As applications move to microservices-based architectures, adoption of containers and Kubernetes has increased. There is strong growth in usage of these technologies across public and private clouds as well as data centers. As these applications get deployed in production and achieve scale, traditional tools are not a fit for Kubernetes. Demand for enterprise-grade and Kubernetes-specific solutions is growing for all application services including application delivery and security. A10 Secure Service Mesh is a purpose-built solution to address these needs and provides advanced application load balancing and traffic management, integrated security, traffic analytics and actionable insights for microservices deployed in Kubernetes environments.

**The Challenge**
Successfully managing applications within Kubernetes environments calls for a new, unified solution that addresses the following key challenges:

1. Providing security and policy enforcement for microservices.
2. Providing deep visibility and insightful analytics needed to keep microservices running optimally.
3. Offering “smart” load balancing and traffic management to ensure consistent availability of container-based workloads.

**Challenge**
When microservices-based applications are deployed in Kubernetes, visibility and security for East-West traffic becomes a prime concern. Legacy solutions addressing these challenges in other environments don’t work well in Kubernetes because of its unique architecture.

**Solution**
A10’s Secure Service Mesh solution provides an easy, automated way to integrate enterprise-grade security and load-balancing/traffic management with comprehensive application visibility and analytics—all with no change to applications, and across their entire lifecycle.

**Benefits**
- Improve traffic management and simplify operations
- Increase security using traffic micro-segmentation and isolation of microservices from one another
- Automatically encrypt traffic between microservices across nodes
- Offload service discovery from individual microservices to central load balancer
- Gain actionable insights for increasing IT agility
A10 Secure Service Mesh Solution

A10 Secure Service Mesh is purpose-built to serve modern microservices and container-based applications. The unified solution offers a highly scalable, software-defined distributed architecture incorporating three key components: A10 Lightning ADC, A10 Kubernetes Connector, and A10 Harmony Controller.

The architecture allows Lightning ADC—the data-plane element—to be lightweight and deployed within Kubernetes environment, while the Harmony Controller handles management functionality. Working with the Ingress Resource, the A10 Kubernetes Connector automatically creates an application using Harmony’s APIs. It also creates load balancing and content-switching rules, configures application delivery and security policies, and attaches the application to Lightning ADC clusters. Kubernetes Connector also monitors application service containers and communicates any change to Lightning ADC via Harmony Controller keeping ADC configuration and infrastructure always in synchronization.

Features and Benefits

Elastic Scaling

Lightning ADC is deployed as Kubernetes Daemonset. As traffic grows and additional nodes are added to the Kubernetes cluster, the A10 Lightning ADC cluster automatically grows with it. New ADC instances automatically interface with the Harmony Controller to get configuration information and are ready to handle traffic without requiring any manual configuration.

Automatic Service Discovery

Kubernetes provides easy ways to scale of nodes, pods, services etc. In addition, it keeps on monitoring the running containers and replaces them with new one in case a container is found faulty. Because of these, IP address of the service containers keep changing. This dynamic environment is a problem for application services when they want to communicate to each other but don’t know current set of IP addresses where service is running.

Secure Service Mesh automatically tracks changing IP addresses of microservices in dynamic Kubernetes environment and facilitate easy communication between microservices.
Micro-segmentation and Secure Traffic between Microservices

Lightning ADC can be configured to intercept traffic flowing between microservices (aka East-West traffic). Once traffic starts passing through the Lightning ADC, appropriate security policies—configured for the micro-segment—are applied to the traffic. Micro-segmentation allows isolation of microservices from one another and secure them individually. It is aimed at making security more granular. As the IP addresses of application service containers can change automatically over time, access policy is based on service labels rather than IP addresses.

Automatic Encryption of Traffic Between Nodes

The solution automatically encrypts traffic when it is leaving a node boundary and decrypts it on target nodes before it is delivered to a microservice, enabling enhanced SSL security without having to make any changes in application.

Centralized Application Management and API-driven Automation

In an elastic and distributed environment like Kubernetes, managing ADCs separately is a major challenge. With the Harmony Controller, maintaining configurations is easy because the controller allows to define configuration at logical application level and intelligently pushes it to appropriate ADC instances. Additionally, all the management as well as analytics functions are exposed via REST APIs called Harmony APIs. This allows high degree of automation for optimizing the application delivery functions.

Per-service Analytics & Insights

In traditional ADC environments, there is little or no visibility into traffic at the application layer, making it difficult to collect data needed to troubleshoot issues. A10 ADCs collect metrics in real-time and push them to an analytics engine that delivers actionable insights, giving users intelligence to fine-tune their applications and infrastructure and enabling faster troubleshooting.
Solution Components

How it Works

A10 Lightning ADC

- Provides innovative Layer 4-7 capabilities, including traffic management, advanced elastic load-balancing, and security and analytics for micro-services deployed in Kubernetes
- Allows micro-segmentation of traffic and granular policy application for North-South as well as East-West traffic
- Supports Blue-Green/Canary deployments for CI/CD application environments
- Increases operational efficiency and reduces cumbersome tasks and risk

A10 Harmony Controller

- Provides management, orchestration and analytics for secure application services in multi-cloud environments
- Collects, analyzes, and reports on traffic flowing through ADCs and provides per-service visibility, analytics, and alerts
- Enables IT to automate the deployment and operations of application services, and thereby increase operational agility, simplify the management of distributed services, shorten troubleshooting times, and reduce TCO

A10 Kubernetes Connector

- Monitors application service containers and Ingress Resources, and in the event of any changes, informs the Harmony Controller to instantly synch up with Lightning ADC
The Ultimate Application Delivery and Security for Applications Deployed in Kubernetes Environments

In addition to operational simplicity, superior microservice performance, and detailed visibility and analytics of all application traffic, A10 Secure Service Mesh offers application layer security for applications deployed in Kubernetes. The security capabilities take care of both North-South and East-West traffic. Actionable insights and excellent troubleshooting capabilities minimize the burden of application delivery administration in Kubernetes environments.

Next Steps
To find out more about the A10 Secure Service Mesh solution, request a free trial of Lightning ADC and let us know you are looking for solutions for your Kubernetes environment.

About A10 Networks
A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit: a10networks.com or tweet @a10networks