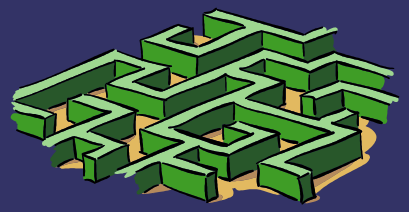
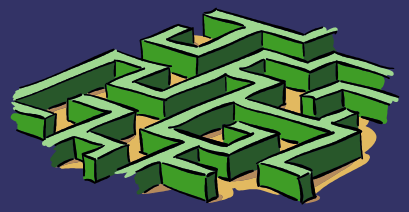
Api Gateway Security Best Practice

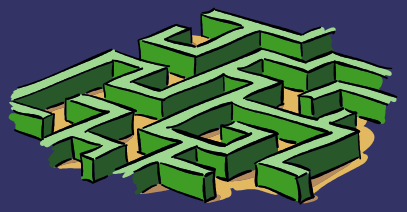


Agenda

- Api Security 101
- All About Api Gateways
- Tips for improving Api Gateways Security
- Api Gateway Implementation walk through

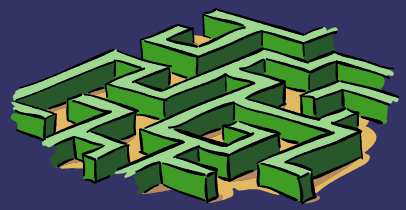


Rajendra shahi
Researcher @Urja Security



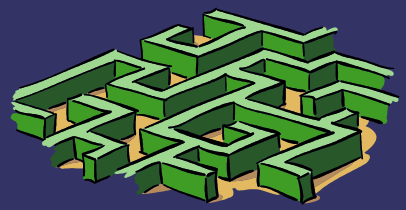
API Security

- Api security is the process of effectively securing APIs owned by the organization and external APIs used by implementating API-specific security strategies.APIs security secures API vulnerability/Misconfigurations and prevents their exploitation by attackers.



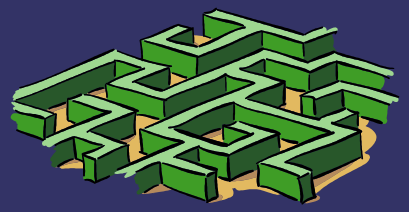
Safety and Security Matters

- „94% of API developers have experienced security problems in production APIs over the past year with 17% habing experienced an API related breach“.(State of API security Q1 Report 2023)
- „78% of cybersecurity professionals have faced an Api security incident in the past years“ (Hacker News,API security Trends 2023)
- „More than half a billion records have already been exosed via vulnerable APIs, and 2023 is on track to be a record-high year for API breaches“ (May 2023 report Firetail)
- According to Gartner,“90% of web enabled applications will have more attack surface area in exposed APIs rather than in the user interface“



Benefits of Strong APIs Security

- Better developer experience overall
- Greater room for innovation
- Increased standardization of your full API program
- Better Trust and assurance built with customers and community
- Less rom for breaches,hackers and issues
- More $$ at the end of the year

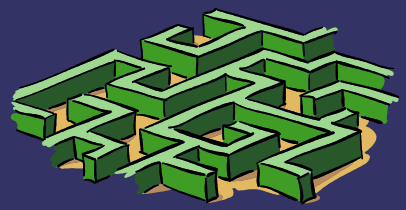


Quizes

- What Percentage of web enabled applications have more attack surface area in exposed APIs rather than in the user interface ?
- → 90%
- 2023 was on track to be a record-high year for what ?
- → API security breaches
- How would you define API security?
- → As given in the above lessons(ALL)
- What have 78% of cybersecurity professionals faced in the past year?
- → An API security incident
- Which of the following are the benefits of improved API security ?
- → Better developer experience & greater room for innovation and Increase standardization & better trust assurance built with customers

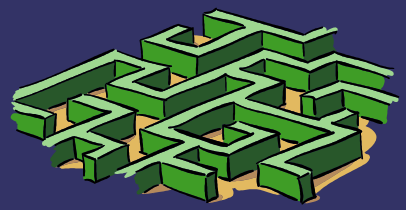
API Gateway

- An intermediary between client applications and backend services architecture
- A software layer that consolidates multiples multiple APIs into a single endpoint
- Provide centralized control, allowing developers to focus on building individual services



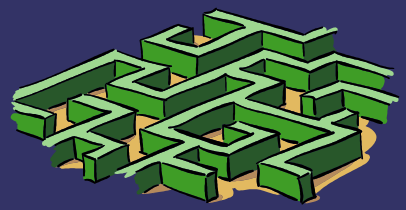
Traffic Management and Routing

- API Gateways distribute incoming requests to the most suitable microservices based on predefined rules and conditions.
- This helps to :
- Ensure your application resources are used efficiently
- Prevent bottleneck
- Provides load balancing capabilities by evenly distrbuting requests accrosss multiple instances of services
- Improve reliability and scalability
- Enhance the user experience & scaling



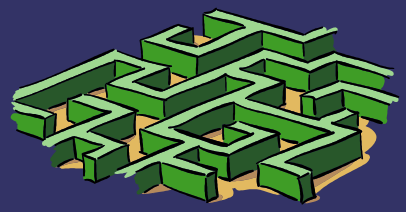
Authentication

- Authentication verifies user or application identify,safeguarding against unauthorized access and enabling accountability
- Api gateway authentication safeguards your systems and information against unwanted access,data breaches,hacks and mistakes
- Gateways establish a secure ecosystem to safeguard the integrity and confidentiality of transmitted data
- Establish clear boundaries between sensitive user data,authentication credentials and valuable resources



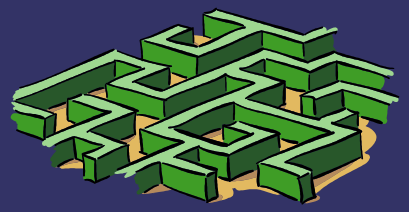
Authorization

- Authorization ensures that authenticated users inly access permitted resources and actions,protecting data integrity and enforcing business rules
- These security measures are essential for preventing breaches,complying with regulations and maintaining user's trust making them integral to the success and reliability of the application.



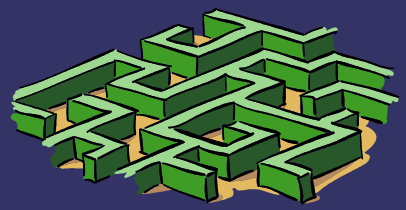
Rate Limiting

- Rate limiting acts as a safeguard,ensuring that regardless of how you scale your services remain protected and operate within their intended capacity limits.
- This in turn:
- Enhance the stability and reliability of your applications
- Ensure fair resource allocation among clients,promoting a positive user experience and efficient resource utilization
- For thse utilization kubernetes,rate limiting becomes even morer improtant. Kubernetes enables dynamic scaling of containers and microservices to handle varying workloads.

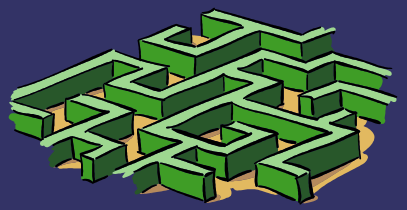


Logging & Monitoring

- Logging and Monitoring lets you gain insights into API traffic and errors .Tracking active requests and traffic patterns helps you anticipate scalling needs and resource allocation,ensuring that your system can handle fluctuations in usage without degradation in performance.
- The four Golden Signals
- Latency
- Traffic
- Errors
- Saturation



What role do they play in the API lifecycle?

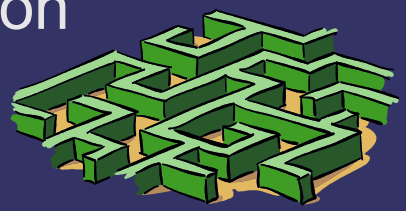


Types of API Gateways

- General API Gateways
- → Options
- Kong
- Gloo
- Gravitee
- Apigee
- Tyk
- → Pros
- Full suite offerings
- Widely ised
- More versatile
- → Cons
- Lesss sca;ab;e
- More expensive
- More plugins needed
- More manual configuration

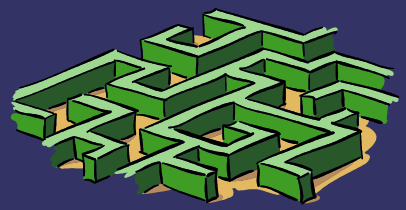
Kubernetes-specific Options

- → options
- Edge stack
- Traefik
- Istio
- → Pros
- More scalable
- Kubernetes-friendly
- Less plugins
- → Cons
- If your orgs uses multiple environment or plans to migrate away from kubernetes.
- Integrating a kubernetes-specific APU gateway with non-kubernetes components or external systems might be more challenging than using a more generic solution



Open source options

- → Options
- Emssary Ingress
- Kong Gateway OSS
- Tyk OSS
- Kraken D
- Gravitee OSS
- → Pros
- Free
- Better for teams who donot need additional security and auth built out
- Customizable potential
- → Cons
- Not as heavily maintained or strongly supported
- Limited capabilities and features
- Lots of manual configuration

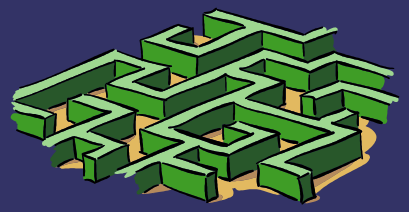


Point to be Noted

- Ask yourself
- Is your gateway going to be a part of a full API solution or a singlar specialized tool that you add on to your tech stack?

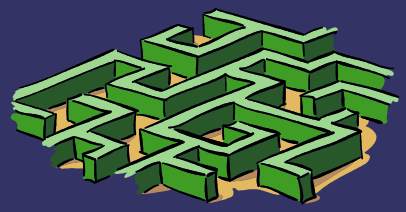
Tips for Better API Gateways

- Use HTTPS communication
- Leverage Serverless functions
- Use a centralized Authentication server
- Limit requests
- Maintain regularly
- Implement Monitoring and Analytics
- Implemented API-led connectivity
- Manage Deprecated APIs



In the end you need an API Gateway for:

- Improves security
- Better standardization & centralization
- Enhanced developer experience
- More scalability



Additional resources to level up Your API security

- APISec university
- Ambassador Labs Blog
- 2023 state of API security
- OWASP API security project