KNOCKNOC

Your infrastructure is exposed today and accessible tomorrow. Nation state adversaries love that fact.

Always-on networks leave even well-defended attack surfaces exposed. Internet facing systems, internal networks or hosts buried deep in your environment are exposed to continuous mapping, scanning, lateral movement and exploitation.

Why leave an open door, when you don't have to?

The Knocknoc Approach

Knocknoc removes pre-auth attack surface without changing architecture.

Knocknoc eliminates network exposure by making access conditional, identity-driven and time-bound.

No user install. No VPNs. No re-routing. Host on-premise.

It works by orchestrating your existing firewalls and control infrastructure to grant **just-in-time access**, only after successful login, requiring minimal privileges and access.

The result? Systems become **invisible by default**, reachable only by authenticated and authorised users for a limited period, and only from their IP address or session.

You simply cannot patch fast enough.
Remove network attack surface, fast and at scale.

Built for Real-World Networks

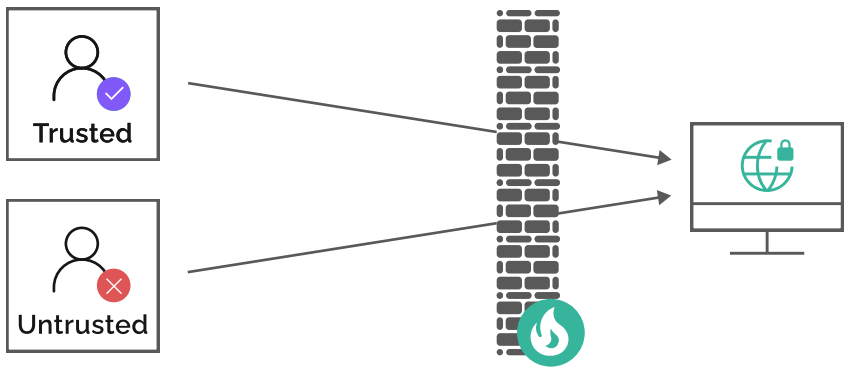
- **Invisible by default:** Network services, subnets or apps, remain hidden - until a user authenticates.
- **Works with what you have:** Extend and amplify existing firewalls and IDPs. On premise and/or Cloud.
- **Control unmanaged devices:** Browser-based access makes roll out simple. Control external third parties.
- **Identity linked access:** Network allow-listing with IP, token and time-bound access. No standing exposure.
- **Gain new visibility:** Track network-allow events in real time, SIEM and SOAR-friendly, actively contain access.
- **Fast, flexible deployment:** Host on-premise or run as SaaS. No changes to routing, direct network access.
- **Effective and extensible:** Zeroing attack surface for legacy environments, internal or custom applications.

Common Use Cases

Use Case	Problem	Ideal state	Knocknoc Solution
Removing always-on network exposure & attack surfaces	Attackers scan constantly, waiting for an exploitable vulnerability - you simply cannot patch fast enough	Systems are invisible to attackers, only authenticated sources can connect. Zero-day risks are mitigated.	Knocknoc orchestrates existing control layers to open short-lived, specific network access after login. Remove attack surfaces fast.
Third-Party Control (Unmanaged devices)	External users need access, but can't use VPNs/ZTNA, managed / SoE devices, nor install software.	Third-party access, ingress or egress flows are open *only* after authentication, optionally capturing work/job numbers.	Unmanaged devices utilize web browsers - without a client install - to authenticate, opening up authorized inbound or outbound traffic flows
Internal segments (Sensitive assets, mgmt. networks)	Critical assets are exposed to internal attack or lateral movement. Flat networks, jump-hosts, high-security subnets; remain exposed.	Networks are segmented at the identity level, only made accessible to specific groups for short periods. Ideally via existing infrastructure.	Internal hosts or subnets are orchestrated without introducing external risks, cloud routing or client installations. On premise. Just in time. Any port, any protocol, IPv4/IPV6.

Network Security - Before and After

Unprotected Network Access

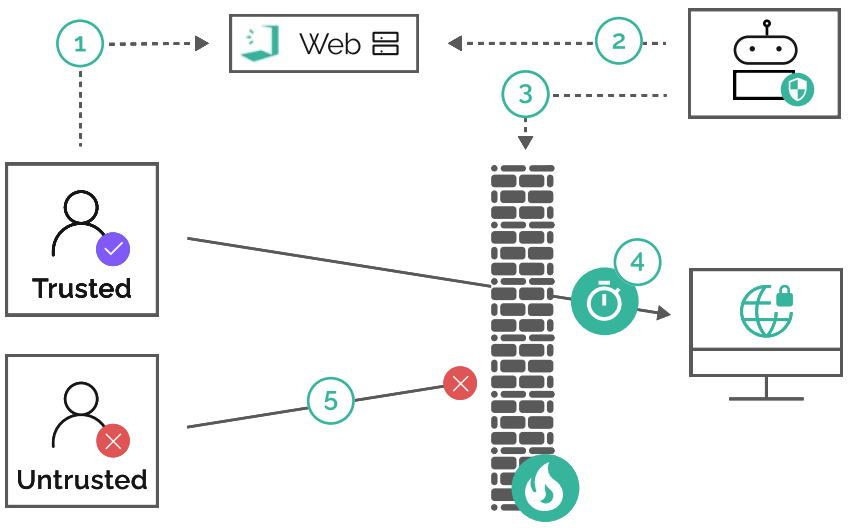


Status Quo.

Your firewalls permit access to ports and services.

- Legitimate/hostile users are indistinguishable.
- Assets are exposed for attack today, or tomorrow.
- Your attack surface is persistent, threats evolve daily.
- Blocking *known-bad* things is no longer sustainable.
- Detection, response and patching daily isn't enough.

Secured by Knocknoc



Network access is blocked until a user authenticates, identity-driven, time-bound access is then permitted.

1. Users login to a self-hosted Knocknoc web-app.
2. Knocknoc obtains the end-user IP address.
3. Out-of-band Agent updates firewalls IP list.
4. Time-bound access granted to authorised IP.
5. Unauthorised access is always blocked.

*No firewall? Utilize Windows or Linux/*Nix host-mode, or our on-premise reverse proxy mode, with layer-7 control.*

Trusted. Proven. Deployed.

- Mature and hardened in operational environments. On-Premise, self-host, air-gap or SaaS.
- Effective, easily integrated and highly extensible.
- Built in Australia, supported and deployed globally.

Integrate your existing infrastructure

paloalto NETWORKS · FORTINET · ivanti · cisco · HAPROXY · Azure · okta · aws · SAP · LDAP

Your attack surface is mapped. Now remove it.

Scan QR code for more info

Watch a product demo on YouTube

Go beyond the PDF, talk to a human.

Email: hello@knocknoc.io
Website: https://knocknoc.io