Network Policy Controller in Weave Net

Blocking unwanted network traffic in Kubernetes

Bryan Boreham
@bboreham
Who knows...

- Kubernetes
- Docker
- Linux
- iptables
Ancient wisdom

For survival, your group needs:

- Leadership
- Hunting skills
- Medical skills
- Someone who knows iptables
What I am going to talk about

Weave Network Policy Controller

Blocking unwanted network traffic in Kubernetes
Traditional defence
Problem
Solution
Now make it dynamic
Example

- Presentation Tier
- Middle Tier
- Data Tier
kind: NetworkPolicy
metadata:
  name: presentation-policy
spec:
  podSelector:
    tier: presentation
  ingress:
    - ports:
      - protocol: tcp
        port: 80
Kubernetes NetworkPolicy

kind: NetworkPolicy
metadata:
  name: middle-tier-policy
spec:
podSelector:
  tier: middle
ingress:
- from:
  - podSelector:
    matchLabels:
      tier: presentation
So how do we implement this?

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipset</td>
<td>Import from weave-npc repo</td>
<td>3 months ago</td>
</tr>
<tr>
<td>metrics</td>
<td>Change rest of npc to weave common logging</td>
<td>2 months ago</td>
</tr>
<tr>
<td>ulogd</td>
<td>SIGKILL ulogd on weave-npc exit</td>
<td>22 days ago</td>
</tr>
<tr>
<td>analyser.go</td>
<td>Import from weave-npc repo</td>
<td>3 months ago</td>
</tr>
<tr>
<td>betatypes.go</td>
<td>Import from weave-npc repo</td>
<td>3 months ago</td>
</tr>
<tr>
<td>constants.go</td>
<td>Import from weave-npc repo</td>
<td>3 months ago</td>
</tr>
<tr>
<td>controller.go</td>
<td>Change to weave common logging</td>
<td>2 months ago</td>
</tr>
<tr>
<td>json.go</td>
<td>Log objects via JSON for better debugging</td>
<td>2 months ago</td>
</tr>
<tr>
<td>namespace.go</td>
<td>fix a bug of updating network policy</td>
<td>a month ago</td>
</tr>
<tr>
<td>rule.go</td>
<td>Change to weave common logging</td>
<td>2 months ago</td>
</tr>
<tr>
<td>selector.go</td>
<td>Change to weave common logging</td>
<td>2 months ago</td>
</tr>
<tr>
<td>hostname.go</td>
<td>Import from weave-npc repo</td>
<td>3 months ago</td>
</tr>
</tbody>
</table>
Controller

Kubernetes Master

watch on policies, pods

host1
weave-npc
iptables

host2
weave-npc
iptables
Top-level iptables rules

FORWARD chain:
- o weave -j WEAVE-NPC
- o weave -j DROP

WEAVE_NPC chain:
- m state --state RELATED,ESTABLISHED -j ACCEPT
- m state --state NEW -j WEAVE-NPC-DEFAULT
- m state --state NEW -j WEAVE-NPC-INGRESS
Overall flow

src → bridge → iptables

weave-npc

ipset

dst
Per-policy iptables rules

WEAVE-NPC-DEFAULT chain:

- m set --match-set weave-v/q_G.;Q?uK]BuDs2 dst -j ACCEPT
- m set --match-set weave-k?Z;25^M}|1s7P3|H dst -j ACCEPT

WEAVE-NPC-INGRESS chain:

- m set --match-set weave-LuMDZrBg:KsT9X11[ src
- m set --match-set weave-hR9K[Olp~d>@1wQu/ dst -j ACCEPT
- m set --match-set weave-hR9K[Olp~d>@1wQu/ src
- m set --match-set weave-hR9K[Olp~d>@1wQu/ dst -j ACCEPT

...
What could possibly go wrong?

Back in the FORWARD chain:

```
-o weave -m state --state NEW -j NFLOG --nflog-group 86
```

We subscribe to this via `ulogd` so we can print:

```
TCP connection from 10.32.0.7:56648 to 10.32.0.11:80 blocked by Weave NPC.
```

Also exported as a Prometheus metric
Interested?

Try it out!

https://weave.works/securing-microservices-kubernetes/

Take a look at the code!

https://github.com/weaveworks/weave/

Visualize, manage and monitor containers and services

https://cloud.weave.works
Fin
3-tier Illustration

- **Presentation**
  - :80
- **Middle tier**
  - :6379
- **Redis**
  - :6379