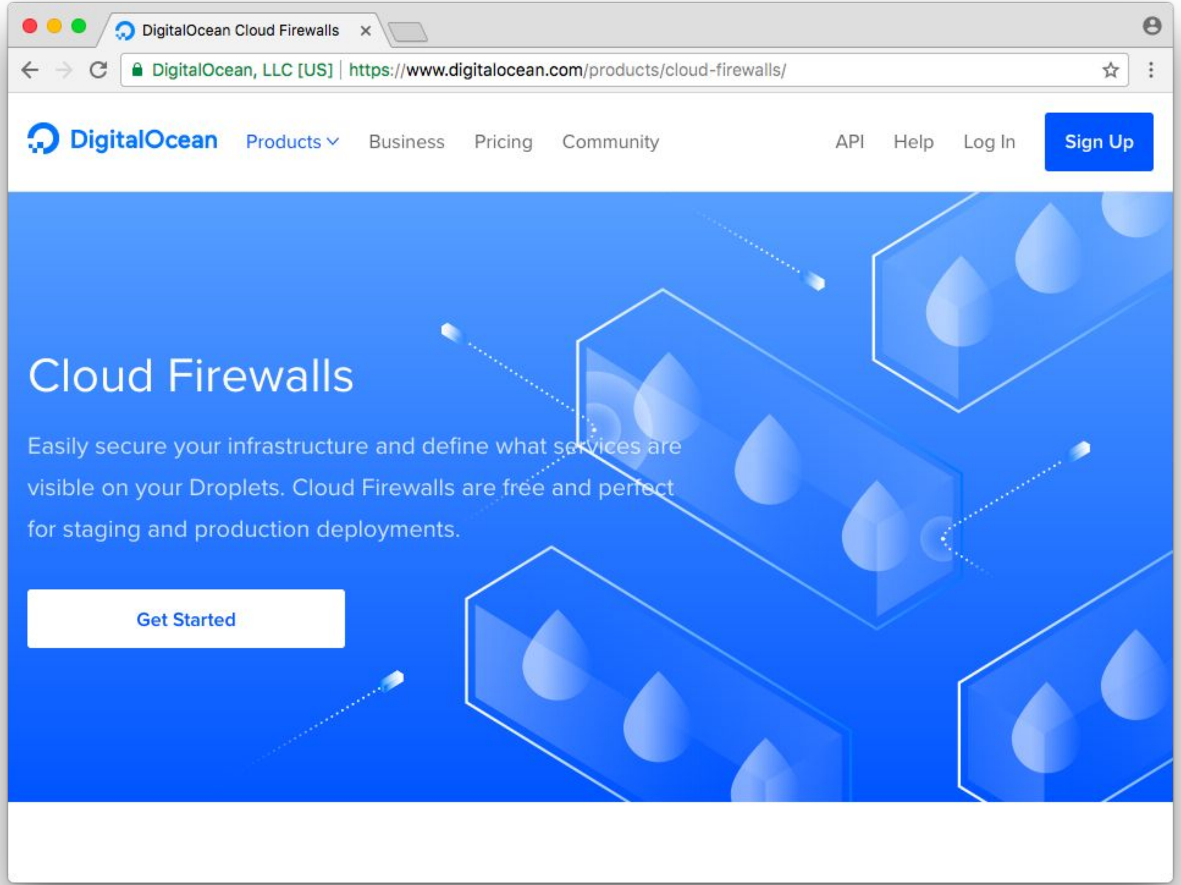
DigitalOcean Cloud Firewalls

Kei Nohguchi
OvSCon 2017
Nov 16, 2017

DigitalOcean Cloud Firewalls

powered by OvS + conntrack

Kei Nohguchi
OvSCon 2017
Nov 16, 2017


DigitalOcean Cloud Firewalls
DigitalOcean, LLC [US] | https://www.digitalocean.com/products/cloud-firewalls/
DigitalOcean
Products
Business
Pricing
Community
API
Help
Log In
Sign Up

Cloud Firewalls

Easily secure your infrastructure and define what services are visible on your Droplets. Cloud Firewalls are free and perfect for staging and production deployments.

Get Started

digitalocean.com

OvS

OvS

+

conntrack

Who

300+

3 stories

1. Open Source & DO

1. Open Source & DO
2. OvS & DO

1. Open Source & DO
2. OvS & DO
3. conntrack & DO

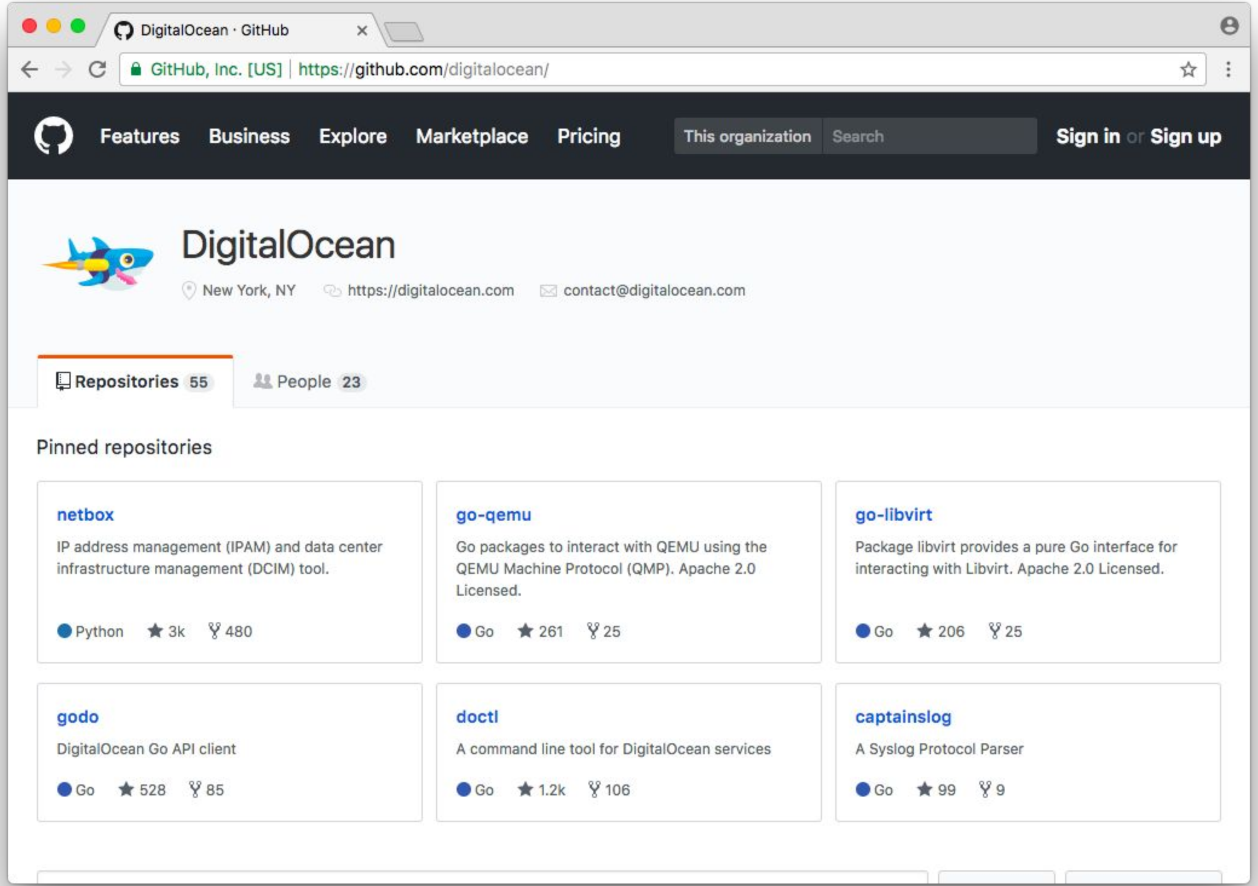
Open Source

KVM

OvS

conntrack

golang



DigitalOcean

New York, NY https://digitalocean.com contact@digitalocean.com

Repositories 55 People 23

Pinned repositories

netbox
IP address management (IPAM) and data center infrastructure management (DCIM) tool.
Python ★ 3k 480

go-qemu
Go packages to interact with QEMU using the QEMU Machine Protocol (QMP). Apache 2.0 Licensed.
Go ★ 261 25

go-libvirt
Package libvirt provides a pure Go interface for interacting with Libvirt. Apache 2.0 Licensed.
Go ★ 206 25

godo
DigitalOcean Go API client
Go ★ 528 85

doctl
A command line tool for DigitalOcean services
Go ★ 1.2k 106

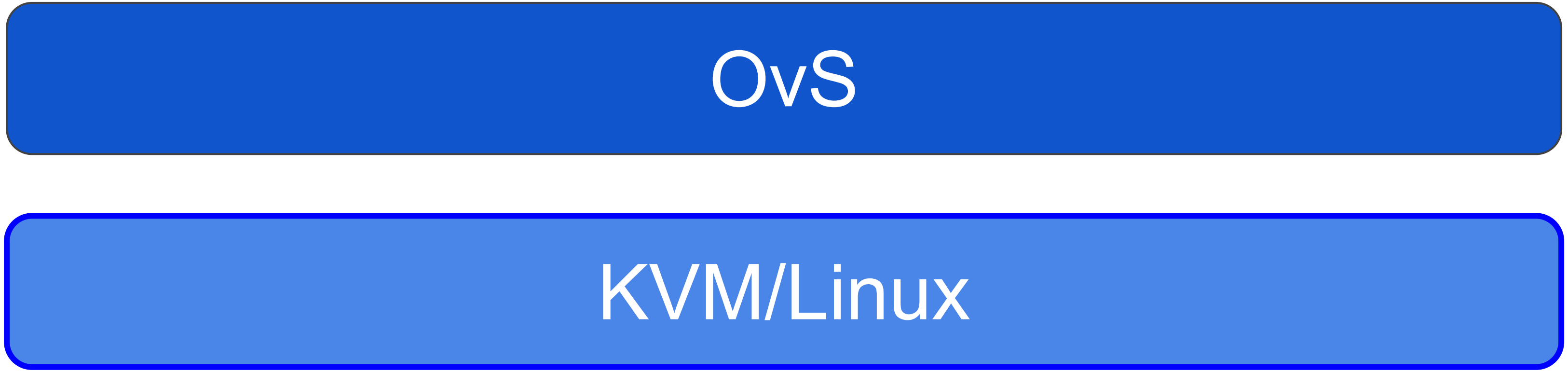
captainslog
A Syslog Protocol Parser
Go ★ 99 9

OvS

Simple

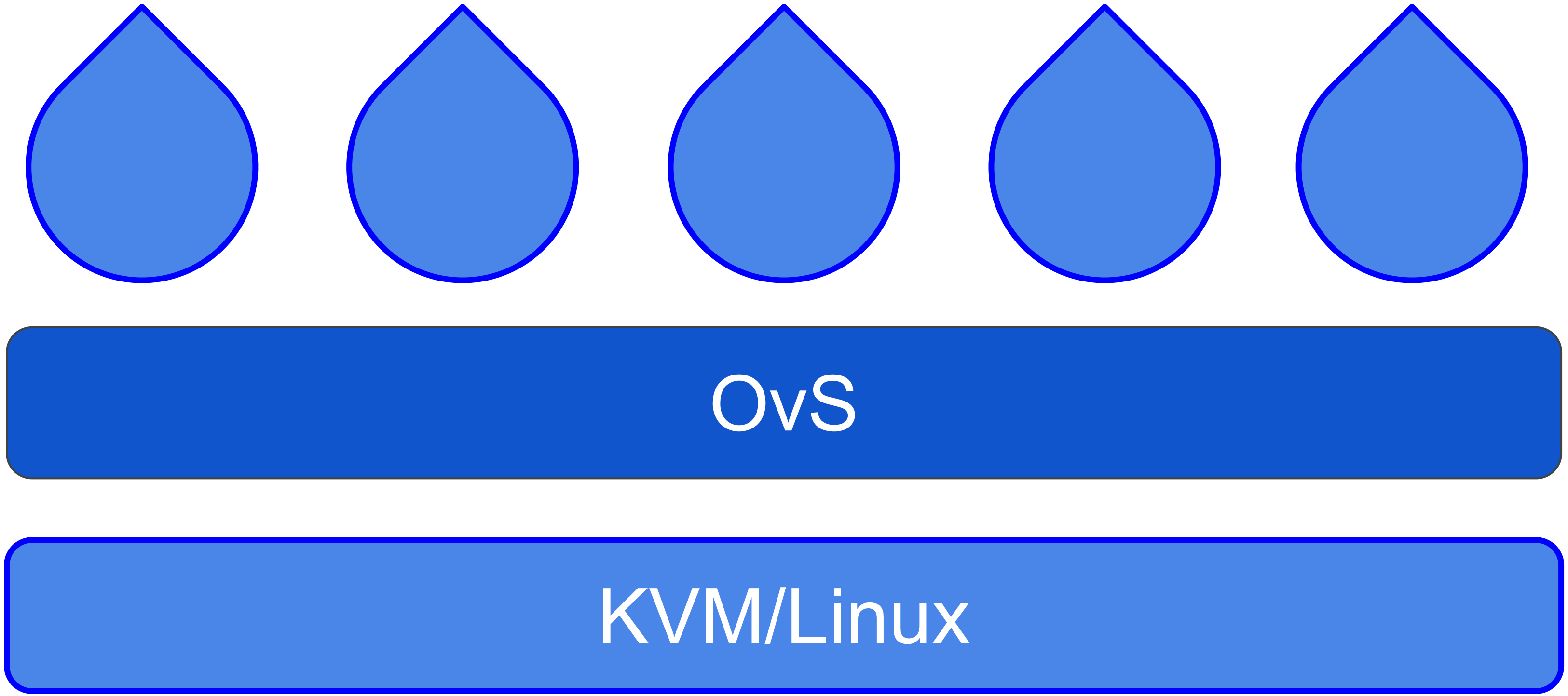
Simple == Scale

KVM/Linux



OvS

KVM/Linux



OvS

KVM/Linux

OvS

br0

OvS

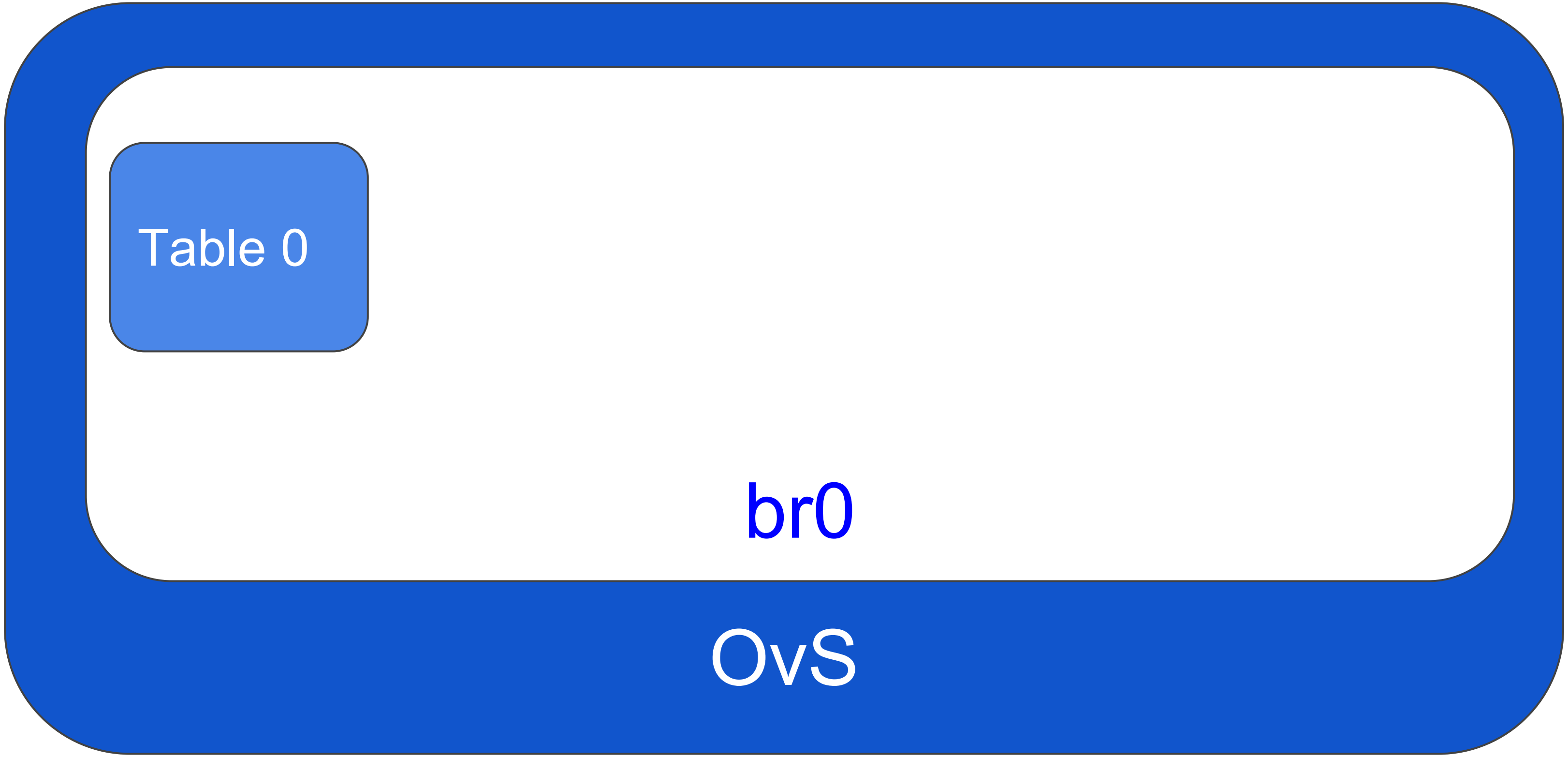


Table 0
br0
OvS

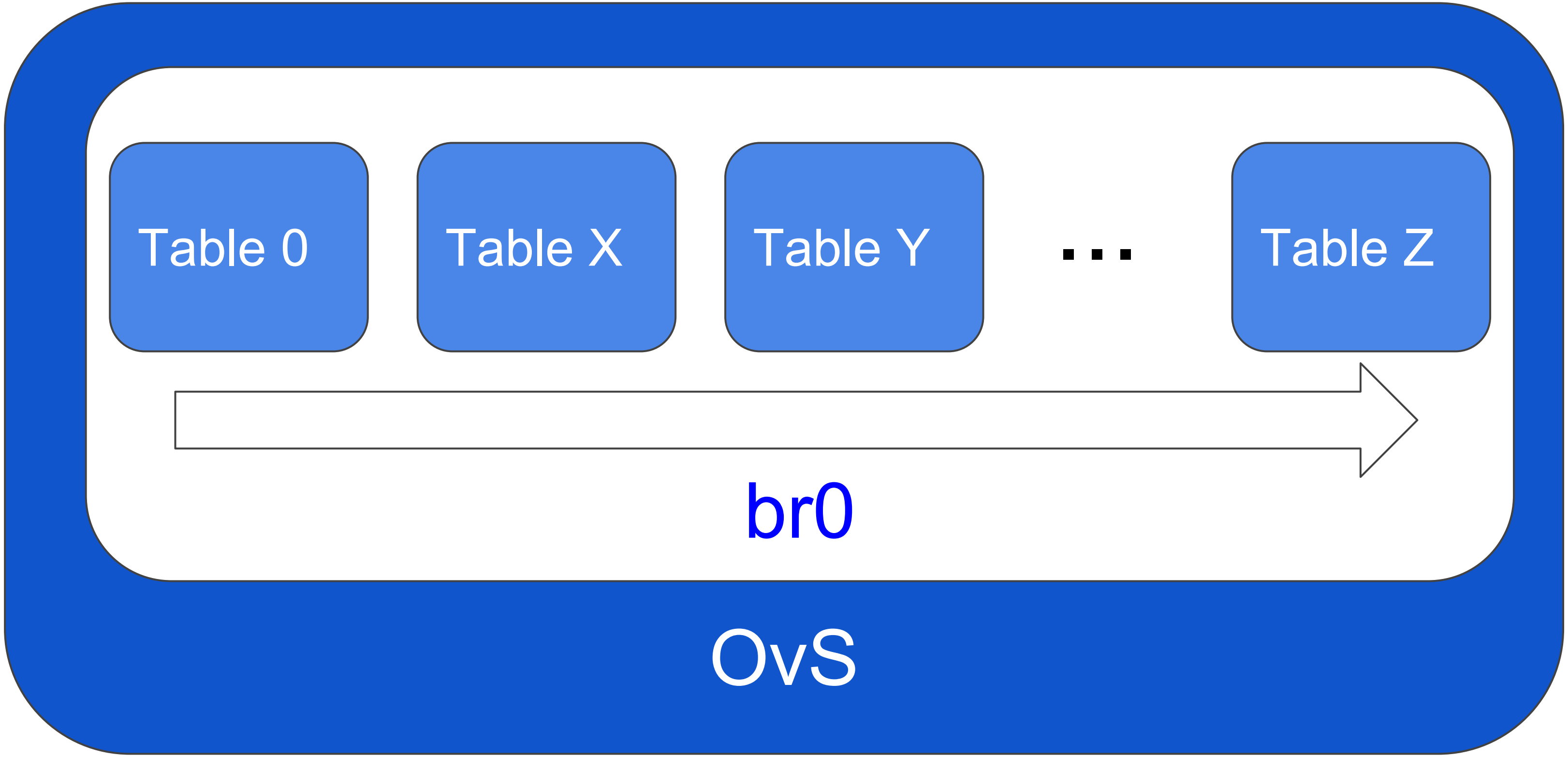


Table 0
Table X
Table Y
...
Table Z
br0
OvS

```
table=0,priority=2010,arp,in_port=1234,\
   arp_sha=00:01:02:03:04:05,arp_spa=1.1.1.2\
   actions=resubmit(,x)
table=0,priority=2000,ip,in_port=1234,\
   dl_src=00:01:02:03:04:05,nw_src=1.1.1.2\
   actions=resubmit(,x)

...

table=0,priority=100 actions=drop
```

conntrack

Stateful

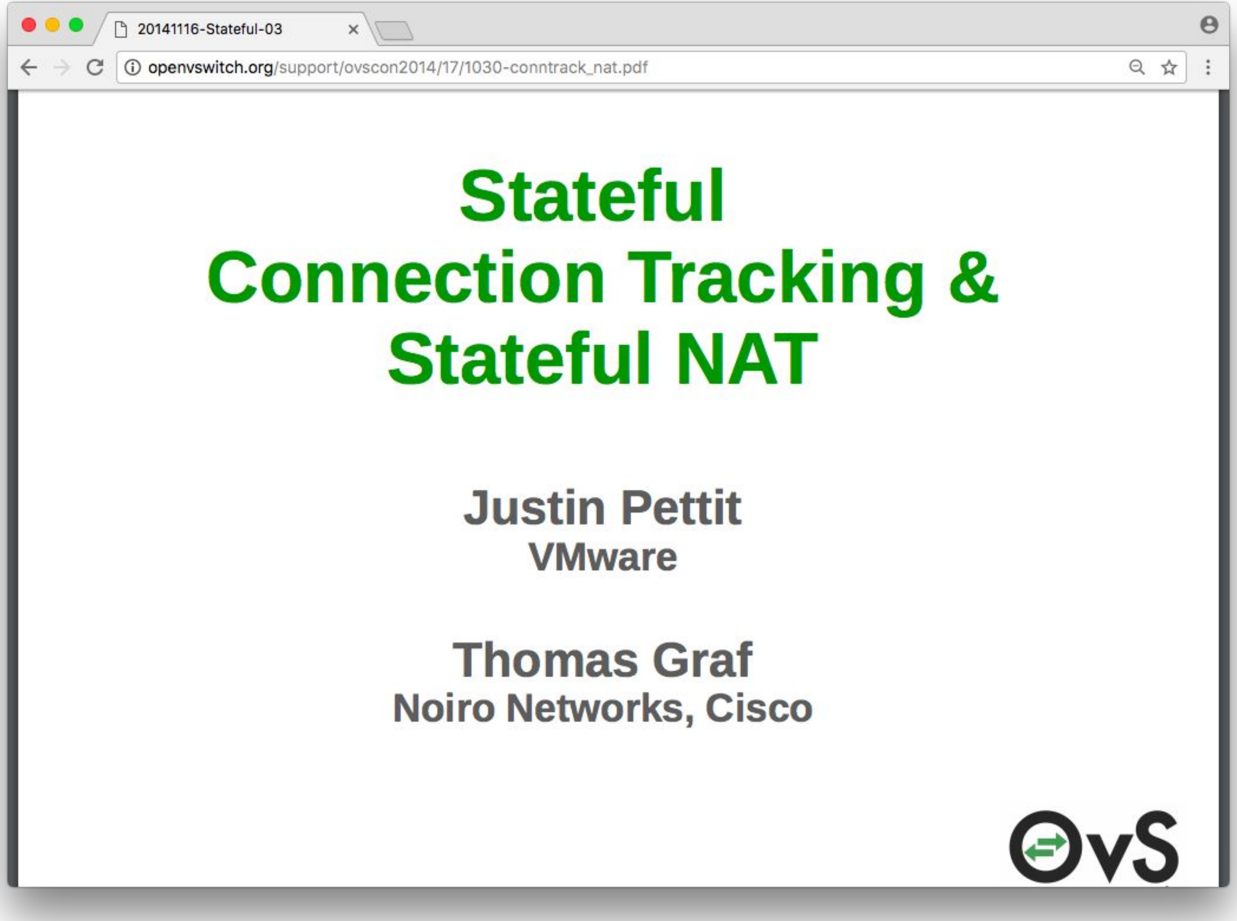
Stateful

vs

Stateless

OvS 2.4

OvS 2.5

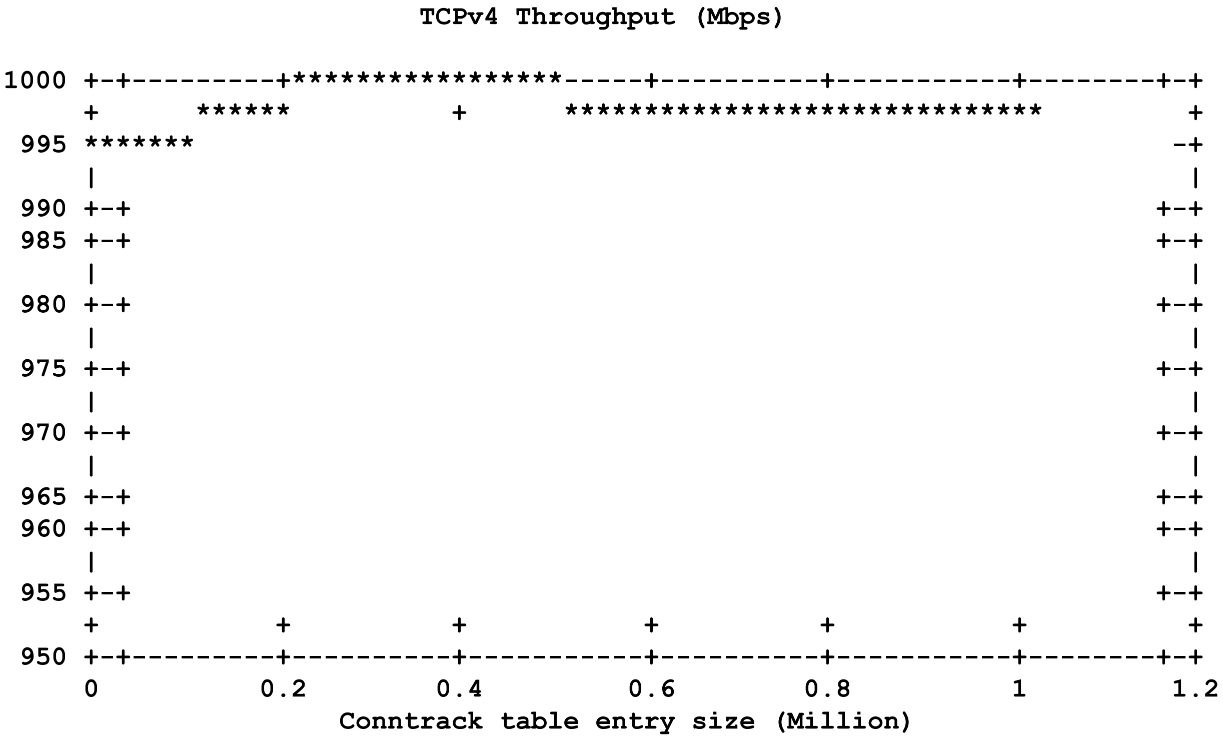


20141116-Stateful-03
openvswitch.org/support/ovscon2014/17/1030-conntrack_nat.pdf

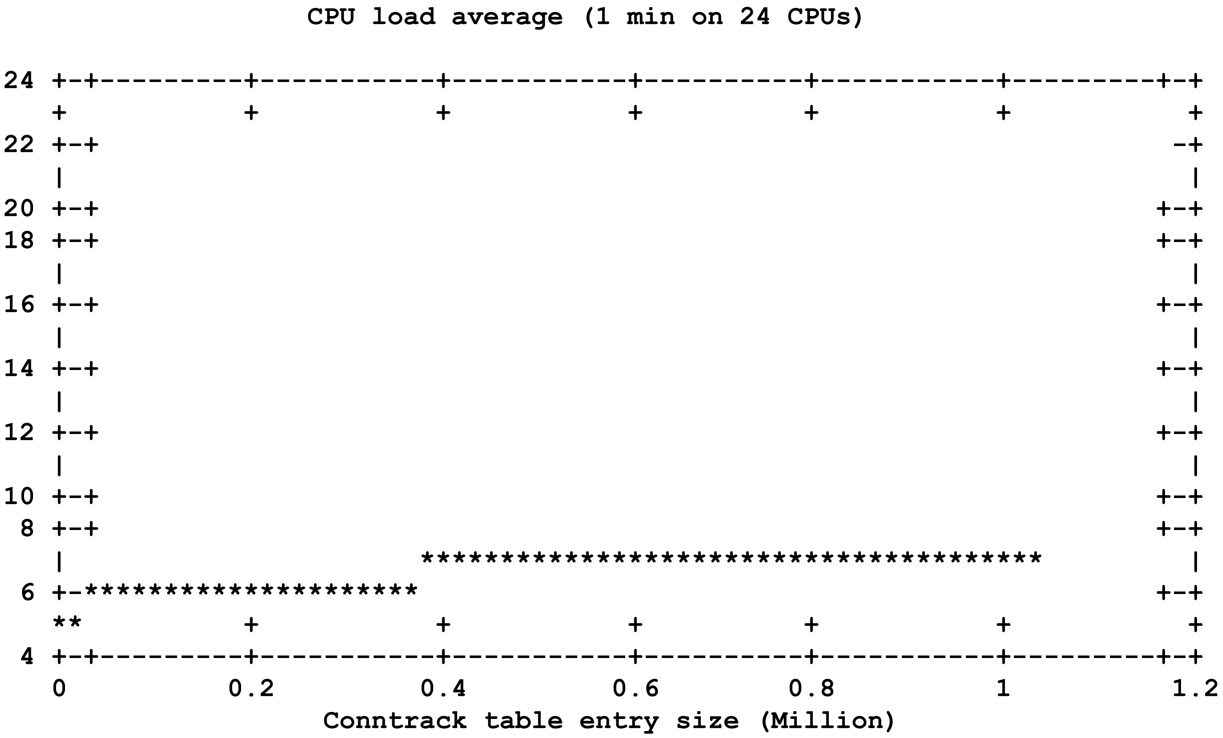
Stateful
Connection Tracking &
Stateful NAT

Justin Pettit
VMware

Thomas Graf
Noiro Networks, Cisco



```
                          TCPv4 Throughput (Mbps)

1000 +-+---------+*****************-----+----------+-----------+--------+-+
     +      ******          +      ******************************         +
 995 *******                                                             -+
     |                                                                    |
 990 +-+                                                                +-+
 985 +-+                                                                +-+
     |                                                                    |
 980 +-+                                                                +-+
     |                                                                    |
 975 +-+                                                                +-+
     |                                                                    |
 970 +-+                                                                +-+
     |                                                                    |
 965 +-+                                                                +-+
 960 +-+                                                                +-+
     |                                                                    |
 955 +-+                                                                +-+
     +           +          +           +          +           +          +
 950 +-+---------+----------+-----------+----------+-----------+--------+-+
     0          0.2        0.4         0.6        0.8          1         1.2
                     Conntrack table entry size (Million)
```



```
                  CPU load average (1 min on 24 CPUs)

24 +-+---------+-----------+-----------+----------+-----------+---------+-+
   +           +           +           +          +           +           +
22 +-+                                                                   -+
   |                                                                      |
20 +-+                                                                  +-+
18 +-+                                                                  +-+
   |                                                                      |
16 +-+                                                                  +-+
   |                                                                      |
14 +-+                                                                  +-+
   |                                                                      |
12 +-+                                                                  +-+
   |                                                                      |
10 +-+                                                                  +-+
 8 +-+                                                                  +-+
   |                      ***************************************         |
 6 +-*********************                                              +-+
   **          +           +           +          +           +           +
 4 +-+---------+-----------+-----------+----------+-----------+---------+-+
   0          0.2         0.4         0.6        0.8          1          1.2
                   Conntrack table entry size (Million)
                   Conntrack Memory Consumption (MBytes)

600 +-+---------+----------+-----------+-----------+----------+---------+-+
    +           +          +           +           +          +           +
    |                                                          **         |
500 +-+                                                    ****         +-+
    |                                                  ****               |
    |                                              ****                   |
400 +-+                                         ***                     +-+
    |                                       ****                          |
    |                                   ****                              |
300 +-+                             ****                                +-+
    |                            ***                                      |
    |                        ****                                         |
200 +-+                  ****                                           +-+
    |                ****                                                 |
    |             ***                                                     |
100 +-+       ****                                                      +-+
    |     ****                                                            |
    + ****      +          +           +           +          +           +
  0 **+---------+----------+-----------+-----------+----------+---------+-+
    0          0.2        0.4         0.6         0.8         1          1.2
                     Conntrack table entry size (Million)
```

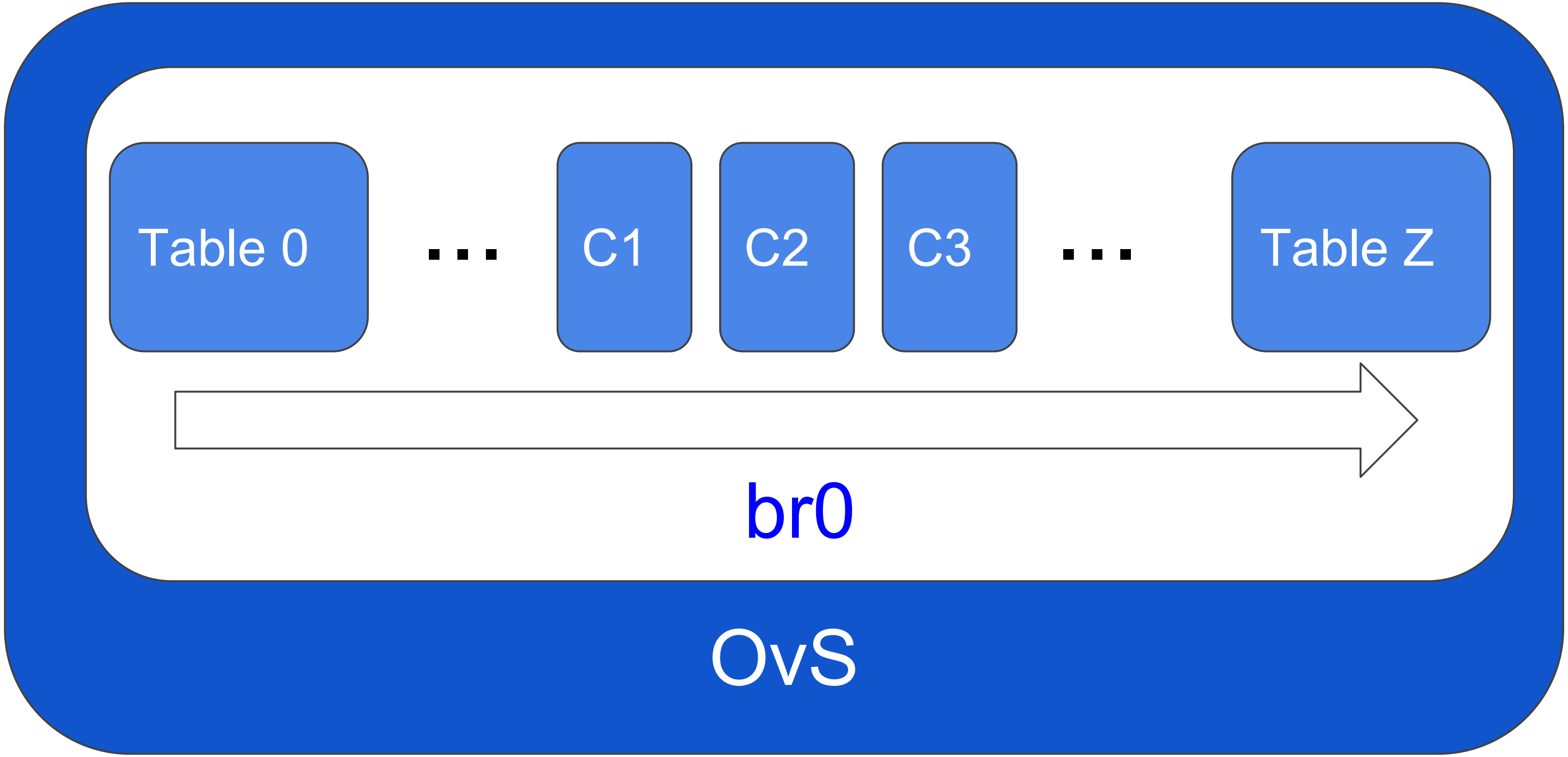
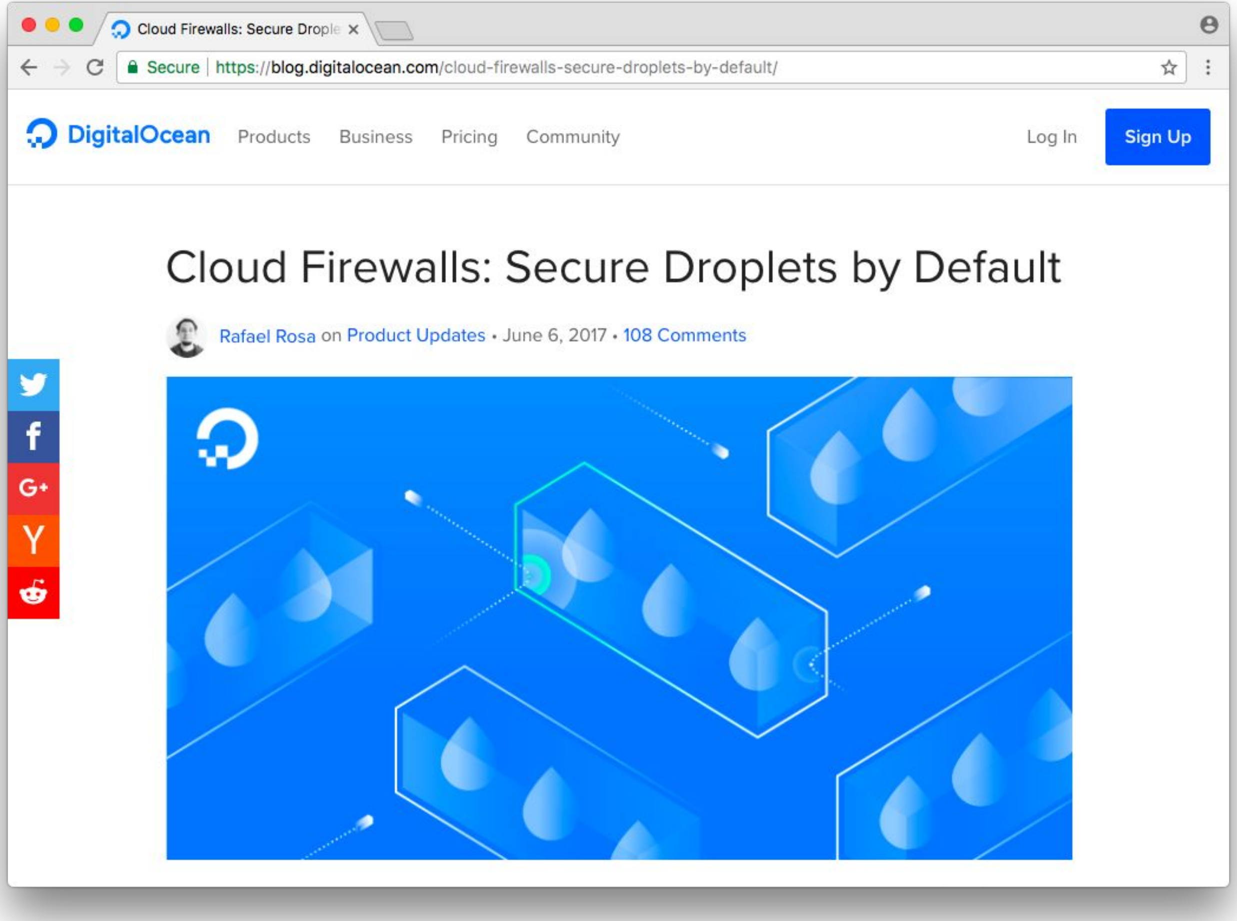


Table 0
...
C1
C2
C3
...
Table Z
br0
OvS

```
table=c1,priority=110,ip,\
  dl_dst=00:01:02:03:04:05\
  actions=ct(table=c2)

...

table=c1,priority=100 actions=resubmit(,z)
```

```
table=c2,priority=202,ct_state=+est+rpl+trk,\
   ip actions=resubmit(,z)
table=c2,priority=200 actions=resubmit(,c3)
```

```
table=c3,priority=1000,ct_state=+new+trk,\
   tcp,dl_dst=00:01:02:03:04:05,\
   nw_src=1.1.2.0/24,tp_dst=443\
   actions=ct(commit,table=z)

...

table=c3,priority=100 actions=drop
```



Cloud Firewalls: Secure Drople
Secure
https://blog.digitalocean.com/cloud-firewalls-secure-droplets-by-default/
DigitalOcean
Products
Business
Pricing
Community
Log In
Sign Up

Cloud Firewalls: Secure Droplets by Default

Rafael Rosa on Product Updates • June 6, 2017 • 108 Comments

Summary

1. DO loves Open Source

1. DO loves Open Source
2. DO loves OvS

1. DO loves Open Source
2. DO loves OvS
3. DO loves conntrack

Thank you!

@keinohguchi

DigitalOcean