NETFOUNDRY™

WHITEPAPER

NetFoundry Platform Architecture

May 2023 |

NETFOUNDRY

The New Application Environment

This paper describes the architecture of the NetFoundry platform in the context of how the NetFoundry layers can integrate with other layers to provide security, reliability and performance over Internet connections for today's distributed, dynamic, automated application environments.

Digital enterprises require agile, automated and quick application lifecycles, while still needing secure and performant network delivery. This is a formidable challenge due to these factors:

1. Massive application distribution. Compute is increasingly distributed across multiple edges, clouds and service meshes. It is difficult to secure and reliably deliver an application when its users are mobile or computers (IoT); when the app is comprised of APIs and microservices which cross multiple administrative domains, clouds and networks; and when the app is portable (containerized) and dynamic (AI or ML infused).

2. Increasing cyberthreat risks and impacts. Cybercrime costs the world hundreds of billions of dollars in direct costs. Our hyperconnected world can result in more attack surfaces and vulnerabilities. Meanwhile, core business processes and sometimes entire supply chains are often dependent on connectivity, so a security breach increasingly disrupts day to day operations.

3. Increased use of consumer-grade Internet. The low costs, global reach and high bandwidth available from consumer grade Internet results in these connections increasingly being used at locations like branch offices and IoT/edge sites. However, these types of locations are often not equipped from systems, skillset and process perspectives to get enterprise-grade security and performance over these connections.

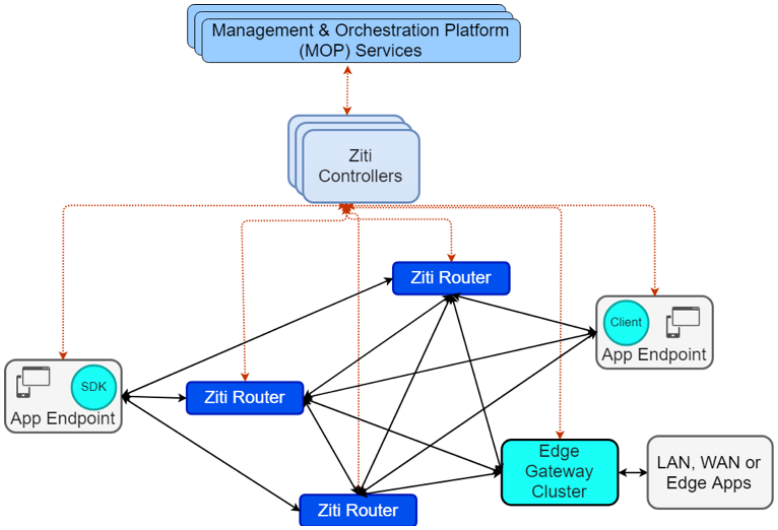
These challenges need to be addressed for each application across both the compute domain (applications and compute infrastructure) and the network domain (LANs and WANs). Increasingly, these domains cross traditional "WAN" boundaries, for example an app needs to be secure and performant across IoT, supply chain and multi-business service meshes.

NetFoundry helps address these challenges from the application side:

1. An application which embeds NetFoundry's connectivity is optimized to get programmable, secure, reliable connections anywhere which it travels.

2. NetFoundry's solution is agnostic of and complementary to any specific vendors used for WAN, network, hardware and security.

3. NetFoundry's APIs and SDKs enable it to be a "pluggable" layer in multi-layered solutions.



There are three main components to the NetFoundry platform:

1. The Management and Orchestration Platform ("NetFoundry MOP"). The NetFoundry MOP, on the top of the diagram, provides the APIs and interfaces by which customers control their NetFoundry networks. Similar to how IaaS abstracts developers from the underlying compute, providing it as a service, NetFoundry MOP abstracts developers from the underlying networking, enabling developers to consume it as a service.
2. The Edge ("NetFoundry Ziti Edge"). Ziti Edge extends NetFoundry application delivery to wherever the application goes:
   A. On the left side of the diagram, the Ziti Edge SDK enables apps to embed NetFoundry. In this case, no software deployment is needed on the endpoints.
   B. On the right side of the diagram, the Ziti Client enables devices to leverage NetFoundry, and the Ziti Gateway enables sites such as DMZs or Edge Compute.
   C. Ziti Controllers, towards the top of the diagram provide zero trust enrollment, authentication and authorization services, which unify the various endpoint types, and. help enforce NetFoundry's Zero Trust, Software Defined Perimeter (SDP).
3. The Fabric ("NetFoundry Ziti Fabric"). To get consistent security, reliability and performance over the Internet, NetFoundry manages the Ziti Fabric - a dynamic, multi-autonomous system (AS), Internet-overlay, software defined network (SDN).

These components are discussed in more detail in context of how they help businesses get the security, reliability and performance they require.

Security

A key pillar of the NetFoundry architecture is to be secure-by-design, using Software Defined Perimeter (SDP) and Zero Trust principles. The layers of the architecture:

NetFoundry's Zero Trust solution layer one: identify, authenticate, authorize.

NetFoundry does not permit any data to flow until it has explicitly and securely been identified, authenticated and authorized. The default rule is to "deny all" in a "guilty until proven innocent" model. Not only does this provide maximum protection for the data, it protects against metadata from being acquired by actions such as probes which might otherwise be exploited to gain insight into sites, users and applications.

NetFoundry's Ziti Edge endpoints (embedded in the app via the Ziti SDK; thin Ziti client on a device or virtualized/containerized/sidecar Ziti Gateway) need to enroll to their private networks in order to be permitted to transit any data. The endpoints need to validate a one-time crypto-signed token (based on RFC 7030) or hardware root of trust identity with distributed NetFoundry Ziti Controller instances in order to even "see" the network. The bidirectional certificate validation is provided by NetFoundry as part of the SaaS service, enabling customers to not need to manage certificates, signing and PKI infrastructure, although customers can opt to manage use their own infrastructure if they prefer.

NetFoundry has software and SDK integrations with leading hardware root of trust identity partners and Trusted Execution Environment (TEE) partners to further secure certain devices.

Each enrolled and authenticated Ziti Edge endpoint is only given access to the specific IP addresses, ports and protocols permitted by the business policies. When integrated with IAM systems, businesses gain centralized control and visibility, eliminating issues causes by trying to manage disparate sets of policies on the application side and the network side.

NetFoundry's Zero Trust solution layer two: application Level microsegmentation

Once the application flow has been authenticated and authorized, each app flow is logically isolated and independent in terms of initiation, permissions, access and path. This extreme microsegmentation ("NetFoundry AppWANs") is important to both strongly secure each data flow, and to prevent collateral damage if a specific flow is breached. For example, a standard VPN or SD-WAN breach often will give an attacker access to an entire network or subnet, because the users and devices in these Trust Network paradigms have access to entire networks or subnets. In contrast, a NetFoundry AppWAN only has access to specific services (IP addresses, ports, protocols) which have been explicitly defined by the administrator, and an end-to-end AppWAN (SDK to SDK) is completely application-specific with no dependencies on local IP addresses, ports or protocols. Although the goal is always to prevent all attacks, NetFoundry believes it is also critical to mitigate damage for any attacks which may happen, and NetFoundry's microsegmented AppWANs uniquely accomplish that goal.

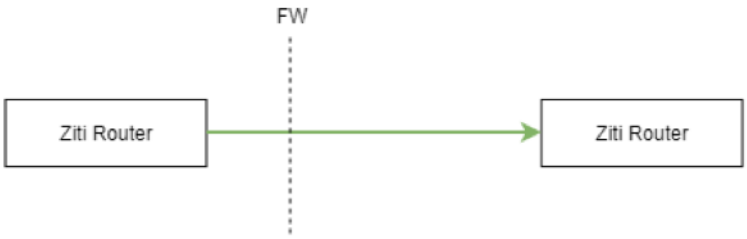
NetFoundry's Zero Trust solution layer three: Dark

NetFoundry's Ziti Edge endpoints and Ziti Fabric Routers include the equivalent of a software firewall with a single policy: block all externally-originated connection attempts (connection attempts from outside the customer's private, authenticated, authorized Ziti network).

Since the Ziti Edge endpoints block or drop all externally attempted connections, the apps and networks which are secured by the Edge endpoints become dark to any externally-originated data flows. This is key to getting software based private networks over the Public Internet, while being dark to the Public Internet. NetFoundry Ziti Edge endpoints and Fabric Routers open authenticated, authorized outbound connection which "listen" only for data sessions which have been authenticated and authorized on the private NetFoundry network overlay.

1. Each Ziti Router needs to authenticate with a Ziti Controller to communicate with any other endpoint. This is initiated outbound from the Routers, making them "dark" to the Internet (they do not accept connections initiated from external endpoints):

2. Similarly, Ziti Routers which are inside of firewalls only need to initiate outbound connections:



This means that even if a device in a network is vulnerable due to weak access credentials or similar, such as we saw in the Mirai botnet, NetFoundry can help mask the deficiency by rejecting the connection attempts (attacks) before they can reach the vulnerable device.

The solution also makes NetFoundry integration simpler and more secure for security teams. The team no longer needs to open inbound firewall ports, because all NetFoundry data sessions are initiated outbound to private NetFoundry infrastructure, only connected upon successful authentication, and use the least privileged access policies described above.

NetFoundry's Zero Trust solution layer four: Data in Motion Protection

NetFoundry's Zero Trust software endpoints encrypt all data per customer policy, using strong encryption, negotiated on a per-session basis Furthermore, NetFoundry can separately encrypt the data headers, and obfuscate the source IPs.

NetFoundry's Console and APIs provide the administrator with the ability to centrally manage encryption on an application-by-application basis. For example, an administrator can choose to not apply NetFoundry encryption if a specific application is already encrypting its own data in a suitable manner, or can choose to use both the app encryption and the NetFoundry encryption.

NetFoundry's Zero Trust solution layer five: dynamic, ephemeral Ziti Fabric

The IP addresses of the dynamic Ziti Fabric Routers are used in the routing of data, such that it is those IP addresses which are the targets for any attacks. This moves the attack surface away from less protected business assets and data. Ziti Fabric Routers store no data of interest and have no access to the encryption keys of the data payloads. The Routers are highly distributed in a resilient mesh architecture in which any Router can talk to any other router, making each Router disposable in the event of an attack, and ensuring that data streams are not reliant on single Routers. An attacker therefore can't compromise the network itself by taking down individual Ziti Routers. Furthermore, the Ziti Routers are spun up and down in an ephemeral manner enabling apps to spin up transient networks which can exist in one minute and be gone in the next to meet certain security goals. In this manifestation, the app developer is essentially creating disappearing networks which can then reappear with new addressing and topologies.

NetFoundry's Zero Trust solution layer six: integrations

The NetFoundry platform is a set of cloud native microservices with APIs and SDKs designed for integrations with any security provider, across any set of hardware, WANs and clouds. For example, NetFoundry has hardware root of trust and TEE integrations, and has pre-built integrations with leading IAM and Identity providers. This enables customers to deploy integrated solutions, for example using NetFoundry AppWANs to transport certain apps from end-to-end, while also being able to transport other traffic to separate on-premises or cloud-based security solutions.

Reliability and Performance

NetFoundry's platform, exposed to customers as a SaaS service, needs to optimize reliability and performance across Internet connections. Although the intrinsic limitations of any network can't be overcome, the NetFoundry architecture is designed to create services which can dynamically adjust to "Internet weather" and ensure that individual component failures don't impact application flows.

Control and Session Management Planes

All NetFoundry Control and Management Plane systems are fully managed by NetFoundry, and exposed to customers as on-demand, instantly-available SaaS. In addition to the convenience and simplicity this provides to NetFoundry customers, it provides increased reliability as well.

NetFoundry's MOP infrastructure is a set of cloud-native microservices which are distributed across NetFoundry managed infrastructure with High Availability (HA) architectures. This enables NetFoundry to provide service availability SLAs of greater than 99.9%.

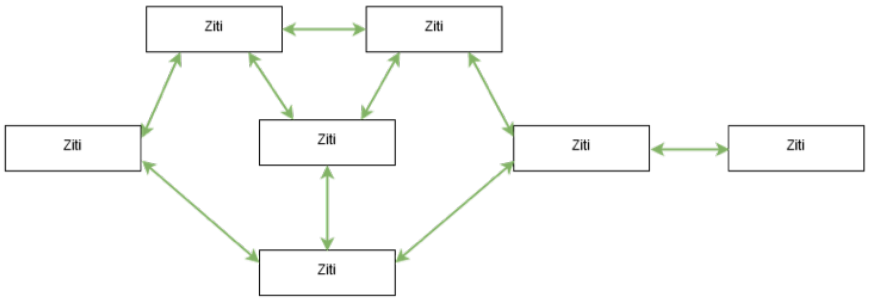
Ziti Controllers are also distributed across NetFoundry's managed infrastructure in HA architectures. This enables the session control plane to have greater than 99.99% availability.

Data Plane – Ziti Fabric

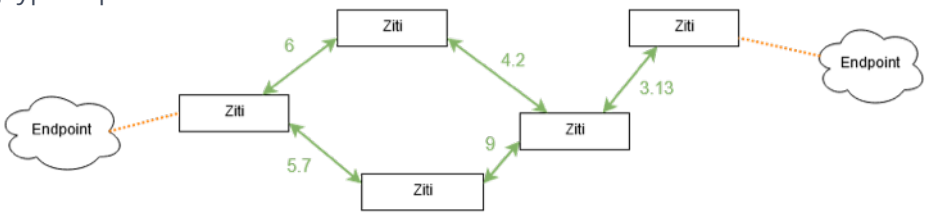
One of the greatest challenges of providing reliability and performance over Internet is adjusting for the quickly changing characteristics of Internet connections. NetFoundry addresses this challenge with the Ziti Fabric, serving as a dynamic Internet overlay with maximum route diversity and endpoint-controlled, real-time routing:

.

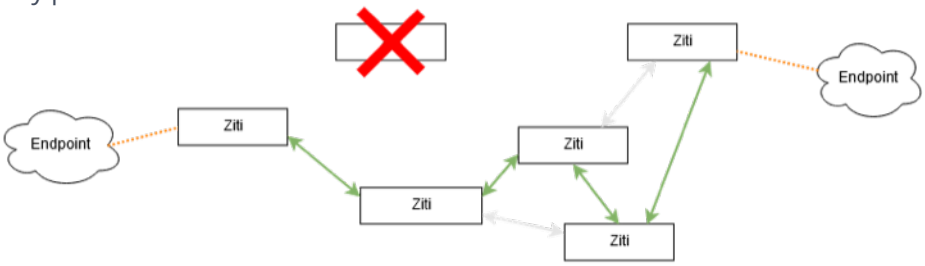
1. The Ziti Fabric is a dynamic mesh which maintains links between each Ziti Router, which is dynamically spun up down according to business policy and in an automated manner in which Ziti Controllers spin up Routers in responses to changes in underlying networks:



2. Real-time, Smart Routing Path Selection algorithms govern which Ziti Routers are used for which application sessions. This is dynamic on a session-by-session basis, adapting to changing business policies and underlying network changes. The default algorithms rely heavily on observed (actual) network performance, and are built to incorporate optional metadata from any other systems or machine learning type implementations.



3. Self-healing algorithms adjust to changes in real-time. This change could have been triggered by performance degradation from the Ziti Router itself, or from a problem with the underlying networks which connect it into the mesh. The Router, or a replacement, is automatically put back into the Mesh when the condition is resolved.authorized Ziti network).



4. Ziti Fabric uses pluggable transports. This enables Ziti to use protocols which are best suited for each individual session. For example, the Ziti Fabric is built to leverage multiple long haul fabric protocols such as QUIC, a new protocol being shepherded through the IETF by Google and others. The Fabric can take TCP-based application sessions (which are not optimized for transport across networks which have more than 50ms of latency or any packet loss, due to the nature of TCP itself), and transport them instead as a different long haul fabric protocol (using different long haul Fabric protocols improves throughput by at least 2x, depending on how much latency and packet loss), without impacting the application itself (which still communicates with TCP on both sides).

Data Plane – Ziti Edge

Ziti Edge enables customers to extend NetFoundry's performance optimization as close to the application edge as possible, and to best utilize whatever connections are available at that location.

Ziti Edge SDKs and thin clients immediately transit data on to the Ziti Fabric. They can simultaneously leverage multiple connections, e.g. wired and wireless.

Ziti Edge Gateways enable customers to leverage the Ziti Fabric from aggregation points such as branch offices, private data center DMZs and Edge Compute sites. The gateways also have he ability to leverage multiple connections in a hybrid WAN type manner in which the Path Selection algorithms choose the best paths, based on the real-time performance of each interface, as well as any business policies.

NETFOUNDRY™

Address —
101 S Tryon Street, Suite 2700
Charlotte, NC 28280

Telephone —
+1.704.762.1405

Contact us

Share

For more information, visit us at www.netfoundry.io