CLOUDNATIVE SECURITYCON

NORTH AMERICA 2023

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Securing user to server access in Kubernetes

Maisem Ali & Maya Kaczorowski

@maisem_ali, @MayaKaczorowski

@maisem@inuh.net, @MayaKaczorowski@infosec.exchange

Maisem Ali
Member of Technical Staff
he/him

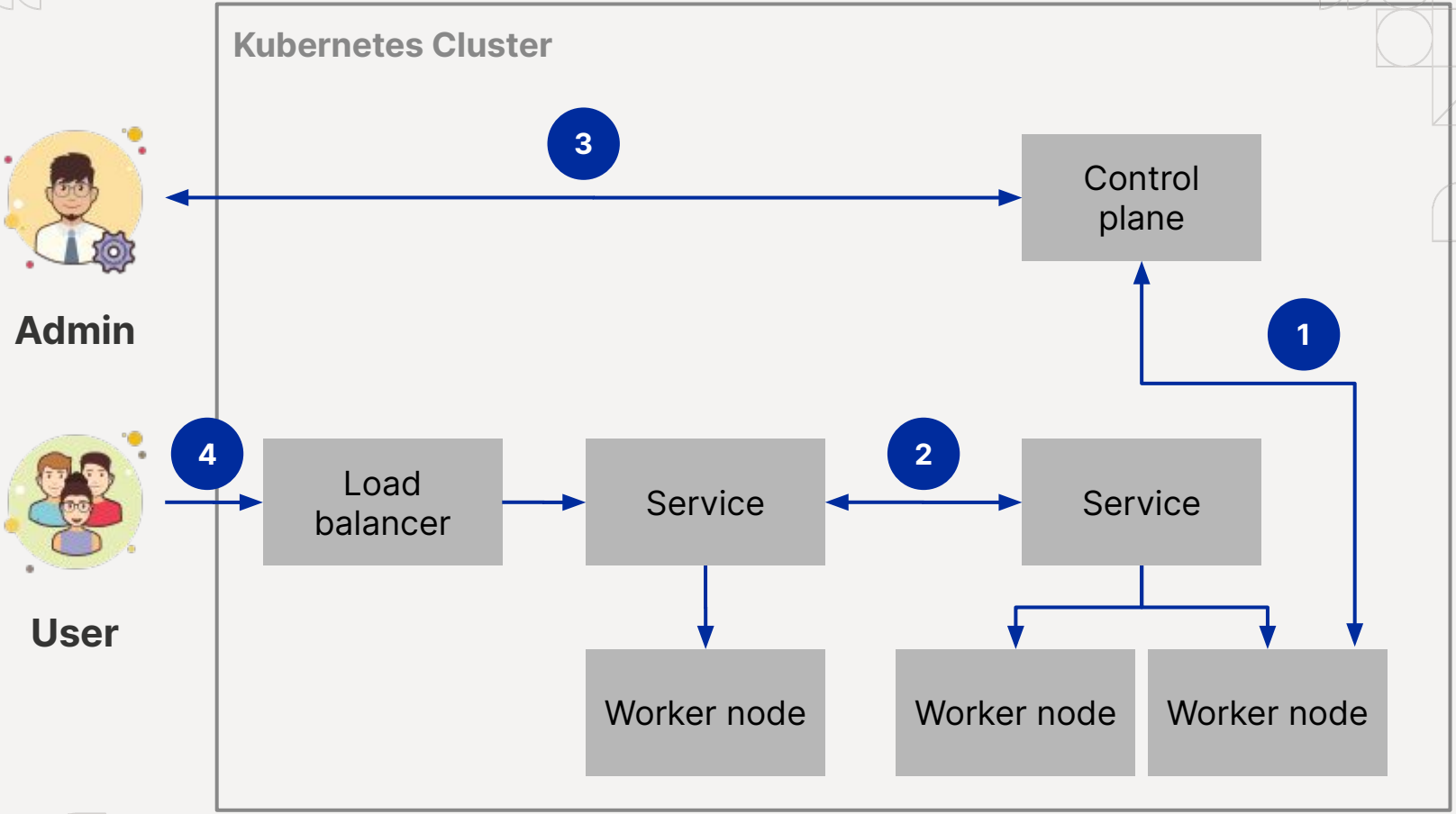
Maya Kaczorowski
Head of Product
she/her

tailscale

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Agenda

- Kubernetes traffic and use cases
- User access to internal services
  - Security properties you want
  - What options you have
  - How these options stack up
- Summary


Kubernetes Cluster
3
Control plane
Admin
1
4
Load balancer
Service
2
Service
User
Worker node
Worker node
Worker node

Kubernetes cluster traffic

Traffic	Typical security
Traffic **between the components of Kubernetes** https://www.youtube.com/watch?v=bXnVI_hUAbk	**Batteries included**
Traffic from a **service** to a **service**	**Service mesh**
Traffic from a **user** to the **Kubernetes control plane**	**Bastion**
Traffic from **a user** to a **service** • Public service • Internal service	**Load balancer** **?**

But does it do its own authentication?

You have several options for connecting to nodes, pods and services from outside the cluster:

- Access services through public IPs.
  - Use a service with type `NodePort` or `LoadBalancer` to make the service reachable outside the cluster. See the services and kubectl expose documentation.
  - Depending on your cluster environment, this may only expose the service to your corporate network, or it may expose it to the internet. Think about whether the service being exposed is secure. Does it do its own authentication?

https://kubernetes.io/docs/tasks/access-application-cluster/access-cluster-services/

Internal services you can run on Kubernetes

- Tools run alongside your service
  - Databases: Postgres
  - Monitoring, logging and tracing: Grafana, Prometheus
  - BI: Metabase
- Internal applications

Security properties for internal services

Visibility: the service isn’t publicly accessible

Authentication: verify the user connecting to the service

Authorization: only the right user can access the service

Encryption: if traffic is intercepted, it’s still protected

Load balancing: share traffic between multiple instances

Traffic filtering: limit traffic flows

Auditability: monitor and log traffic flows

@maisem_ali @MayaKaczorowski

Options to consider

- Kubernetes cluster service
- Kubernetes load balancer
- Kubernetes Ingress
- Kubernetes network policy
- Service mesh
- Bastion
- IPsec
- WireGuard

Kubernetes Cluster Services


Visibility


Authentication


Authorization


Encryption


Load balancing


Traffic filtering


Auditability

- Exposes pods inside a cluster as single addressable unit
- Load balances across replicas of a pod
- Only reachable from inside the cluster
- BYO encryption, authentication and authorization
- No traffic filtering

@maisem_ali @MayaKaczorowski

Kubernetes load balancers


Visibility


Authentication


Authorization


Encryption


Load balancing


Traffic filtering


Auditability

- Exposes pods inside a cluster as single addressable unit
- Load balances across replicas of a pod
- Publicly reachable
- BYO encryption, authentication and authorization
- cloud provider may allow traffic filtering at the infrastructure layer

Kubernetes Ingress

- Visibility
- Authentication
- Authorization
- Encryption
- Load balancing
- Traffic filtering
- Auditability

- (everything that cluster IP gives you, plus)
- Provides L7 HTTP load balancing
- TLS Encryption
- Targets ClusterIP services

https://kubernetes.io/docs/concepts/services-networking/ingress/

Kubernetes Network Policy


Visibility


Authentication


Authorization


Encryption


Load balancing


Traffic filtering


Auditability

- Restricts network access to pods and services
- Only provides L3/L4 filtering
- Can be paired with LoadBalancers to restrict which external IPs can access services

Service mesh


Visibility


Authentication


Authorization


Encryption


Load balancing


Traffic filtering


Auditability

- Uses a sidecar proxy
- Provides authentication and e2e encryption between services using mTLS
- Load Balances among service instances
- Provide observability via metrics, tracing and logging

Bastion


Visibility


Authentication


Authorization


Encryption


Load balancing


Traffic filtering


Auditability

- Point of entry to your network through your firewall
- Typically OpenSSH running on a host
- Gives you a single place where you can enforce access policies
- Sits on the public web
- Authentication and authorization based on SSH username/password, keys, or certs

IPsec & IPsec-based VPN


Visibility


Authentication


Authorization


Encryption


Load balancing


Traffic filtering


Auditability

- Layer 3 encryption protocol between two IPs
- Just a protocol, so you are probably using it as part of an IPsec-based VPN
- IPsec provides authentication and encryption
- VPN should provide authorization and logs
- VPN concentrator might allow you to manage traffic

WireGuard & WireGuard-based VPN


Visibility


Authentication


Authorization


Encryption


Load balancing

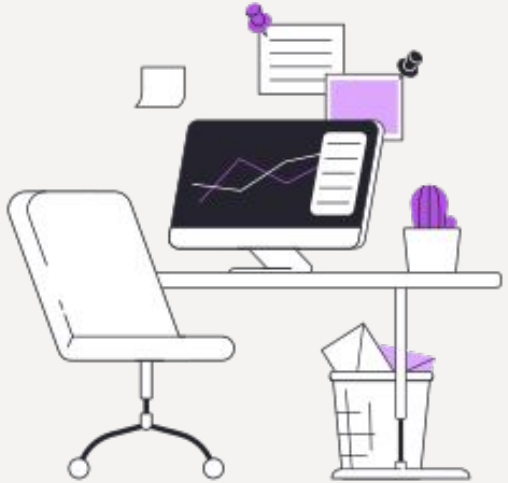

Traffic filtering


Auditability

- Layer 3 encryption protocol between two peers, identified by their public keys
- Compared to IPsec, less configuration thanks to opinionated cryptography
- WireGuard provides authentication and encryption
- VPN should provide authorization and logs
- VPN concentrator might allow you to manage traffic

Demo: connect to an internal application running in a cluster using Tailscale

- Set up Tailscale for a service running in a Kubernetes cluster using LoadBalancer type
- Connect to the service directly using its service name
- Expose the service to the wider internet using Tailscale Funnel



	Kubernetes load balancer	Kubernetes Ingress	Kubernetes Network Policy	Service mesh	Bastion	IPsec	IPsec-based VPN	WireGuard	WireGuard-based VPN
Visibility				✓					✓
Authentication				✓	✓	✓	✓	✓	✓
Authorization				✓	✓		✓		✓
Encryption		✓		✓	✓	✓	✓	✓	✓
Load balancing	✓	✓	✓	✓			✓		✓
Traffic filtering			✓	✓			✓		✓
Auditability				✓	✓		✓		✓

@maisem_ali @MayaKaczorowski

Learn more

Accessing services run on clusters:
https://kubernetes.io/docs/tasks/access-application-cluster/access-cluster-services/

Tailscale Kubernetes operator:
https://tailscale.com/kb/1236/kubernetes-operator/

Get these slides: bit.ly/3wH2IFT

Please scan the QR Code above
to leave feedback on this session