УДК 004
Chekushkin N.D. student of group 125м-24-1
Research supervisor: Shevtsova O.S. associate professor of department of software of computer systems
(Dnipro University of technology, Dnipro, Ukraine)

USING SERVICE MESH TO INCREASE THE LEVEL OF SECURITY IN MICROSERVICE ENVIRONMENTS

Microservice architecture has become the basis of modern distributed systems due to its ability to provide flexibility, scalability and simplified management of software components. However, this creates challenges in ensuring reliable protection of connections between services. Using Service Mesh helps solve these issues by automating traffic management and security. The article discusses the main aspects of Service Mesh, its key components, role in ensuring security, advantages for microservice environments, as well as the concept of Ambient Mesh as an ideological continuation of Service Mesh. Microservices architecture is the main paradigm for developing scalable applications in cloud environments. It allows you to break large monolithic programs into separate, independent services that communicate with each other using APIs. One of the most important aspects in such architectures is safe and reliable interaction between services. Standard network mechanisms do not always provide the necessary level of protection and traffic management. Service Mesh technology is actively used to solve these challenges.

Service Mesh is a specialized layer of infrastructure that automates network management and security between services in distributed systems[1-4]. Service Mesh acts as an intermediary, controlling traffic between microservices, providing routing, load balancing, traffic encryption, monitoring, and metrics collection capabilities. The main idea is to move the network logic out of the application, leaving programmers to focus on the business logic of the services. Service Mesh consists of two main components: Data Plane and Control Plane.

Data Plane: consists of proxy servers (most often Envoy), which are deployed together with each microservice in the form of sidecar containers. Control Plane: provides centralized management and coordination of proxy servers.

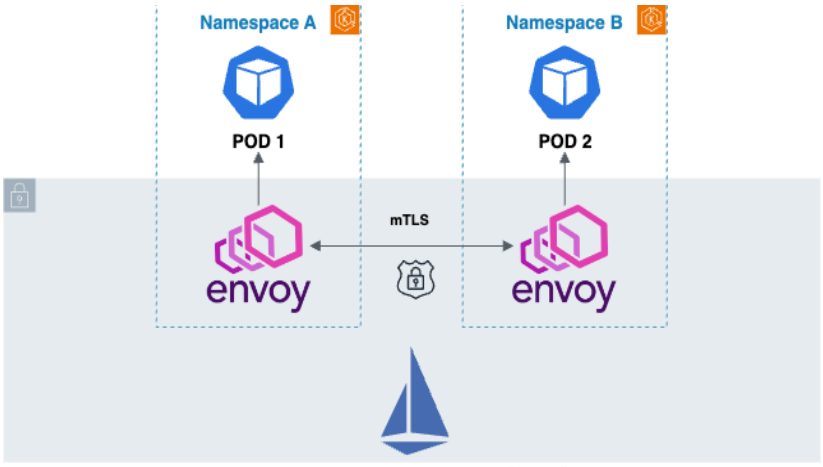

Fig. 1 Istio Service Mesh scheme

One of the most important aspects of using Service Mesh is to increase the level of security in microservice architectures. The traditional approach to security involves manually setting up secure communication channels between services. This complicates the process and can become a source of errors. Istio Service Mesh offers an automated security solution through:

1. Traffic encryption (mTLS)

Service Mesh supports encryption of traffic between all microservices using mutual TLS (mTLS). Every request between services is encrypted and authenticated, which guarantees protection against man-in-the-middle (MITM) attacks.

2. Authentication and authorization

Service Mesh allows you to apply authentication and authorization policies at the network level. For example, administrators can control which services can communicate with each other by setting authorization rules for each connection.

3. Monitoring and observability

With built-in monitoring mechanisms, Service Mesh provides detailed traffic information in real time, allowing you to identify potential problems or unauthorized access attempts.

4. Traffic management policies

Traditional approaches to security include using firewalls, VPNs, or individual configurations for each service. These methods have several disadvantages, such as complexity in setup, scalability, and increasing maintenance costs. Compared to these methods, Service Mesh provides a more flexible and automated solution that greatly simplifies the process of integrating security into scalable microservice environments.

Ambient Mesh is a new approach designed to further optimize and simplify the Service Mesh architecture. Ambient Mesh, first introduced in Istio version 1.19, eliminates the need to use a sidecar proxy in each pod, which significantly reduces resource consumption and simplifies network management. Ambient Mesh continues to use pod-level traffic encryption with Ztunnel, a zero trust/mTLS proxy that provides secure connections between microservices. This allows you to maintain a high level of security by isolating components and protecting them from unauthorized access.

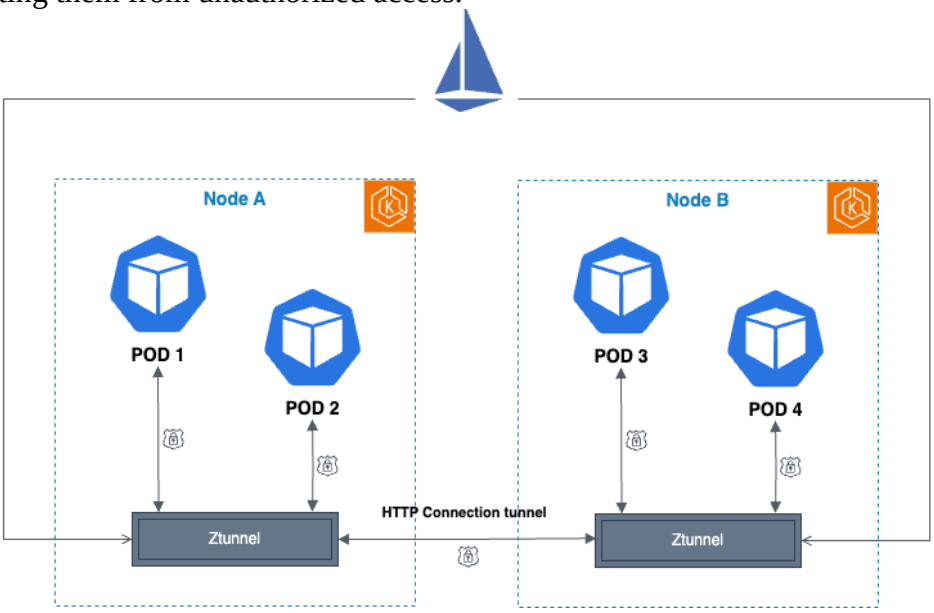

Fig. 2 Istio Ambient Mesh scheme

Flexibility of implementation: Ambient Mesh allows you to gradually add new features and implement improvements without having to update all services at once. This allows you to start with basic L4 capabilities, such as traffic encryption, and gradually add more sophisticated L7 features.

The implementation of Ambient Mesh in our team has shown a significant reduction in overhead costs for computing resources, in particular due to the elimination of sidecar proxies. At the same time, a high level of traffic security between microservices was maintained. Ambient Mesh also provided more flexible network management and simplified the process of introducing new features.

When using Service Mesh, after deploying and configuring the core Istio resources, you must add the “istio-injection=enabled” tag to all namespaces to be included in the Istio Service Mesh. After that, the pods should be rebooted so that the sidecar proxy is added to each pod in the specified namespace. One of the key drawbacks of traditional Service Mesh is

the need to have a copy of the sidecar proxy in each pod and in each namespace where the "istio-injection=enabled" tag is applied.

In turn, only two DaemonSets — Istio CNI and Ztunnel — need to be deployed for Istio Ambient Mesh to work. In addition, each namespace that is planned to be included in the mesh must have the tag "istio.io/dataplane-mode=ambient". Istio CNI is responsible for configuring traffic routing for components in the Istio Mesh and runs as a DaemonSet on each elevated node.

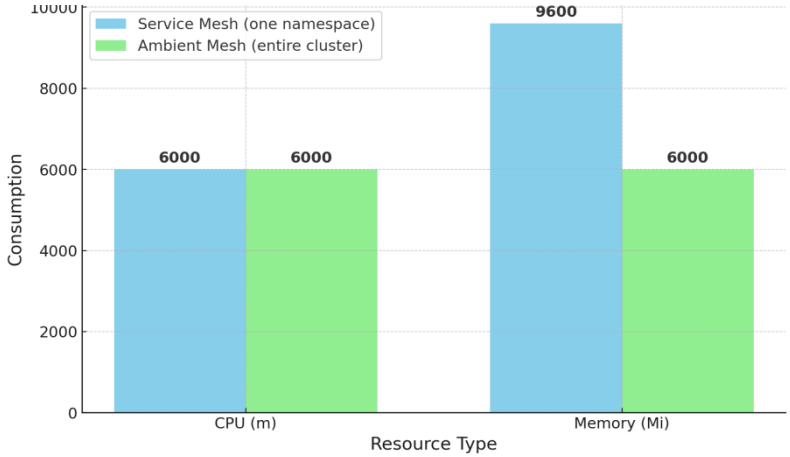

Fig. 3 Resource Consumption: Service Mesh vs Ambient Mesh

CONCLUSION

Using Service Mesh significantly increases the level of security in microservice environments thanks to centralized traffic management, automated encryption and authentication tools. Ambient Mesh as an ideological continuation of Service Mesh allows to further optimize the operation of the infrastructure, reducing overheads and simplifying the network architecture. This makes Ambient Mesh a promising solution for security and performance in today's cloud environments.

REFERENCE

1. OLISHEVSKYI I.H. Automated methodology of calculating parameters for non-traditional technology of heating mode of hydro-storage power plant station / OLISHEVSKYI I.H., GUSEV O.YU., OLISHEVSKYI H.S. // Електротехніка та електроенергетика. / Запорізький нац. ун-т «Запорізька політехніка». – Запоріжжя, 2023. – № 1. – С. 36-42. https://doi.org/10.15588/1607-6761-2023-1-4

2. OLISHEVSKYI I.H. (2024). DATAWARE AND SOFTWARE OF THE AUTOMATED TECHNOLOGY FOR COMPUTER-INTEGRATED CONTROL OF HEAT PUMP SYSTEMS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (2), 205–212. https://doi.org/10.31891/2219-9365-2024-78-23

3. OLISHEVSKYI I.H. (2024). RESULTS OF DEVELOPMENT AND RESEARCH OF THE TECHNOLOGY FOR AUTOMATED ENERGY-EFFICIENT CONTROL OF HEAT PUMP SYSTEMS BY MEANS OF COMPUTER EXPERIMENT. Herald of Khmelnytskyi National University. Technical Sciences, 335(3(1), 419-428. https://doi.org/10.31891/2307-5732-2024-335-3-58

4. Khabarlak, K. S. (2022). FASTER OPTIMIZATION-BASED META-LEARNING ADAPTATION PHASE. Radio Electronics, Computer Science, Control, (1), 82. https://doi.org/10.15588/1607-3274-2022-1-10