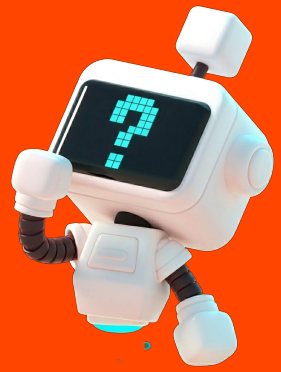
reddit

The Zero Trust Odyssey

Our Journey to Modernize Internal Access



Nathan Handler
Security Engineer, Reddit
nathan.handler@reddit.com
linkedin.com/in/nhandler

Pratik Lotia
Security Engineer, Reddit
pratik.lotia@reddit.com
linkedin.com/in/pratiklotia

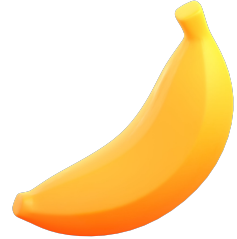
reddit

Background

What You'll Get From This Talk

- How we manage internal access to services
- Migrating from perimeter-based security
- Automation and UX for developers
- Resiliency strategies
- Lessons learned from 2 years of zero trust

Reddit's Initial State...



- Independent infrastructure bits duct-taped together
- 25 copies of: nginx intranet proxies / bastions / Pritunl VPN / k8s clusters
- Distributed auth and session management - Google OIDC, private keys in puppet, Okta, bespoke service auth
- Impetus to 'do better' - 2023 breach

https://www.reddit.com/r/reddit/comments/10y427y/we_had_a_security_incident_heres_what_we_know/

What We Were Looking For...

- **Ingress Consolidation**: Reduce three access points (VPN, bastion, proxy) to one.
- **Identity-Aware Security**: Common Okta IdP backed authX control plane
- **Device-Based Access Policies**: Use device identity and posture in authX decisions

What We Were Looking For...

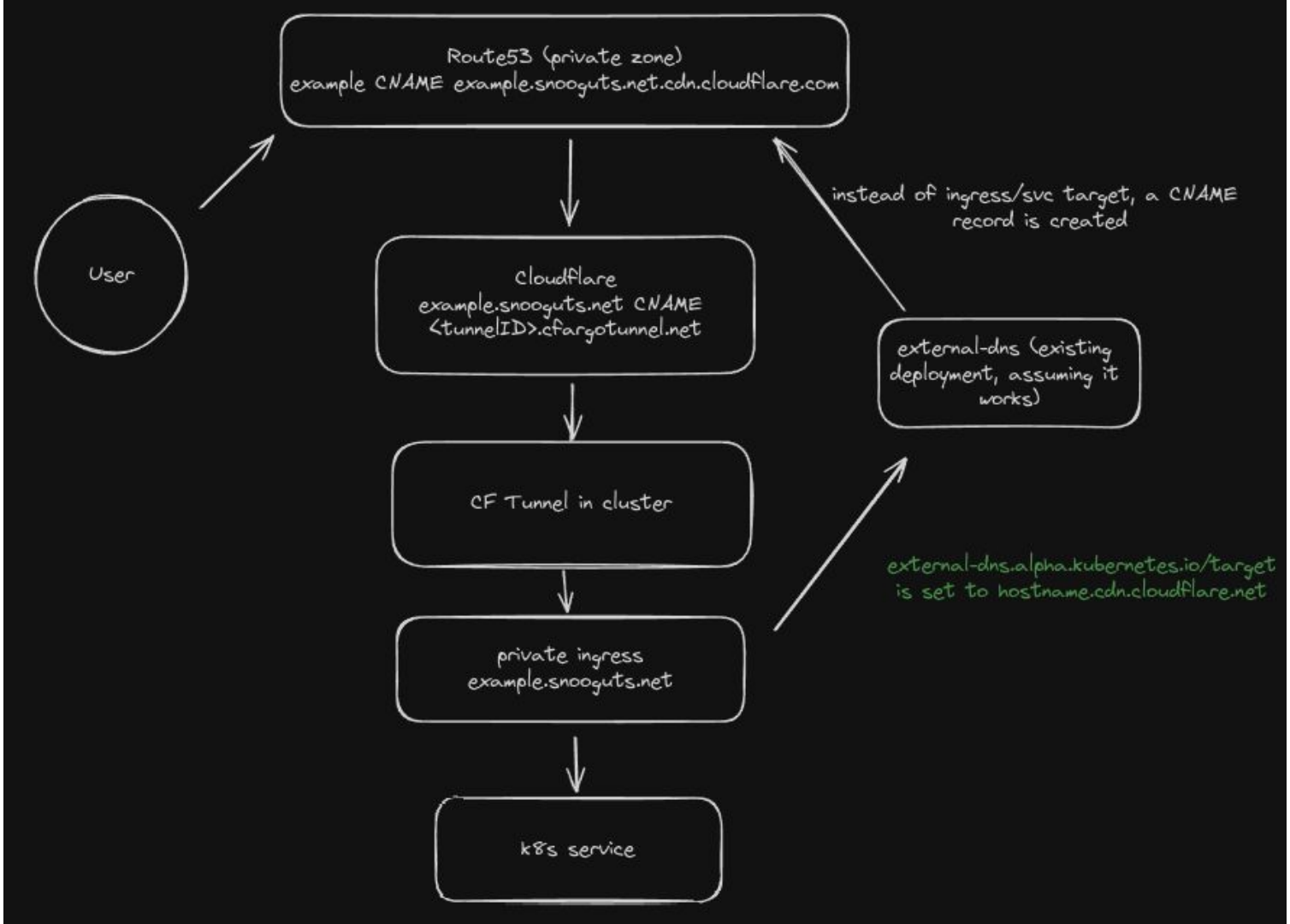
- **Enhanced Logging**: Log all ingress activity to correlate user, device, and resource access.
- **Improved User Experience**: Provide a faster and geo-diverse connection to Reddit infra in us-east-1.
- **Improved CLI / Service Access Story**: Simplify machine-to-machine and CLI authentication without browser login flows.

reddit

Architecture

How We Migrated...

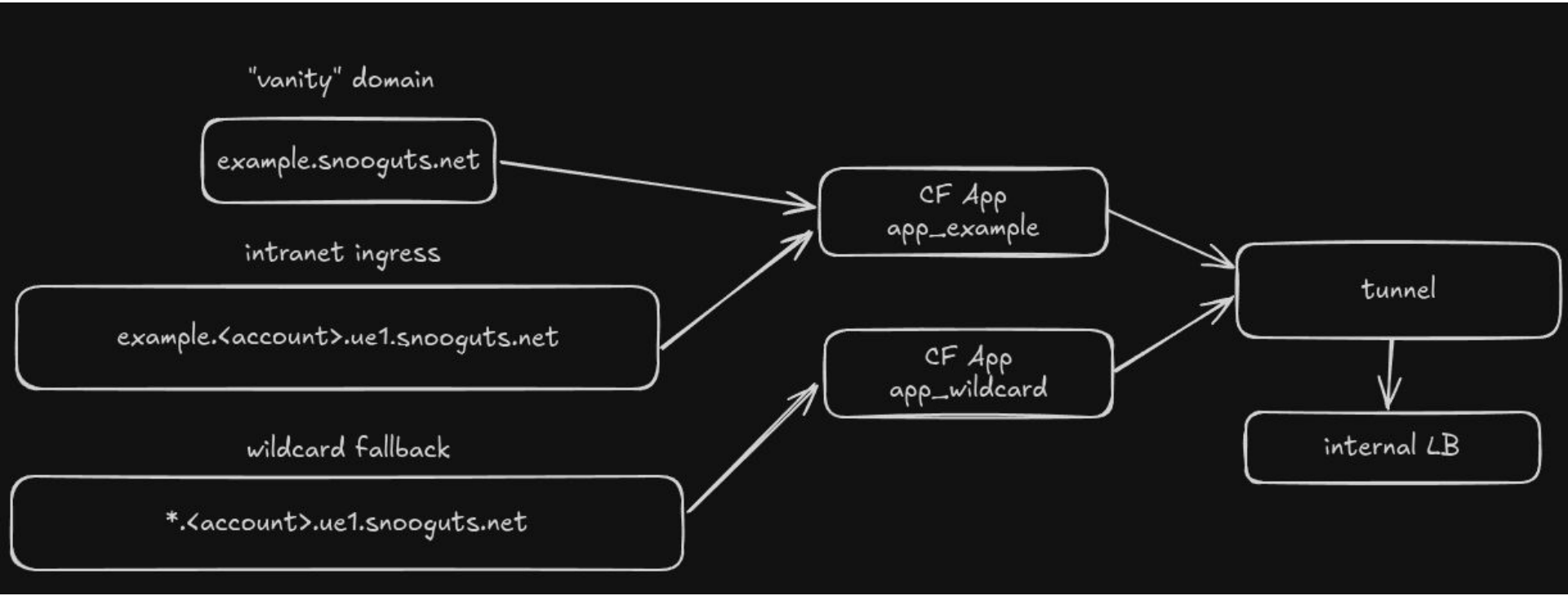
- **The DNS Strategy**
  - Partial CNAME resolution
  - Public / private DNS resolution
  - K8s and external-dns automation


Route53 (private zone)
example CNAME example.snooguts.net.cdn.cloudflare.com
User
Cloudflare
example.snooguts.net CNAME
<tunnelID>.cfargotunnel.net
CF Tunnel in cluster
private ingress
example.snooguts.net
k8s service
instead of ingress/svc target, a CNAME record is created
external-dns (existing deployment, assuming it works)
external-dns.alpha.kubernetes.io/target is set to hostname.cdn.cloudflare.net

How We Migrated...

- **The DNS Strategy**
  - Partial CNAME resolution
  - Public / private DNS resolution
  - K8s and external-dns automation
  - Maintain our AWS Route53 management
  - Wildcard resolution strategy and CF ZT Apps

Wildcard Logic



Resolver Policies

- AWS private zone routing
  - Traffic: domain matches regex .*<some-prefix>
  - DNS resolver: 10.x.y.2 resolver for AWS account
  - This depends on tunnel CIDR mapping
- K8s apiserver - in private, not in public
- Internal DNS for CI / secrets systems vs human access

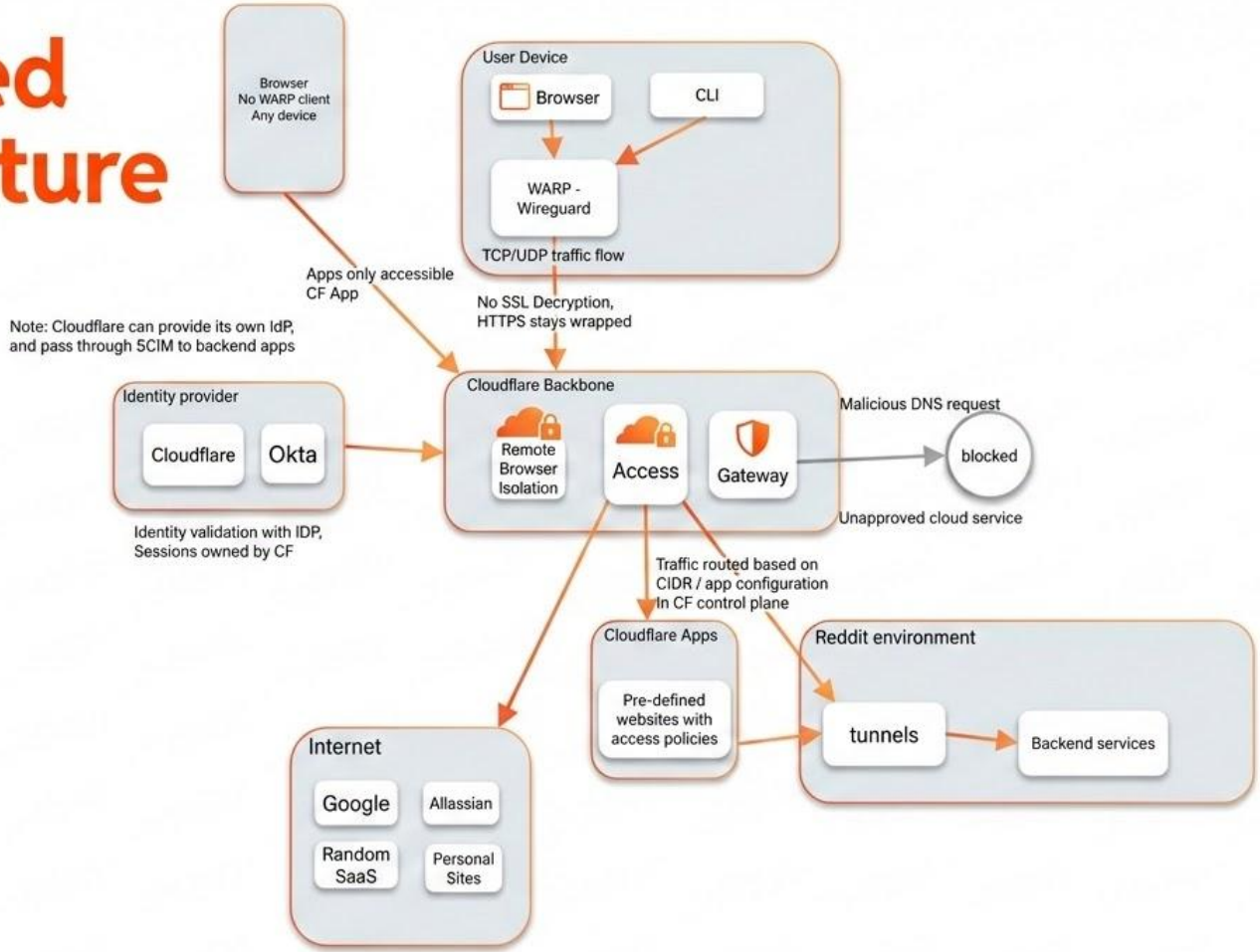
How We Migrated...

- **Cloudflared Tunnels**
  - Deployed to each k8s cluster or bespoke EC2
  - Allocate a CIDR block for routing
  - Deal with CIDR block overlaps with vnets (pain)
  - Correct AWS security group mismatches from EC2 intranet proxy migration
  - Scaling with KEDA/HPA on `cloudflared_tunnel_concurrent_requests_per_tunnel`

How We Migrated...

- **WARP Split Tunneling vs. Full Tunneling Tradeoff**
  - Reduce human change element via Split
  - Difficulties with ancillary services (Airdrop, home networking)
  - Handful of domains needing routing
  - Not routing Okta IdP traffic to not lose signal

Simplified Architecture



reddit

Automation

Scale Challenges

- **Platform & Automation**
  - No public, official CF ZT terraform modules or guidance on structure
  - Per account worked fine
  - ZT Access Policies paradigm changed midflight (unique to reusable)
  - Optimization of cloudflared-tunnels to scale in our dev environments (max connections HPA)

Scale Challenges

- **Achilles Controller**
  - Reddit's k8s operators approach
  - ***CFTunnelOperator* -** automatically spin a tunnel deployment in new k8s cluster
  - ***CFApplicationOperator* -** automatically spin a CF App for new ingress

https://www.reddit.com/r/RedditEng/comments/1gp11ui/open_source_of_achilles_sdk/

reddit

Rollout and Operationalization

IT Foundations

- **Gateway Policies**
  - Handle DNS records in the public/private zone
  - Block risky web categories
  - Apply custom egress geo rules
- **Managed WARP Client:** MDM deployment of WARP
- **Communications**
  - Internal comms, migration plans
  - Runbooks for infrastructure teams, service owners, and end users

Security Foundations

- **Cloudflare Tenant**: Terraform and productionalize the CF tenant
- **Network Coverage**: Establish tunnels across all Accounts / VPCs
- **App-Specific Policies**
- **CF Worker**: Handle CORS, header manipulation

Turndown

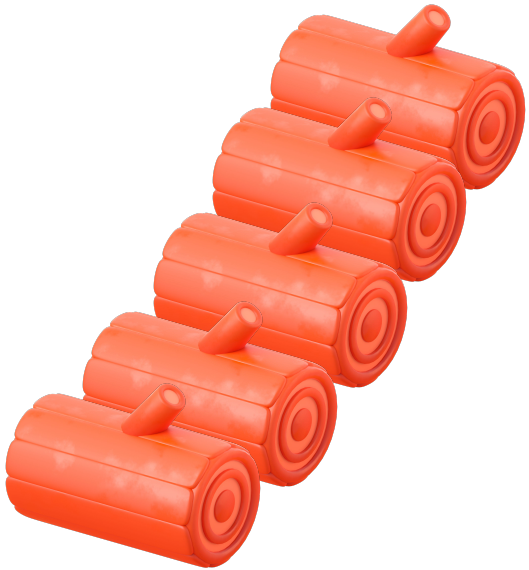
- **VPN Access Policies:** Where to handle authX decisions (app or VPN)
- **SSH**: Remove bastions and limit attack surface with fallback.
- **Intranet**: Proxy by proxy and webhook bypass

reddit

Reliability and Observability

Unified Monitoring & Observability

- **Cloudflare Logpush → Cribl:** Centralized log collection
- **BigQuery SIEM:** Deep analysis with familiar tooling
- **Real-time Alerts:** Detect suspicious activity immediately
- **Data-driven Dashboards:** Company-wide visibility



https://www.reddit.com/r/RedditEng/comments/1riyeam/how_reddit_does_threat_detection/

Incidents and Break-glass

- **Friday panic**: Curious case of disappearing tunnel configurations
- **Testing**
- **June 12 Cloudflare/GCP outage**: Single bastion fallback using temporary group membership

reddit

Lessons Learned

Employee Privacy

- **Addressing Employee Privacy:** Change in company culture with VPN requirement
- **Transparency:** Document what we capture, who has access, and how we review logs/access
- **Eliminate FUD:** No we can’t see all the traffic on your home network, just our device

What Would We Do Differently?

- **Standardize First**
  - How internal apps are accessed
  - Eliminate wildcards
  - Not have a CIDR block overlap?
- **Environment Uniformity**
  - Simpler transition
  - Reduced surprises.

In Conclusion

- **Automation & Resilience:** Reduced developer friction with custom Kubernetes operators; IaC provided fast recovery, but exposed tech debt (e.g., CIDR overlaps).
- **Security & Dev UX Balance:** Prioritized enhanced Developer UX (e.g., seamless CLI access via Warp flag) while maintaining transparency on privacy.
- **Critical Missing Features (Cloudflare):** Lack of support for gRPC (for CLIs) and Load Balancing (for multi-region HA) limits scalability.
- **Next Steps:** Roll out Full Tunnel after successful prototype; address high manual effort for Device Posture and SaaS app migration.

Questions?

reddit

That’s a wrap

Find Us:
nathan.handler@reddit.com
pratik.lotia@reddit.com

https://reddit.jobs