


Tigera / Calico - Update

Mar 2021



Tigera: Leader in Kubernetes Security & Observability



- Inventor and maintainer of Project Calico
 - Most adopted open source Kubernetes networking & security solution
 - 1+ Million nodes in 166 countries
- eBPF, Standard Linux, Windows
 - Pluggable data plane
- Envoy  envoy
- Customers include
 - Fortune 500 companies
 - Premier financial services institutions
 - Cloud-native companies
 - Telcos and eCommerce giants

Customers



Partners



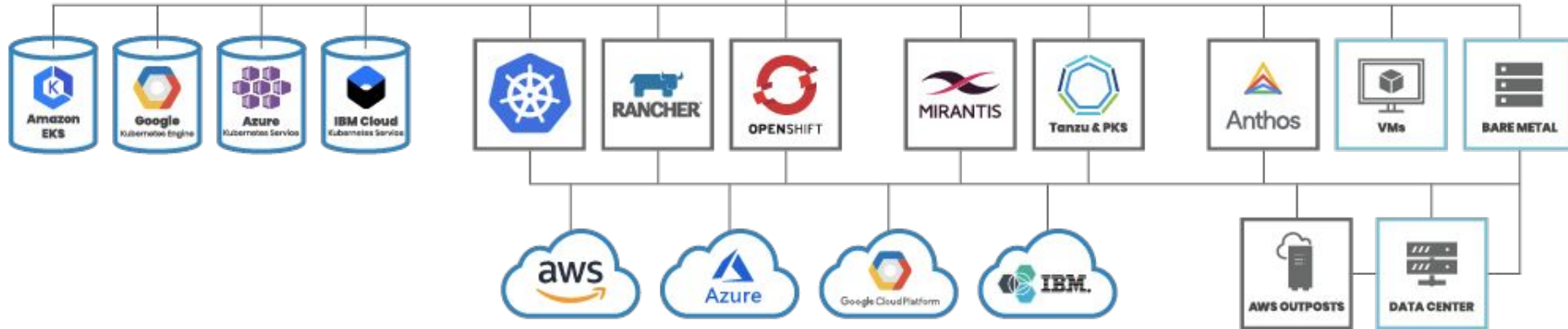
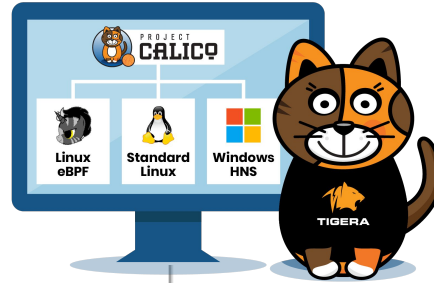
Industry Standard for Kubernetes Security

Outcomes

- Scale
- Performance
- Resource Utilization

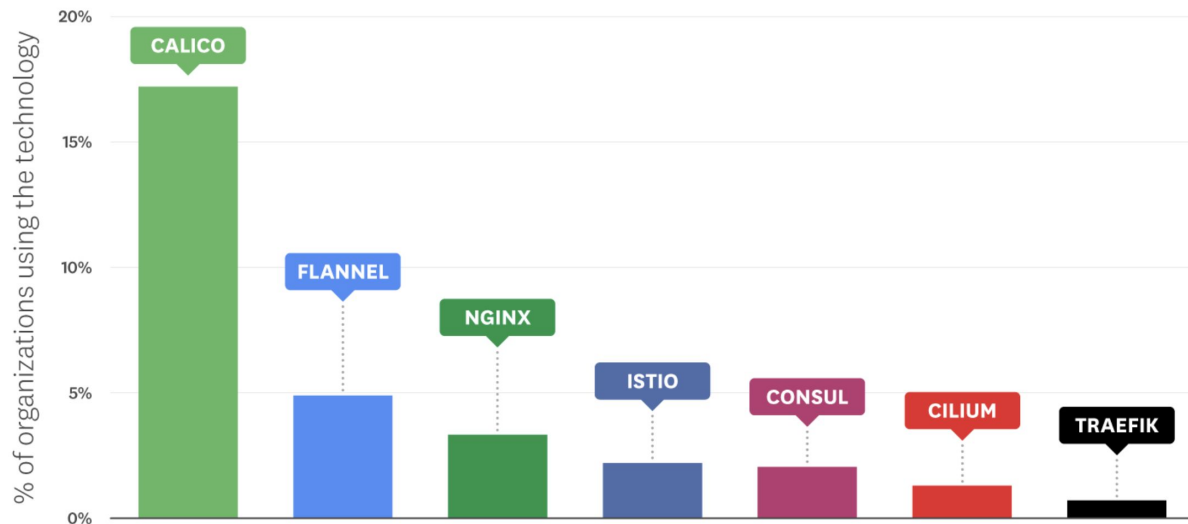
Invisible

“It just works!”



Continuing to grow our adoption

Top Networking Technologies Running as DaemonSets



Source: Datadog, Container Report 2020

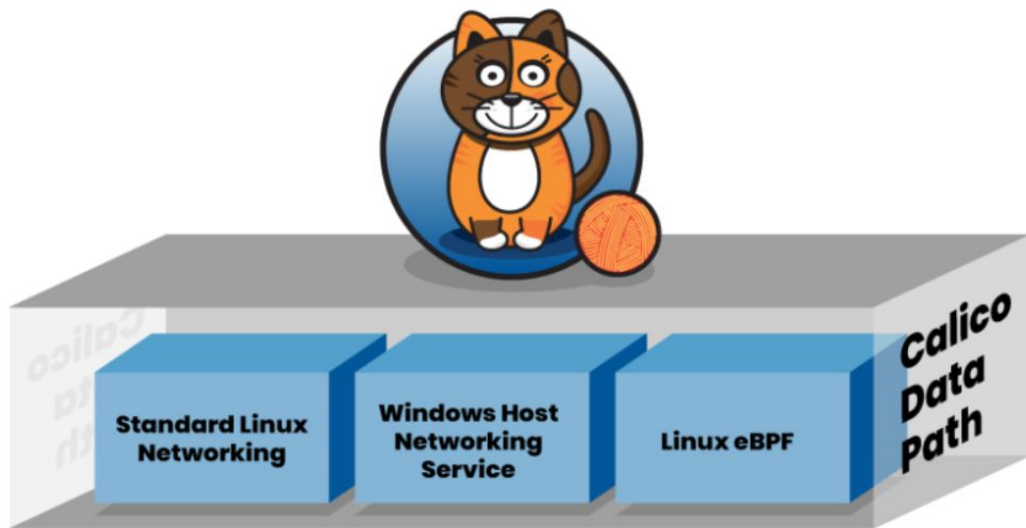
85% (YoY) growth in number of clusters.

Third-party CNI Benchmark Tests

CNI Benchmark August 2020 infraBuilder	Config	Performances (bandwidth)				Resources consumption (cpu/ram)					Security features			
	MTU	Pod to Pod		Pod to Service		Idle	Pod to Pod		Pod to Service		Network Policies		Encryption	
	setting	TCP	UDP	TCP	UDP	none	TCP	UDP	TCP	UDP	in	out	activation	Performance
Antrea	auto	Very fast	Very fast	Very fast	Slow	Low	Low	Low	Low	Low	yes	yes	at deploy time	Slow
Calico	manual	Very fast	Very fast	Very fast	Fast	Low	Very low	Very low	Very low	Very low	yes	yes	anytime	Very fast
Canal	manual	Very fast	Very fast	Very fast	Very fast	Low	Very low	Very low	Very low	Very low	yes	yes	no	n/a
Cilium	auto	Fast	Very fast	Very fast	Very fast	High	High	High	High	High	yes	yes	at deploy time	Slow
Flannel	auto	Very fast	Very fast	Very fast	Very fast	Very low	Very low	Very low	Very low	Very low	no	no	no	n/a
Kube-OVN	auto	Fast	Very slow	Fast	Very slow	High	High	High	High	High	yes	yes	no	n/a
Kube-router	none	Slow	Very slow	Slow	Very slow	Low	Very low	Low	Very low	Low	yes	yes	no	n/a
Weave Net	manual	Very fast	Very fast	Very fast	Fast	Very low	Low	Low	Low	Low	yes	yes	at deploy time	Slow

- [Configure MTU in Calico](#)
- Use Wireguard for encryption. Minimal performance impact
- Leverage [benchmarking suite](#) for your own clusters

Calico supports multiple data planes



Works with native cloud provider SDN/CNI



Google Kubernetes Engine

Policy	IPAM	CNI	Overlay	Routing	Datastore
Calico	Host Local	Calico	No	VPC Native	Kubernetes



Policy	IPAM	CNI	Overlay	Routing	Datastore
Calico	AWS	AWS	No	VPC Native	Kubernetes

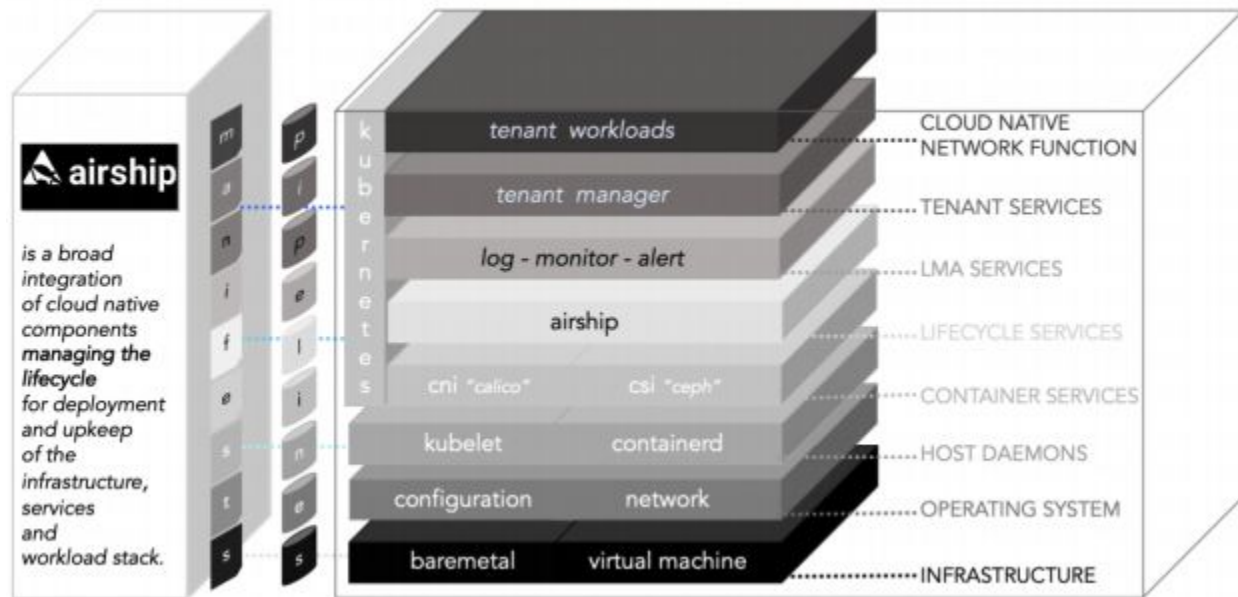
Policy	IPAM	CNI	Overlay	Routing	Datastore
Calico	Calico	Calico	VXLAN	Calico	Kubernetes



Azure Kubernetes Service (AKS)

Policy	IPAM	CNI	Overlay	Routing	Datastore
Calico	Azure	Azure	No	VPC Native	Kubernetes

AirShip 2.0 Architecture

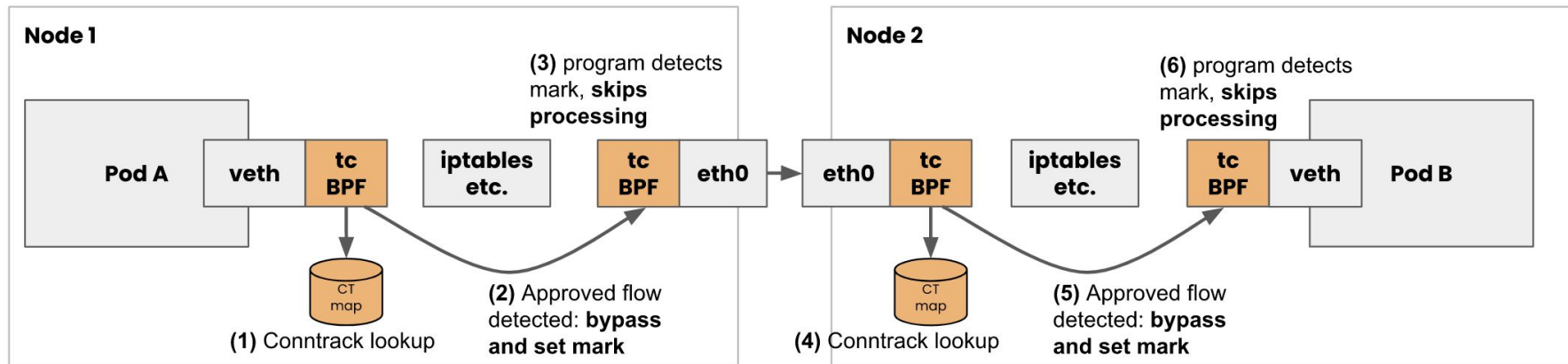


- Layer3 SDN for Control Plane, independent of the tenant network
- Integrate routing announcements for control plane directly into physical fabric
- Multi-NIC
- Optimized service load balancing

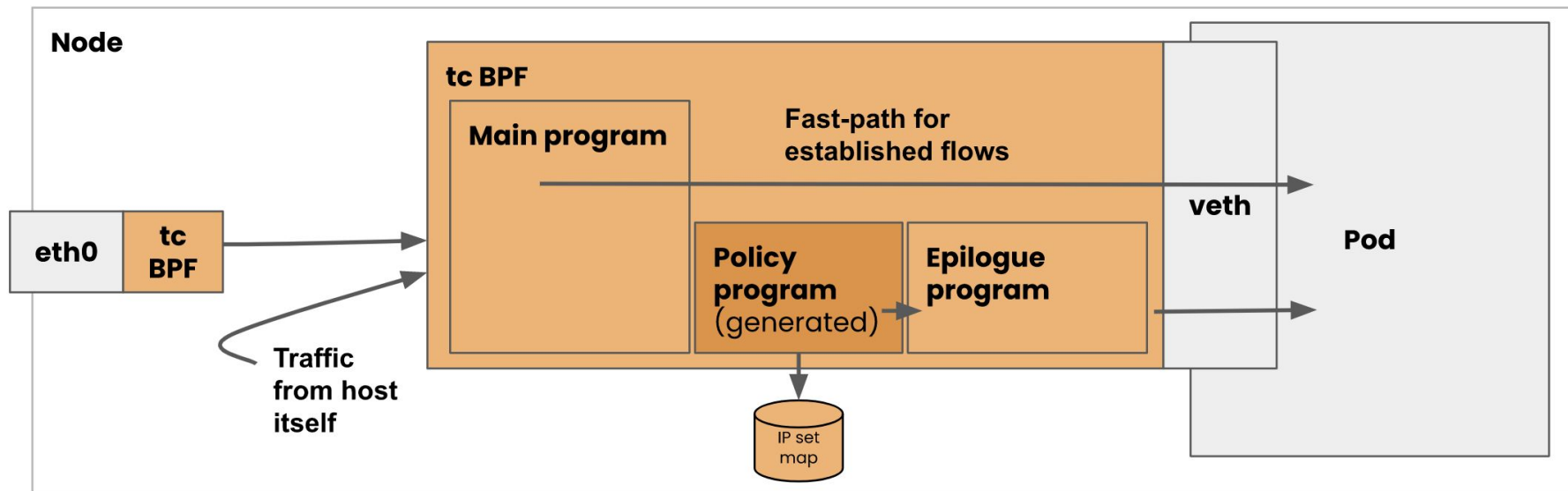
Next Generation Dataplane (eBPF)

- Full support for Calico network policies
- Networking optimization leveraging eBPF for traffic to/from Pods
- No kube-proxy needed (full support for kube proxy functionality e.g. node ports and services)
- Connection time load balancing for traffic originating from workloads
- Integrated with the Calico Policy engine
- Support for Direct Server Return optimization
 - DSR is to optimize the return path for traffic originating outside the cluster destined to workloads to avoid additional hops on the return path
 - Source IP preservation for public cloud

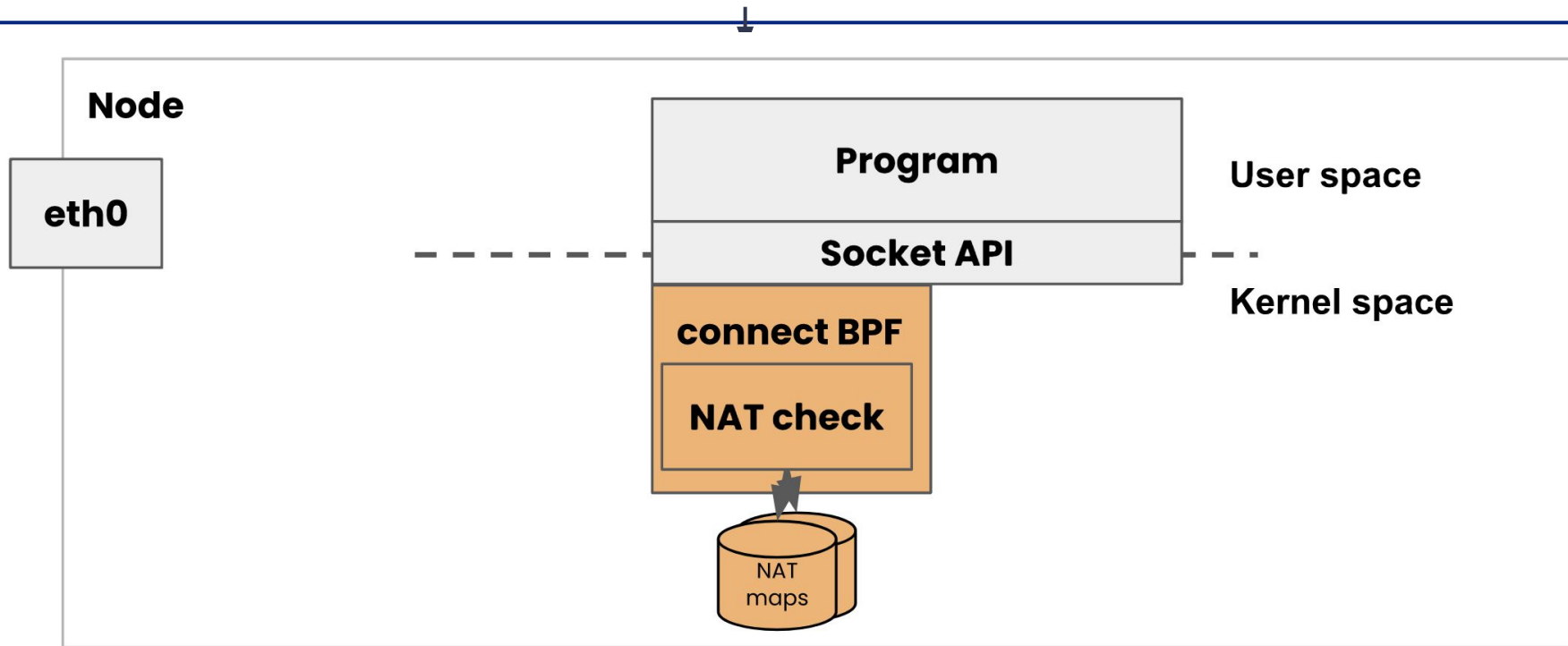
Architecture: Network Optimization



Architecture: Policy Application



Architecture: Service Optimization



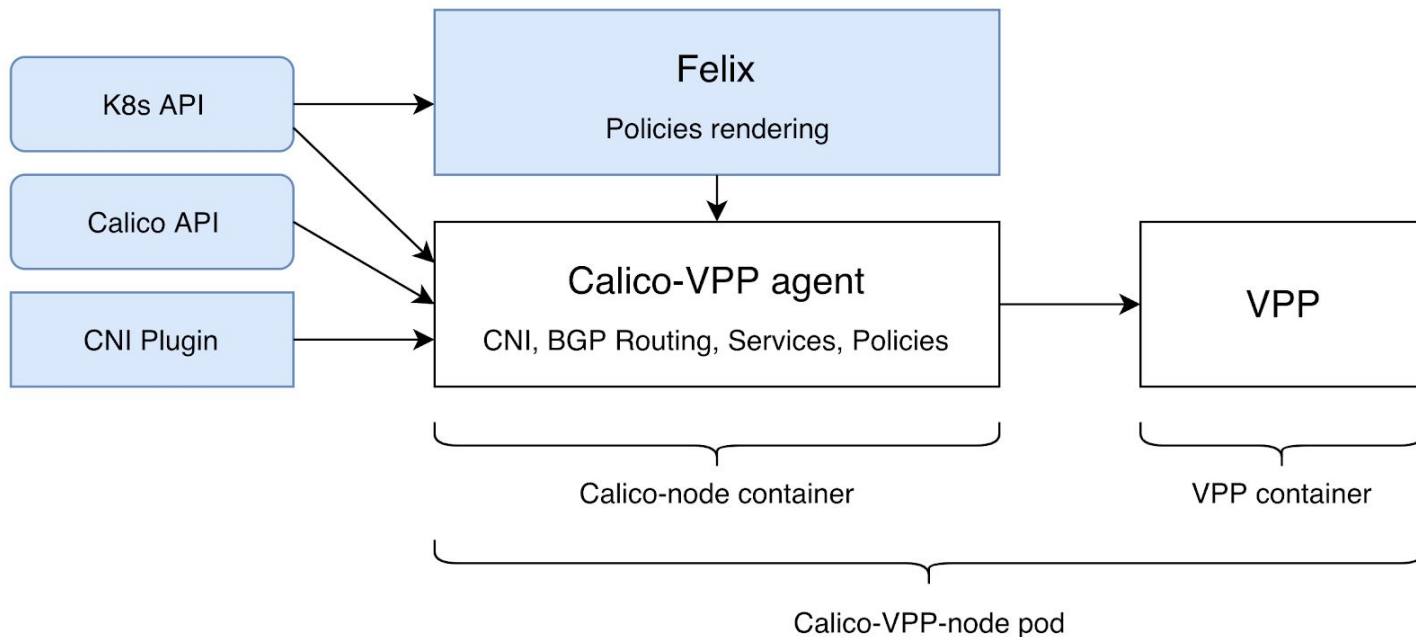
Calico/VPP integration

- VPP dataplane option for Calico
 - Transparent for users except for basic initial interface configuration
- Custom VPP plugins for K8s networking:
 - Optimized NAT plugin for service load balancing
 - Specific plugin for efficient Calico policies enforcement
- VPP configuration optimized for container environments:
 - Interrupt mode, SCHED_RR scheduling
 - No hugepages required
 - GRO / GSO support for container interfaces

Benefits

- Performance
 - World-class encryption performance: IPsec / Wireguard
 - Reduced overall CPU consumption
- Operational simplicity
 - Network stack decoupled from OS - easier to upgrade
 - VPP is packaged as a regular container
 - Very limited kernel dependencies
- Better control over resources dedicated to container networking
- Extensibility through VPP plugins

Software architecture



: Regular Calico / K8s components



: VPP-specific components

References

- Calico: <https://www.projectcalico.org/>
- Join the Calico/VPP slack to stay up to date!
 - <https://calicousers.slack.com/archives/C017220EXU1>
- Check out our docs if you'd like to learn more or try it out:
 - <https://github.com/projectcalico/vpp-dataplane/wiki>
- Calico dataplane driver for VPP:
 - Code: <https://github.com/projectcalico/vpp-dataplane>
 - Doc: <https://github.com/projectcalico/vpp-dataplane/wiki>
 - Slack channel: <https://calicousers.slack.com/archives/C017220EXU1>
- 40Gbps pod-to-pod IPsec for Calico with VPP:
 - <https://medium.com/fd-io-vpp/getting-to-40g-encrypted-container-networking-with-calico-vpp-on-commodity-hardware-d7144e52659a>



TIGERA

Follow us on:

