prosimo

QUICK START GUIDE:

Getting started with Prosimo and AWS Cloud WAN

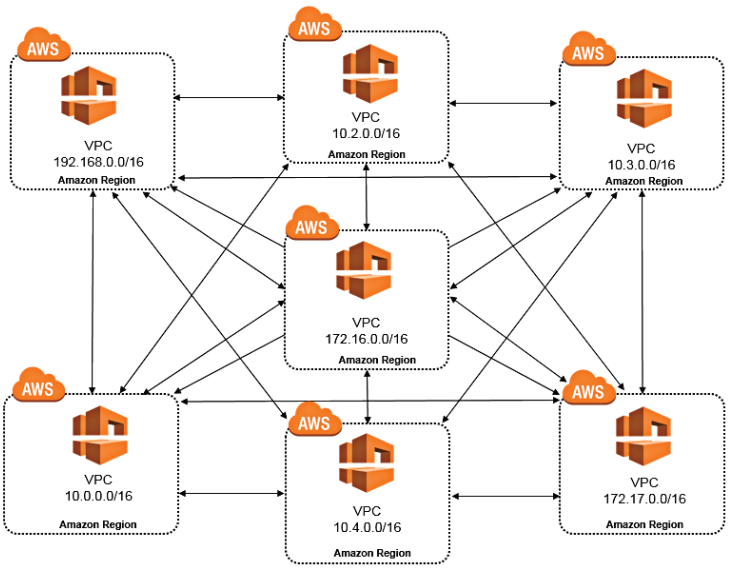
What is AWS Cloud WAN?

AWS Cloud WAN is a powerful networking innovation that allows customers to steer their cloud networks away from complex peering relationships to facilitate workload communication across regions. Customers can now create simple global networks and segments that set up membership-based forwarding for VPCs, subnets, and tunnels to communicate with each other.

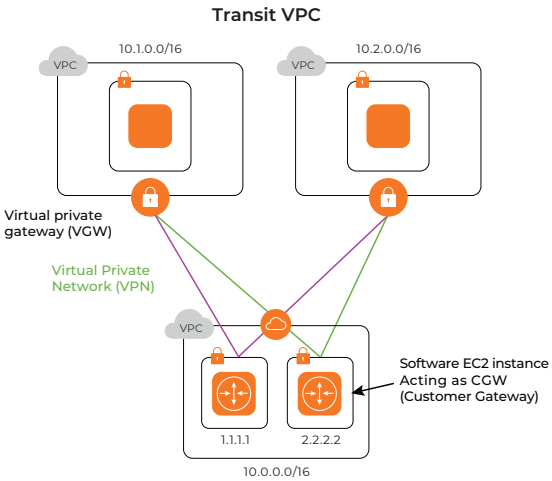
Compare and contrast that with DIY “hub and bespoke” models or setting up complex TGW peering relationships while juggling route scale and policy.

The evolution of Cloud Networking

Some context is in order here. The lack of an excellent cloud-native connectivity model for inter-VPC communication gave birth to the hub and spoke solutions, most of which relied on repurposing the existing on-premises networking stack, virtualizing it, and passing on the burden of managing these appliances in the cloud to the end customer. Several AWS innovations sought to address these gaps, including VPC peering (intra region and cross-region), private link, and eventually, TGW and the GRE-based TGW connect.



VPC peering mesh



TGW – Cloud-native hubs

However, as customers scaled up their use of VPCs and their geographical footprint, the local hub and spokes, based on legacy stacks or even cloud-native constructs based on TGW, began to look like a peering mesh at the networking layer. These architectures are extraordinarily complex and unwieldy to operate, manage or scale. Adding services such as load-balancers and firewalls introduced additional complexity to the networking layer.

Peering relationships based on policy belong in the application layer, and the networking architecture must facilitate the forwarding path between these cross-region workloads.

The question to ask is, "Does my networking layer configuration need to be a direct instantiation of the communication relationships between my application endpoints or subnets?" because that would imply an exponential change matrix every time you need to add a new VPC or a service or make changes to an existing one.

AWS Cloud WAN – Customer benefits

AWS Cloud WAN solves a valid customer pain point. By introducing a flat, global transit network where communication is made possible by segment membership or sharing, the forwarding path is simple and easy to maintain. Networking change management will be faster as setting up VPCs or subnets to communicate with each other globally will no longer require TGWs to peer with each other or, worse setup BGP tunnels or route leaks between regional gateways, instead workloads can hop on or off the global highways (read segments) based on when they need to communicate. The addition of services might mean sharing a load-balancer or a firewall service on a common segment.

AWS anticipates the global network policy to reflect business constructs and how these organizational or functional entities communicate with each other. For example, an M&A activity might result in the addition of VPCs to an existing HR segment or the creation of a new one based on further development groups.

Prosimo Point of View

Customers' usage of Cloud WAN will likely fall in one of the following categories –

- **Coarse and Elastic Segmentation** – The global network policy is kept coarse-grained and straightforward by design to be easy to manage and does not change that frequently. Fine-grained policy-based segmentation and security is the mandate of the upper layers. Orchestration will likely need to focus on security and performance. Benefits of the "simple core network, fewer changes model" are likely to diminish if appliances' security and path setup cause changes to the core network itself. The global network policy is designed to be elastic, dynamically created, and extended to where workloads appear. Optimizing costs and security are likely drivers for choosing this strategy. High automation and operational maturity are vital capabilities that will likely underpin this strategy.

- **Hassle-free multi-region connectivity** – Regardless of how customers approach the core network policy, they will seek to achieve hassle-free multi-region connectivity, at a minimum. Costs and security envelopes will drive the choice for more cloud-savvy customers who have mature operating models.

- **Modern cloud / NetDevOps teams focused on higher layer value** – Internal constituents such as modern cloud or NetDevOps teams will be able to achieve a higher change frequency, more agile development and deployment models while adhering to security and compliance guardrails and maintaining operational consistency and simplicity.

Prosimo's Architectural Alignment with the Cloud-Native Transit Strategy

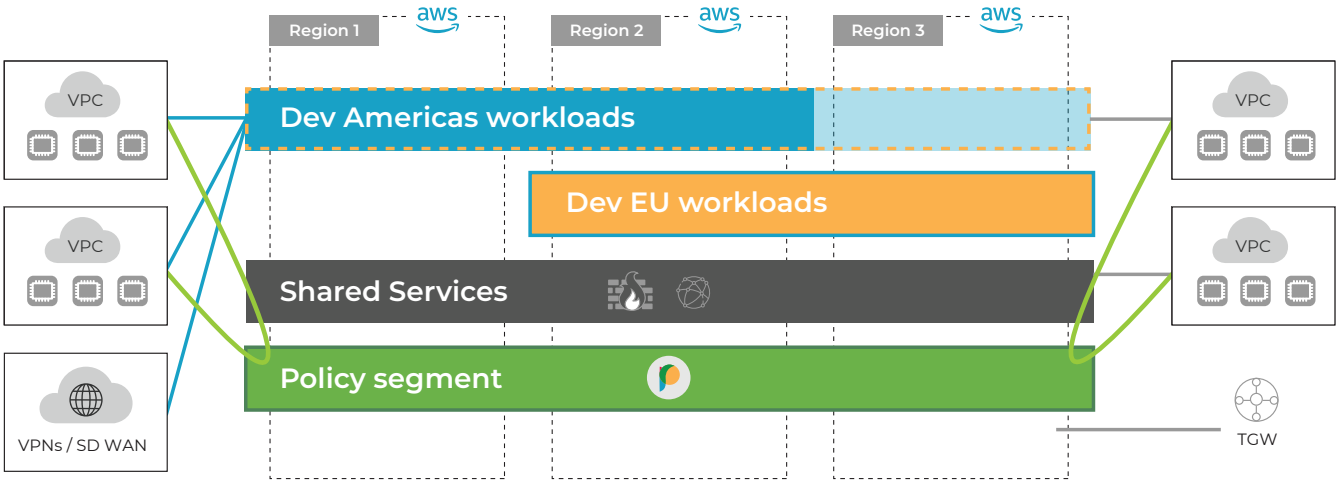
Prosimo focuses on delivering business outcomes for our customers- Zero trust security, Performance anywhere, Operational simplicity, and Cost optimization. L3 connectivity and security provide one or two of these outcomes but force the customer to deal with operationally complex solutions that have ripple effects, managing a disjointed appliance stack, siloed and complex operations, and procedures. Overlapping CIDRs … anyone? In short, carrying the legacy networking architectures to a multi-cloud leads to sub-optimal outcomes.

Prosimo Autonomous transit – Architected to be Cloud Native and in your Control

Prosimo's autonomous multi-cloud transit orchestrates AWS's cloud-native constructs such as TGW, VPC peering, which are optimized for the AWS's infrastructure to create a "cloud as a network-hub "architecture across geographically dispersed regions. Operating at the upper layers of the stack, the Prosimo transit allows users and applications to interact in a globally secure, performant manner and provides operations teams unprecedented visibility, insights

and AI/ML driven optimization recommendations. Since the Prosimo transit infrastructure is in the customer's own account, traffic never crosses a control and governance boundary that the operations teams do not directly view. Security, access, and Performance are not bound to an external network provider's reach. Instead, the transit network scales elastically to provide these outcomes wherever users and applications have a presence. All this is possible because Prosimo's solution orchestrates cloud-native constructs to take advantage of AWS's global presence.

Simpler flatter networks - Coarse grained segmentation with fine grained policy



Prosimo with AWS GlobalWAN

Orchestrate Global networks, Segments and services
Granular L7 policy overlay
Elastically scale segments
Migrate to AWS GlobalWAN

Seamless Orchestration:
Now say, for example, your cloud footprint already extends to multiple regions, and you have built your infrastructure from the ground up for your connectivity and security needs. You likely have a mix of TGWs, peered VPCs, and a static mesh of tunnels to connect these islands. When new regions or workloads appear, you carefully manage your CIDRs, hub and spoke attachments, tunnels, and routes to extend this infrastructure gingerly. Managing a flat, segmented network based on AWS GlobalWAN provides the building blocks for a simpler networking architecture. Prosimo's orchestration of the Global networks, GlobalWAN segments, and routing will lighten our customers' burden of figuring out and maintaining optimal segment sizes and routing.

Autonomous App Transit:
With the Prosimo AppTransit, customers can define granular access policies for applications and a zero-trust model for users. If, for example, you wanted to restrict access to an application for users from a specific geographical region or you wanted to gain insights into the user experience in a particular region, the Prosimo App Transit provides a single pane of glass with which to operate your GlobalWAN based transit network. A simpler, flatter networking architecture reduces the operational burden of maintaining peering relationships at the network level. Instead, it allows customers to define peering policies where they belong – at the application layer.

Faster Migration:
We expect customers to continue juggling multiple cloud-native networking paradigms as they slowly migrate over to a more modern, simpler global cloud network. The complexity of managing VPNs, peering relationships between VPCs and hubs, and simultaneously migrating to GlobalWAN can be daunting. Prosimo customers can continue to live in these multiple worlds and migrate at their own pace as Prosimo seamlessly orchestrates connectivity between these different workloads while enforcing zero-trust access for users and policy-based app to app peering, regardless of how these constituents connect to the global cloud transit.

With AWS GlobalWAN, customers have a simple yet powerful new way to describe a global cloud transit network. With the Prosimo App Transit overlay, customers can deploy an elastic, seamlessly orchestrated network that allows them to migrate and connect their brownfield cloud deployments.

Prosimo Architecture is Future-Proof

Our view is that as the adoption of AWS Cloud WAN increases and customers start to migrate a variety of workloads, more advanced uses of core network segments are likely to appear.

- **Serverless** – as serverless workloads with ephemeral networking presence start to comprise a higher percentage of workflows, the speed and scale of orchestration and policy enforcement will need to improve. Legacy appliance-based approaches that rely on network layer identity to enforce forwarding or security are grossly insufficient to address these needs. AWS Cloud WAN will likely evolve to include functional or tagged identities to allow forwarding on segments based on the functional tagged identities.

- **Segment stitching** – It is not hard to imagine an end-to-end business workflow being comprised of functional steps that are executed by workloads in their own segments likely with their own data gravity and compliance requirements. The ability to seamlessly direct a series of workflows steps or packets through their respective segment chains with segment specific policy enforcement will probably drive additional architectural innovations for AWS Cloud WAN.

Traditional L3 approaches will not be able to meet these new requirements. However, a modern app transit, such as Prosimo's, that operates on app-layer constructs and peering relationships in a cloud-native manner, is best suited to future-proof your cloud networking infrastructure. You can continue to add new workload constituents, define the communication policies or even policy chains, and the app transit will take care of setting up the underlying cloud networking infrastructure in the most secure, performant, and cost-optimized manner. Customers can scale their teams around a uniform operational and governance model with a direct line of sight into operational KPIs such as MTTR, change window reduction, uptime and SLAs. With a modern SaaS platform and deep visibility and insights architected into the Prosimo solution, customers can seamlessly scale their people, processes, and technologies around a uniform framework.

Getting started

Prosimo autonomous multi cloud transit based on the Prosimo Application eXperience Infrastructure (AXI) delivers the desired level of application experience and ensures context-aware Zero trust access to users. This is done using data-driven insights powered by ML on top of a cloud-native infrastructure.

The solution comprises of a data plane component and a SaaS control plane that customers can use to manage the Prosimo overlay in their own cloud infrastructure accounts.

The key building blocks of the solution are:

1. **Prosimo AIR Engine** provides ML-powered application experience recommendations based on actual behavior culled from sensors distributed across global infrastructure. AIR Engine continuously monitors, reacts and improves experiences while delivering enterprise network and security services.

    - Secure eXperience (SX) provides Zero Trust Access, app layer protection and adaptive risk control by delivering the appropriate enterprise security services across your entire organization regardless of the underlying infrastructure. This includes SAML and OIDC based Identity federation, MFA, web application firewall (WAF), IP reputation, distributed denial of service (DDOS) prevention and UEBA.

    - eXperience Delivery (XD) ensures desired application experience wherever they log on using a private Content Delivery Network (CDN), multi-cloud networking, private link, cloud peering, load balancing and communications service provider (CSP) edge. Enterprises can provide the desired experiences automatically without the operations team having to configure and spend time manually optimizing cloud infrastructure.

    - CIRRUS is Prosimo's Machine Learning engine that provides the following recommendations, per customer, based on its learnings: cost and performance optimization, dynamic user risk score and infrastructure expansion based on user access.

2. **AXI Edges** are Prosimo data enforcers and sensor networks distributed across the globe that act as the ingress points for users when they need access to a given application. They also enforce SX and XD services. These sensors are application driven so they can understand the composition of the application and provide adequate capabilities underneath.

Unlike conventional approaches, Prosimo is delivered within your existing cloud architecture—giving you complete visibility and control into application experiences without having to make any changes to the infrastructure. This allows enterprises to take advantage of the cost, flexibility, and scalability of the cloud without unnecessary complications.

Prosimo Dashboard

Prosimo provides a multi-tenant SaaS dashboard where each customer gets their own tenant slice with a tenant-specific URL to access. The dashboard keeps configuration metadata, access, the path to push down server-side certificates to the edges in the customer's own cloud, dynamic and static policy rulesets, telemetry/logging information.

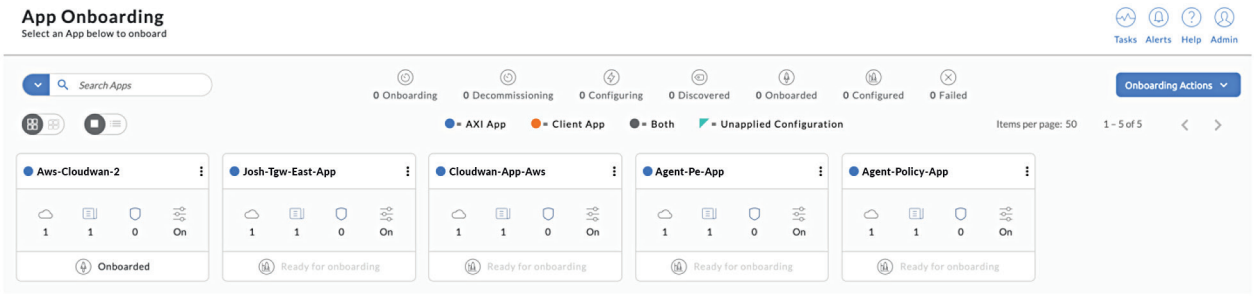
To onboard applications for app to app peering or for zero trust access using AWS Cloud WAN is extremely simple.

What you need to get started

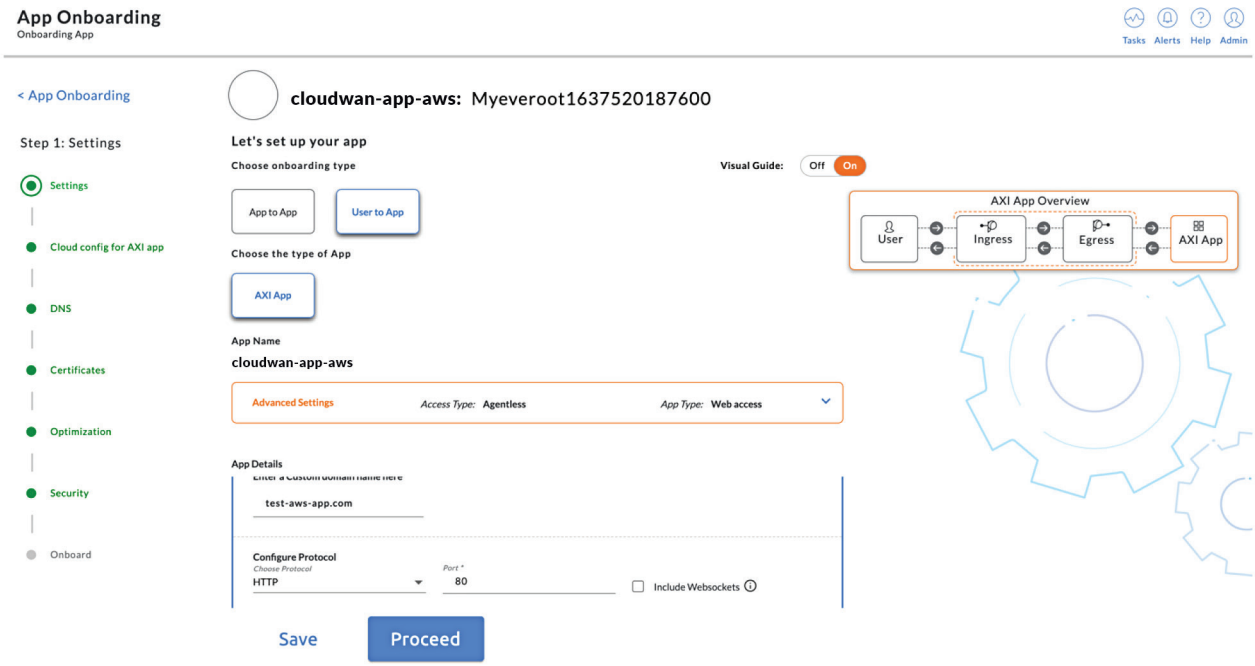
- An account on for Prosimo service.
- Cloud account with required privileges (contributor role) to spin up Prosimo fabric edges in the cloud.
- Admin privileges in Identity federation provider to create SAML/OIDC endpoint or API token endpoint for fabric authentication/authorization.
- IP address or hostname of an enterprise application you want to onboard first.

Onboarding your applications to use Cloud WAN

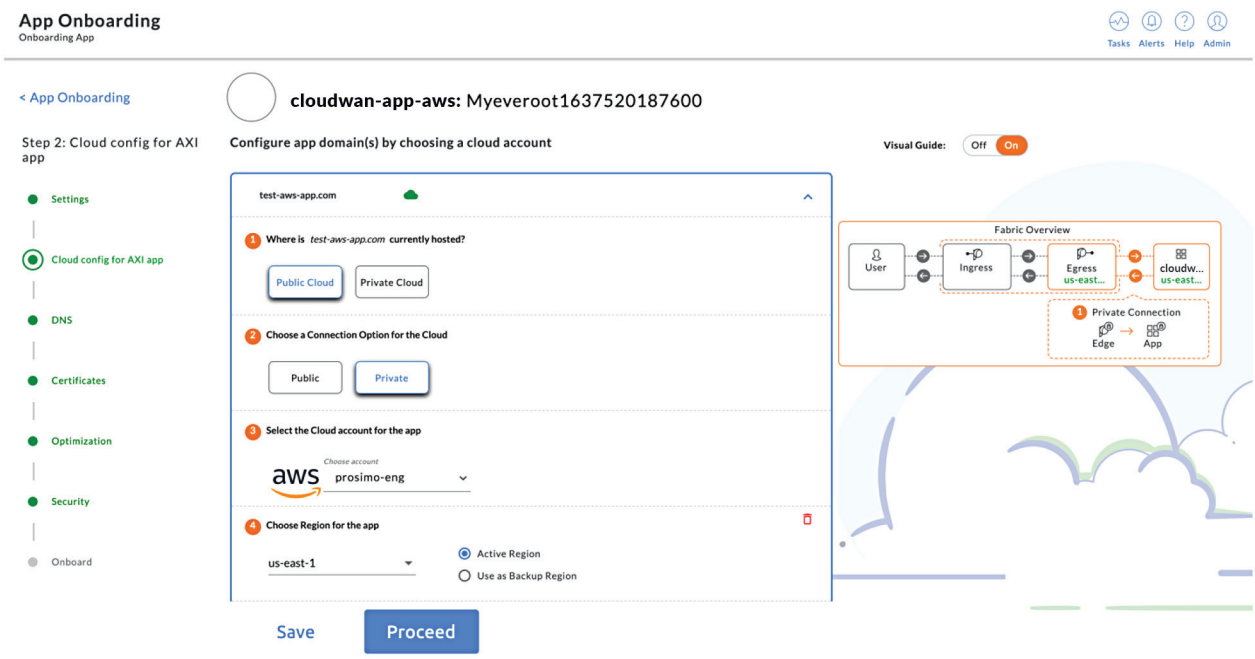
After Cloud accounts and Identity providers have been configured in the Prosimo Dashboard management portal, you can onboard and publish your applications through Prosimo. As a first step to experience the Prosimo capabilities, pick a simple Web application that you can access through your browser when you are on your intranet. For example, Jira, Jenkins, Confluence, or Wordpress etc. You can use your own custom build application web fronts as well.



— On the application onboarding page “create a new app” from “Onboarding actions”

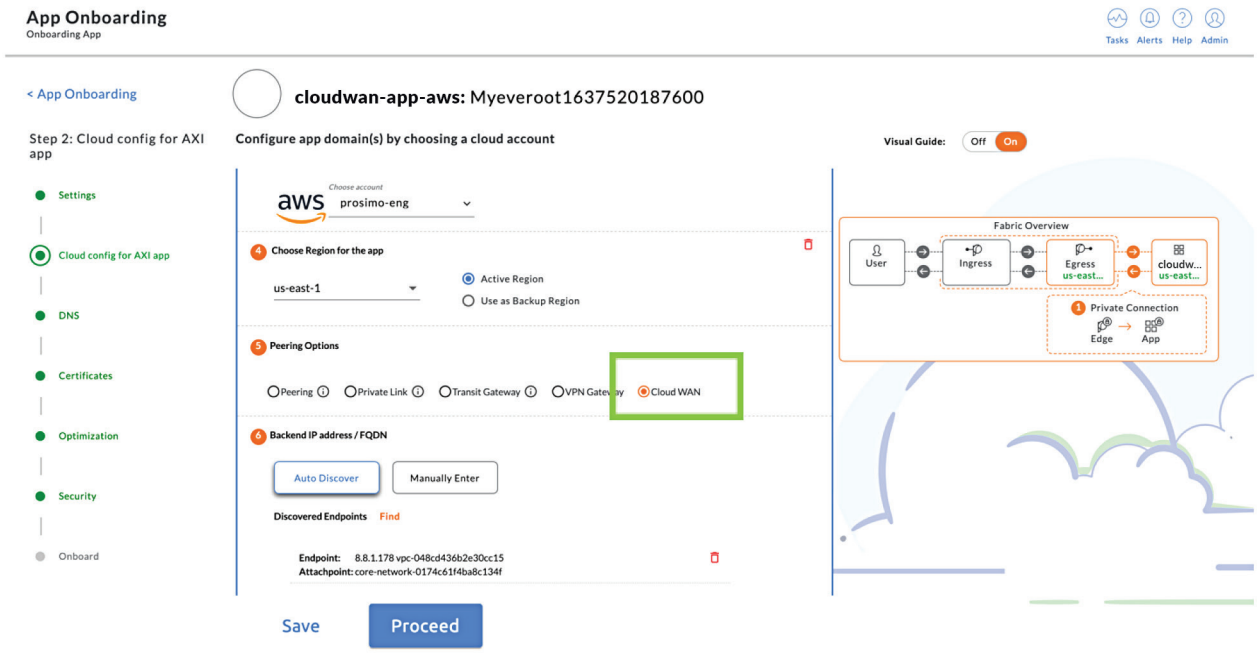


— Specify the access type and domain name for the application.
— Choose the app protocol type (HTTP(s)/RDP etc)

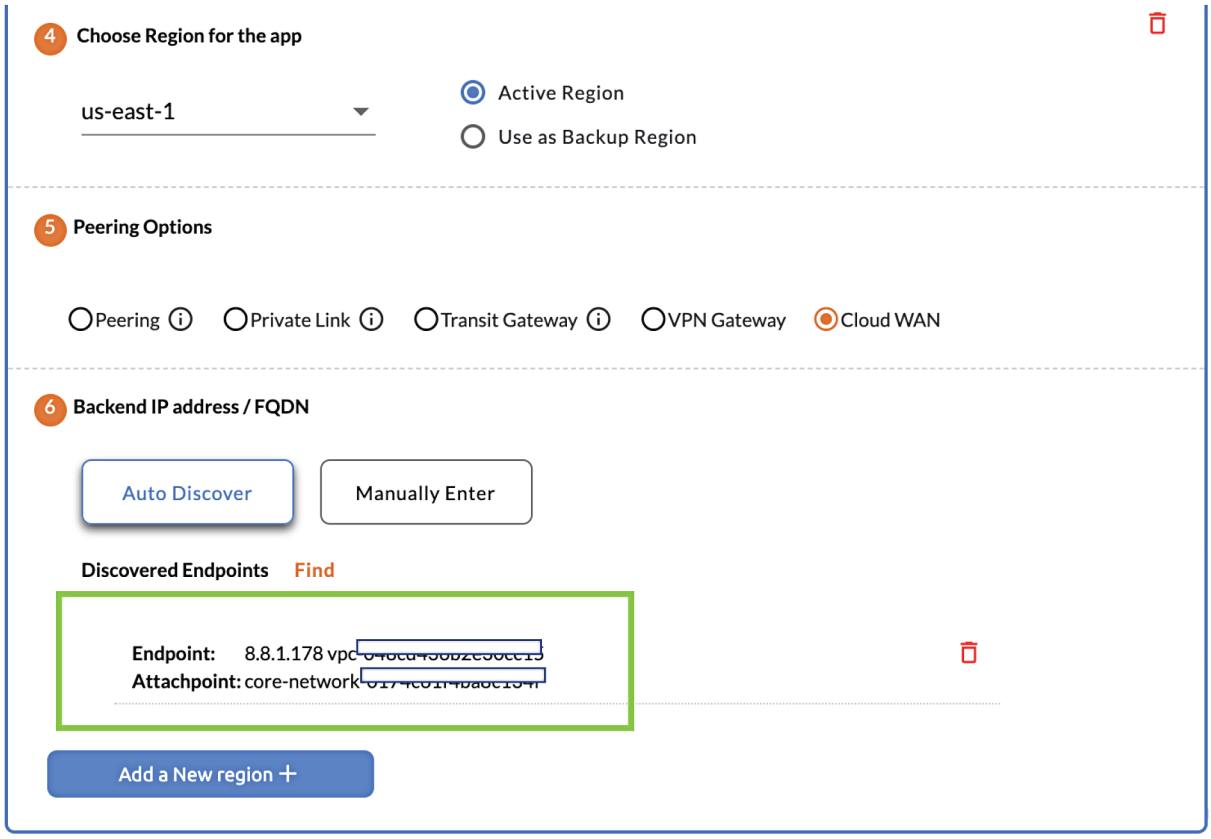


— Specify the cloud deployment details for the application being onboarded
- Cloud
- Region
- Account
- Deployment mode

In the same step where you specify the connection type you need for this application , in addition to VPC peering/Transit Gateway etc you will see the Cloud Wan option



— Select Cloud WAN to onboard your app



The endpoint address and core network attachpoints are displayed.

— Configure the rest of the application onboarding information and your new app is now accessible based on policy to be accessed by users or applications all over AWS Cloud WAN

It is extremely simple to configure AWS Cloud WAN connectivity through Prosimo for your application workloads allowing for granular policy enforcement while maintaining a simpler flatter network. Migrating and connecting workloads with different connectivity options is extremely simple to setup as well without compromising on the security posture.