citrix

Solution Brief

Secure your Microservices-based Applications with Citrix ADC

Microservice architecture describes a particular way of designing applications where the functionality of the traditional, large monolithic block of code is distributed among independent microservices. This methodology brings many benefits to business—quicker time to market, faster innovation, better response to change, easier scalability and the portability to deploy anywhere. As with all applications, however, there is still a need to ensure microservices are secured. This includes the microservices themselves and both their internal and external communications.

Understanding Microservice Security Needs

In microservices-based applications, two types of traffic must be protected. Traffic into the application (North-South traffic) and traffic among the microservices themselves (East-West traffic).

Many of the same security challenges that are present with monolithic applications exist in microservices-based applications, especially with N-S traffic.

- Access to the application needs to be controlled
- Requests need to be checked for unwanted bot traffic and application attacks
- Traffic needs to be guided to the right resources to be processed
- Traffic needs to be encrypted to protect the data in transit

Inter-microservice traffic (East-West traffic) often requires similar protections (authentication, encryption, inspection), predominantly to ensure that only authorized applications and microservices can interact. Further, the ephemeral nature of the microservices environment means that the security must be dynamic and has to be automatically updated as things change. Securing the microservices also means fitting in with the different cluster deployment architectures, such as service mesh.

Citrix Application Delivery Controller (ADC) helps you secure and deliver your microservices-based applications. It is designed to fit into your microservices ecosystem to help you develop, deploy and deliver

applications quickly and securely. With a rich set of integrated security features, including web application firewall (WAF), bot mitigation, SSL termination and API gateway functionality, it provides comprehensive protection from Layer 3-7 to your applications. Citrix Application Delivery Controller (ADC) comes in multiple form factors, including a containerised and public cloud version, to protect all your application types and the communications between them, wherever they are deployed.

Consistent Security Posture

Citrix ADC is designed to enable you to provide a consistent security posture across all your applications. The multiple form factors and single code base of Citrix ADC mean that the same security policies can be used to protect your traditional monolithic application and microservices-based application. This ensures that you always follow your corporate security best practices, while reducing the operational overhead of deploying, managing and monitoring different security devices. You can easily migrate applications to a new environment with the correct levels of associated security. Most importantly, it helps you ensure that you minimize security errors during deployment.

Protect North-South Traffic

Citrix ADC is an industry-leading ADC that protects your microservices by acting as an ingress proxy. As an ingress proxy, it will intercept and inspect your north-south traffic as it enters your Kubernetes cluster.

Citrix ADC offers comprehensive Layer 3-7 security. An advanced suite of SSL/TLS termination capabilities enable you to decrypt and inspect traffic inbound to your application. The bot management module enables you to detect and defend against the automated attacks and infrastructure strain that bots can cause. The integrated web application firewall (WAF) protects your microservices-based application's front end from known and unknown (zero-day) attacks, including the OWASP top 10 most critical attacks (SQL Injection attacks, cross-site scripting, etc.) Citrix ADC also acts as an API gateway for your N-S API traffic. It will enforce security measures on API calls like IP white listing/blacklisting, authentication, content routing, rate limiting and more.

The consolidated approach means that it will secure and manage your traffic in a single pass for better performance, lower complexity and lower TCO.

Figure 1: Citrix ADC protects microservices-based applications in many ways

Protect E-W Traffic

Communication and requests among microservices need to be secured. To ensure that microservices only communicate with other allowed microservices, the API calls need to be authenticated. Similarly, to prevent the traffic being read by unauthorised entities and stop man-in-the-middle attacks, it is the best practice to encrypt it end to end. To prevent an individual microservice being overwhelmed with requests and being taken offline, API calls need to be rate limited.

Citrix ADC is available in a container form factor, CPX, and can be deployed in your microservice cluster to secure communications between you microservices. It can be deployed as a sidecar proxy in service mesh architectures or as an aggregation proxy, through which all your east-west traffic flows, in service mesh-lite architectures.

Because Citrix ADC CPX acts as a proxy between your microservices, it enables you to enforce your E-W security policies. Citrix ADC can enforce mutual TLS authentication between pairs of microservices to ensure that each communication is allowed and tracked.

Limits can be defined and enforced for the rate of APIs requests for each microservice. The Citrix ADC also enables you to enforce encryption policies on your microservices E-W traffic to prevent sniffing and altering of your API requests or the responses.

By proxying all your E-W traffic and securing the communications with a Citrix ADC device, you remove the burden of writing all of the security into each individual microservice. This makes the coding simpler and, because the security is handled separately, it minimizes security errors during code updates.

Integration with Istio Open Source Control Plane

Istio is a popular open source control plane for service mesh architectures. As a control plane device, Istio enables you to define your traffic policies—for routing and security for example—in one place and then push these as configurations to suitable data plane devices, like Citrix ADC, for enforcement. Istio also acts as a central point for tracing, monitoring and logging of events in your service mesh.

Citrix ADC integrates with Istio as a data plane enforcement device. It listens for security configuration changes and implements them on the relevant devices. Citrix ADC can be deployed as an Istio gateway and act as an ingress proxy for traffic into your microservices cluster. You can use a physical (MPX/SDX) or virtual Citrix ADC as a gateway device outside the cluster or even an containerised version (CPX) as a pod inside the cluster. This provides you the flexibility you need to make architectural design choices to suit your microservices environments.

Citrix CPX can also be deployed as a sidecar to applications pods. This allows you to intercept traffic among the microservices and apply security policies. Citrix CPX integrates with Istio as a sidecar and enforces the security polies defined in it. For example, it is possible to define mutual TLS authentication policies in Istio and enforce them with the Citrix CPX.

Offload Select Security Functions to Sidecars

Additional security workloads can be offloaded to Citrix ADC when deployed as a sidecar.

Things like mutual TLS authentication and circuit breaking can be handled independently of the microservices themselves. The removal of these functions means that you don't need to build the functionality multiple times into your microservices code. This creates a simpler, more consistent codebase that is easier to manage and update and minimizes security errors.

Moreover, this process can be automated. With Istio Citadel for example, managing and controlling the SSL/TLS certificates, Citrix has created an adaptor that checks for updated certificates and retrieve and install them on the ADC automatically.

Protect APIs

Citrix ADC has integrated API gateway functionality to protect the communications among your microservices and between your applications and the outside world.

Because Citrix ADC sees all the API calls, it can inspect and enforce authentication, authorization, encryption and content routing, as well as IP address access controls and rate limiting for all the APIs. This will protect your application communications and keep it compliant with your defined standards.

Troubleshoot Faster

Citrix Application Delivery Management (ADM) collates telemetry from all your ADCs and uses AI and machine learning techniques to provide detailed insights for all of the security functionalities—WAF, bot management, APIs and SSL. This makes it easier to understand the threat your applications face and enables you to react more quickly to remediate security issues.

You are able to see immediately the number and type of violations your applications are facing with IP address and geolocation details on their origins. This will help you assess your security posture and start your remediations more quickly. Citrix ADM even lets you know which applications are under the most threat so that you can prioritize your response accordingly.

You can monitor the security of your APIs with Citrix ADM. For example, you can track the authentication success and failure rates to determine if your applications are under attack. Similarly, you can monitor the TLS protocols, ciphers and key-strengths used.

By bringing all the security telemetry from your multi-cloud environment into a single place, you can get holistic visibility and analytics across your applications.

The interactive nature of the Citrix ADM dashboard enables you to drill down into the different violations and determine which remediations are required quickly.

The Citrix application delivery portfolio—Citrix ADC and ADM—is designed to ensure that you have the detection and enforcement technologies required to protect your microservices-based applications.

Flexible Options for Microservice Protection Across Multi-cloud

Microservice protection is available as part of the Citrix ADC offering and is included with the Premium edition license. Citrix ADC is available in multiple form factors and on the major public clouds (AWS, Azure, GCP) to suit your deployment needs. The single code base enables you to maintain operational consistency across your deployments and applications. The single license approach, which includes security features including WAF, bot mitigation and API protection, brings simplicity and reduces TCO. Keeping it simple lets you keep it secure.

citrix

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States