

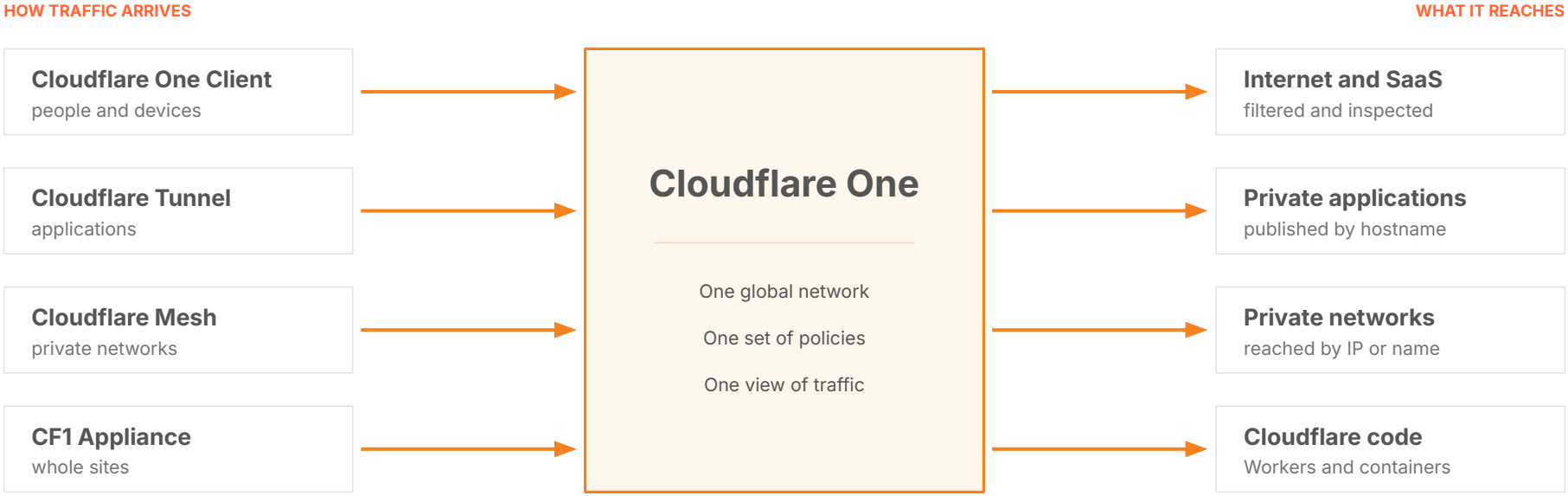
System sketch:

Understanding and architecting Cloudflare on-ramps and off-ramps

Nikita Cano
Senior Product Manager
Cloudflare

CLOUDFLARE

Connect once. Cloudflare does the rest.



Choose the connector that matches what you are connecting.

CLOUDFLARE

Two headline products, two specialists

TUNNEL

Publish an application

Public HTTP/S traffic to a private origin.

cloudflared connects out. No inbound port.

MESH

Connect a private network

Private TCP, UDP and ICMP, in both directions.

The default software connector for private traffic.

WORKERS VPC

Connect Cloudflare code

Workers and agents call private APIs and databases.

CF1 APPLIANCE

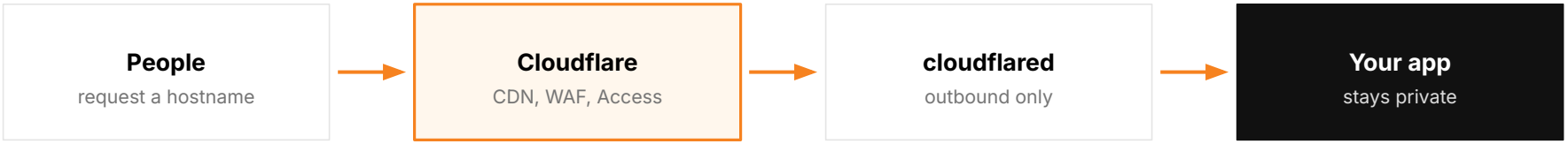
Connect a whole site

Managed box or VM for branches and data centers.

If it is an application, use Tunnel. If it is a network, use Mesh.

CLOUDFLARE

Any application becomes a Cloudflare application



NO OPEN PORTS

The origin hides

Block all inbound traffic and keep serving.

FULL EDGE STACK

Security comes free

DDoS, WAF, bots and API rules apply.

ANY PROTOCOL

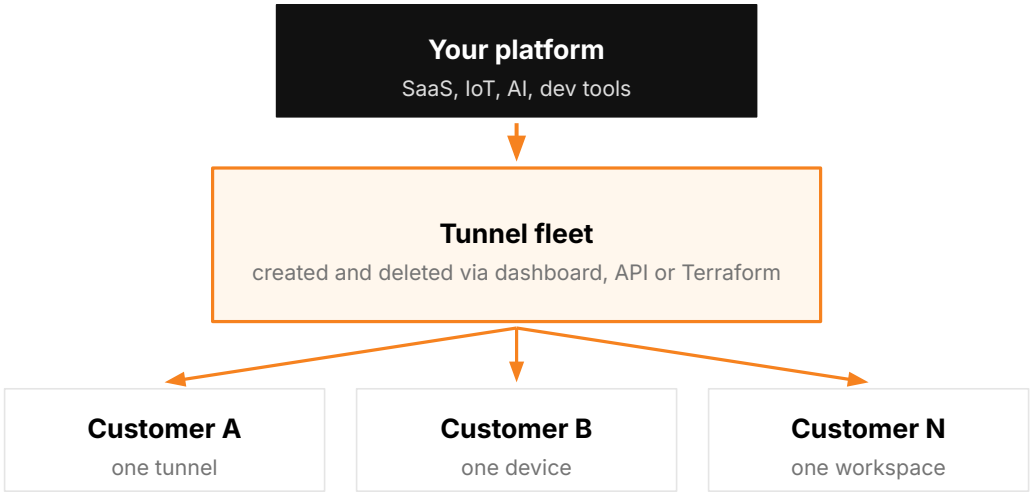
Not only web

SSH, RDP and other services can be proxied.

Best fit: public and app-level access. For private networks, reach for Mesh.

CLOUDFLARE

Cloudflare Tunnel, packaged for products that need millions



INCLUDED

1,000 tunnels in every account

Enjoy Cloudflare Tunnel for free!

THE ADD-ON

Add extra tunnels above 1,000

A configurable per-account limit, GA today.

UNCHANGED

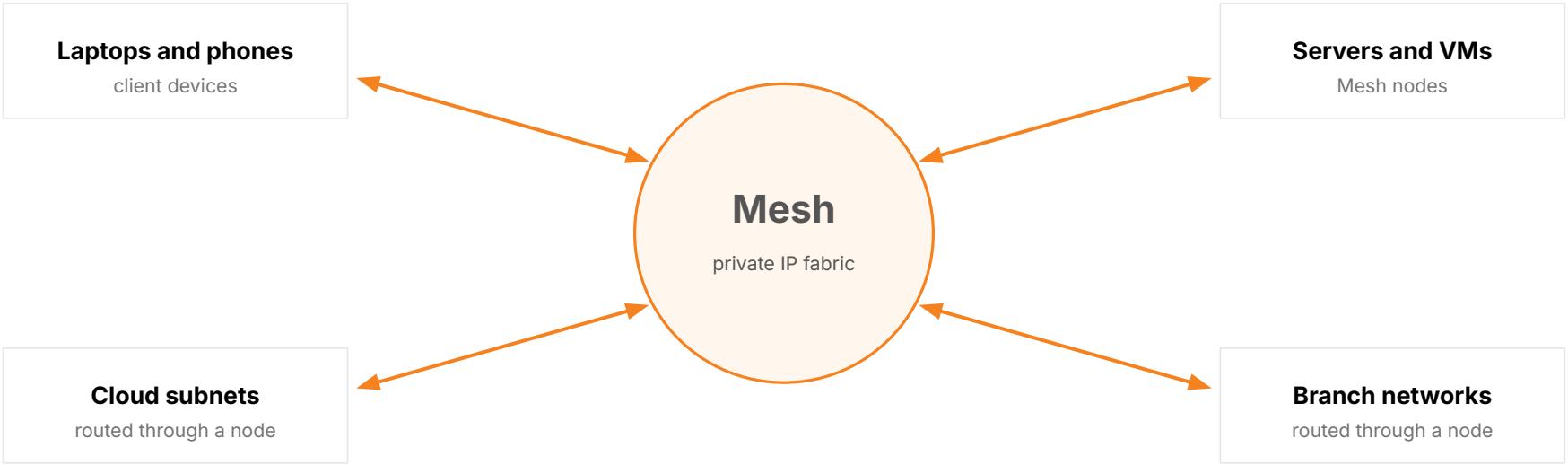
Same cloudflared, same behaviour

You can customise, embed and ship the binary.

Not included: bandwidth stays on the customer plan, and the standard Enterprise SLA applies.

Account teams set the limit for Enterprise based on contract. Self-service for PayGo is available via dashboard.

Mesh is the private network inside Cloudflare One



Every participant gets a private Mesh IP. Any side can start the conversation.

Cloudflare stays in the path, so policy, posture and logs apply to every flow.

CLOUDFLARE

Six things that make Mesh a real network

CONNECT

TCP, UDP, ICMP

Servers, laptops, phones and subnets.

NAME

Hostname routes

Reach services by name, not by IP list.

DEPLOY

Linux or containers

Install on a host or run the image.

SIMPLIFY

Source NAT

Replies come back with no extra routes.

SURVIVE

High availability

Replicas fail over automatically.

PROTECT

Post-quantum

Modern encryption on by default.

One connector covers connectivity, naming, resilience and encryption.

CLOUDFLARE

Run Mesh wherever the workload already runs

cloudflare/mesh

one image, amd64 and arm64

DOCKER COMPOSE

Connect a stack

Add one service to compose.yaml.

KUBERNETES

Node or sidecar

StatefulSet, or a sidecar in the Pod.

CI / CD

Join and leave

Test against private infra, then exit.

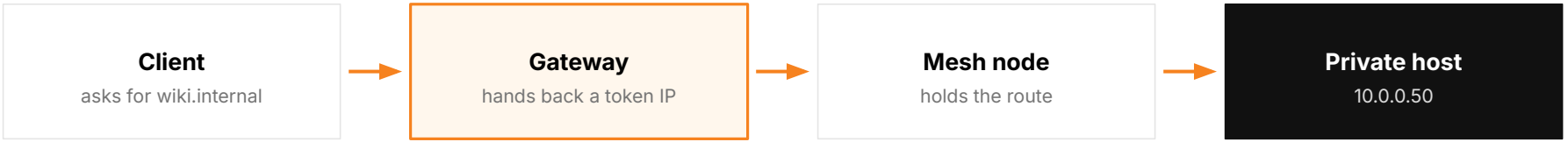
Source NAT is built in, so private services can reply without route changes.

Persist the registration volume to keep a stable identity. Run replicas with one token for failover.

No host packages. No route-table project. The node lives with the workload.

CLOUDFLARE

Route by name, not by IP address



PRIVATE NAME

Reach an internal app

Works when the private IP is unknown or changes.

PUBLIC NAME

Pick the exit point

Send a public hostname out through this node.

One hostname maps to one connector, so there is never an ambiguous answer.

CLOUDFLARE

Your code becomes part of the private network

BINDING

```
binding = "PRIVATE_NETWORK"
network_id = "cf1:network"
```

The address you pass at runtime picks the destination.

Services behind Cloudflare Tunnel

Nodes and subnets on Mesh

Destinations behind Cloudflare WAN

HTTP with fetch. Raw TCP with connect.

Good for private APIs, internal dashboards and agent workloads.

Next: TLS and stable names

Makes private Redis, Kafka and MQTT production ready.

One binding reaches private services no matter how they connect.

CLOUDFLARE

Bring an entire site onto Cloudflare



ZERO TOUCH

Ship and plug in

Connectivity and config come down automatically.

THROUGHPUT

Built for scale

Steering and shaping for busy sites.

ONE DASHBOARD

Managed centrally

Health, policy and updates in one place.

The right answer when you need a managed box, not a software agent.

CLOUDFLARE

Four questions. Four answers.

A public or internal web application	Cloudflare Tunnel
A private network, subnet or device	Cloudflare Mesh
Compute running on Cloudflare	Workers VPC
A branch office or data center	CF1 Appliance

Most deployments use two or three of these together.

CLOUDFLARE

What to remember tomorrow

01 **Applications go through Tunnel.**

Including the Tunnels for Platforms pattern, where tunnel count grows with customer count.

02 **Networks go through Mesh.**

Containers, hostname routes, Source NAT, HA and post-quantum make it production ready.

03 **Compute and branch sites have their own doors.**

Workers VPC for Cloudflare code. CF1 Appliance for branches and data centers.

04 **The future is one named private network.**

Mesh DNS this year, private Workers and containers next.

Start with what the customer is connecting. The rest follows.

Thank you!