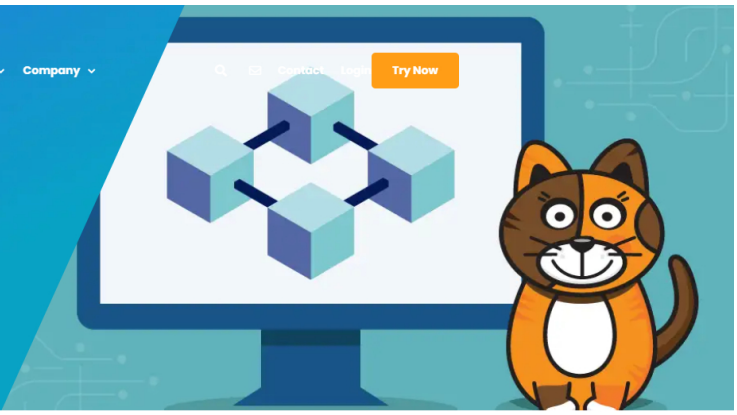
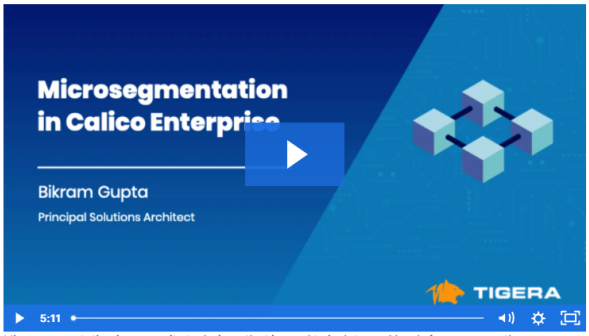


Technical Blog

Enabling Microsegmentation with Calico Enterprise

By Bikram Gupta on Aug 06, 2020



Microsegmentation is a security technique that is used to isolate workloads from one another. Microsegmentation limits the blast radius of a data breach by making network security more granular. Should a breach occur, the damage is confined to the affected segment. Application workloads have evolved over time – starting from bare metal, to a mix of on-prem and cloud virtual machines and containers. Similarly, the pace of change has dramatically increased, both in terms of release updates and auto-scaling.

Enforcement of network security has also evolved over time, with organizations using a mix of physical/virtual firewalls and platform-specific security groups to manage network security. This creates the following challenges:

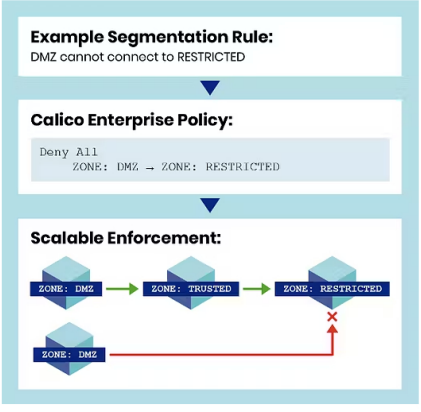
1. **Management Overhead** – Organizations have to maintain different products, teams and workflows to manage and operate segmentation across containers, VMs and bare metal. The diagram above shows how different platforms may require different approaches to segmentation, thereby creating a burden on the operations team.
2. **Lack of Cloud-Native Performance** – With hybrid cloud becoming a norm, products built for traditional workloads can neither scale nor enforce security for cloud-native deployments with minimal latency.

Calico Enterprise provides a common policy language for segmentation that works across all of your hybrid cloud and scales with the growth of your microservices environment. You can create and enforce a single security policy across different workloads (containers, VMs, bare metal) for dynamic enforcement. Calico Enterprise also provides a single pane of glass for cluster monitoring.

How Does It Work?

As a first step, Calico Enterprise needs to discover all the endpoints that you want to secure. It already knows about the workloads (pods) running on Kubernetes. For other endpoints (eg. Kubernetes nodes and other VMs), you will need to create host endpoints and assign labels. A host endpoint refers to a host running a Calico Enterprise agent. The host endpoint object itself is stored as part of the Calico configuration in the Kubernetes datastore. So Calico Enterprise has a complete view of the entire inventory of endpoints. At this stage, there's no segmentation as no policies have been created.

The next step is to create and enforce the policies. An example policy for denying all traffic from "Zone: DMZ" to the "Zone Restricted" is shown in the diagram on the right. Calico Enterprise segments endpoints per policy definition and based on metadata/labels attached to those endpoints. This enables you to securely deploy new or updated workloads/VMs without having to add or change your segmentation policies.



Finally, Calico Enterprise creates flow logs enriched with workload names, labels, applied policies etc. for all the network connections. These logs

enable monitoring, security and troubleshooting. This approach eliminates the complexity and operational overhead associated with managing your segmentation policies.

An interesting thing to note here is the declarative, pull-based model used by Calico Enterprise. It means whenever a new endpoint (e.g., workload or VM) is added/removed, the agent on the endpoint pulls the policy. Calico Enterprise doesn't need to monitor the endpoints and look for changes. The agent running on the endpoint is responsible for maintaining the configuration. This avoids unpleasant scenarios like having to wait for hours for policy changes to be applied to your infrastructure. With Calico Enterprise, it's easy to scale and convergence is in minutes.

Enabling Microsegmentation

Microsegmentation is a core feature of Calico Enterprise. Its Global Network Policy is the only policy spec you need to follow. A global network policy applies to a set of endpoints.

```
spec:
  tier: internal-access
  selector: role == 'database'
```

As shown in the example, above, Calico Enterprise will apply the policy to all endpoints (bare metal, VM, pods) having a label role == 'database'. So how does Calico Enterprise know about the VMs? You have to install the agent on every node that you want to manage, and then have the agent connect to the same Kubernetes configuration datastore.

Finally, Calico Enterprise requires a hostendpoint object to be created for every non-Kubernetes endpoint you want to manage. This can be automatically created by Calico Enterprise if configured. The hostendpoint has labels, and that's how Calico Enterprise knows about all the non-Kubernetes endpoints. Automation of this is fairly straightforward, and we recommend automation of the on-boarding of non-Kubernetes nodes using your preferred tool.

Want to learn more? Explore these resources...

Here are some helpful working samples that you can reference:

- Using Calico Enterprise for microsegmentation
- Protect Kubernetes workloads
- Protect hosts
- Automatic host endpoints

How-To Products

Related posts

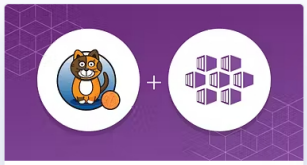
Technical Blog

Zero trust in the cloud: Best practices and potential pitfalls

By Ratan Tipirneni on Oct 25, 2022

Architecturally speaking, cloud-native applications are broken down into smaller components that are highly dynamic, distributed, and ephemeral. Because each of these components is communicating with other components inside or outside the cluster, this architecture introduces...

Read more ›



Technical Blog

How Calico CNI solves IP address exhaustion on Microsoft AKS

By Dhiraj Sehgal on Oct 18, 2022

Companies are increasingly adopting managed Kubernetes services, such as Microsoft Azure Kubernetes Service (AKS), to build container-based applications. Leveraging a managed Kubernetes service is a quick and easy way to deploy an enterprise-grade Kubernetes cluster,...

Read more ›

Technical Blog

Automate Calico Cloud and EKS cluster integration using AWS Control Tower

By Suki Lam on Oct 4, 2022

Productive, scalable, and cost-effective, cloud infrastructure empowers innovation and faster deliverables. It's a no-brainer why organizations are migrating to the cloud and containerizing their applications. As businesses scale their cloud infrastructure, they cannot be bottlenecked...

Read more ›

Email Address

SUBSCRIBE