NetFoundry

WHITE PAPER

Align with NIST SP 800-207 using:

NetFoundry Identity-First™ Connectivity

Learn more at www.netfoundry.io

Executive Summary

The fundamental flaw of traditional IP-based networking is that it establishes network reachability first, and only later relies on the application layer to fully authenticate the session. This 'route-first' architecture expands blast radius, increases exposure, and makes least-privilege enforcement operationally brittle. Most cyber breaches are enabled by the ability of attackers to connect to servers for the purpose of either exploiting vulnerabilities or leveraging stolen secrets to impersonate permitted use. This legacy architecture relies heavily on network perimeters, leaving organizations vulnerable to lateral movement, compromised credentials, and expanding attack surfaces.

NIST Special Publication 800-207 is generally considered the most widely respected and authoritative definition of Zero Trust. It fundamentally redefines enterprise security by mandating a shift from location-based trust to identity-centric, resource-level protection. NetFoundry delivers a programmable Zero Trust Overlay Network (ZTON) built on the open-source OpenZiti project. By abstracting the network from the underlying infrastructure and embedding security directly into the application layer, NetFoundry enables organizations to achieve a "dark network" posture. This whitepaper details how NetFoundry's architecture implements and exceeds the core tenets of NIST 800-207, providing a cryptographic, deny-all-by-default environment that neutralizes lateral movement and eliminates inbound attack vectors.

DEMYSTIFYING NIST SP 800-207

Outcomes and Architectural Drivers

NIST 800-207 outlines a framework where trust is never granted implicitly based on physical or network location. The architecture relies on three logical components: the Policy Engine (PE), the Policy Administrator (PA), and the Policy Enforcement Point (PEP).

The framework is designed to drive several critical security outcomes:

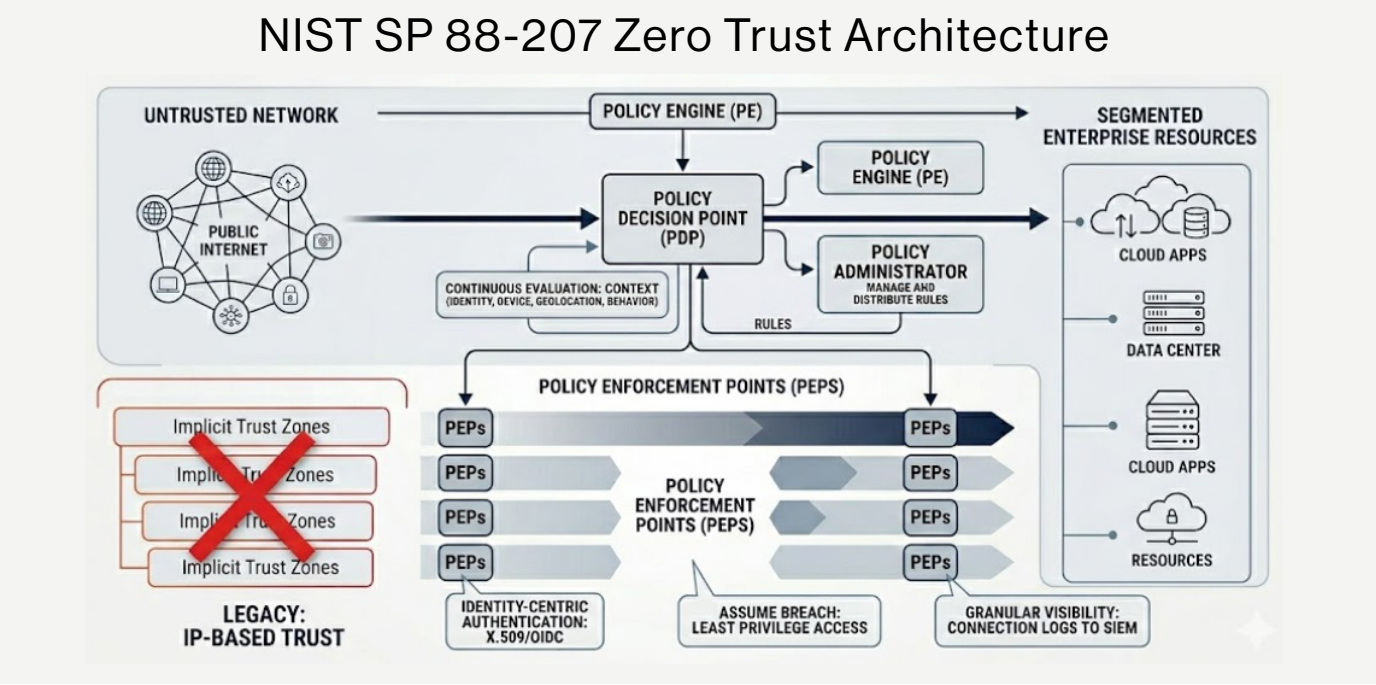
Assume Breach and Containment
Networks must be treated as inherently hostile. Micro-segmentation must restrict access to the absolute minimum necessary, containing the "blast radius" of any compromised endpoint.

Identity-Centric Authentication
IP addresses and MAC addresses are easily spoofed. Security must be tied to cryptographically verifiable identities of users, devices, and workloads.

Continuous Evaluation
Trust is ephemeral. Access rights must be continuously re-evaluated based on contextual data, device posture, and behavioral anomalies.

Granular Visibility
Security teams require deep, application-level telemetry to audit connections and refine access policies dynamically.

In NIST SP 800-207 terms, Zero Trust security posture is operationalized through a continuous policy evaluation with context and telemetry for an informed trust evaluation. The policy engine issues an allow/deny decision, then the policy administrator distributes the needed commands to enforce that decision and finally the distributed policy enforcement points admit or block each access request.



THE NETFOUNDRY ARCHITECTURE

Open Source Roots and Enterprise Scale

NetFoundry is the enterprise orchestration platform built atop OpenZiti, an open-source zero-trust networking platform. OpenZiti's open-source nature ensures that its cryptographic primitives and routing logic are transparent, community-vetted, and free from proprietary black-box obscurity.

NetFoundry overlay networks provide a strong separation between the control plane functions (identity, policy, orchestration) and the data plane (packet routing and forwarding by identity), aligning with the NIST 800-207 logical model and reducing blast radius:

The Controller (PE/PA)
The centralized brain of the network. It manages identities, validates posture checks, and distributes routing policies. Optionally, identity and posture context can also be sourced from external systems (IdP/MDM/EDR/SIEM) and incorporated in the policy evaluation.

The Fabric Routers (PEP - Data Plane)
A globally distributed mesh of routing nodes that securely transport encrypted traffic between endpoints.

The Edge Endpoints
Lightweight software agents, virtual gateways, or application-embedded SDKs that serve as the localized PEP, bridging the gap between the application and the overlay fabric.

Operationalizing NIST SP 800-207 with an Identity-First Overlay

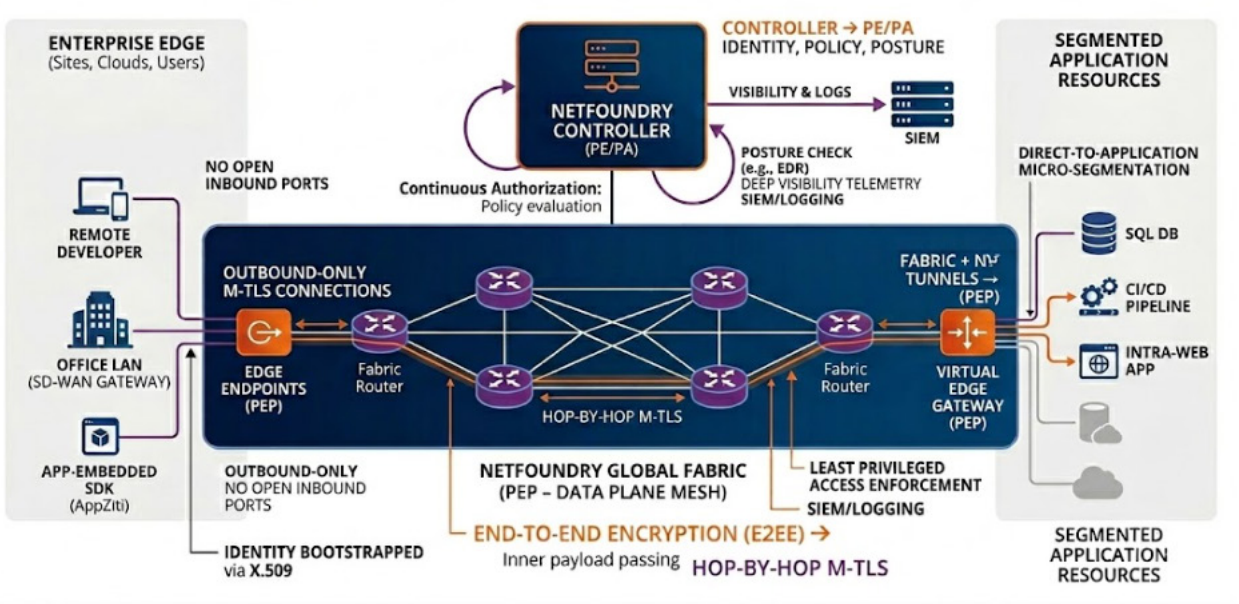
NetFoundry operationalizes the NIST SP 800-207 logical model by shifting access decisions from IP reachability to cryptographically verifiable identity and service-level policy.

Zero Exposed Inbound Attack Surface: A 'Dark' Network Posture

Traditional VPNs and firewalls require open inbound ports (listening sockets) to accept connections, exposing them to port scanners (like Shodan) and DDoS attacks. NetFoundry implements an "authenticate-before-connect" paradigm. Endpoints and gateways do not listen on any open inbound TCP or UDP ports. Instead, they establish outbound-only, mutually authenticated TLS connections to the NetFoundry Fabric. Because the firewall drops all unsolicited external traffic, the internal network becomes completely dark and undiscoverable to the public internet.

NetFoundry Zero Trust Overlay Architecture

Align with NIST SP 800-27



Cryptographic Identity via X.509 Bootstrapping

NIST SP 800-207 shifts trust decisions away from network location and toward identity and context. NetFoundry abandons IP-based access control. Upon provisioning, every entity (user, device, server, or microservice) undergoes a secure enrollment process to generate a unique X.509 certificate. The private key never leaves the endpoint. This hardware-attested or software-bound cryptographic identity must be presented to the Controller before a single packet of application data can be routed.

Direct-to-Application Micro-Segmentation & Eradicating Lateral Movement

Legacy micro-segmentation relies on complex VLANs and subnets, which still allow broad reachability and discoverability inside the perimeter. NetFoundry shifts segmentation to a connection-defined, service-centric model: identities are granted access to specific services, and access is evaluated per service, per identity, per connection attempt and not per subnet. To preserve application compatibility, clients can use hostname/DNS interception or leverage inbuilt private DNS for synthetic local addressing. In deployments that require it, this synthetic DNS/IP mapping can be configured to be unique per identity (and even per session) so that the destination is meaningful only in the context of an authorized connection. Regardless of the addressing scheme, unauthorized services remain invisible, non-routable and undiscoverable from that client endpoint, sharply reducing scanning and lateral movement opportunities.

Continuous Authorization and Posture Checks

NetFoundry enforces continuous evaluation of trust. The Controller continuously polls endpoints for Continuous Posture Checks (CPC). Administrators can define policies based on OS versions, domain verification, presence of specific registry keys, running processes (e.g., ensuring an EDR agent is active), and MAC addresses. If an endpoint falls out of compliance during an active session, the Controller immediately instructs the Fabric to cryptographically sever the data path.

Extensible Secondary Authentication (MFA and IdP)

To fulfill strict authentication mandates, NetFoundry integrates seamlessly with modern Identity Providers (Okta, Entra ID, Ping) via OIDC. Furthermore, NetFoundry supports Service-Level MFA. While a user may authenticate via their IdP to access the general overlay, accessing highly sensitive resources (like a production database or source code repository) triggers a secondary Time-based One-Time Password (TOTP) prompt. Even if a device is physically compromised while unlocked, the attacker cannot access high-value services.

FIPS-Compliant End-to-End Encryption and Hop-by-Hop mTLS

NetFoundry treats the underlying physical network (the "underlay") as actively hostile. Every piece of data traversing the NetFoundry overlay is double-encrypted using (optionally) FIPS 140-2 validated cryptographic modules. First, the payload is End-to-End Encrypted (E2EE) from the source endpoint to the destination endpoint. Second, the connection between every Fabric Router in the transit path is secured via hop-by-hop Mutual TLS (mTLS). This ensures data integrity and confidentiality across any public or private transit link.

Deep Visibility and Telemetry

NIST requires comprehensive logging for dynamic policy refinement. Because every connection requires cryptographic routing, the NetFoundry Controller acts as a centralized visibility hub. It provides deep, granular telemetry on every connection attempt, active session, latency metric, and denied access event, seamlessly exporting this data to SIEMs (like Splunk or Datadog) to satisfy compliance auditing and incident response requirements.

Case Study

Achieving NIST and FIPS Compliance for a top military contractor

The Challenge

A major defense contractor, faced an urgent mandate to align with NIST 800-207 and secure their distributed CI/CD pipelines across AWS, Azure, and on-premises data centers. Their legacy architecture relied on site-to-site IPsec VPNs, which created a flat network topology. A red-team exercise revealed that a compromised developer laptop could scan the internal network and pivot into secure enclaves. Furthermore, managing overlapping IP subnets across multiple cloud providers was causing severe routing conflicts and operational overhead.

The Solution

The customer deployed NetFoundry Zero Trust Overlay. They replaced their IPsec tunnels with NetFoundry Edge Tunnelers on developer workstations and deployed virtual Edge Routers within their cloud VPCs.

The Implementation and Results

- **Eliminated the Perimeter:** Closed all inbound ports on their cloud firewalls. The infrastructure went completely dark to the outside world, immediately halting a barrage of automated internet scanning.
- **Application-Embedded Security:** For their most critical internal web apps, the customer used the NetFoundry SDKs to compile zero-trust connectivity directly into the application code. These apps no longer even had an open port on the host OS; they only communicated via the NetFoundry fabric.
- **Stopped Lateral Movement:** During the subsequent red-team audit, testers were given a fully authenticated developer laptop. However, because the developer's identity was only authorized for specific Git repositories and Jira servers, the red team was entirely blind to the rest of the network. Network mapping tools (like Nmap) returned zero results.
- **Continuous Compliance:** Customer implemented posture checks ensuring that CrowdStrike was running and the hard drive was BitLocker-encrypted. If a tester disabled the EDR agent, the NetFoundry Controller instantly revoked the endpoint's routing privileges, cleanly satisfying continuous authorization mandates.

CALL TO ACTION

Architect Your Dark Network

Transforming your architecture to meet NIST SP 800-207 requires more than bolting on another layer of perimeter defense. It requires a fundamental shift to cryptographic routing.
NetFoundry empowers your engineering teams to build software-defined, zero-trust networks that are secure by default, agile by design, and invisible to attackers.

Ready to see it in action?

Start Building
Spin up your first completely dark, end-to-end encrypted connection in under 15 minutes.

Request a demo and a free trial

About NetFoundry

NetFoundry helps businesses secure connectivity between components of their widely distributed workloads, across any set of networks. Founded by the inventors and maintainers of the world's most used open source zero trust software, OpenZiti, NetFoundry's Identity-First Connectivity™ enables zero trust connectivity with no VPNs, no open inbound ports, and no firewall changes. Software and IoT solution providers use it for secure communications with workloads at their customers' sites. Enterprises secure access to their APIs and agentic AI services in order to avoid any opening that can be leveraged by an attacker. They also use NetFoundry to simplify the operation of hybrid IT/OT segmentation and enable identity-based microsegmentation.

Learn more at www.netfoundry.io

NetFoundry