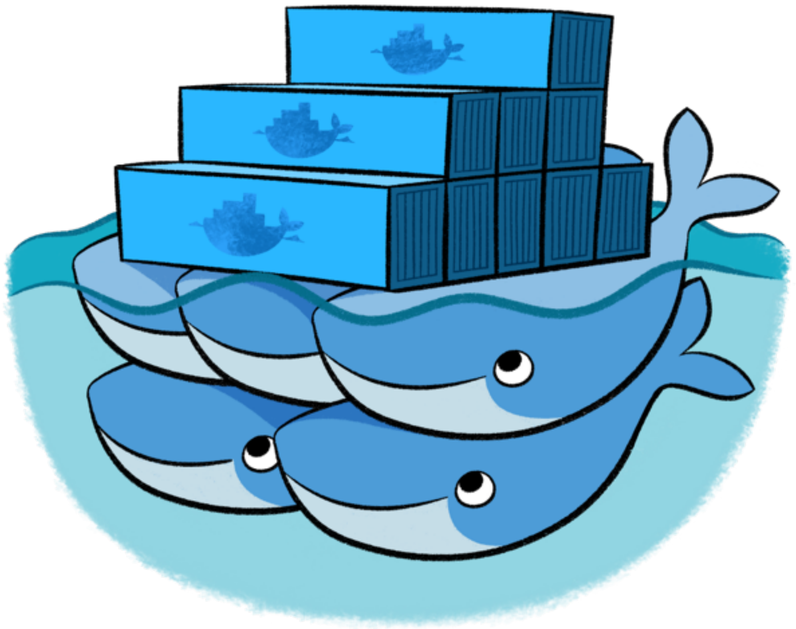


CC photo by arbyreed

PaaS gives us the chance to ‘bolt in’



But Docker adoption shows a movement against opinionated platforms



If a security event happens and it isn’t monitored

Some challenges remain

ToDo: SecDevOps

APIs are necessary but not sufficient:

Need to have them integrated into the overall system

Control metadata (and its mutability):

Must be visible and understandable

Security events need to be captured:

Then turned into something humans can action

goto; conference

Please

Remember to rate this session

Thank you!

Join the conversation #gotoldn

goto; conference

Thanks !

Join the conversation #gotoldn