SERVICE MESH SUMMIT 2022
服务网格峰会

主办方 云原生社区 Cloud Native Community

英特尔Envoy TLS性能优化方案与实践

英特尔软件与先进技术部 胡伟 云原生软件方案架构师
英特尔软件与先进技术部 赵复生 云原生软件研发经理

英特尔服务网格工作介绍

Service Mesh

Develop features and optimizations in service mesh layer driving IA differentiation and broad adoption.

Performance — Deliver 10%-80% performance(QPS) improvements in use cases such as TLS Handshakes, Compression operations in Cloud Native Environments.

Feature Enablement — Enable Hardware Security features like QAT, SGX and enable functionality for 5G features to drive IA adoption and differentiation.

Acceleration

- Envoy Crypto signing operations
- Bypass TCP/IP stack for communication with sidecar & sidecar comms within a node
- Performance Improvements on ISTIO (open-ssl, boringssl).
- TLS Handshake with AVX-512 – ICX.
- TLS Handshake with QAT (SPR)
- Compression using QAT(SPR)

Security (SGX)

- CA Private key security (secure signing) – Manual Key Management
- CA Private key security (secure signing) – Auto Key Management
- Envoy Private Key Security.
- ISTIO Multi Tenancy with PKI

Threat Security

- ISTIO modsecurity WASM plugin
- TLS Splicing
- TLS Bumping

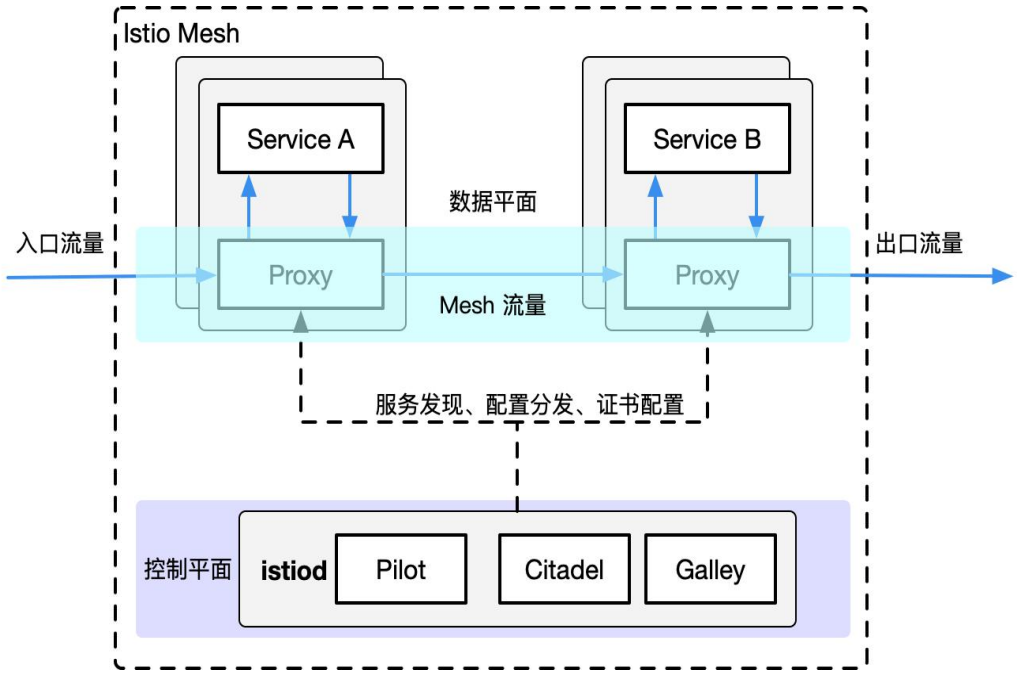
5G Enablement

- Adding IPv6 Support to ISTIO and ENVOY.
- Enabling SM on Secondary Interfaces

云原生场景下Envoy TLS的性能挑战

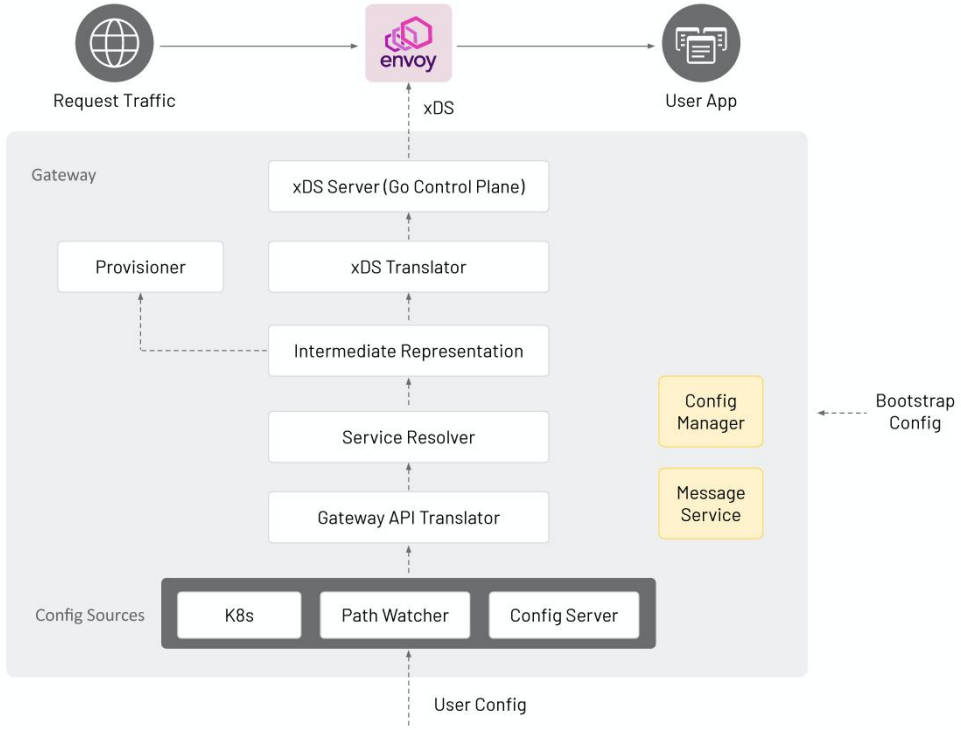
SERVICE MESH SUMMIT 2022 服务网格峰会

服务网格



服务网格技术已经成为一个云原生用户应用服务通信的首选通用架构。在目前非常流行的服务网格项目Istio中，数据面是通过 Envoy 来实现的。

云原生网关



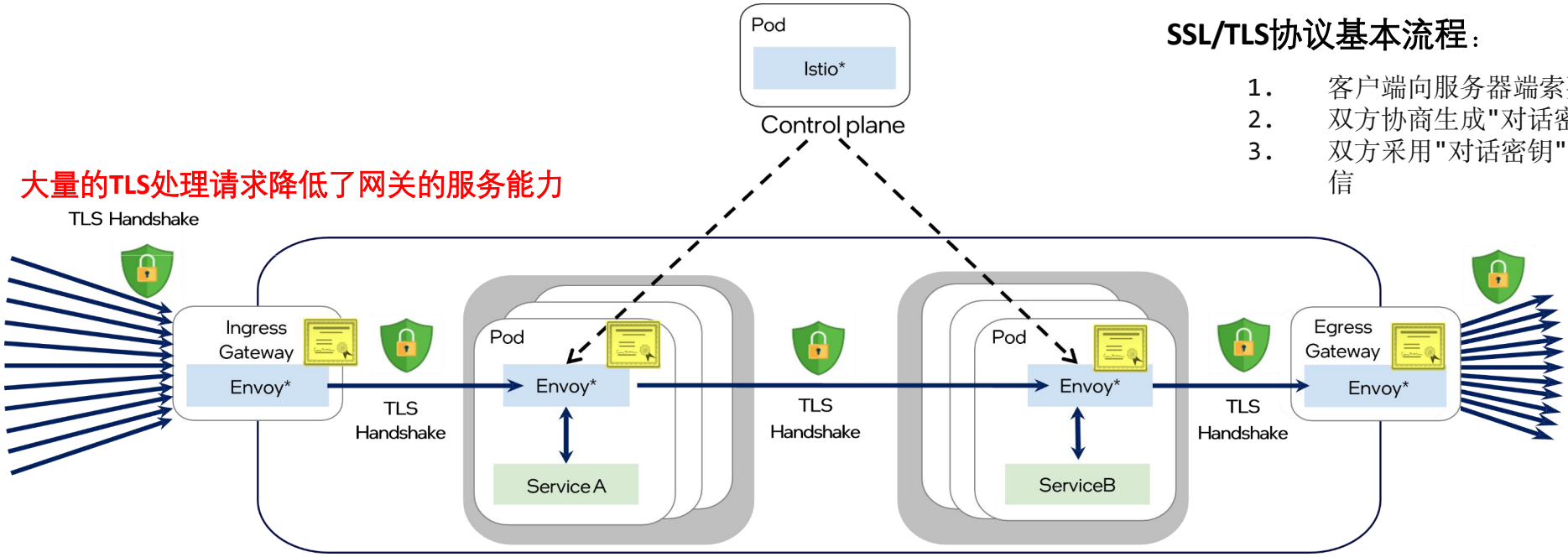
基于Envoy 强大的可扩展性和易用性，在 Kubernetes 架构下，Envoy 重新定义了网关的定位和能力，被誉为云原生网关。

云原生场景下Envoy TLS的性能挑战

Istio提供TLS作为服务到服务身份验证的安全解决方案。因此服务网格中Envoy数据面无论是作为集群入口流量网关还是作为集群内部微服务的代理，都是通过TLS安全连接来进行服务间通信，因此需要处理大量的 TLS 请求。

SSL/TLS协议基本流程：

1. 客户端向服务器端索要并验证公钥
2. 双方协商生成"对话密钥"
3. 双方采用"对话密钥"进行加密通信



TLS增加了服务之间调用的延迟时间

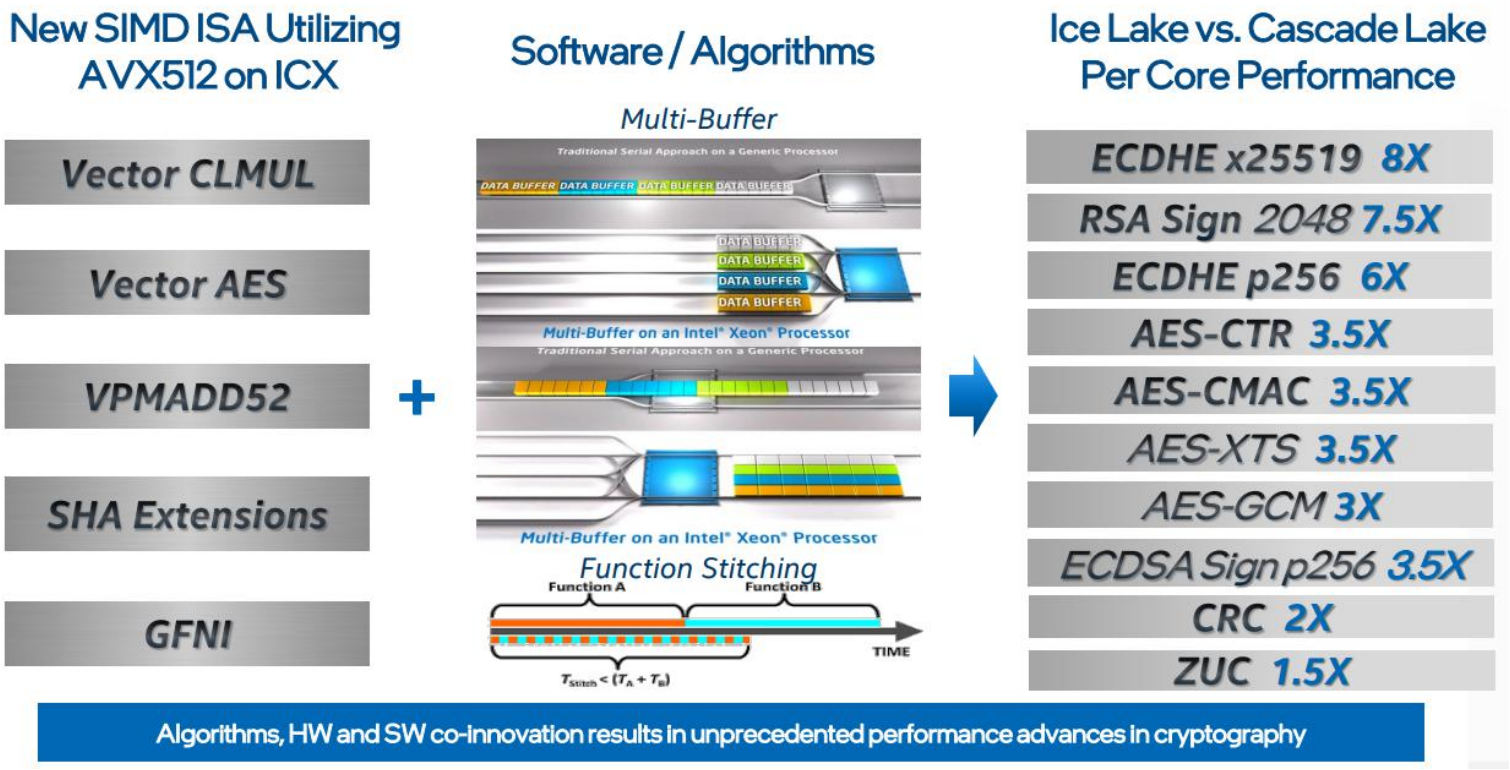
SSL/TLS协议过程的前两步又称为“握手阶段”。握手阶段执行非对称加解密的操作需要消耗大量的 CPU 资源，也会增加微服务之间调用的延迟时间，这在大规模微服务场景，以及边缘计算场景计算资源有限的情况下会成为一个系统性能瓶颈。

英特尔 Crypto Acceleration 技术介绍

Multi-Buffer 多缓冲区处理 - 多缓冲区处理是一种用于并行处理密码算法中多个独立数据缓冲区的创新高效技术。多缓冲区处理最多可收集八个RSA操作请求。每个请求都是相互独立，因此可以同时进行处理。对于每个相互独立且同类（加密或解密）的RSA操作请求，可以使用SIMD指令比如AVX512提高性能

AVX512指令集 – AVX-512 Integer Fused Multiply Add(IFMA), AVX-512 Vector AES instructions (VAES)

英特尔 Crypto Acceleration 技术介绍

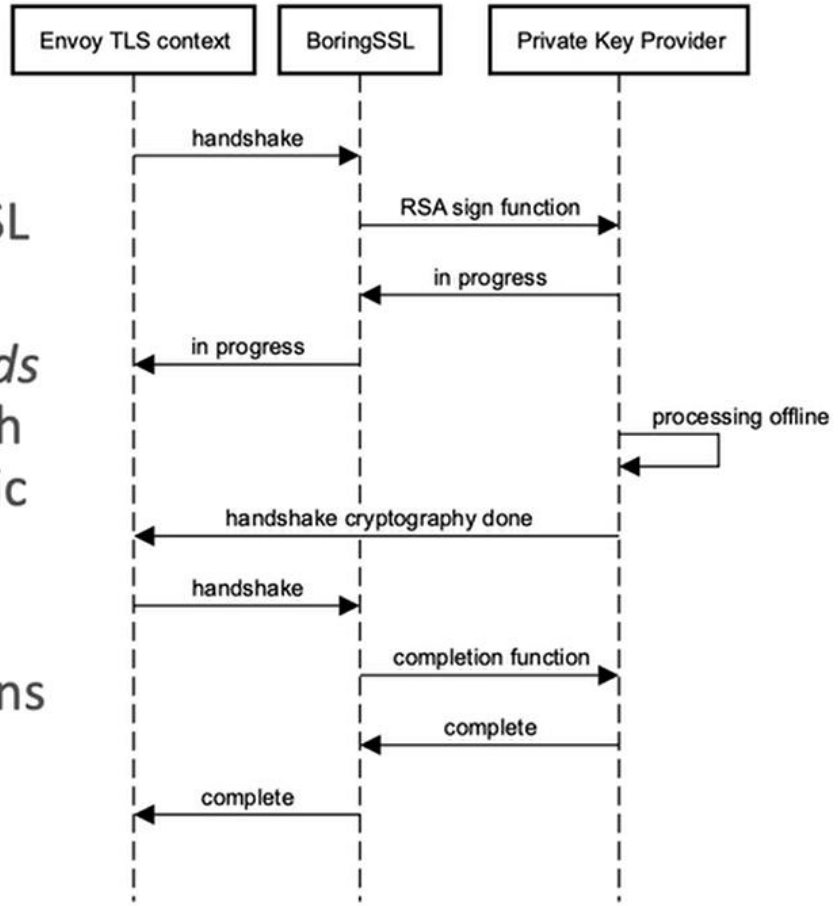


https://www.intel.cn/content/dam/www/central-libraries/us/en/documents/cryptography-processing-with-3rd-gen-intel-xeon-scalable-processors-19-may-2021.pdf

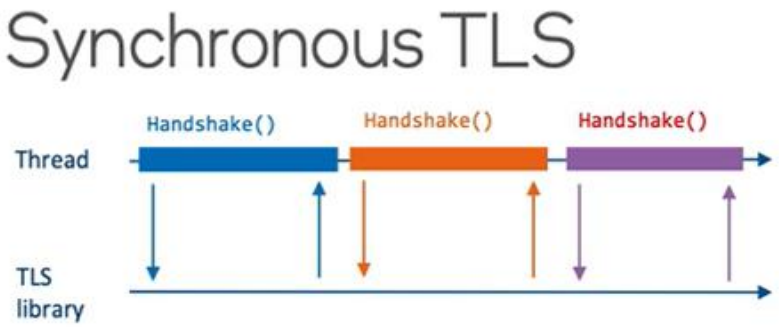
- Intel Multi-Buffer多缓冲区技术是通过一个名为 Intel® Integrated Performance Primitives (Intel® IPP) Cryptography 的加密库来向上对TLS协议实现提供接口调用。Intel IPP专门针对Intel Multi-Buffer多缓冲区技术提供了一个子库Crypto Multi-buffer Library，该库基于Intel AVX-512 IFMA 指令提供了RSA、ECDSA、SM3、x25519多缓冲算法的优化版本。

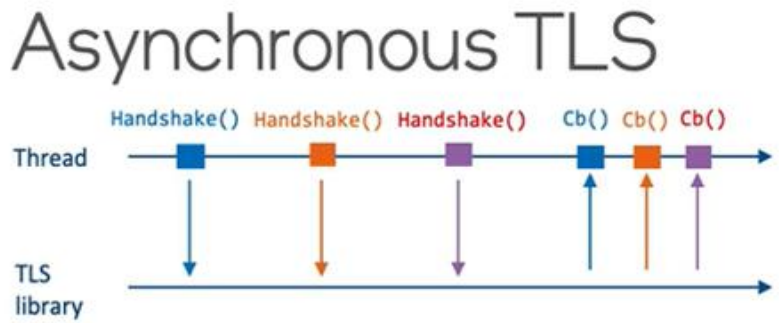
Envoy* and asynchronous handshakes

- Envoy uses BoringSSL as the default SSL library
- BoringSSL supports *private key methods* as a way to set custom callbacks, which are called when a certain cryptographic operation (such as RSA signing) is requested
- Envoy exposes access to these functions with a *private key provider framework*
- *Private key provider extensions* implement the functionality



英特尔 Envoy TLS加速方案及实践介绍





同步TLS握手调用会受到阻塞，直到握手完成为止，因此必须相应的将TLS握手阶段实现为异步模式，才能利用Intel Multi-Buffer多缓冲区技术的优势。

同时为了平衡Envoy中TLS握手处理吞吐量和时延的关系，我们还引入了计时器的变量进行控制，如图中Timer计时器。在TLS操作填满8个缓冲区或者Timer计时器触发两个条件满足其一时，当前缓冲的所有TLS操作将会被一次性处理。

数据面 Envoy CryptoMB Private Key Provider 配置 Envoy1.20

TLS configuration with just a private key.

```
tls_certificates:
  certificate_chain: { "filename": "/path/cert.pem" }
  private_key: { "filename": "/path/key.pem" }
```

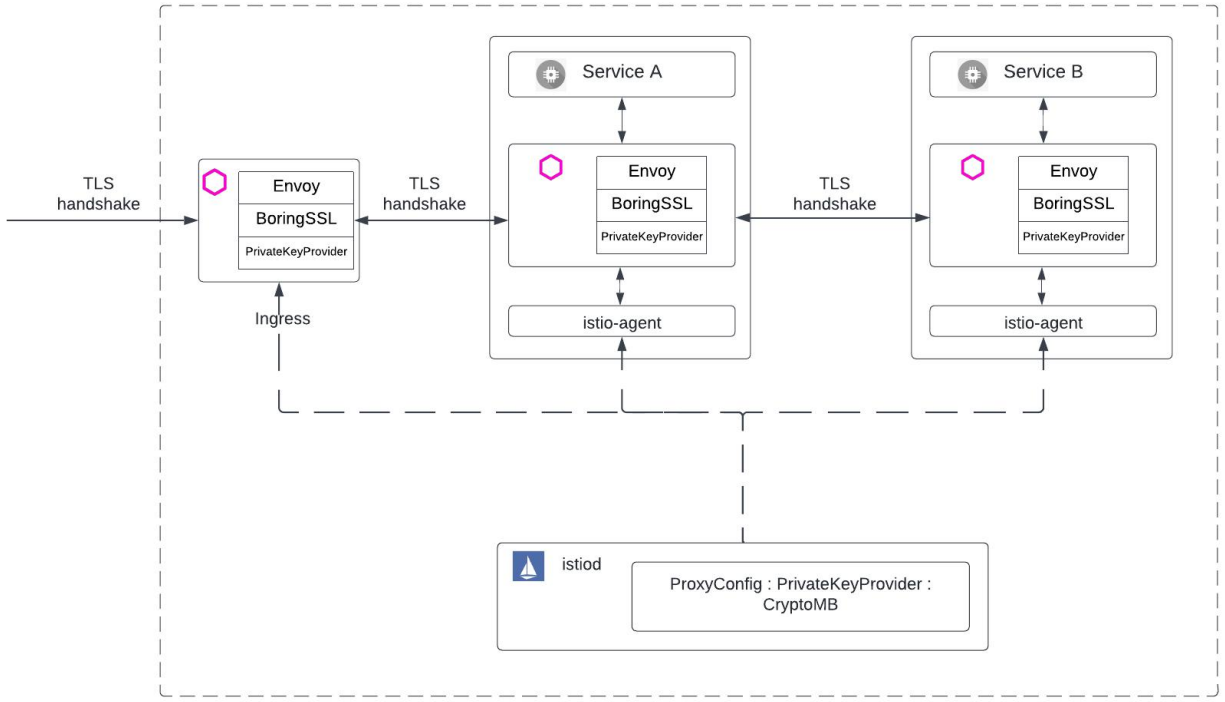
TLS configuration with CryptoMB private key provider.

```
tls_certificates:
  certificate_chain: { "filename": "/path/cert.pem" }
  private_key_provider:
    provider_name: cryptomb
    typed_config:
      "@type": type.googleapis.com/envoy.extensions.private_key_providers.cryptomb.v3alpha.CryptoMbPrivateKeyMethodConfig
      private_key: { "filename": "/path/key.pem" }
      poll_delay: 10ms
```

英特尔 Envoy TLS加速方案及实践介绍

SERVICE MESH SUMMIT 2022 服务网格峰会

控制面 Istio CryptoMB Private Key Provider 配置 Istio1.14 ： mesh wide configuration




```yaml
apiVersion: install.istio.io/v1alpha1
kind: IstioOperator
metadata:
  namespace: istio-system
  name: example-istiocontrolplane
spec:
  profile: demo
  components:
    egressGateways:
    - name: istio-egressgateway
      enabled: true
    ingressGateways:
    - name: istio-ingressgateway
      enabled: true
  meshConfig:
    defaultConfig:
      privateKeyProvider:
        cryptomb:
          pollDelay: 10ms
```

控制面 Istio CryptoMB Private Key Provider 配置： Gateways & Sidecar

```yaml
apiVersion: install.istio.io/v1alpha1
kind: IstioOperator
metadata:
  namespace: istio-system
  name: example-istiocontrolplane
spec:
  profile: demo
  components:
    egressGateways:
    - name: istio-egressgateway
      enabled: true
    ingressGateways:
    - name: istio-ingressgateway
      enabled: true
      k8s:
        podAnnotations:
          proxy.istio.io/config: |
            privateKeyProvider:
              cryptomb:
                pollDelay: 10ms
```

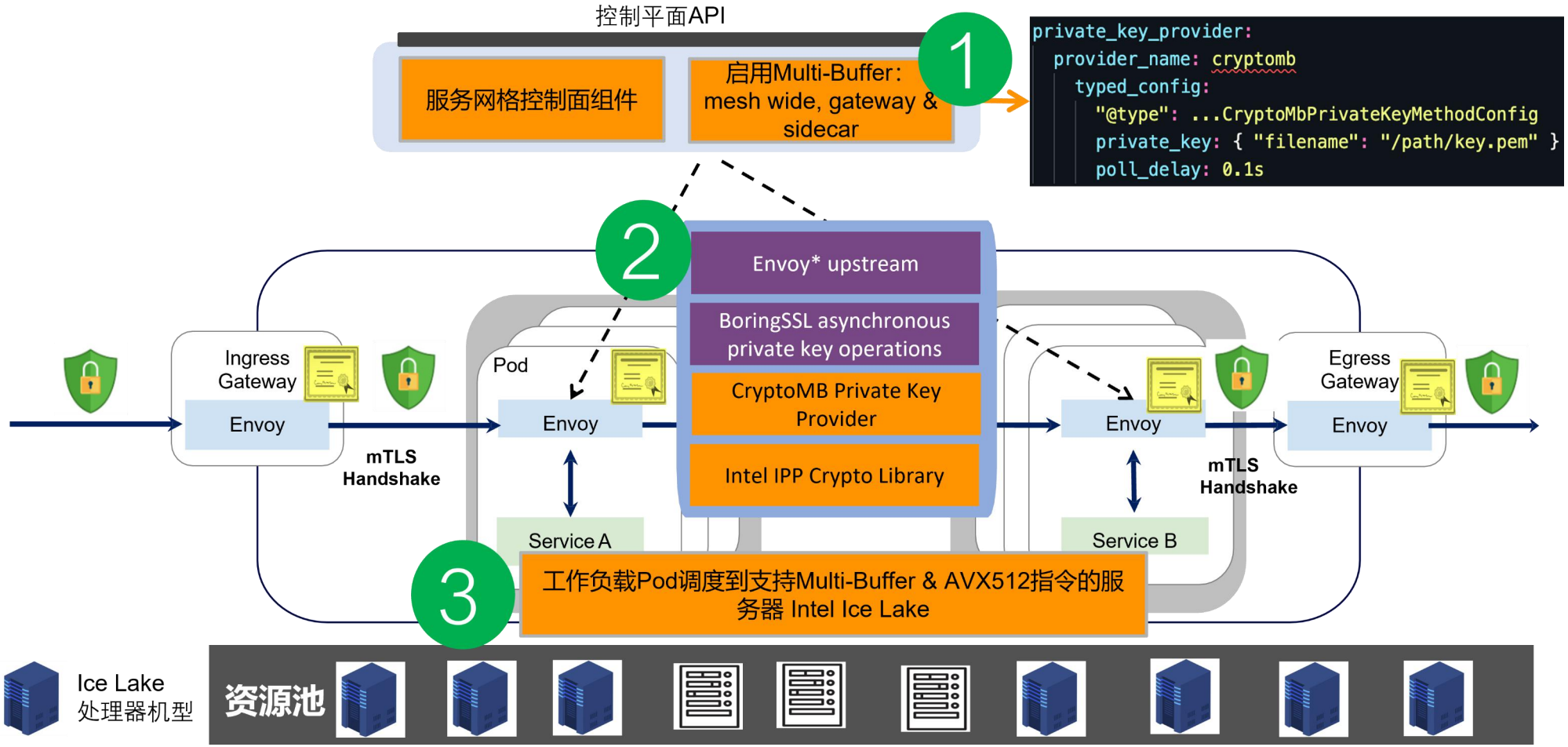
private key provider configuration for ingress gateway only

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: httpbin
spec:
  replicas: 1
  selector:
    matchLabels:
      app: httpbin
      version: v1
  template:
    metadata:
      labels:
        app: httpbin
        version: v1
      annotations:
        proxy.istio.io/config: |
          privateKeyProvider:
            cryptomb:
              pollDelay: 10ms
    spec:
      serviceAccountName: httpbin
      containers:
      - image: docker.io/kennethreitz/httpbin
        imagePullPolicy: IfNotPresent
```

private key provider configuration to application specific pods

英特尔 Envoy TLS加速方案及实践介绍

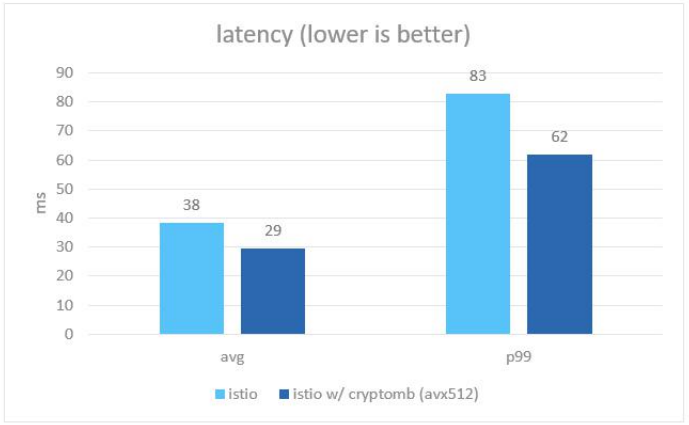
SERVICE MESH SUMMIT 2022 服务网格峰会



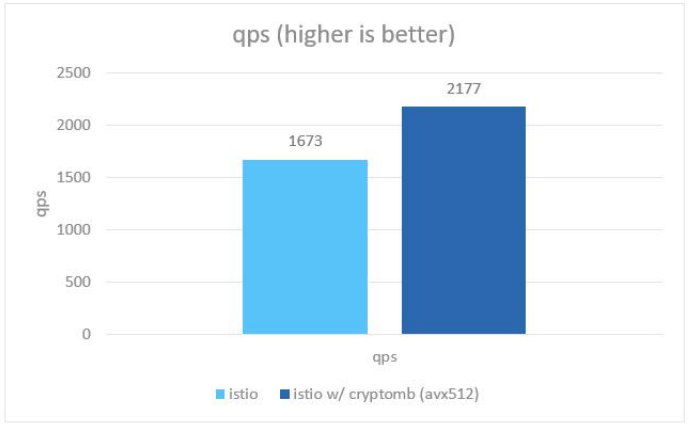
英特尔 Envoy TLS加速方案及实践介绍

SERVICE MESH SUMMIT 2022 服务网格峰会

“Istio” vs. “Istio with CryptoMB (AVX-512)”



23-25% improvement



30% improvement

https://istio.io/latest/blog/2022/cryptomb-privatekeyprovider/

- Azure AKS Kubernetes cluster
  - v1.21
  - Three-node cluster
  - Each node Standard_D4ds_v5: 3rd Generation Intel® Xeon® Platinum 8370C (Ice Lake), 4 vCPU, 16 GB memory
- Istio
  - 1.14-dev
  - Istio ingress gateway pod
    - resources.request.cpu: 2
    - resources.request.memory: 4 GB
    - resources.limits.cpu: 2
    - resources.limits.memory: 4 GB
- K6
  - loadimpact/k6:latest

英特尔 Envoy TLS加速方案及实践介绍

SERVICE MESH SUMMIT 2022
服务网格峰会

参考资料

- Crypto Acceleration: Enabling a Path to the Future of Computing
  https://newsroom.intel.com/articles/crypto-acceleration-enabling-path-future-computing/#gs.g58r5t
- Cryptography processing with 3rd gen Intel® Xeon® Scalable processors
  https://www.intel.cn/content/dam/www/central-libraries/us/en/documents/cryptography-processing-with-3rd-gen-intel-xeon-scalable-processors-19-may-2021.pdf
- Intel® Integrated Performance Primitives Cryptography - Crypto Multi-buffer Library
  https://github.com/intel/ipp-crypto/blob/develop/sources/ippcp/crypto_mb/Readme.md
- Demo showcase video:
  http://players.brightcove.net/2379864814001/default_default/index.html?videoId=6300380963001

开源实现

- CryptoMB provider is upstreamed to Envoy in the following PR:
  https://github.com/envoyproxy/envoy/pull/17826
- CryptoMB provider configuration is upstreamed to Istio in the following PRs(available in 1.14 release):

  https://github.com/istio/istio/pull/37681

  https://github.com/istio/api/pull/2261

  https://github.com/istio/proxy/pull/3752

SERVICE MESH
SUMMIT 2022
服务网格峰会

Thank you
谢谢

云原生社区
Cloud Native Community

活动由云原生社区主办