Rethinking the K8s DNS for the Modern Enterprise

KubeCon NA 2019

Deepa Kalani
Staff Engineer 2
NSX Service Mesh
VMware
dkalani@vmware.com

Venil Noronha
Member of Technical Staff
NSX Service Mesh,
VMware
veniln@vmware.com

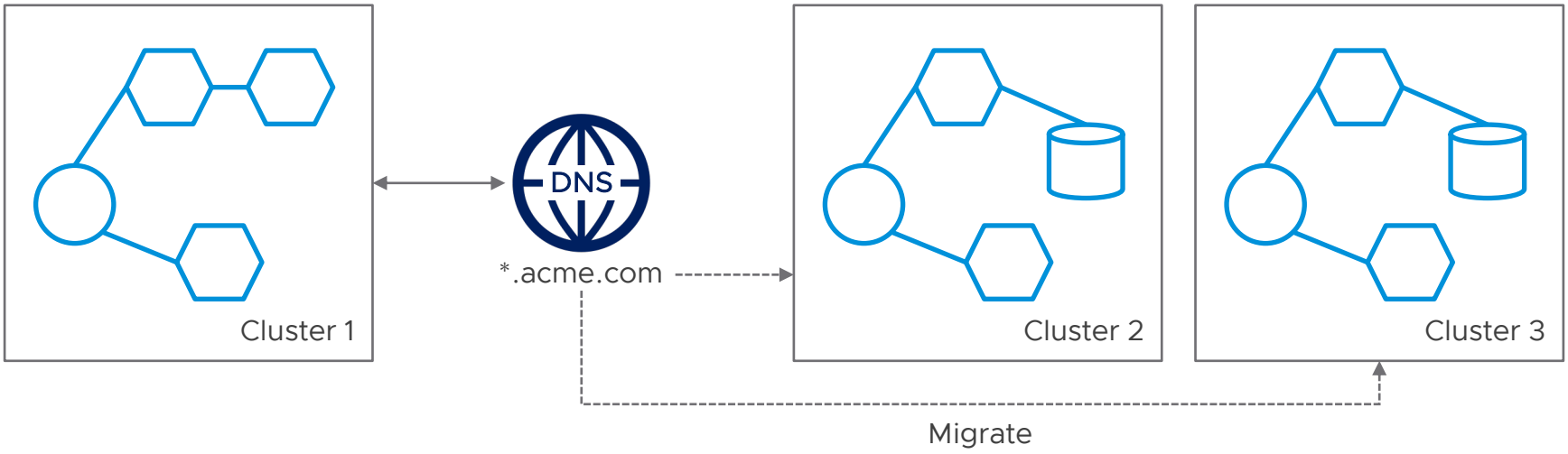
vmware

Agenda

- Application Migration and Service Discovery
- Need For Multi-Tenant Clusters in the Enterprise
- DNS Virtualization
- DNS Observability and Security
- DNS Policy
- Context-based Service Discovery
- Current State of Kubernetes DNS
- Envoy Proxy as an Enabler for Secure DNS
- Multi-Tenant Service Discovery via Indirection to Envoy Proxy
- Applying DNS Policies via Envoy Proxy
- Demo
- Conclusion

Application Migration and Service Discovery

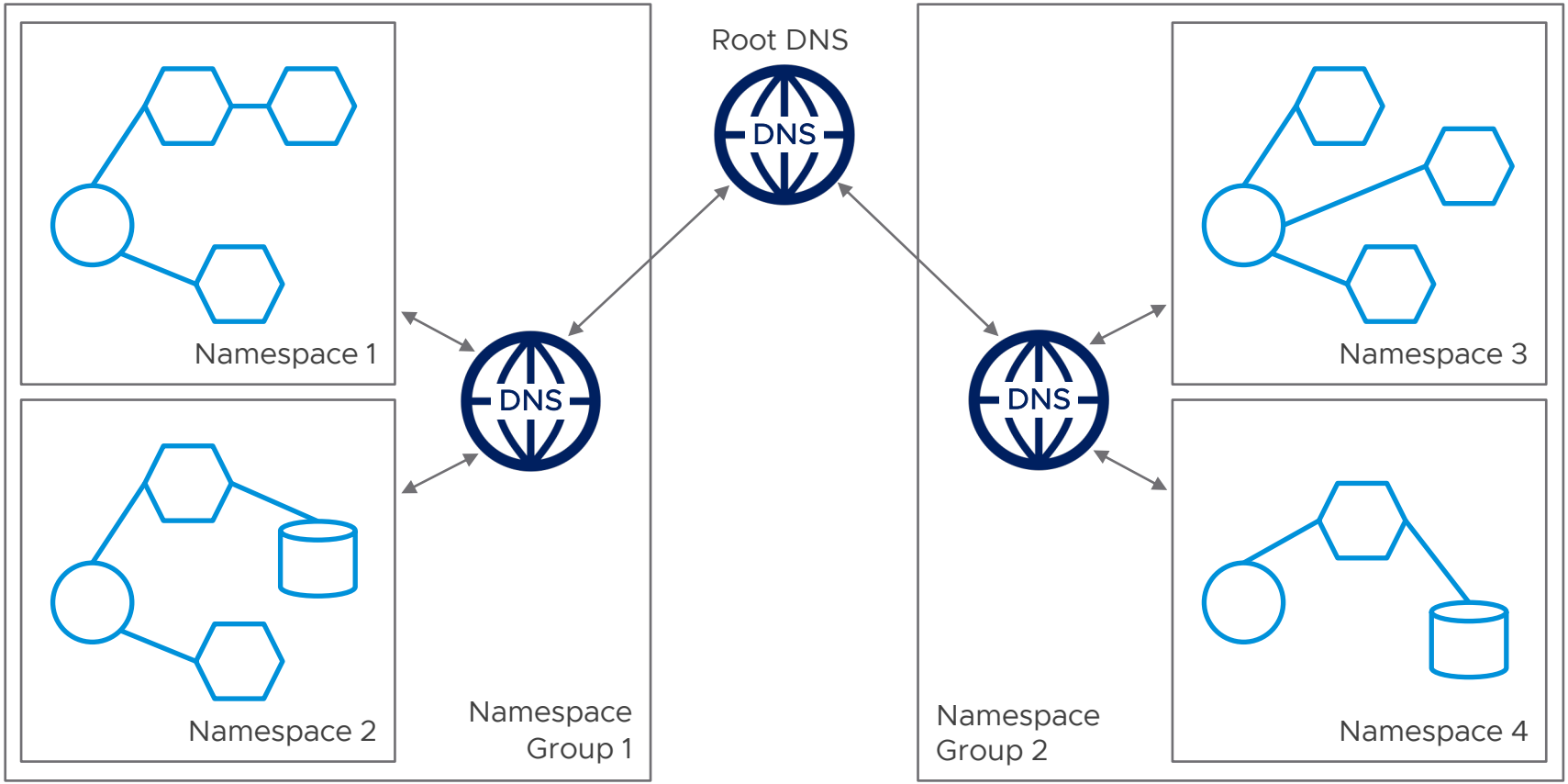
- Multi-cloud and hybrid-cloud systems
- In a multi-cloud world, applications may be deployed on prem and in the cloud
- Developers should be able to deploy and migrate applications across any cloud provider without changing their native workloads



Need for Multi-Tenant Clusters in the Enterprise

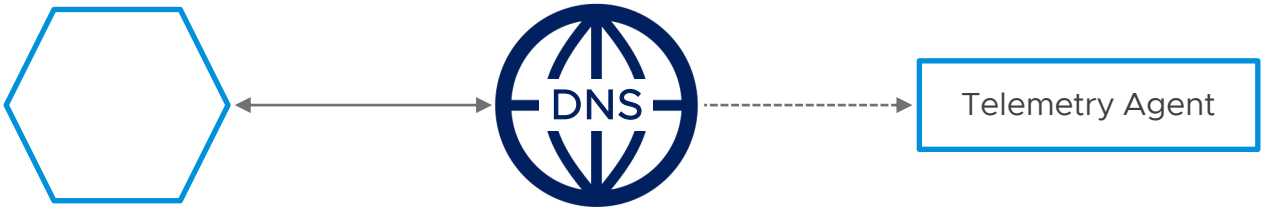
- Multiple tenants can be using the same cluster - operators need to ensure that tenants are not able to access resources in namespaces not belonging to them
- Tenants of a SaaS application are typically customers accessing a service - operators may deploy the service as an isolated resource owned by an organization or a business unit
- Operators must ensure strong isolation of these services across namespaces - this can be accomplished through network policies; however, services can still be discovered across namespaces
- Need a fundamental way to isolate and secure services

DNS Virtualization



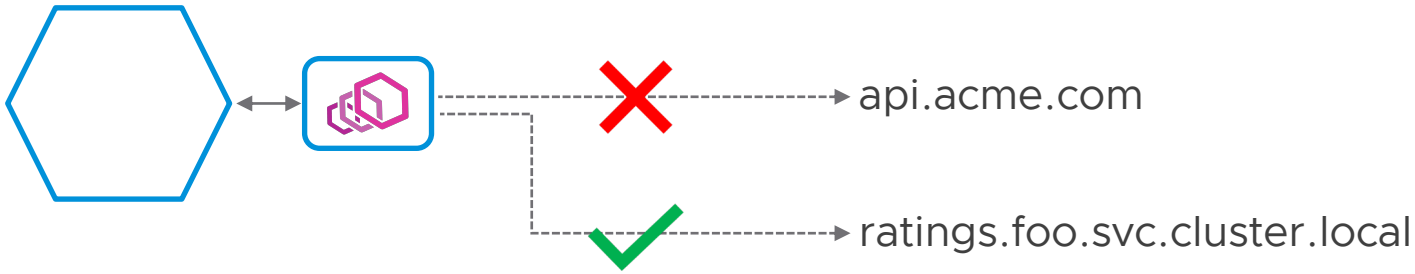
DNS Observability and Security

- Mesh operators need visibility into what services an application is trying to reach
- Rich telemetry for DNS queries and responses
- Telemetry per tenant
- Encryption of DNS queries right after inspection (DoT/DoH)



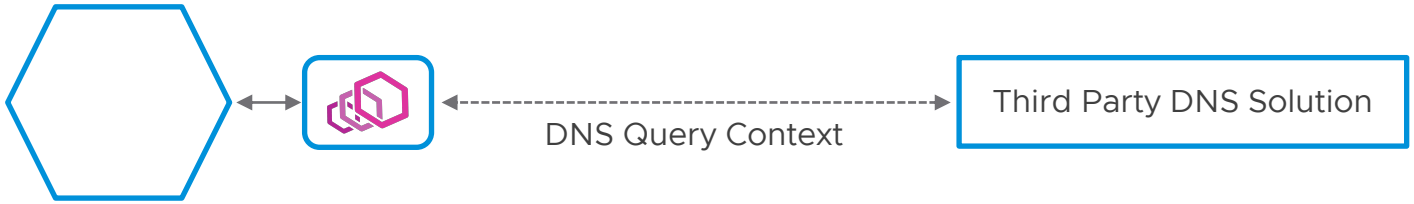
DNS Policy

- Operators need a way to specify policies at the DNS layer
- DNS policies allow for access control and logging
- Example: Deny the frontend service from discovering *.com and log such requests
- Treat DNS just as another entity in the Kubernetes cluster
- Apply L4/L7 policies based on DNS queries/responses



Context-based Service Discovery

- Discovery based on service level identifiers
- Allows operators to specify policy of which and what type of service is discoverable by an application
- Third party solutions can utilize telemetry and contextual information to provide richer service discovery features

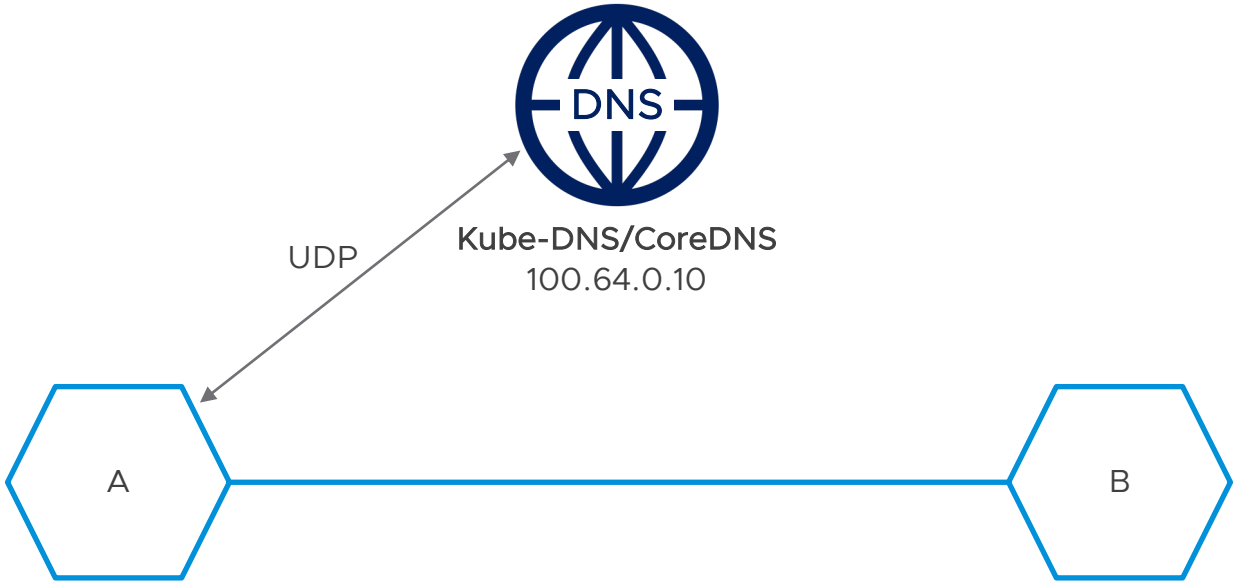


Current State of Kubernetes DNS

- No tenant isolation for DNS
- No dynamic configuration of DNS
  - Can’t configure search domains dynamically
  - Can’t configure nameservers dynamically
- Policies cannot be enforced at the DNS layer
- Doesn’t provide first-class support for Secure DNS
  - DNS-over-TLS (DoT)
  - DNS-over-HTTPS (DoH)

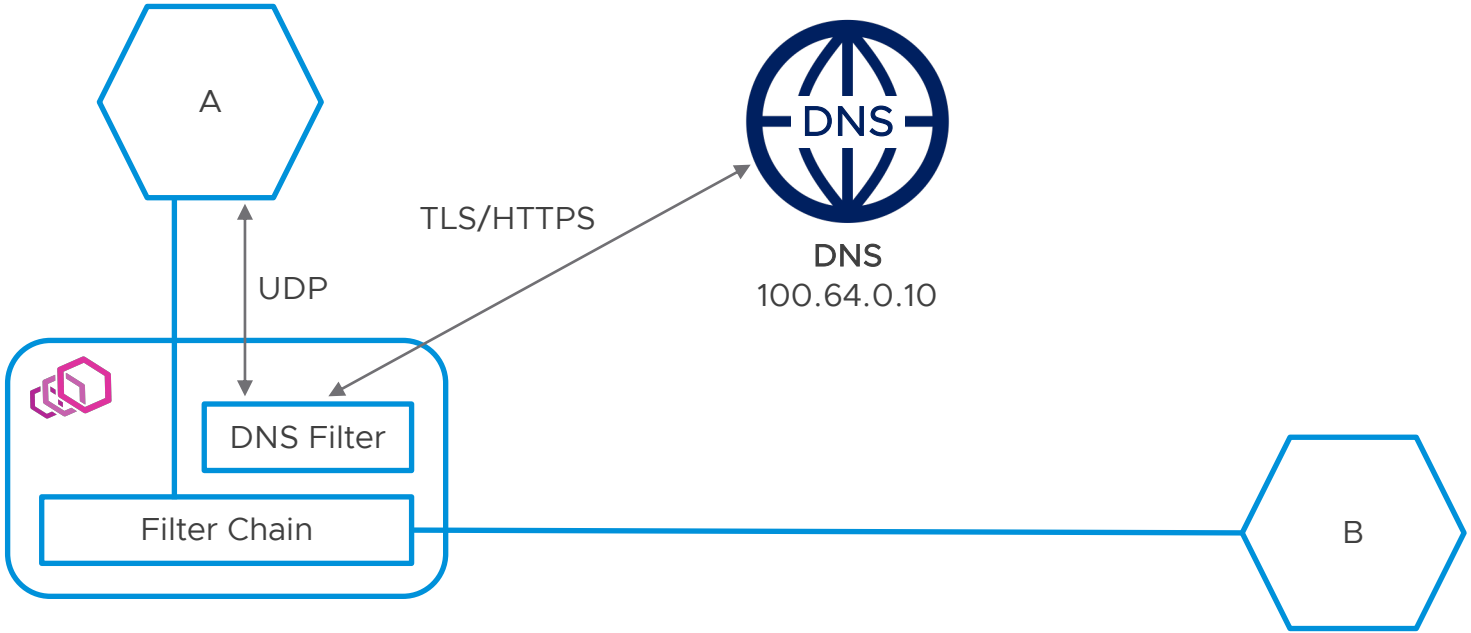
Envoy Proxy as an Enabler for Secure DNS

Kubernetes DNS

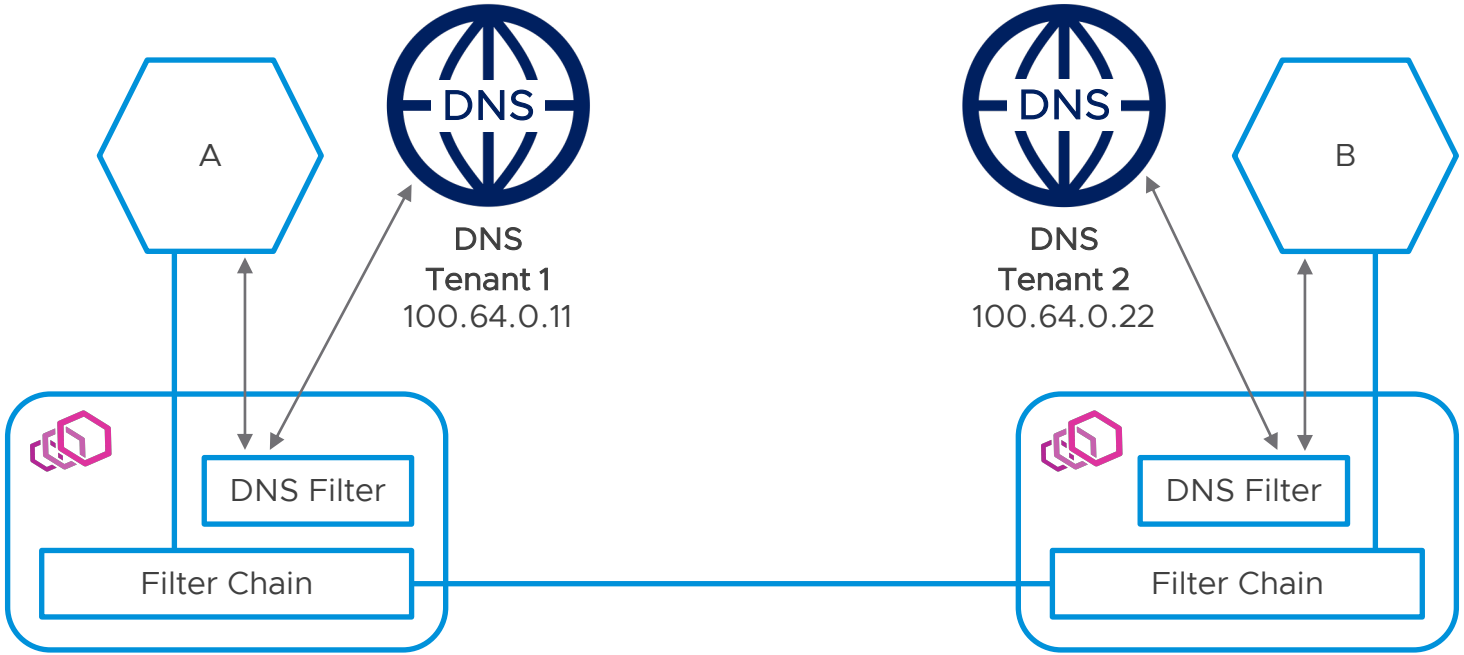


Envoy Proxy as an Enabler for Secure DNS

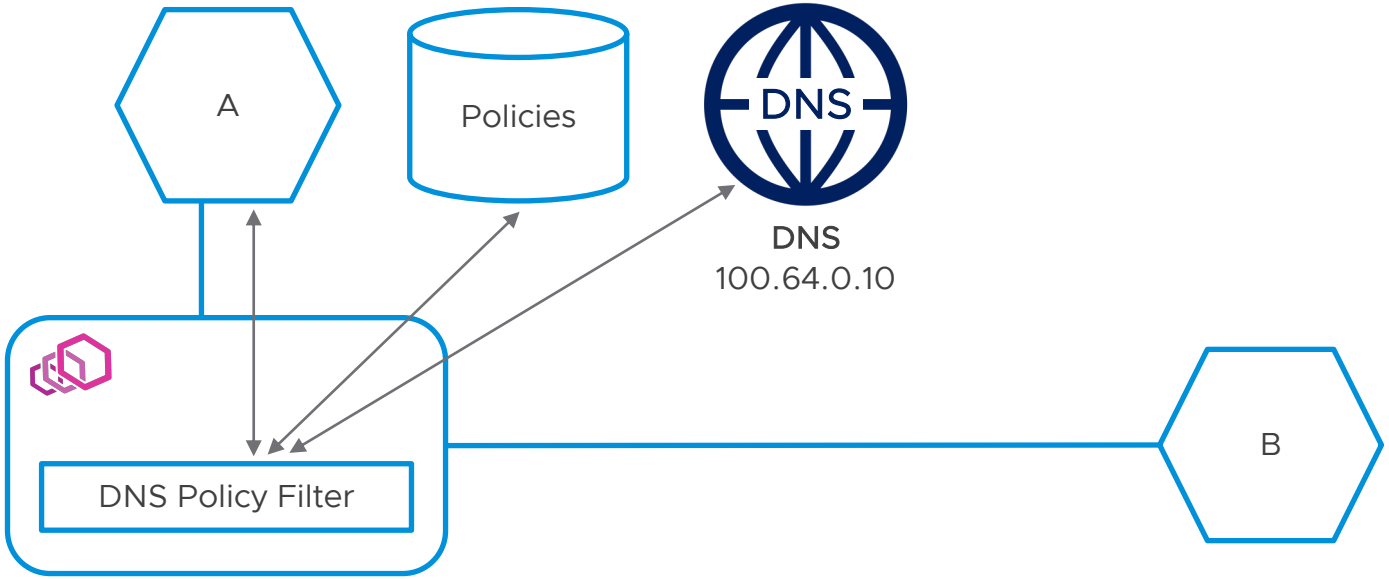
DoH/DoT with Envoy Proxy



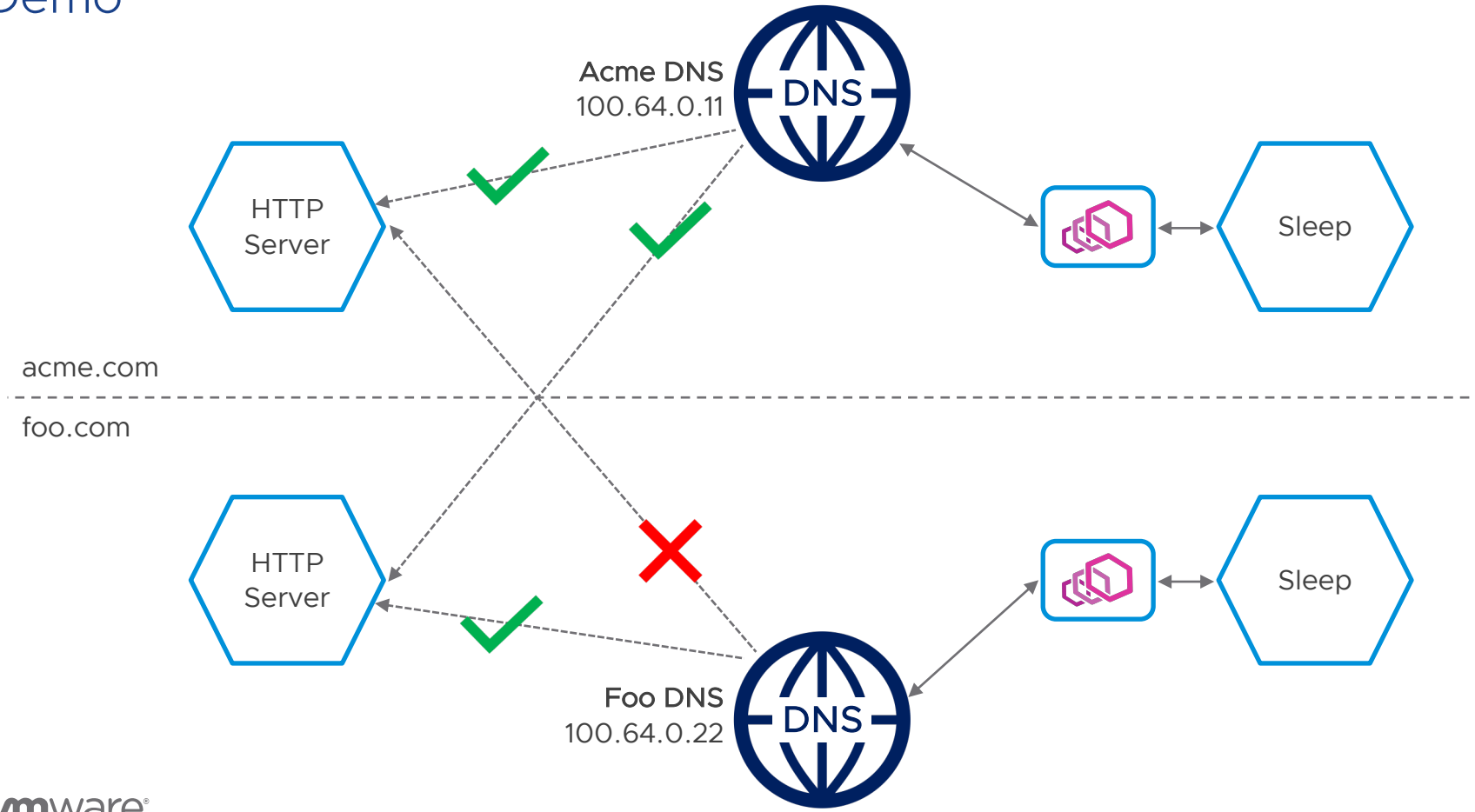
Multi-Tenant Service Discovery via Indirection to Envoy Proxy



Applying DNS Policies via Envoy Proxy



Demo



Conclusion

- DNS plays a key role for service discovery in enterprise and cloud-based systems
- Multi-tenancy at the DNS layer is very critical for the functioning of enterprise systems
- A level of indirection to Envoy proxy can solve some interesting challenges with DNS
- Envoy proxy can also help in scenarios where dynamic DNS configurations need to be applied to workloads
- A DNS filter in Envoy can also be integrated with third-party systems to provide richer observability, security, and policy features

Thank You

Deepa Kalani | dkalani@vmware.com
Venil Noronha | veniln@vmware.com

istio.io
envoyproxy.io
venilnoronha.io