IP FABRIC

Network Security

In a perfect world, you'd be confident that all your devices are known, all your policies are enforced, and all your configurations are compliant. But the truth is: most organizations are missing **20%** of their infrastructure. The only way to close that gap is by deploying IP Fabric to automatically discover the network and validate security controls such as:

- [ ] **Firewall policies**

  IP Fabric collects URL filtering rules and FortiGate threat feed configurations directly from firewalls themselves, including next-gen and transparent firewalls. Your SSoT (e.g. **Nautobot**, **NetBox**) can be configured to extract that data for centralized policy creation, management, and validation.

- [ ] **Segmentation**

  IP Fabric simulates actual end-to-end paths in your network to validate that Zero Trust policies (e.g. segmentation and IPSec tunnels) are in place. These simulations serve as timestamped proof of compliance with security frameworks like NIST CSF and ISO 27001.

- [ ] **Lifecycle management**

  IP Fabric uses CLI commands and API calls to discover all network devices from core to cloud to edge. During this process it also gathers interface states and other operational data, surfacing all devices that are nearing EoL, EoM, or EoS milestones for more proactive governance.

- [ ] **Management protocols**

  IP Fabric gathers data on all existing management protocols (e.g. SNMP, syslog, and NTP). Every time you discover the network with IP Fabric, you can choose to deploy 160+ built-in intent checks, or to create your own custom checks, to validate that all protocols are applied according to your business intent.

- [ ] **Telnet access**

  IP Fabric highlights insecure protocols like Telnet to preemptively address any risks tied to secure system communication. If a Telnet connection is detected, IP Fabric can populate **ServiceNow ITSM** tickets with highly contextualized data for swift remediation.

- [ ] **Authentication, Authorization, and Accounting (AAA)**

  IP Fabric continuously validates access control policies to ensure adherence with Zero Trust architecture and Identity and Access Management (IAM) policies.

- [ ] **Configuration compliance**

  Deploy out-of-the-box intent checks based on NIST CSF, CIS, and ISO 27001 frameworks, or choose to build your own custom checks (no advanced knowledge of coding or query languages required). The results of all checks are presented in a normalized dashboard for year-round audit readiness.

Get in touch.

Visit IP Fabric's website for demos, customer stories, and more.