DigitalOcean
Cloud Firewalls

Kei Nohguchi
OvSCon 2017
Nov 16, 2017
DigitalOcean
Cloud Firewalls
powered by OvS + conntrack

Kei Nohguchi
OvSCon 2017
Nov 16, 2017
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
OvS
+
conntrack
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
golang
### Pinned repositories

<table>
<thead>
<tr>
<th>Repository</th>
<th>Description</th>
<th>Language</th>
<th>Stars</th>
<th>Forks</th>
</tr>
</thead>
<tbody>
<tr>
<td>netbox</td>
<td>IP address management (IPAM) and data center infrastructure management (DCIM) tool.</td>
<td>Python</td>
<td>3k</td>
<td>490</td>
</tr>
<tr>
<td>go-qemu</td>
<td>Go packages to interact with QEMU using the QEMU Machine Protocol (QMP). Apache 2.0 Licensed.</td>
<td>Go</td>
<td>251</td>
<td>25</td>
</tr>
<tr>
<td>go-libvirt</td>
<td>Package libvirt provides a pure Go interface for Interacting with Libvirt. Apache 2.0 Licensed.</td>
<td>Go</td>
<td>206</td>
<td>25</td>
</tr>
<tr>
<td>godo</td>
<td>DigitalOcean Go API client</td>
<td>Go</td>
<td>528</td>
<td>85</td>
</tr>
<tr>
<td>doctl</td>
<td>A command line tool for DigitalOcean services</td>
<td>Go</td>
<td>1.2k</td>
<td>106</td>
</tr>
<tr>
<td>captainslog</td>
<td>A Syslog Protocol Parser</td>
<td>Go</td>
<td>99</td>
<td>9</td>
</tr>
</tbody>
</table>
OvS
Simple
Simple == Scale
KVM/Linux

OvS

KVM/Linux
<table>
<thead>
<tr>
<th>Table 0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>br0</strong></td>
</tr>
</tbody>
</table>

| 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
Stateful
Stateful vs Stateless
OvS 2.4
OvS 2.5
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 +------------------------------+------------------------------+

---

Conntrack table entry size (Million)
CPU load average (1 min on 24 CPUs)

Conntrack table entry size (Million)
Conntrack Memory Consumption (MBytes)

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

...
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
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