Max Black

Principal Infrastructure Engineer

Dublin, Ireland (UTC) · hello@maxblack.dev · linkedin.com/in/mblck

SUMMARY

Principal Infrastructure Engineer with 18 years of experience across networking, security, and cloud platforms — including 10 years at Workday spanning network engineering, multi-cloud architecture (GCP, AWS), and Kubernetes-based platform engineering on a security team. Recognized for deep production troubleshooting and incident resolution across hybrid environments — equally comfortable diagnosing F5 connection-table behavior, debugging Kubernetes operator logic in Go, or analyzing BGP and TLS issues in datacenter networks. Native networking background with hands-on experience across Cisco, Juniper, F5, Palo Alto, and Check Point. Deep familiarity with Linux internals and packet-level analysis.

CORE SKILLS

Infrastructure & Cloud: AWS, GCP (multi-region, hybrid connectivity); Terraform; Kubernetes (EKS, GKE); operator development (Kubebuilder, controller-runtime, Go); Flux, ACK, GCP Config Connector; CUE/Kapitan; HashiCorp Boundary, Vault; Atlantis.

Networking: BGP, OSPF, IPSec, OTV; F5 (BIG-IP, iRules), Cisco (Nexus, Catalyst, ASA), Juniper (SRX/MX/EX/QFX), Palo Alto, Check Point, Arista; packet analysis (Wireshark, tcpdump); SNMP, Netflow.

Security: PKI, TLS, IPSec, NGFW; privileged access management; hybrid policy design.

Languages & Automation: Go, Python, Bash; Ansible; CI/CD (Jenkins, Atlantis, Flux, Tekton).

Observability: Prometheus, Grafana, VMware Tanzu Observability (Wavefront), OpsAgent, Splunk.

EXPERIENCE

Workday — Dublin, Ireland 2016 — Present

Principal Cloud & Platform Engineer (Security / Boundary Platform team) Apr 2021 — Present

- Lead infrastructure engineer on Workday's privileged access management platform (HashiCorp Boundary), serving ~5,000 internal users connecting to ~200,000 targets across datacenters and public cloud (12 AWS regions, GCP). Stack: Go, Kubernetes, CUE/Kapitan, Flux, Tekton, Lighthouse.
- Took ownership of and built out the entire GCP deployment from scratch: bootstrap Terraform, admin cluster, Atlantis CI/CD; ported multiple Kubebuilder controllers from AWS ACK to GCP Config Connector. Wrote Go operators that consume SQS events and provision Boundary plus cloud resources.
- Diagnose and resolve cross-stack production issues spanning Kubernetes, cloud networking, Linux internals, and application behavior — frequently the engineer escalated to when issues touch multiple layers.
- Designed and implemented an AWS L4 load balancer blue/green pattern (parallel NLBs and F5 fleets with Cloudflare cookie-based routing); reduced production migration downtime by ~90%.
- Designed a GCP-to-AWS service mesh bridge over IPSec, unblocking GCP teams while native GCP mesh infrastructure was in progress. Provisioned dedicated direct-connect links (4×10 Gbps per datacenter) between GCP and on-premises datacenters; reduced tenant-migration times by ~80% versus IPSec VPN.
- Built Workday's GCP landing zone greenfield (multi-region VPC, internal services, Private Service Connect endpoints) and led CentOS 7 → CentOS 9 platform migration.

Principal Network Engineer May 2016 — Apr 2021

Promoted from Network Engineer → Senior → Principal

- Built a Python-based YAML-driven templating system generating Wavefront alerts and dashboards as Terraform JSON via Jenkins CI/CD; replaced manual dashboard editing across 10 datacenters. Coverage improved from ~60% to ~95%. Closed parallel observability gaps in the Prometheus SNMP collector, bringing core networking device coverage from ~60-70% to 100%.
- Designed a weighted-alert single-pane-of-glass health dashboard with per-device-tier-per-datacenter tiles, eliminating the need to traverse multiple dashboards before weekly maintenance windows. Approach later adopted by other operations teams.
- Led troubleshooting on multiple high-profile production incidents across the global network. Most prominent example: diagnosed a long-standing F5 connection-table exhaustion issue affecting external customer connectivity after multiple engineers had failed to find root cause. Identified the cause as an

iRule pattern routing VS → VS → Pool (rather than VS → Pool directly) triggering a session-cleanup bug in F5 firmware, later confirmed and fixed by F5. Recognized with Outstanding Contributor Award.

- Resolved company-wide Jira latency complaints from European and APAC offices through F5 TCP profile tuning and endpoint relocation across paired Portland datacenters. Complaints dropped to zero.
- Overhauled Juniper SRX firewall policy management organization-wide: built a Python CLI tool that exported policy as JSON, normalized formatting, identified shadowed/redundant rules, and proposed CIDR consolidations. SRX policy-matching performance improved by ~20% and audit-report generation became substantially easier.
- Built first automated F5 HA cluster configuration management at the company (Ansible). Led network tap and packet-capture infrastructure rollout in Dublin and Amsterdam datacenters (BigSwitch/Arista, NetScout).

AKON Technologies — Moscow, Russia Feb 2010 — Apr 2016

Promoted from Junior Engineer → Network/Security Engineer → Senior Network/Security Engineer → Solution Architect

Service integrator delivering networking and security solutions to enterprise customers across financial services, oil & gas, telecommunications, and insurance.

- Led Cisco Catalyst 6500 → Nexus 7000 backbone replacement for a major insurance customer with architectural transition from L2/L3 to L3-only backbone using OTV overlay technology.
- Executed simultaneous overnight Nortel Passport → Cisco Catalyst 6500 (VSS) migration across two main sites of a major Russian oil company.
- Migrated bank external firewall and VPN infrastructure (Cisco ASA → Check Point cluster) with zero downtime, including policy and VPN tunnel migration across multiple sites. Designed route-based VPN with encrypted-traffic load-balancing across separate links between HQ and datacenter.
- Deployed Check Point appliances in bridge mode at carrier scale into a Russian telecom backbone to mitigate malware exposure under tight delivery timeline.
- Additional implementations: QoS policy design and Cisco Prime LMS SLA monitoring; Radware DefensePro anti-DDoS; Radware AppWall WAF PoC; Alcatel-Lucent VitalQIP IPAM migration across 150+ sites; Check Point SmartEvent SIEM.

Earlier: Java Developer at Informika (State Institute of Information Technologies and Telecommunications), Moscow, Sep 2008 — Feb 2010.

EDUCATION

Specialist Degree (5-year program), Information Systems and Technologies — Russian State University for Innovation Technologies and Business, Moscow, 2004 — 2009.

CERTIFICATIONS

Active: Certified Kubernetes Administrator (CKA), 2026.

Previously certified: (ISC)² CISSP; Cisco CCNP, CCDP, CCNA Security; Check Point CCSM, CCSE; HashiCorp Terraform Associate; GCP Professional Cloud Architect; Wireshark WCNA; Stanford/Coursera Cryptography I.