NETFOUNDRY

AUTOMATE & SIMPLIFY CLOUD APP CONNECTIONS

SOFTWARE-ONLY, SECURE, SEAMLESS ACCESS TO HETEROGENEOUS ENVIRONMENTS: PRIVATE, PUBLIC, & HYBRID CLOUDS

Microsoft Partner
Microsoft

aws partner network
Advanced Technology Partner

Enterprises are migrating from on-premises data centers and moving applications to the cloud in record numbers. Gartner estimates that by 2025, 80% of on-premises data centers will be replaced by public cloud, or private cloud housed in a co-location facility*. As a result, DevOps, DevNetOps, and DevSecOps teams often bounce between different cloud environments. This heterogeneous cloud ecosystem complicates access management and operational support as the tools required to support them are dispersed across many instances and locations, with interfaces that vary widely from vendor to vendor. The result is a management, scalability, and security overhead that is neither agile nor automated.

What enterprises and application teams need is a seamless application-specific networking and security approach that is agnostic to the diverse cloud environments. NetFoundry abstracts the vendor-specific differences in cloud environments away, with a uniform SaaS based management console and APIs for integrating into native environments & toolsets. Access policies for individuals and developers are simplified, the overhead of managing bastion hosts to support remote access disappears, and developers no longer struggle to establish secure connectivity from their desktops to these heterogeneous clouds. Devops and Infrastructure teams can use Netfoundry to automate CI/CD pipeline and workflows such as Jenkins(TM) and Spinnaker(TM) across heterogeneous cloud environments.

EMBRACE THE CLOUD WITH CONFIDENCE

The NetFoundry platform provides a vendor-agnostic, secure, remote connections management solution over all types of connectivity, enabling adminstrators to instantly spin up secure, performant, application-specific, Zero Trust networks called AppWANs with public Internet reach and scale.

A secure, private virtual mesh network over the Internet can be created and set up in minutes across any physical or virtual site, and also works for remote users, mobile devices, embedded applications, and IoT solutions.

*https://blogs.gartner.com/david_cappuccio/2018/07/26/the-data-center-is-dead/

Key Benefits

- Undetectable networks that cannot be found or penetrated by unauthorized users on the Internet
- Zero trust network architecture with secure network isolation and app specific micro-segmentation in a least privilege access model
- Programmable using REST API and IaC tools like Terraform & CloudFormation
- Equalized heterogeneous environments that abstracts the differences between cloud vendors
- Hardware, telco, and cloud provider agnostic
- Developer friendly network deployment with support for critical enterprise network functions
- Networks driven by the identities, contexts, & needs of each app and set of IAM policies
- Available in AWS & Azure marketplace

Contact us

Share

Start spinning up networks for free at netfoundry.io

NETFOUNDRY

AUTOMATION, AGILITY, SIMPLICITY, & SECURITY

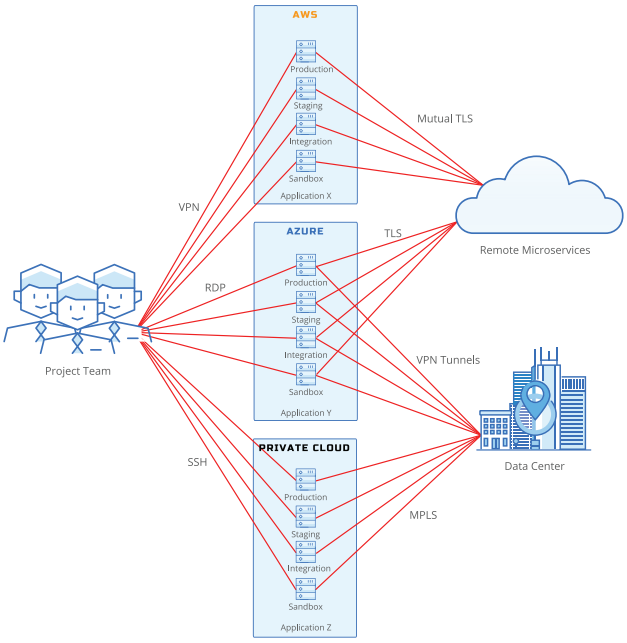
THE PROBLEM

As Applications are evolving from monolithic to modern architectures such as micro-services, they are becoming increasingly disaggregated and distributed across multiple cloud environments. Each cloud-based application hosted in one or more environments is deployed within an instance of a public or private cloud. A growing enterprise, utilizing cloud services for a large number of applications will eventually experience a Virtual Private Circuit sprawl of (and/or Azure VNETs) beyond what is manageable - as the result of having a separate cloud instance for each application environment. Most companies use three-to-four environments to develop, integrate, stage, and deploy a single application. An enterprise with just 40 applications must manage upwards of 160 application environments, for which connections, both inbound and outbound, must be available on demand and need to carefully provisioned and monitored. In addition, application-specific access control and management become a nightmare.

The challenge goes beyond remote access, to microservices - back-end connections from an application to a remote service that provides data for the application to function. Most often, these far-flung micro-services live elsewhere - on the Internet, in a private cloud, or a remote data center. DevOps culture demands repeatable, automated creation of secure connections for remote services.

Historically, the process of managing access across the many-to-many relationships of modern distributed application environments have proven to be surprisingly complex. DevOps teams struggle to set up continuous integration and/or continuous deployment (CI/CD) pipelines and work-flows that span across heterogeneous cloud environments for Dev, QA, Staging and production needs with secure access to relevant teams within the organization. Fortunately, NetFoundry AppWANs provide a simpler, more secure, and automated solution to address these concerns.

Legacy Remote App Management



THE SOLUTION

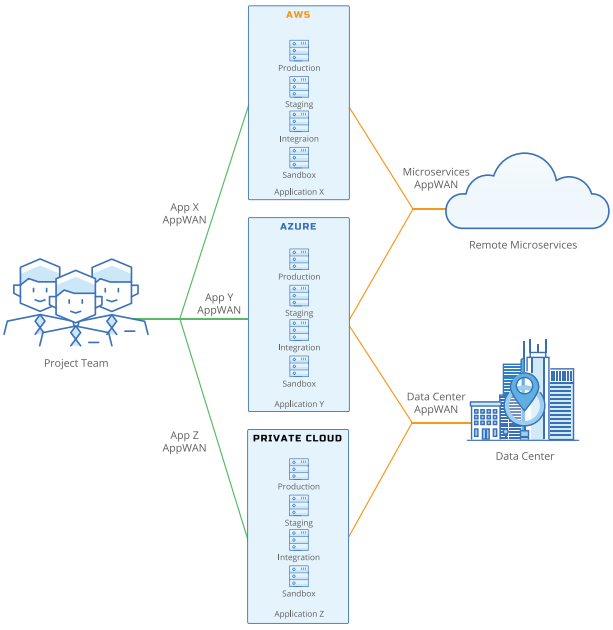
Software-only, micro-segmented application specific networks called AppWANs, created using the NetFoundry platform, can now replace the traditional, complex connectivity models used by developer teams. Netfoundry offers a streamlined, automated, and secure alternative that offers cloud-to-cloud and edge-to-cloud models for connecting users to applications and applications to applications with a Zero Trust approach.

NetFoundry integrates with popular DevOps tools, can be codified into an Infrastructure as Code (IaC) plan, and is network and cloud vendor agnostic. Within AppWANs, pre-authorized and authenticated endpoints route each session across the NetFoundry virtual mesh network. This is a secure, global Internet overlay orchestrated by a cloud-native, instance-specific network controller which integrates with business and application systems such as IAM, IoT identity, and cloud policies. It does this while securing traffic across multiple layers and adaptively optimizing performance and throughput.

Application teams can easily configure and operate AppWANs. Each AppWAN is a selected subset of endpoints associated with an application with which, authorized endpoints are allowed to exclusively communicate, creating a zero trust relationship. NetFoundry AppWANs enable non-expert Line-of-Business and IT project teams to quickly and independently spin up and scale out secure, compliant, performant, distributed applications as easily as they spin up services inside a public or private cloud

In the past, each time a new VPC was created, it had to be connected to the enterprise network, and that typically took a few days of manual IT NetOps processes to complete. In fact, this process has remained one of a few components of the cloud ecosystem that hasn't been replaced with a Terraform or CloudFormation plan. NetFoundry offers integration and the ubiquitous reach and security of micro-segmented AppWANs thus reducing the time it takes for this key step from days to only minutes. Reduce downtime, eliminate complexity, automate connectivity, & infinitely scale with NetFoundry.

Simple, Secure Remote App Management



Contact us

Share

Start spinning up networks for free at netfoundry.io