Policy-as-code on-premise with Bamboo Firewall

GHTK

OpenInfra DAYS

VIETNAM

About me

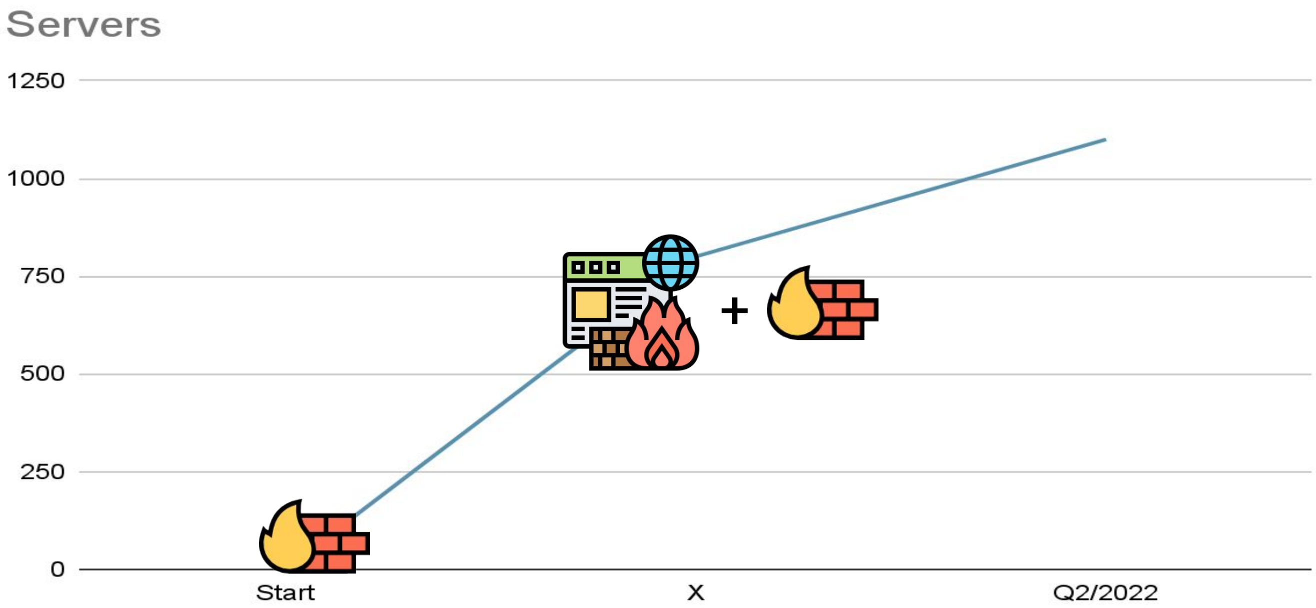
- Name: Trịnh Đình Biên
- Website: bienkma.github.io
- Linkedin: linkedin.com/in/bienkma
- Role: Head of Infrastructure at GHTK

Agenda

- Bamboo Firewall: What, Why?
- Architecture of Bamboo Firewall
- GHTK use case
- Q&A

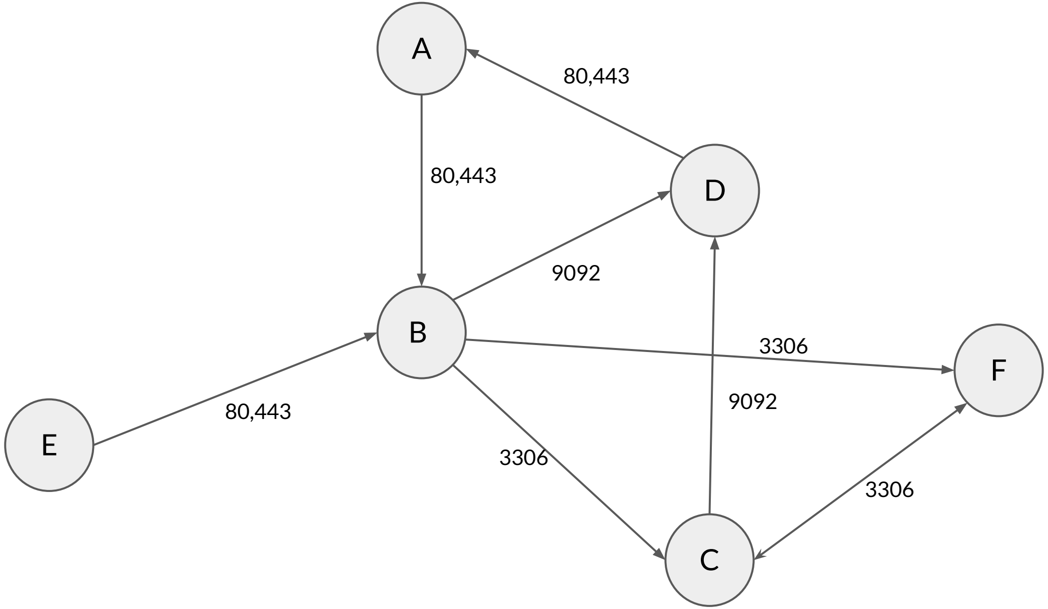
Bamboo Firewall: What, Why?

Bamboo Firewall: What, Why?



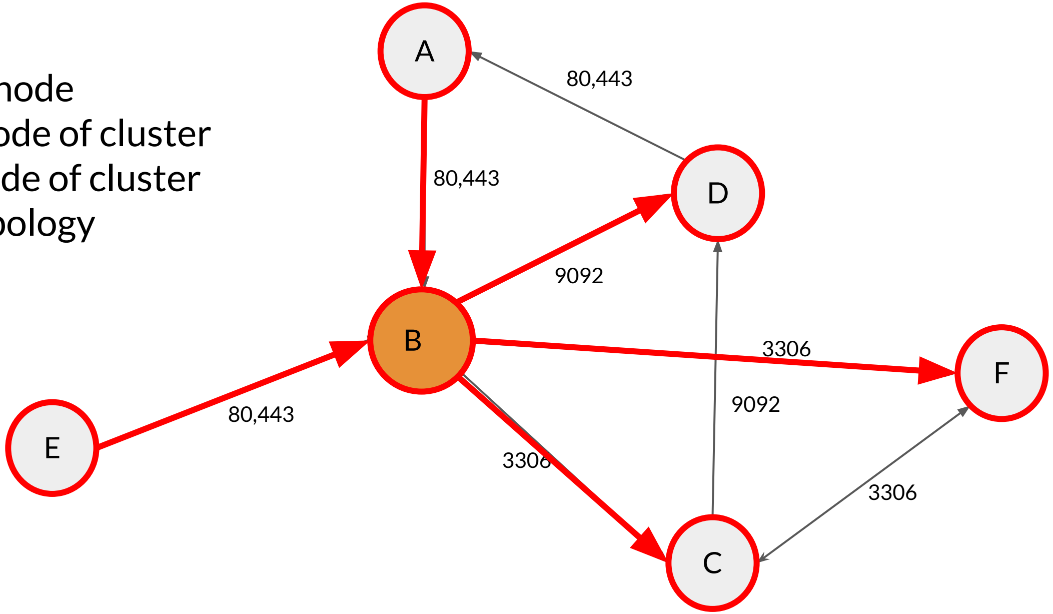
Iptables → Iptables
Hardware Firewall

Bamboo Firewall: What, Why?



Bamboo Firewall: What, Why?

- Change IP node
- Add new node of cluster
- Remove node of cluster
- Change topology



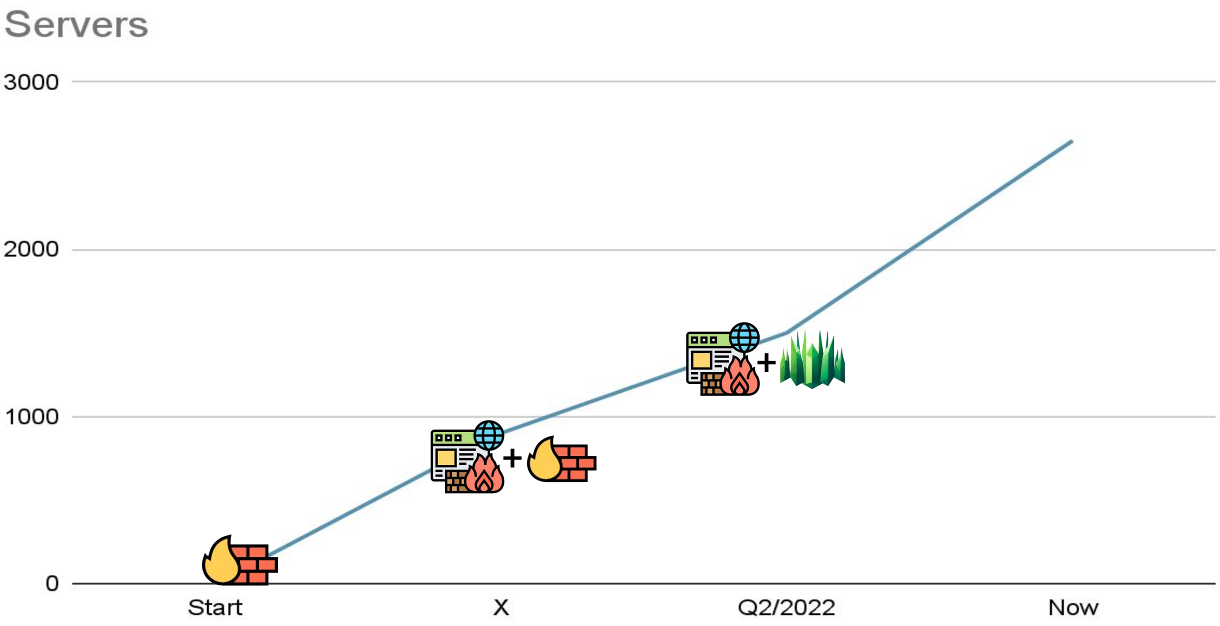
Bamboo Firewall: What, Why?

- Simple
- Fast & Flexible
- Version control policy
- Reusable
- Management central
- Distributed Firewall
- Low cost
- PaC/IaC (basically, as-code)

GHTK

OpenInfra DAYS VIETNAM

Bamboo Firewall: What, Why?



Iptables → Iptables
Hardware Firewall → Bamboo Firewall
Hardware Firewall → Bamboo Firewall
Hardware Firewall

Bamboo Firewall: What, Why?

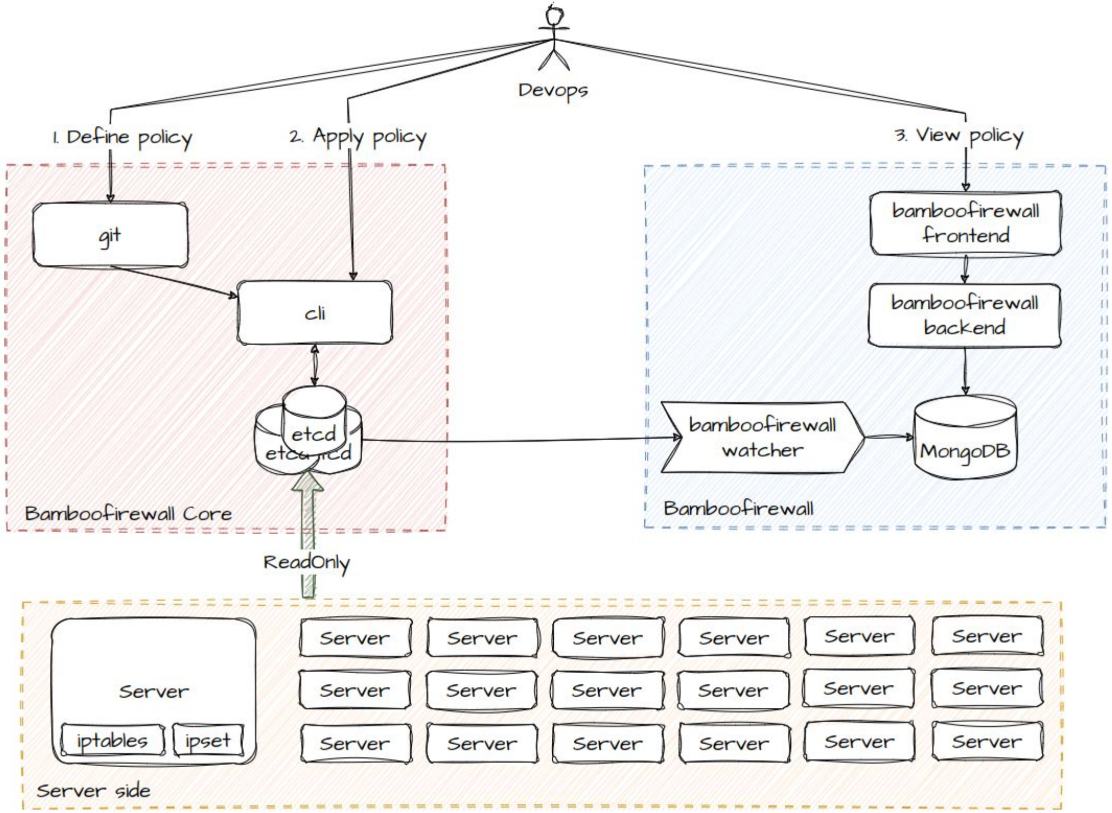
- Bamboo Firewall is a distributed firewall and a soft firewall, Stateful firewall
- Focus on servers on-premise
- Based on Calico Felix
- Policy-As-Code (PaC/IaC)

Architecture of Bamboo Firewall

GHTK

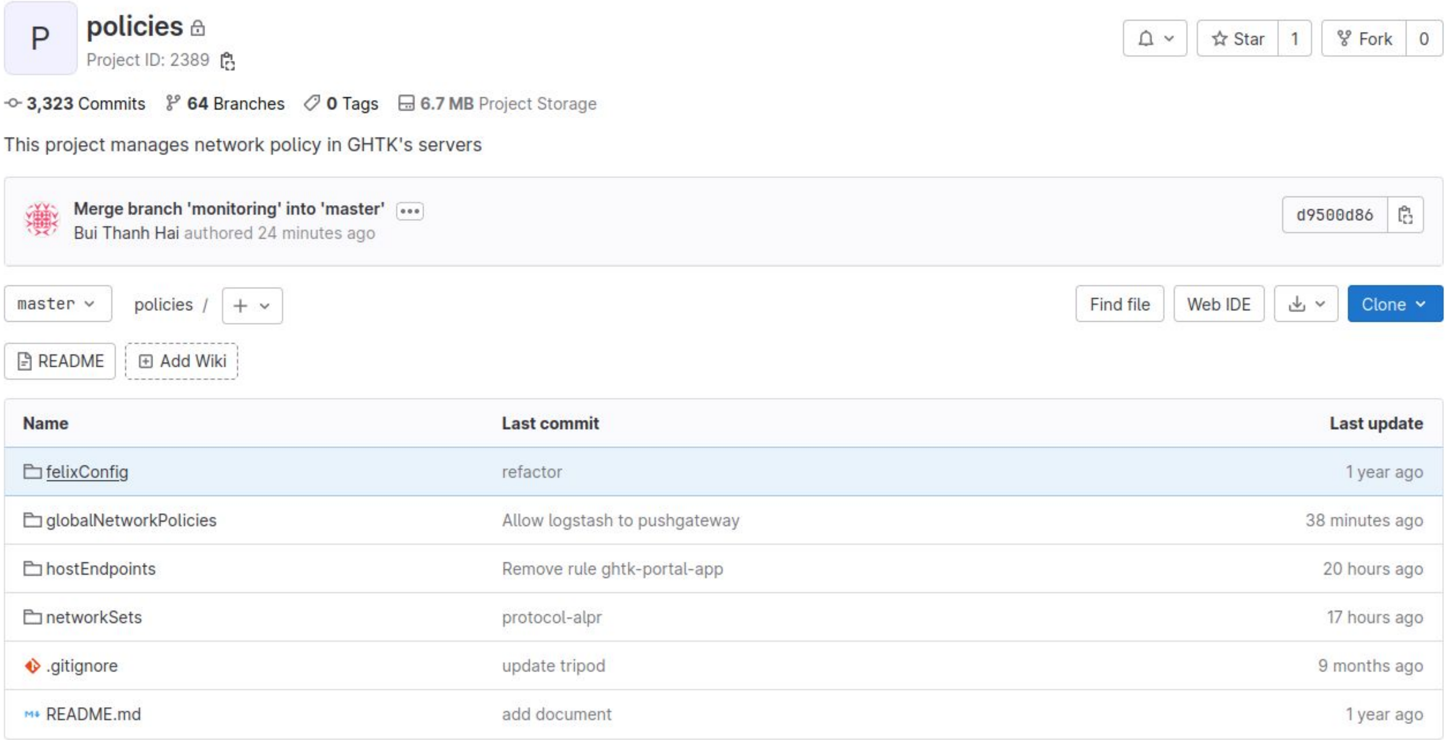
OpenInfra DAYS VIETNAM

Architecture



GHTK Use case

Bamboo Firewall: PaC-VersionControl



P policies

Project ID: 2389

3,323 Commits 64 Branches 0 Tags 6.7 MB Project Storage

This project manages network policy in GHTK's servers

Merge branch 'monitoring' into 'master'

Bui Thanh Hai authored 24 minutes ago

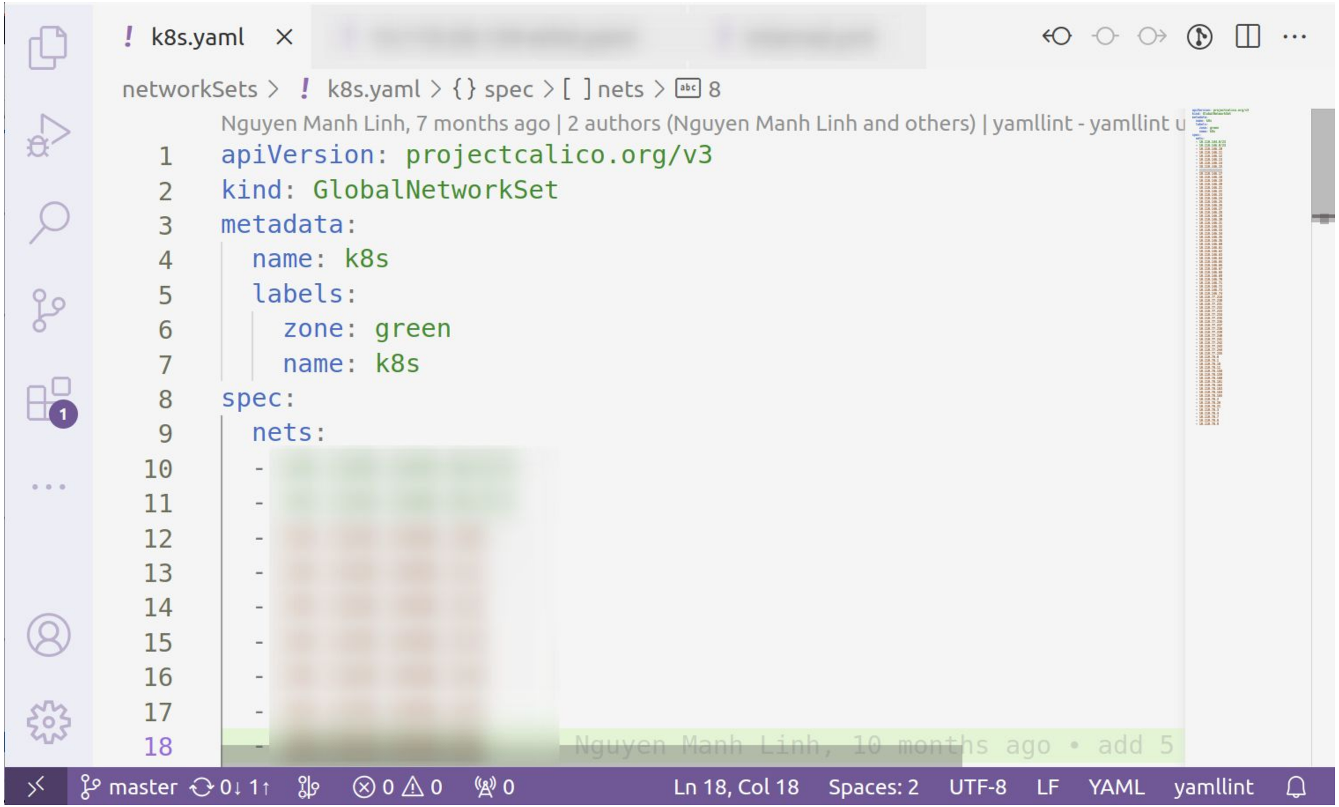
d9500d86

Name	Last commit	Last update
felixConfig	refactor	1 year ago
globalNetworkPolicies	Allow logstash to pushgateway	38 minutes ago
hostEndpoints	Remove rule ghtk-portal-app	20 hours ago
networkSets	protocol-alpr	17 hours ago
.gitignore	update tripod	9 months ago
README.md	add document	1 year ago

GHTK

OpenInfra DAYS VIETNAM

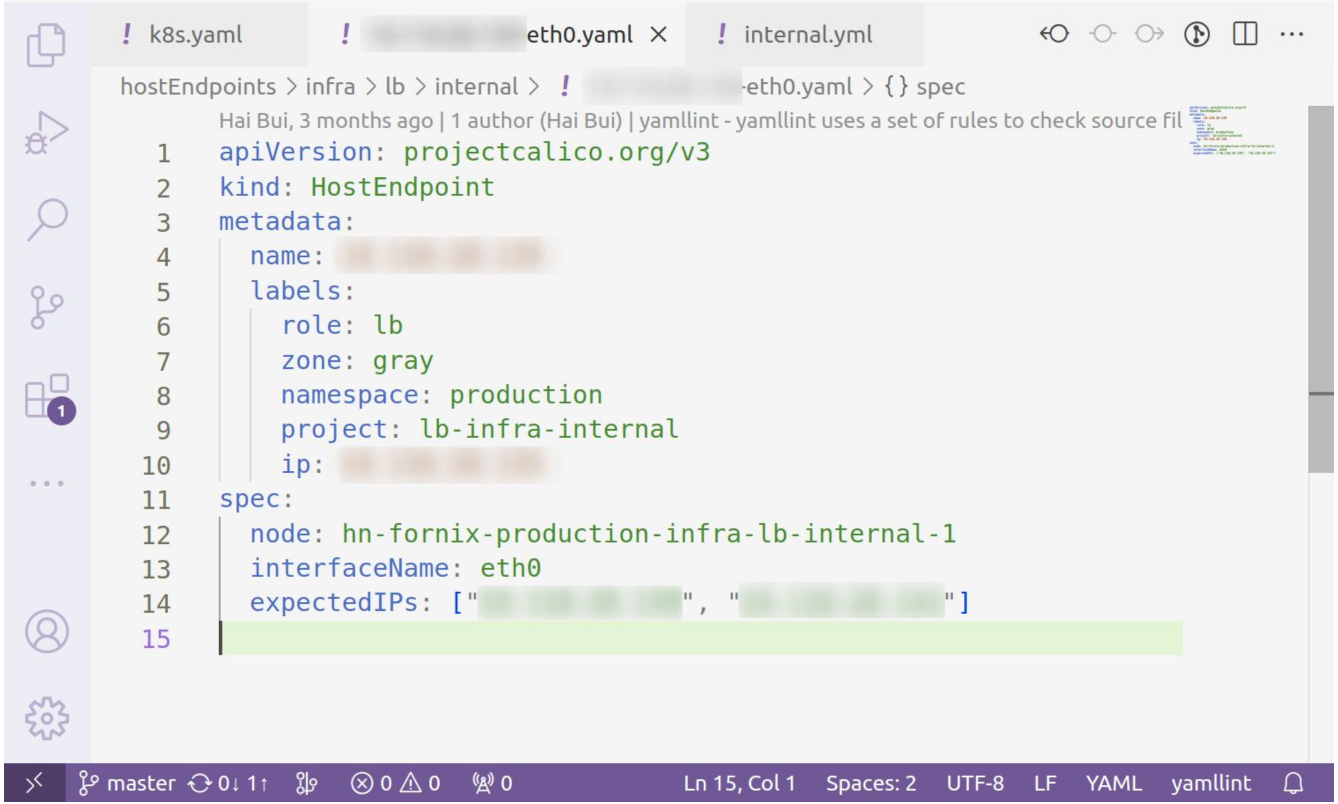
Bamboo Firewall: PaC-GlobalNetworkSet



Nguyen Manh Linh, 7 months ago | 2 authors (Nguyen Manh Linh and others) | yamllint - yamllint u

```yaml
apiVersion: projectcalico.org/v3
kind: GlobalNetworkSet
metadata:
  name: k8s
  labels:
    zone: green
    name: k8s
spec:
  nets:
  - [redacted]
  -
  -
  -
  -
  -
  -
  -
  -                Nguyen Manh Linh, 10 months ago • add 5
```

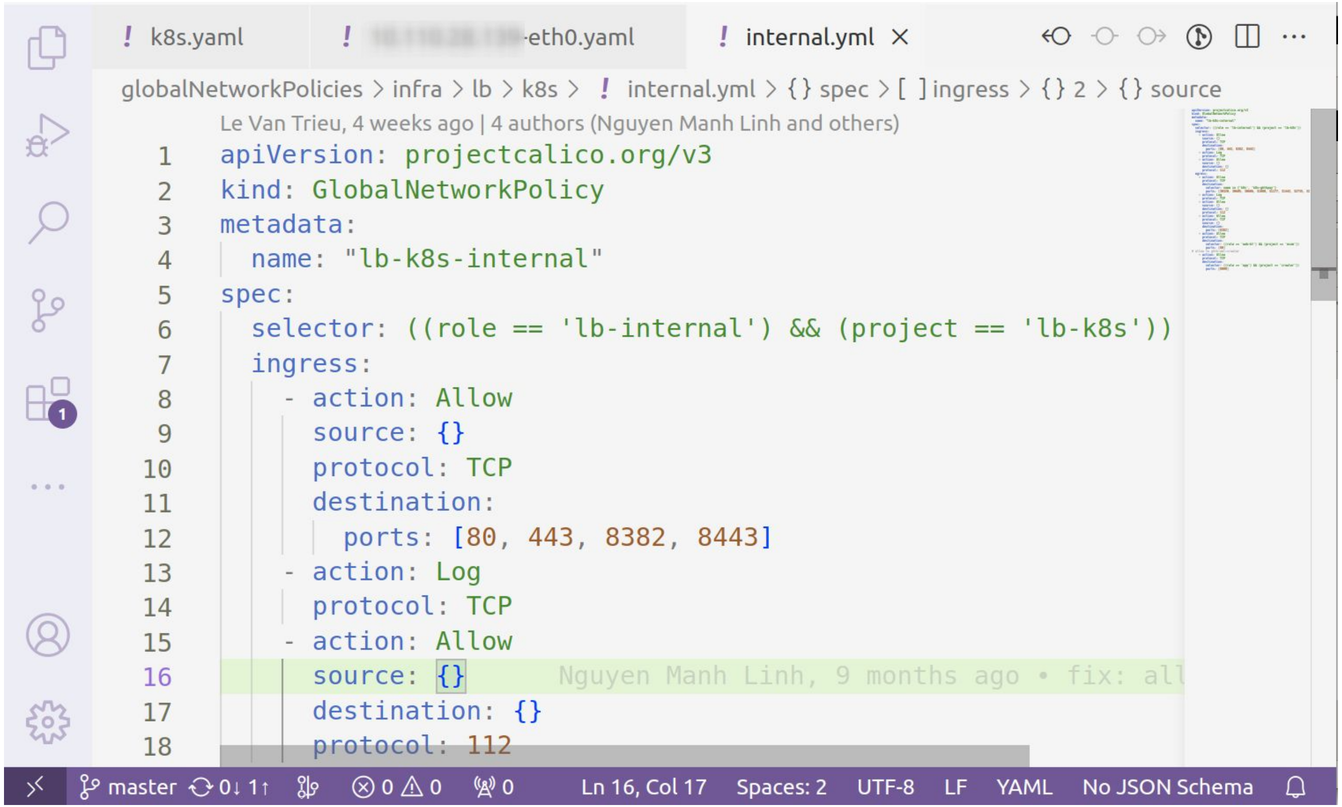
Bamboo Firewall: PaC-HostEndpoint


! k8s.yaml
! [redacted]eth0.yaml ×
! internal.yml
hostEndpoints > infra > lb > internal > ! [redacted]-eth0.yaml > { } spec
Hai Bui, 3 months ago | 1 author (Hai Bui) | yamllint - yamllint uses a set of rules to check source fil

```yaml
apiVersion: projectcalico.org/v3
kind: HostEndpoint
metadata:
  name: [redacted]
  labels:
    role: lb
    zone: gray
    namespace: production
    project: lb-infra-internal
    ip: [redacted]
spec:
  node: hn-fornix-production-infra-lb-internal-1
  interfaceName: eth0
  expectedIPs: ["[redacted]", "[redacted]"]

```

master 0↓ 1↑
⊗ 0 ⚠ 0
0
Ln 15, Col 1
Spaces: 2
UTF-8
LF
YAML
yamllint

Bamboo Firewall: PaC-GlobalNetworkPolicy



Le Van Trieu, 4 weeks ago | 4 authors (Nguyen Manh Linh and others)

```yaml
apiVersion: projectcalico.org/v3
kind: GlobalNetworkPolicy
metadata:
  name: "lb-k8s-internal"
spec:
  selector: ((role == 'lb-internal') && (project == 'lb-k8s'))
  ingress:
    - action: Allow
      source: {}
      protocol: TCP
      destination:
        ports: [80, 443, 8382, 8443]
    - action: Log
      protocol: TCP
    - action: Allow
      source: {}      Nguyen Manh Linh, 9 months ago • fix: all
      destination: {}
      protocol: 112
```

Bamboo Firewall: PaC-Apply Policy

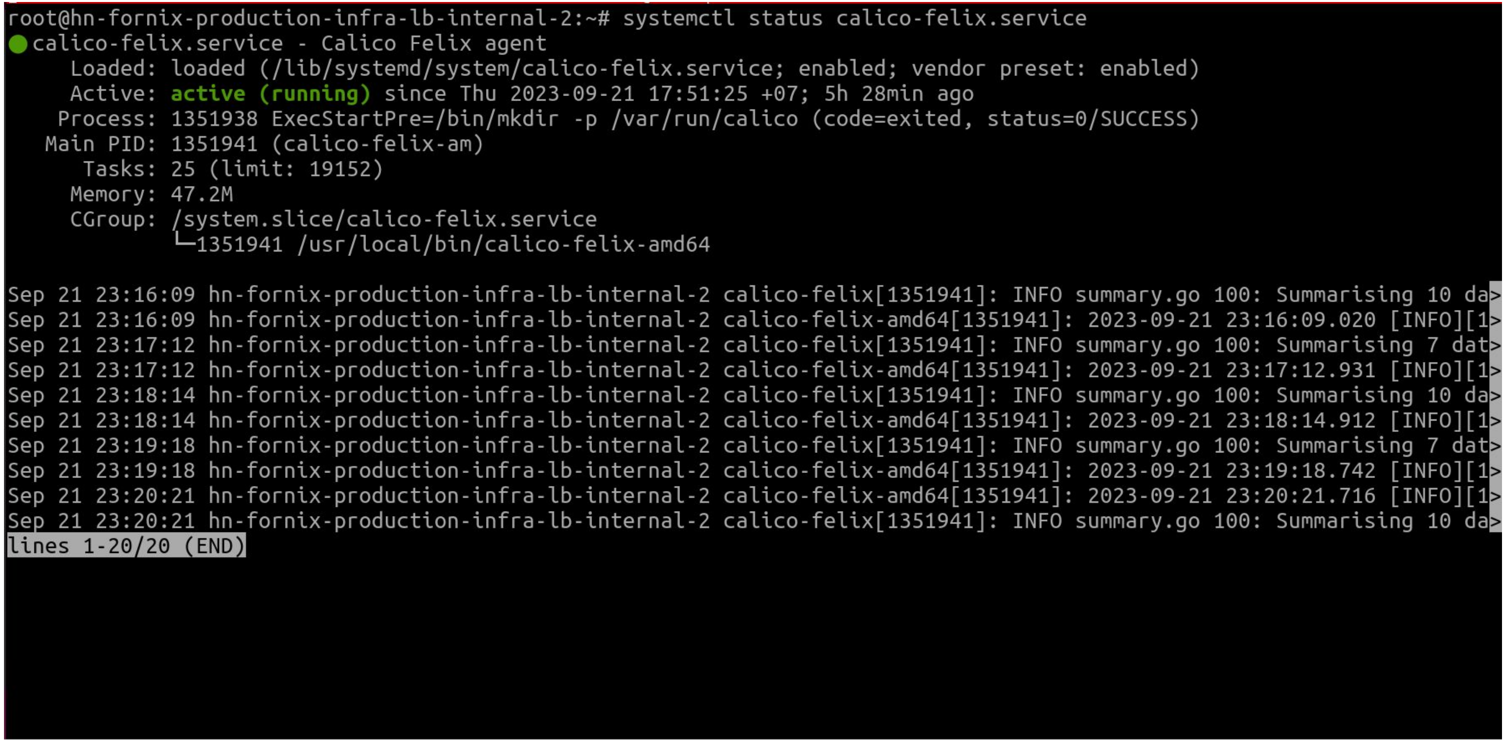
Apply policy

```
git clone https://git.example.com/devops/bamboofirewall-policies
cd bamboofirewall-policies
calicoctl apply -f networkSets/k8s.yaml
calicoctl apply -f hostEndpoints/192.168.1.100-eth0.yaml
calicoctl apply -f globalNetworkPolicies/lb.yaml
```

View policy/hep/gns by cli

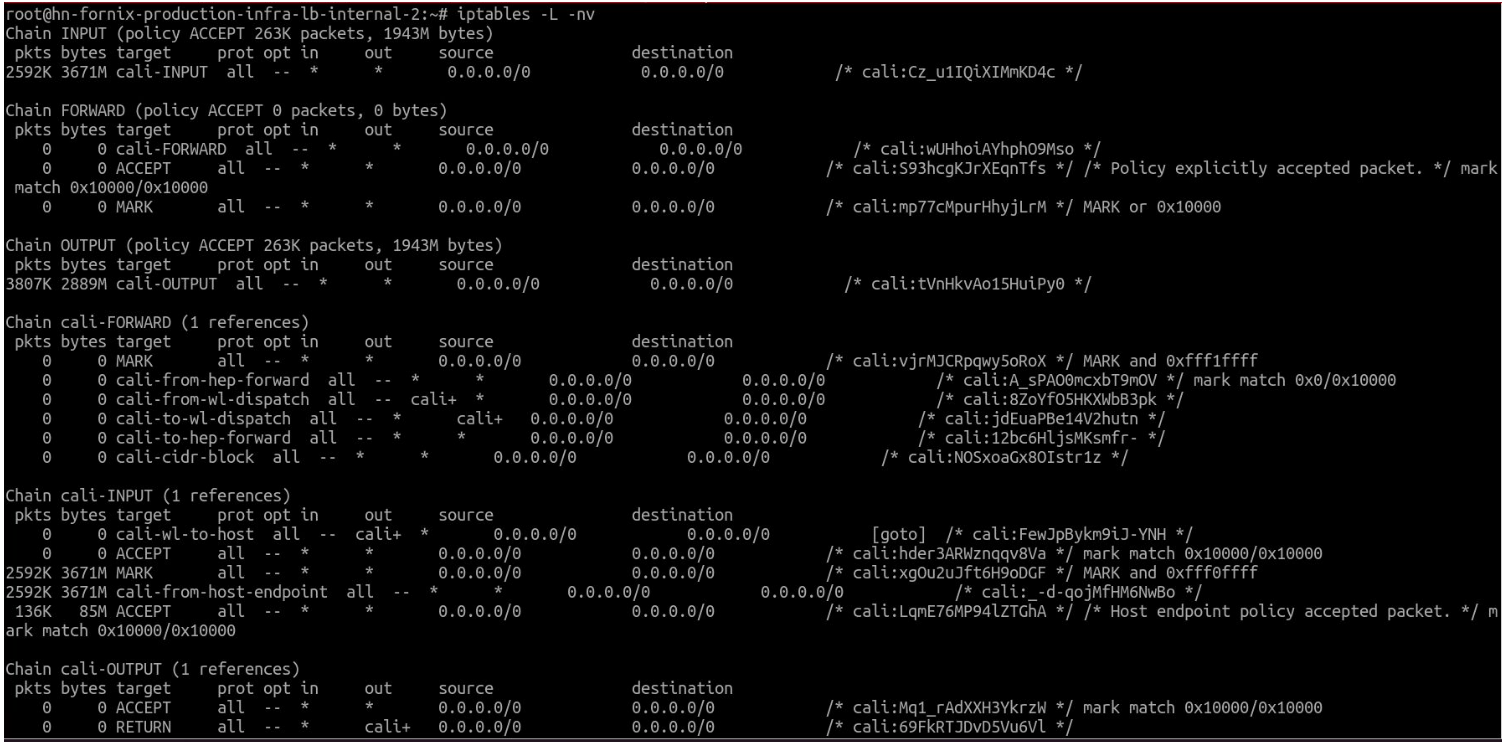
```
calicoctl get hep 192.168.1.100 -o wide
calicoctl get globalnetworkpolicy lb -o yaml
calicoctl get globalnetworkset k8s -o yaml
```

Bamboo Firewall: Client



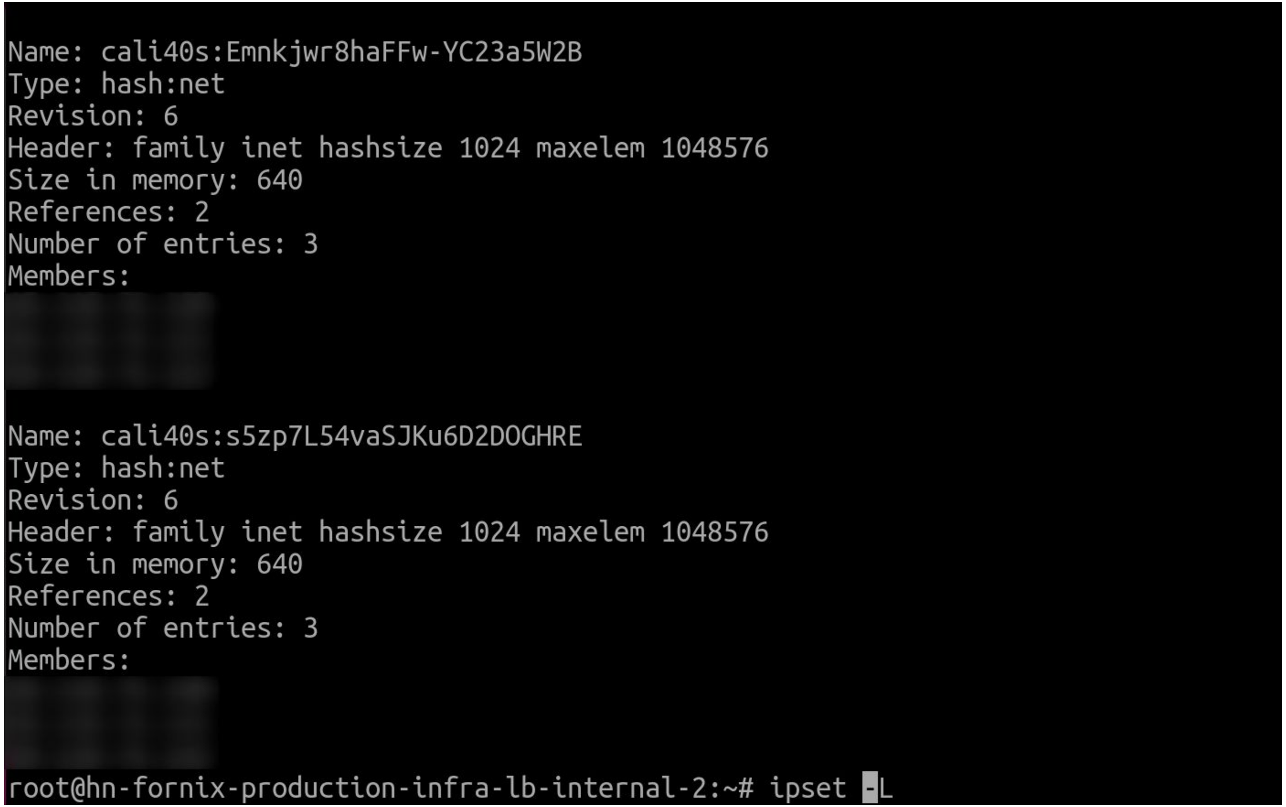
```
root@hn-fornix-production-infra-lb-internal-2:~# systemctl status calico-felix.service
● calico-felix.service - Calico Felix agent
     Loaded: loaded (/lib/systemd/system/calico-felix.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2023-09-21 17:51:25 +07; 5h 28min ago
    Process: 1351938 ExecStartPre=/bin/mkdir -p /var/run/calico (code=exited, status=0/SUCCESS)
   Main PID: 1351941 (calico-felix-am)
      Tasks: 25 (limit: 19152)
     Memory: 47.2M
     CGroup: /system.slice/calico-felix.service
             └─1351941 /usr/local/bin/calico-felix-amd64

Sep 21 23:16:09 hn-fornix-production-infra-lb-internal-2 calico-felix[1351941]: INFO summary.go 100: Summarising 10 da>
Sep 21 23:16:09 hn-fornix-production-infra-lb-internal-2 calico-felix-amd64[1351941]: 2023-09-21 23:16:09.020 [INFO][1>
Sep 21 23:17:12 hn-fornix-production-infra-lb-internal-2 calico-felix[1351941]: INFO summary.go 100: Summarising 7 dat>
Sep 21 23:17:12 hn-fornix-production-infra-lb-internal-2 calico-felix-amd64[1351941]: 2023-09-21 23:17:12.931 [INFO][1>
Sep 21 23:18:14 hn-fornix-production-infra-lb-internal-2 calico-felix[1351941]: INFO summary.go 100: Summarising 10 da>
Sep 21 23:18:14 hn-fornix-production-infra-lb-internal-2 calico-felix-amd64[1351941]: 2023-09-21 23:18:14.912 [INFO][1>
Sep 21 23:19:18 hn-fornix-production-infra-lb-internal-2 calico-felix[1351941]: INFO summary.go 100: Summarising 7 dat>
Sep 21 23:19:18 hn-fornix-production-infra-lb-internal-2 calico-felix-amd64[1351941]: 2023-09-21 23:19:18.742 [INFO][1>
Sep 21 23:20:21 hn-fornix-production-infra-lb-internal-2 calico-felix-amd64[1351941]: 2023-09-21 23:20:21.716 [INFO][1>
Sep 21 23:20:21 hn-fornix-production-infra-lb-internal-2 calico-felix[1351941]: INFO summary.go 100: Summarising 10 da>
lines 1-20/20 (END)
```

Bamboo Firewall: Client



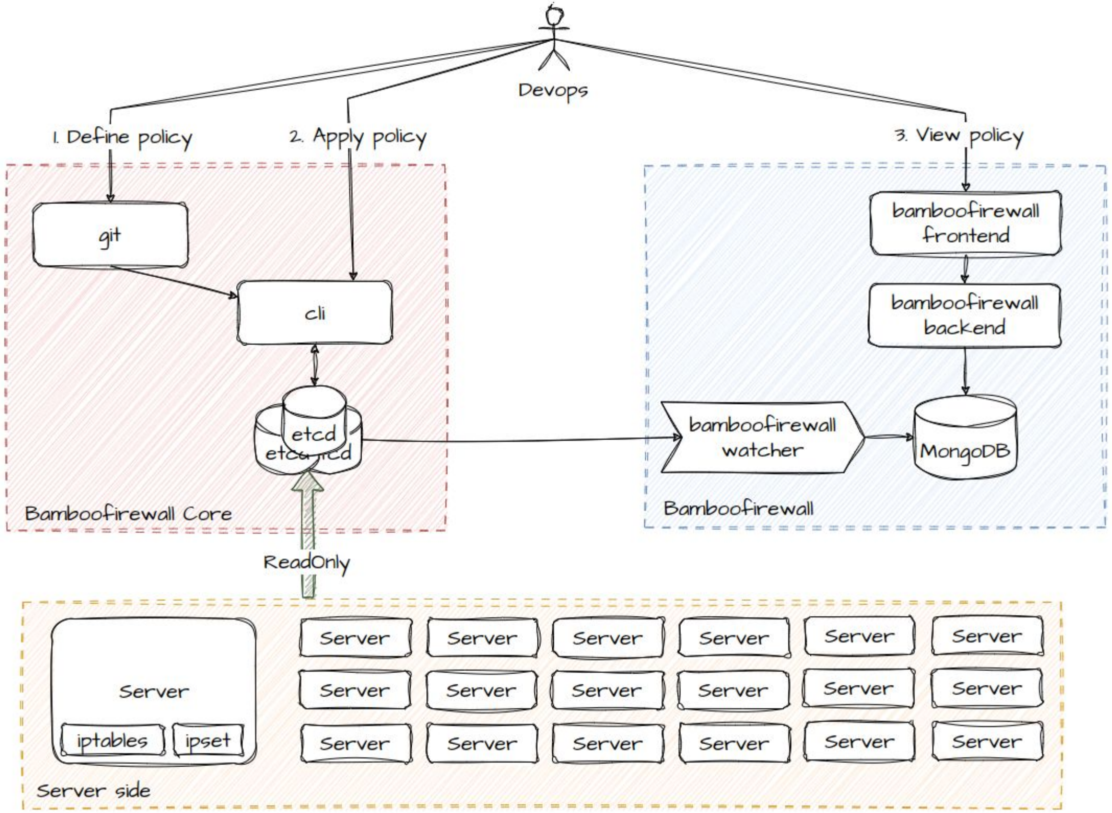
```
root@hn-fornix-production-infra-lb-internal-2:~# iptables -L -nv
Chain INPUT (policy ACCEPT 263K packets, 1943M bytes)
 pkts bytes target     prot opt in     out     source               destination
2592K 3671M cali-INPUT  all  --  *      *       0.0.0.0/0            0.0.0.0/0            /* cali:Cz_u1IQiXIMmKD4c */

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 cali-FORWARD  all  --  *      *       0.0.0.0/0            0.0.0.0/0            /* cali:wUHhoiAYhphO9Mso */
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            /* cali:S93hcgKJrXEqnTfs */ /* Policy explicitly accepted packet. */ mark
 match 0x10000/0x10000
    0     0 MARK       all  --  *      *       0.0.0.0/0            0.0.0.0/0            /* cali:mp77cMpurHhyjLrM */ MARK or 0x10000

Chain OUTPUT (policy ACCEPT 263K packets, 1943M bytes)
 pkts bytes target     prot opt in     out     source               destination
3807K 2889M cali-OUTPUT  all  --  *      *       0.0.0.0/0            0.0.0.0/0            /* cali:tVnHkvAo15HuiPy0 */

Chain cali-FORWARD (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 MARK       all  --  *      *       0.0.0.0/0            0.0.0.0/0            /* cali:vjrMJCRpqwy5oRoX */ MARK and 0xfff1ffff
    0     0 cali-from-hep-forward  all  --  *      *       0.0.0.0/0            0.0.0.0/0            /* cali:A_sPAO0mcxbT9mOV */ mark match 0x0/0x10000
    0     0 cali-from-wl-dispatch  all  --  cali+  *       0.0.0.0/0            0.0.0.0/0            /* cali:8ZoYfO5HKXWbB3pk */
    0     0 cali-to-wl-dispatch  all  --  *      cali+  0.0.0.0/0            0.0.0.0/0            /* cali:jdEuaPBe14V2hutn */
    0     0 cali-to-hep-forward  all  --  *      *       0.0.0.0/0            0.0.0.0/0            /* cali:12bc6HljsMKsmfr- */
    0     0 cali-cidr-block  all  --  *      *       0.0.0.0/0            0.0.0.0/0            /* cali:NOSxoaGx8OIstr1z */

Chain cali-INPUT (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 cali-wl-to-host  all  --  cali+  *       0.0.0.0/0            0.0.0.0/0           [goto]  /* cali:FewJpBykm9iJ-YNH */
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            /* cali:hder3ARWznqqv8Va */ mark match 0x10000/0x10000
2592K 3671M MARK       all  --  *      *       0.0.0.0/0            0.0.0.0/0            /* cali:xgOu2uJft6H9oDGF */ MARK and 0xfff0ffff
2592K 3671M cali-from-host-endpoint  all  --  *      *       0.0.0.0/0            0.0.0.0/0            /* cali:_-d-qojMfHM6NwBo */
 136K   85M ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            /* cali:LqmE76MP94lZTGhA */ /* Host endpoint policy accepted packet. */ m
ark match 0x10000/0x10000

Chain cali-OUTPUT (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            /* cali:Mq1_rAdXXH3YkrzW */ mark match 0x10000/0x10000
    0     0 RETURN     all  --  *      cali+   0.0.0.0/0            0.0.0.0/0            /* cali:69FkRTJDvD5Vu6Vl */
```

Bamboo Firewall: Client



```
Name: cali40s:Emnkjwr8haFFw-YC23a5W2B
Type: hash:net
Revision: 6
Header: family inet hashsize 1024 maxelem 1048576
Size in memory: 640
References: 2
Number of entries: 3
Members:
[redacted]

Name: cali40s:s5zp7L54vaSJKu6D2DOGHRE
Type: hash:net
Revision: 6
Header: family inet hashsize 1024 maxelem 1048576
Size in memory: 640
References: 2
Number of entries: 3
Members:
[redacted]
root@hn-fornix-production-infra-lb-internal-2:~# ipset -L
```

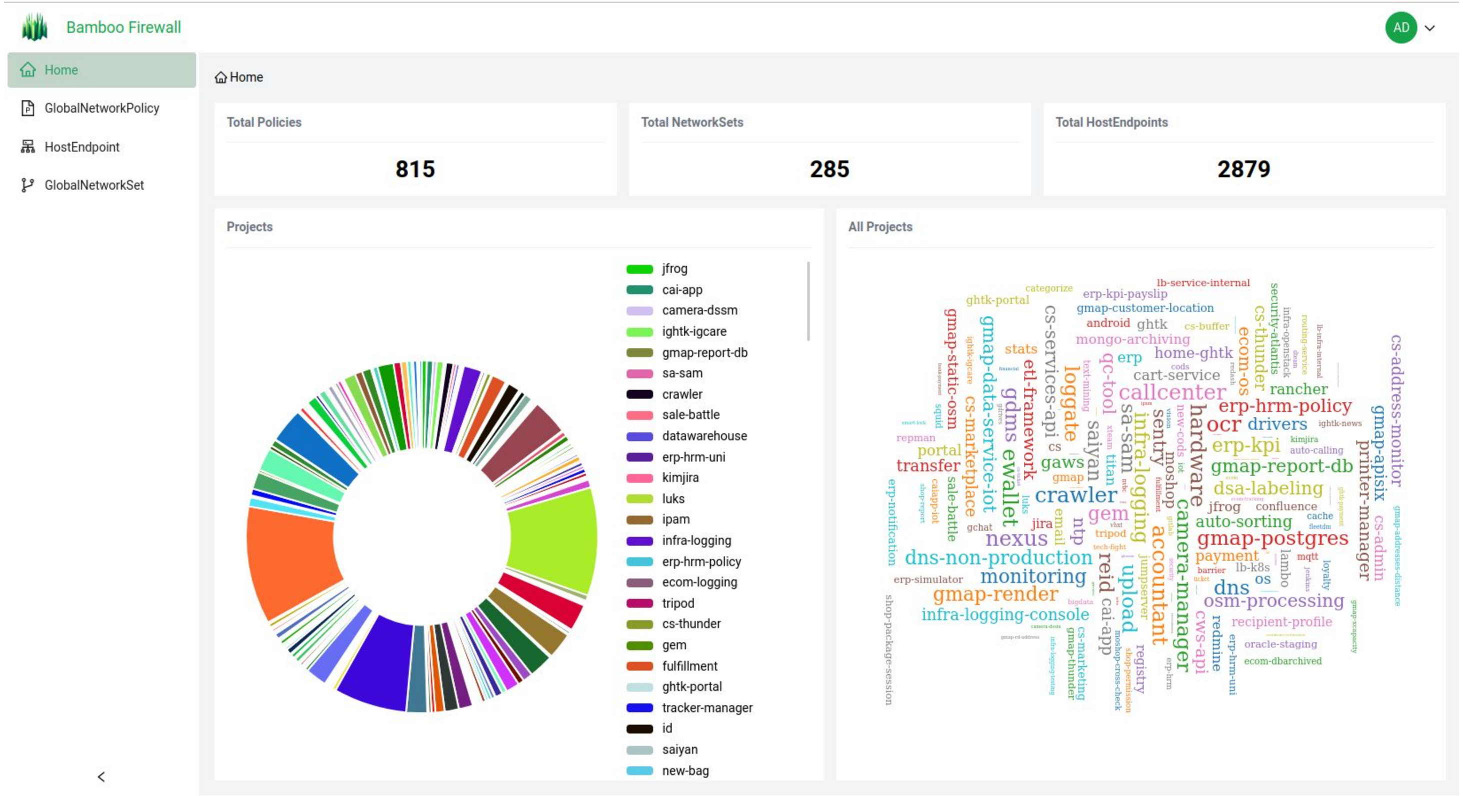
Architecture



GHTK

OpenInfra DAYS VIETNAM

Bamboo Firewall: GUI-Overview



Bamboo Firewall

- Home
- GlobalNetworkPolicy
- HostEndpoint
- GlobalNetworkSet

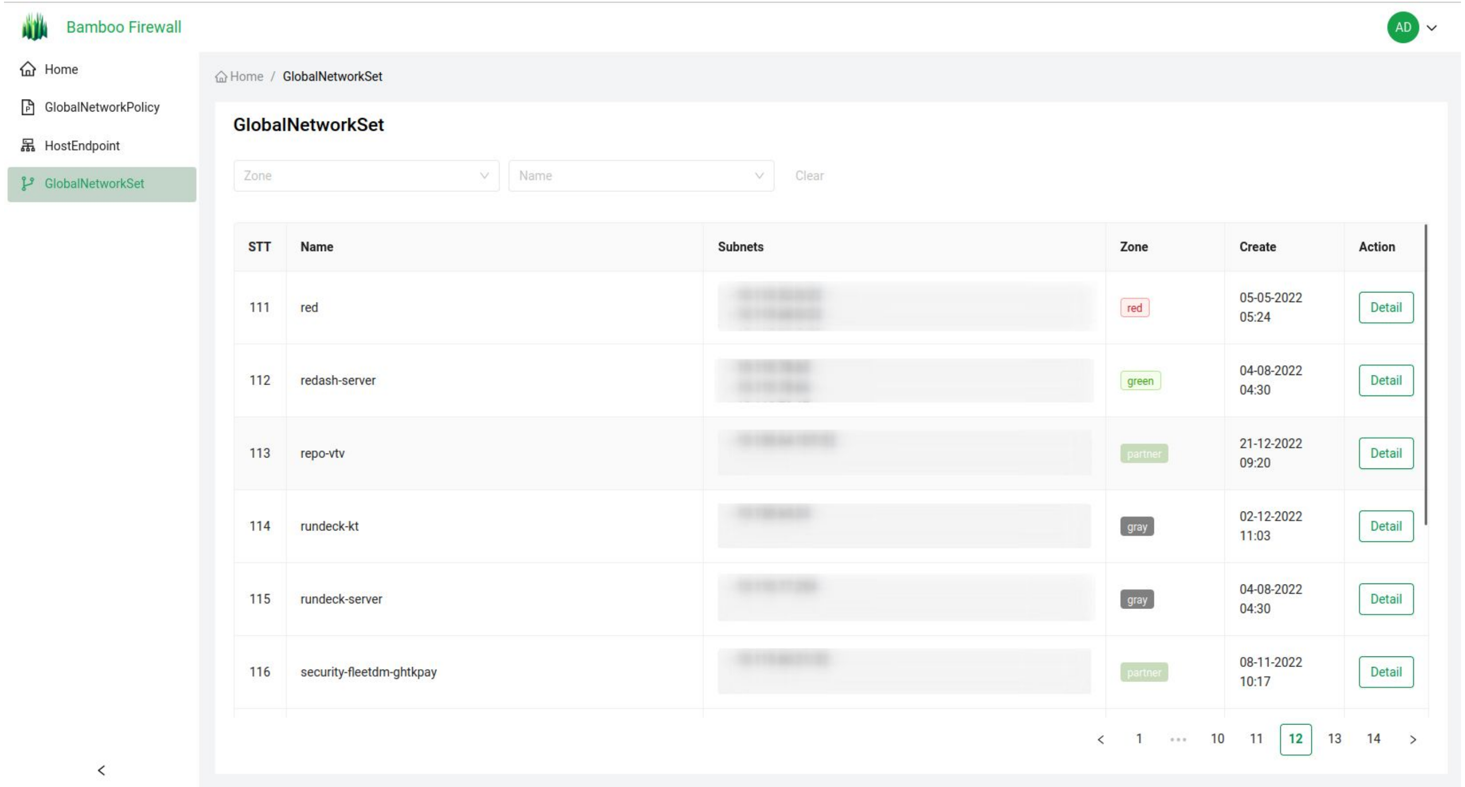
Home

Total Policies: 815

Total NetworkSets: 285

Total HostEndpoints: 2879

Bamboo Firewall: GUI-GlobalNetworkSet



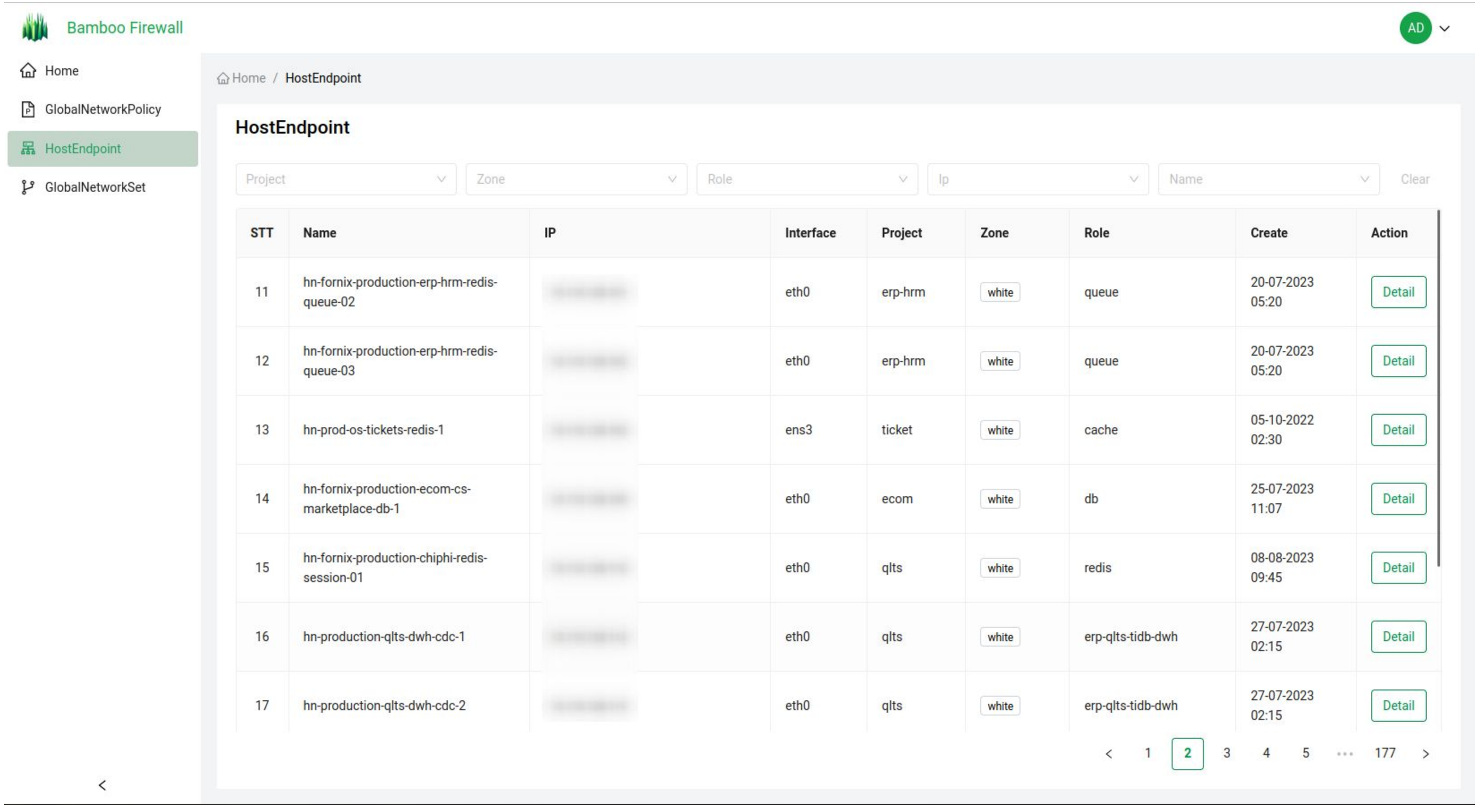
GlobalNetworkSet

STT	Name	Subnets	Zone	Create	Action
111	red	[redacted]	red	05-05-2022 05:24	Detail
112	redash-server	[redacted]	green	04-08-2022 04:30	Detail
113	repo-vtv	[redacted]	partner	21-12-2022 09:20	Detail
114	rundeck-kt	[redacted]	gray	02-12-2022 11:03	Detail
115	rundeck-server	[redacted]	gray	04-08-2022 04:30	Detail
116	security-fleetdm-ghtkpay	[redacted]	partner	08-11-2022 10:17	Detail

GHTK

OpenInfra DAYS VIETNAM

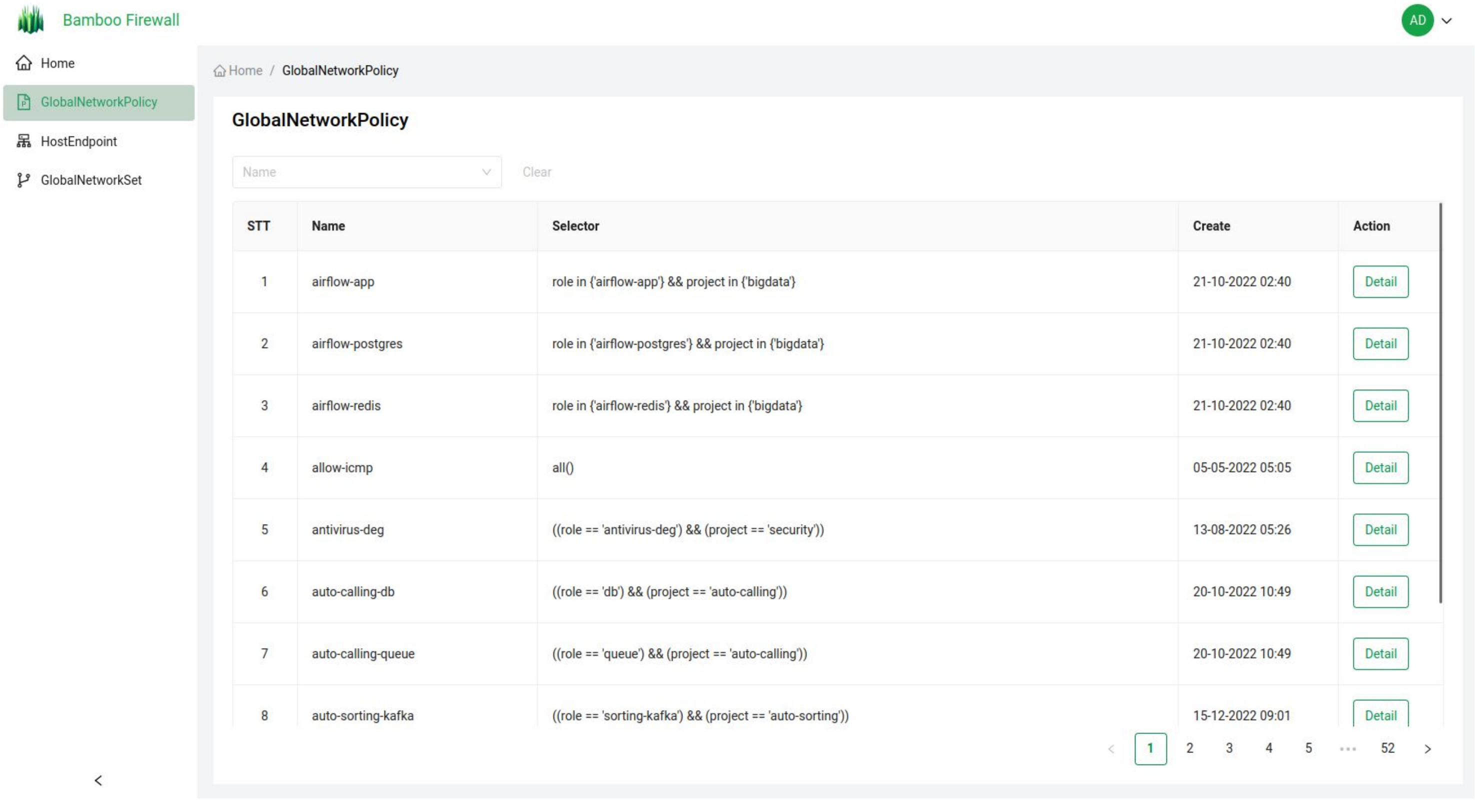
Bamboo Firewall: GUI-HostEndpoint



HostEndpoint

STT	Name	IP	Interface	Project	Zone	Role	Create	Action
11	hn-fornix-production-erp-hrm-redis-queue-02	[redacted]	eth0	erp-hrm	white	queue	20-07-2023 05:20	Detail
12	hn-fornix-production-erp-hrm-redis-queue-03	[redacted]	eth0	erp-hrm	white	queue	20-07-2023 05:20	Detail
13	hn-prod-os-tickets-redis-1	[redacted]	ens3	ticket	white	cache	05-10-2022 02:30	Detail
14	hn-fornix-production-ecom-cs-marketplace-db-1	[redacted]	eth0	ecom	white	db	25-07-2023 11:07	Detail
15	hn-fornix-production-chiphi-redis-session-01	[redacted]	eth0	qlts	white	redis	08-08-2023 09:45	Detail
16	hn-production-qlts-dwh-cdc-1	[redacted]	eth0	qlts	white	erp-qlts-tidb-dwh	27-07-2023 02:15	Detail
17	hn-production-qlts-dwh-cdc-2	[redacted]	eth0	qlts	white	erp-qlts-tidb-dwh	27-07-2023 02:15	Detail

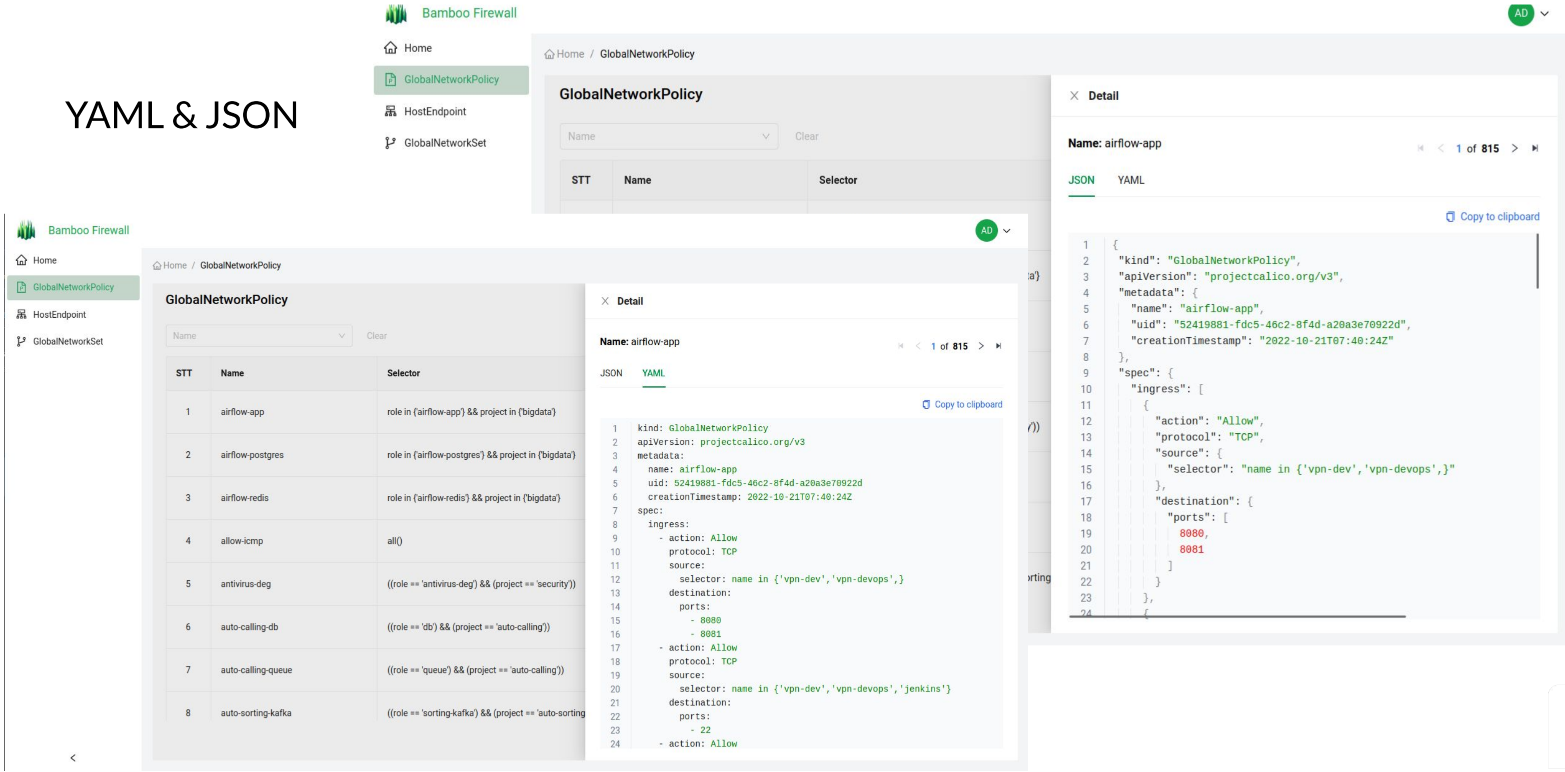
Bamboo Firewall: GUI-GlobalNetworkPolicy



STT	Name	Selector	Create	Action
1	airflow-app	role in {'airflow-app'} && project in {'bigdata'}	21-10-2022 02:40	Detail
2	airflow-postgres	role in {'airflow-postgres'} && project in {'bigdata'}	21-10-2022 02:40	Detail
3	airflow-redis	role in {'airflow-redis'} && project in {'bigdata'}	21-10-2022 02:40	Detail
4	allow-icmp	all()	05-05-2022 05:05	Detail
5	antivirus-deg	((role == 'antivirus-deg') && (project == 'security'))	13-08-2022 05:26	Detail
6	auto-calling-db	((role == 'db') && (project == 'auto-calling'))	20-10-2022 10:49	Detail
7	auto-calling-queue	((role == 'queue') && (project == 'auto-calling'))	20-10-2022 10:49	Detail
8	auto-sorting-kafka	((role == 'sorting-kafka') && (project == 'auto-sorting'))	15-12-2022 09:01	Detail

Bamboo Firewall: GUI-Details

YAML & JSON



Name: airflow-app   1 of 815

```
{
 "kind": "GlobalNetworkPolicy",
 "apiVersion": "projectcalico.org/v3",
 "metadata": {
   "name": "airflow-app",
   "uid": "52419881-fdc5-46c2-8f4d-a20a3e70922d",
   "creationTimestamp": "2022-10-21T07:40:24Z"
 },
 "spec": {
   "ingress": [
     {
       "action": "Allow",
       "protocol": "TCP",
       "source": {
         "selector": "name in {'vpn-dev','vpn-devops',}"
       },
       "destination": {
         "ports": [
           8080,
           8081
         ]
       }
     },
     {
```

STT	Name	Selector
1	airflow-app	role in {'airflow-app'} && project in {'bigdata'}
2	airflow-postgres	role in {'airflow-postgres'} && project in {'bigdata'}
3	airflow-redis	role in {'airflow-redis'} && project in {'bigdata'}
4	allow-icmp	all()
5	antivirus-deg	((role == 'antivirus-deg') && (project == 'security'))
6	auto-calling-db	((role == 'db') && (project == 'auto-calling'))
7	auto-calling-queue	((role == 'queue') && (project == 'auto-calling'))
8	auto-sorting-kafka	((role == 'sorting-kafka') && (project == 'auto-sorting

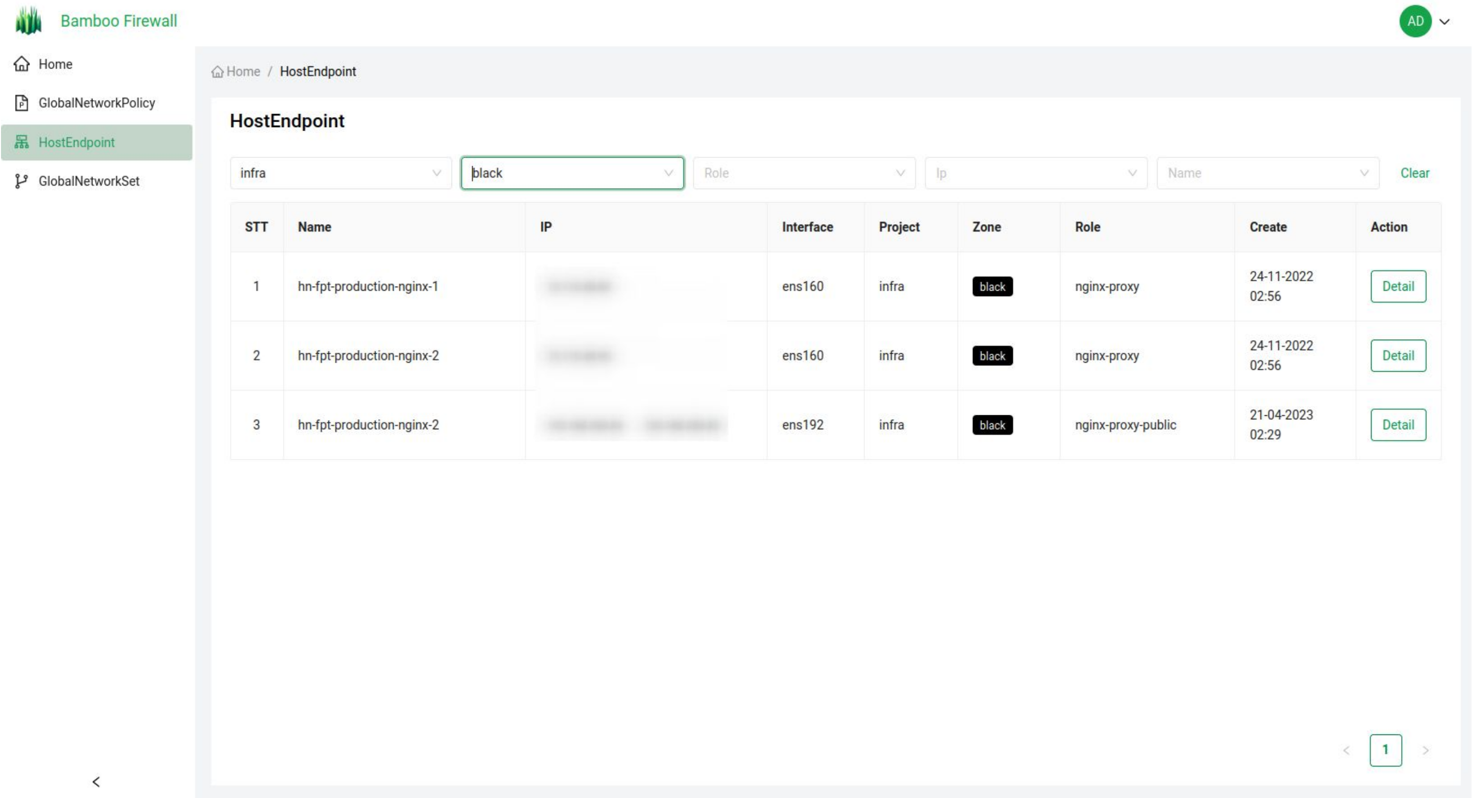
Name: airflow-app   1 of 815

```
kind: GlobalNetworkPolicy
apiVersion: projectcalico.org/v3
metadata:
  name: airflow-app
  uid: 52419881-fdc5-46c2-8f4d-a20a3e70922d
  creationTimestamp: 2022-10-21T07:40:24Z
spec:
  ingress:
    - action: Allow
      protocol: TCP
      source:
        selector: name in {'vpn-dev','vpn-devops',}
      destination:
        ports:
          - 8080
          - 8081
    - action: Allow
      protocol: TCP
      source:
        selector: name in {'vpn-dev','vpn-devops','jenkins'}
      destination:
        ports:
          - 22
    - action: Allow
```

GHTK

OpenInfra DAYS VIETNAM

Bamboo Firewall: GUI-Filter



HostEndpoint

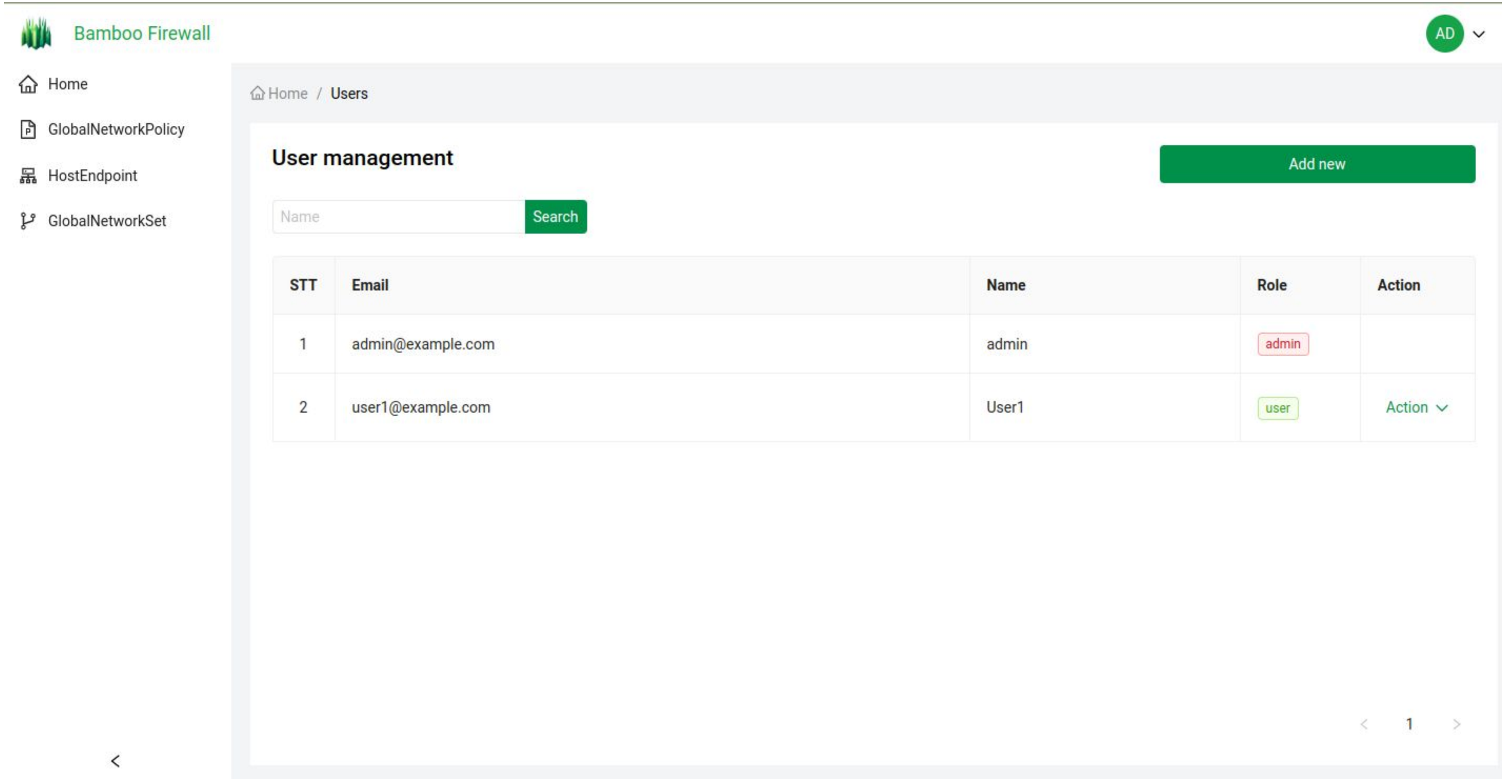
infra | black | Role | Ip | Name | Clear

STT	Name	IP	Interface	Project	Zone	Role	Create	Action
1	hn-fpt-production-nginx-1	[redacted]	ens160	infra	black	nginx-proxy	24-11-2022 02:56	Detail
2	hn-fpt-production-nginx-2	[redacted]	ens160	infra	black	nginx-proxy	24-11-2022 02:56	Detail
3	hn-fpt-production-nginx-2	[redacted]	ens192	infra	black	nginx-proxy-public	21-04-2023 02:29	Detail

GHTK

OpenInfra DAYS VIETNAM

Bamboo Firewall: GUI-RBAC



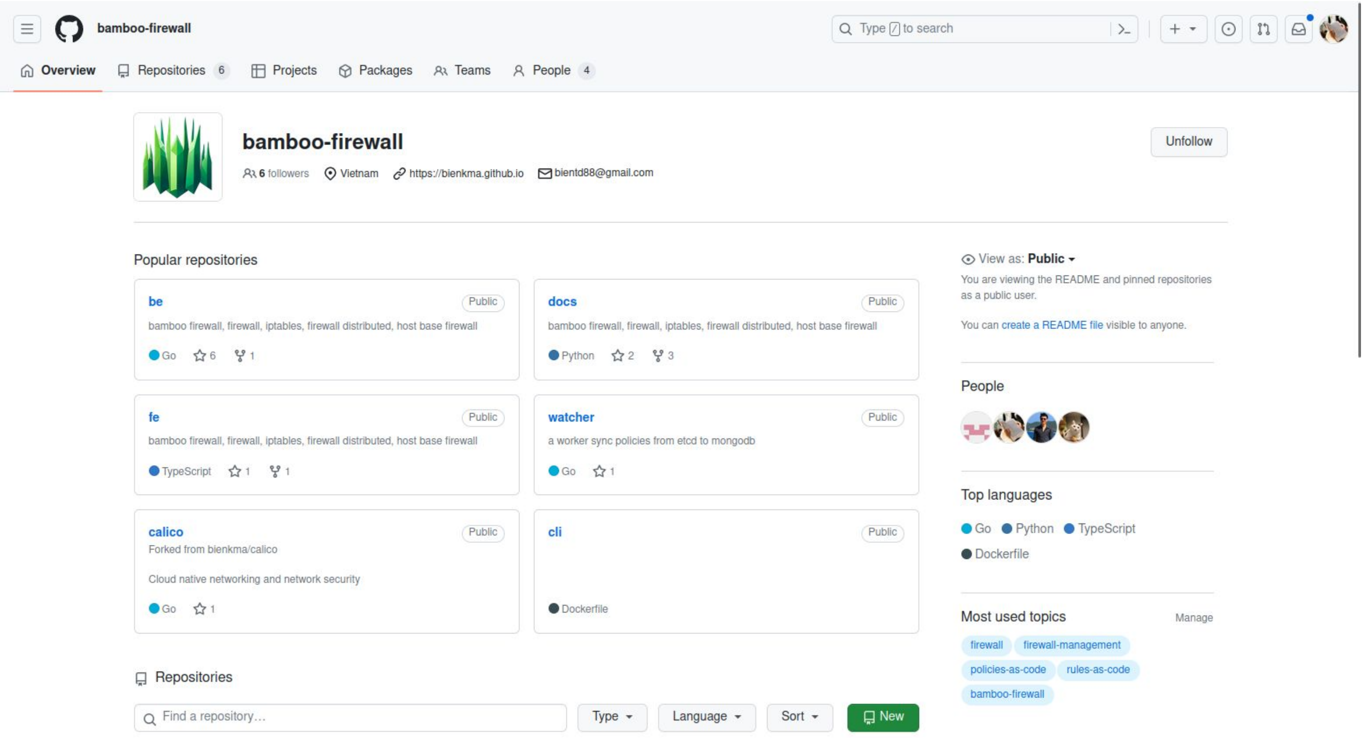
User management

STT	Email	Name	Role	Action
1	admin@example.com	admin	admin	
2	user1@example.com	User1	user	Action

GHTK

OpenInfra DAYS VIETNAM

Bamboo Firewall: Open Sources



bamboo-firewall

Type / to search

Overview · Repositories 6 · Projects · Packages · Teams · People 4

bamboo-firewall

6 followers · Vietnam · https://bienkma.github.io · bientd88@gmail.com

Unfollow

Popular repositories

Repository	Visibility	Description	Language	Stars	Forks
be	Public	bamboo firewall, firewall, iptables, firewall distributed, host base firewall	Go	6	1
docs	Public	bamboo firewall, firewall, iptables, firewall distributed, host base firewall	Python	2	3
fe	Public	bamboo firewall, firewall, iptables, firewall distributed, host base firewall	TypeScript	1	1
watcher	Public	a worker sync policies from etcd to mongodb	Go	1	
calico	Public	Forked from bienkma/calico Cloud native networking and network security	Go	1	
cli	Public		Dockerfile		

View as: Public

You are viewing the README and pinned repositories as a public user.

You can create a README file visible to anyone.

People

Top languages

● Go ● Python ● TypeScript ● Dockerfile

Most used topics · Manage

firewall · firewall-management · policies-as-code · rules-as-code · bamboo-firewall

Repositories

Find a repository… · Type · Language · Sort · New

https://github.com/bamboo-firewall

Contributors

Trịnh Đình Biên
Devops & Big Data
Engineer

Cao Xuân Anh
Devops & Backend
Engineer

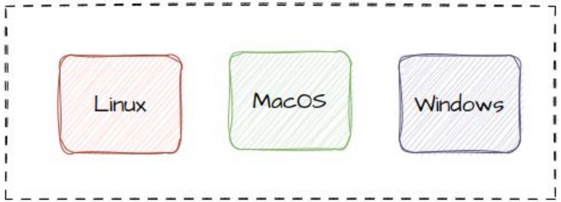
Đặng Xuân Cảnh
Senior Devops
Engineer

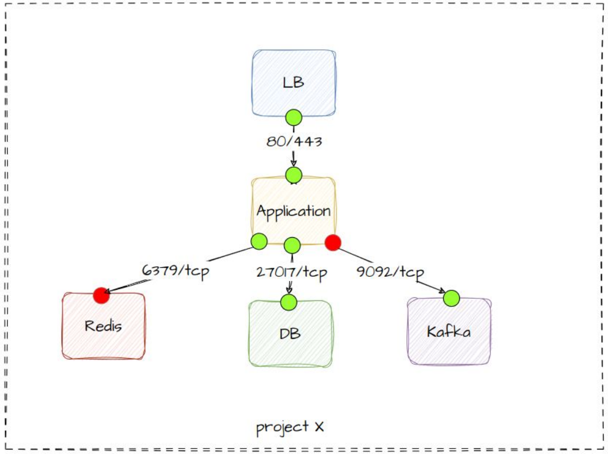
Nguyễn Thế Quân
Junior Frontend
Engineer

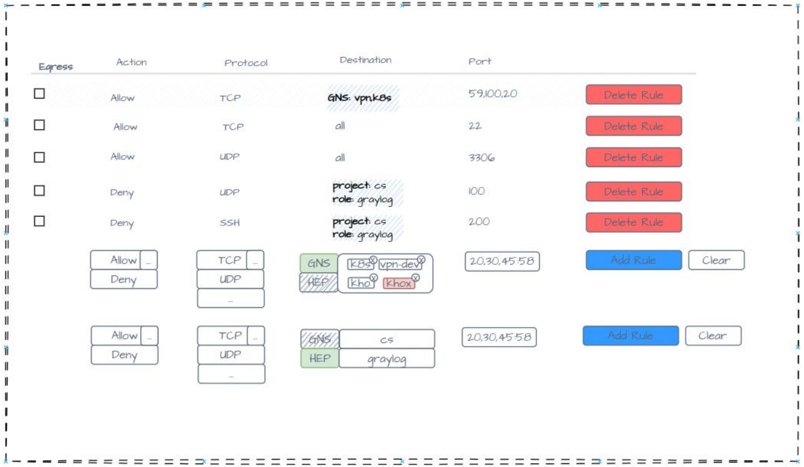
Vũ Đức Long
Senior Frontend
Engineer

Bamboo Firewall: Development roadmap

- Support multiOS
- Define policy on GUI
- View policy between servers/groups as a diagram







Egress	Action	Protocol	Destination	Port	
□	Allow	TCP	GNS: vpn.k8s	59,100,20	Delete Rule
□	Allow	TCP	all	22	Delete Rule
□	Allow	UDP	all	3306	Delete Rule
□	Deny	UDP	project: cs role: graylog	100	Delete Rule
□	Deny	SSH	project: cs role: graylog	200	Delete Rule
	Allow ... Deny	TCP ... UDP ...	GNS: k8s ⊗ vpn-dev ⊗ HEP: kho ⊗ Khox ⊗	20,30,45:58	Add Rule Clear
	Allow ... Deny	TCP ... UDP ...	GNS: cs HEP: graylog	20,30,45:58	Add Rule Clear

Q/A

Thank you

Project link: https://github.com/bamboo-firewall

GHTK

OpenInfra DAYS

VIETNAM