Graphiant Technical Whitepaper

graphiant

Contents

An Introduction to Graphiant

Graphiant was founded in 2020 and spent two years building the service, architecture, and product. Beginning in April 2022, Graphiant started ongoing early field trials and pilots with large enterprise customers.

Graphiant officially launched the company on September 8, 2022. Graphiant seeks to change how the world builds networks, replacing failing technologies like MPLS and SD-WAN with a simple, fast, scalable, secure, and highly cost-effective Network-as-a-Service.

Graphiant's CEO and Founder, Khalid Raza, co-founded Viptela and is considered the father of SD-WAN. Former Cisco and Viptela executives, thought leaders, architects, and developers comprise the majority of Graphiant's team. This team has a deep understanding of enterprise networking and extensive experience with product development, customer experience, and technical support.

The Problem with Today's Connectivity Solutions

MPLS was designed in the late 1990s for a different era. Networks were simpler. The enterprise connected the data center(s), HQ office workers, and perhaps a few branch offices. Workloads were well-known and traffic was predictable. MPLS became the de facto connectivity solution for enterprises.

By 2010, enterprises were seeing an explosion in traffic coming from things like video, Office 365 and VPN traffic. As more traffic was added to MPLS circuits, costs exploded. Large enterprise customer networks were spending $200-400 million a year on MPLS connectivity.

Enterprises needed more cost-effective bandwidth. The obvious choice was cheap commodity bandwidth that was flooding the market, but IT needed to be able to manage this bandwidth with MPLS, and to do so in a secure fashion.

This is precisely what Khalid Raza co-founded Viptela to provide. They introduced SD-WAN to the market in 2013. Viptela became the dominant leader in the new SD-WAN market.

So, by 2017 enterprises had a solution which combined the extreme performance and security of MPLS (at a high cost) with SD-WAN's relatively easy to provision, inexpensive bandwidth (albeit not as reliable nor secure). It was an uneasy pairing that lasted for the next 5 years.

But by 2022 this pairing was starting to fail as network topologies became complex, dynamic, and unpredictable. Applications are now spun up in the cloud on infrastructure that the enterprise does not control. And, they're connected over networks and services the enterprise neither owns, controls, or has visibility into.

Enterprises were forced to build their WANs on top of this digital wilderness. Trying to use a technology like SD-WAN, or trying to use something that is dedicated to pre-building bespoke networks and configurations, or building an overlay over an underlay transport doesn't work in this kind of environment.

This is the problem that Khalid Raza founded Graphiant to solve. But to solve this required a complete rethinking of how to deliver connectivity:

- **Private Network.** For the same reasons MPLS is a private network, Graphiant needs to be a private network. You simply cannot deliver a performant, reliable, secure network if you use the public internet for your transport.

  Disaggregate As-a-Service. We don't have the ability to build unlimited overlays, and we often don't have the support staff. We can't build all the tunnels needed to connect branches, cloud, machines, SaaS, business partners, etc. We need to have enterprise grade reliability. One of the great things about MPLS is that it provided service level agreements. We knew what kind of loss, latency, and jitter to expect, so we need to provide this as well. We must do all of this, and deliver any-to-any connectivity as a service.

- **Fast, simple, easy provisioning.** The one thing SD-WAN got right was simplifying network provisioning. Except, of course, for all the tunnels. But Graphiant knew our next generation solution needed to be just as simple.

  That's why Graphiant made our next-generation edge an "as-a-Service solution". There is no network to build, enterprises simply provision what they need from a simple, easy portal in the cloud. New networks are configured in clicks and minutes, not months.

- **Disaggregate for Cost Efficiency.** Why is MPLS so expensive? The reason is that MPLS is old technology in which the control and data plane are coupled. This means every part of MPLS infrastructure requires enormous compute capacity to power the control plane functionality.

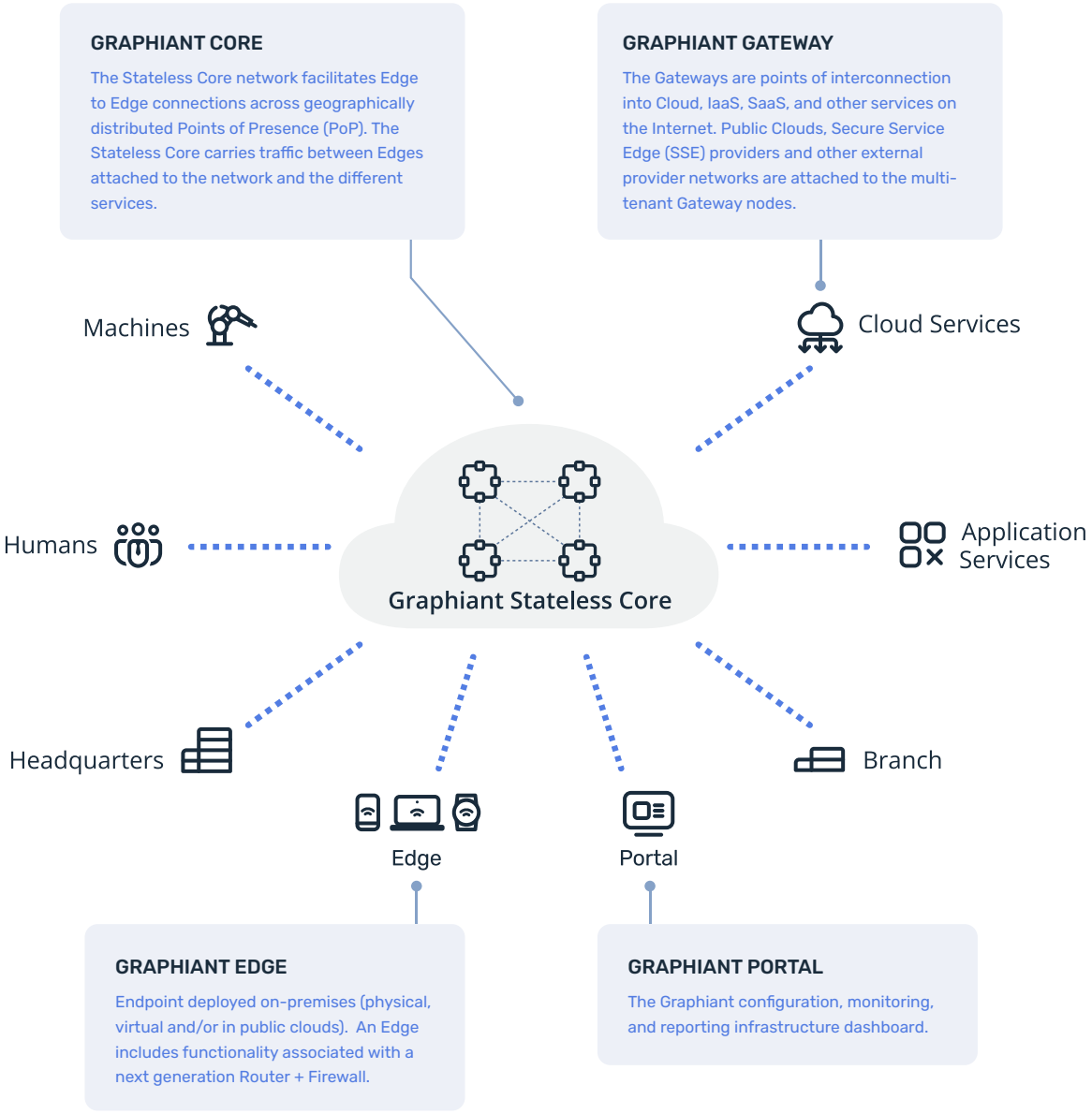
  This isn't how modern networks work. Today, the control plane is separate from the data plane, meaning most infrastructure requires less compute capacity. The ultimate version of this concept is to have control run in the cloud, where there is unlimited (and extremely affordable) compute capacity.

  That's why Graphiant next-generation edge solution separates the control and data planes, placing control in the cloud. This drives up to 67% lower costs than MPLS, without sacrificing performance, reliability, scale, or security.

Graphiant Network Edge

The Graphiant Network Edge is a Network-as-a-Service that gives enterprises a fast, simple, easy way to build enterprise networks. The result is a network that is

- As performant as MPLS (fast, scalable, reliable, and secure)
- Simple, fast, and easy to provision
- Dramatically less expensive than legacy network options (MPLS, SD-WAN)



How?...

Graphiant has developed a cloud-delivered Network-as-a-Service (NaaS) that incorporates full control and policy management over the enterprise Wide Area Network. It does this by using a unique architecture that keeps routing and control in the cloud, while allowing customer to use policies to program metadata in data packet headers which is used by networking devices in the stateless Core to route the traffic with little overhead. This enables users to enforce specific networking service levels to be programmed across all the devices and endpoints in the network.

In other words, the Graphiant service ensures all enterprise applications are delivered from source to destination with guaranteed SLA, across a private network, between the customer's own network endpoints, or to another enterprise. From the hardware router or VM connecting your enterprise edge, to the last miles connecting them to Graphiant's private Core, or to the cloud of you and your business partners choice, Graphiant has you covered.

Ways to Consume

This first principle of the Graphiant network is, customers should not have to build the network, it should already exist. Instead of deploying or subscribing to a new or 3rd party middle mile backbone, or designing policies constructs for an overlay before migrating sites, you should be able to just subscribe to the connectivity you want. Your sites just show up and from there you configure how each application should be handled. For example, we no longer think about the fact that cloud providers are a huge physical farm of datacenter compute. We just call it the cloud and subscribe and buy however much compute we need. Thinking of enterprise connectivity in that way is how we approach the Graphiant Service model. With Graphiant, you subscribe to the service based on the amount of bandwidth required, decide how applications should be prioritized, and what kind of transport they should take. We take care of the rest.

We offer flexible choices in how the enterprise edge connects to the Graphiant Stateless Core via the Graphiant Service. We are committed to the path of all options being programmatic, so will never use proprietary boxes or custom hardware. We've initially established a partnership with Lanner, but are working on options with Dell, HP and others. The idea being "if it's X86", it should be able to run our software".

For customers with existing edge compute, KVM, ESXi, and other popular options are available. In all scenarios, network operators will have control over the edge to configure local traffic polices, utilize troubleshooting tools, and have deep visibility into how traffic is being handled as it crosses the boundary from the internal network to the destination of choice. Either direct to Internet, or through the Graphiant Stateless Core in-route to the SSE providers of your choice, branch sites, or CSPs, all options can be

configured through the Graphiant Portal that each edge is always connected to. To use the cloud service analogy, a server inside an AWS data center is AWS owned, but the customer controls the compute and how they decide to use it. With Graphiant, the network is already built and delivered as service, but our customers have control and agency over how to consume it.

Service Delineation

Graphiant provides a comprehensive support service that avoids the trappings normally associated with traditional split-support models. In short, wherever or on whatever platform our edge software is installed, we are involved in every aspect of the support process. Our solution is collapsing most of the PE function directly into the edge device, so that the Core doesn't have the overhead of the PE routers regarding VRF state and customer routing information. This means the edge is becoming more intelligent, and critically important to be fully covered as part of our service.

Regarding the choice of platforms that run our software, customers may either use approved hypervisors, or have the option to buy or lease certified edge hardware. Regardless of the route taken, Graphiant is the central source for support. Whether customers chose to purchase or lease, via partner or provider, support for the certified Graphiant hardware is always covered. There are no 3rd party orchestration shims or control software in play with our service. We understand deeply that our customers want to avoid situations where they call a software vendor for support and are then referred to hardware manufacturers when issues are identified.

We have designed our service model to avoid these issues by taking a partner lead approach. Since our partners are already providing the Graphiant solution, they provide RMA support for the hardware, in conjunction with us owning the software, service, and everything else. Our partners being integrated into the service model allows them to address potential hardware issues directly with the manufacture, on behalf of the customer.

We are providing a service, not selling hardware or software. We help our customers isolate problems, then either we fix them directly, or help customers pinpoint the issue so they have actionable data points to resolve and recover (i.e., circuit degraded, HW fault, hypervisor issue, etc.).

In the event there are issues with customer owned hardware edge, we help them communicate with the vendor until they understand it's their problem. We understand this is rare in the marketplace, and that doing so it critical to our customer's success as well as ours.

Architecture

Today's Routing Stack is Broken

Graphiant's vision is to evolve past MPLS and SD-WAN towards a more advanced Network-as-a-Service (NaaS). Our vision is a private and virtualized Internet exchange for business. To do this, we've used tried and true SDN principles but made specific advancements in areas like encryption and data-plane management. Further, we designed a new routing stack that lets us adjust this new "Internet" quickly based on business needs.

The innovation around SD-WAN was centered on the separation of the control and data plane. Encryption key exchange for the data plane was automated and transmitted via the control plane. This was an improvement over traditional pre-shared-key and other methods. However, today's data planes still rely on full IPsec tunnel association from edge to edge. In other words, today's data planes are using 20 year old technology, only a slight improvement over DMVPN.

The SD-WAN industry has started to recognize issues inherent to using the indeterminant Internet as transport. While SD-WAN can respond to issues, there comes a point when applications and their users are affected. Middle Mile Optimization and SDCI providers try to address these challenges, but can't address problems with IPsec security associations between the edge and other points along the path.

Every time data is encrypted or decrypted, it takes more processing power. Also, each point in the middle can now see the unencrypted data while it's being transferred, and additional checks and inspections happen before the data is encrypted again. Current solutions create control and data plane relationships and then add an encryption layer. This approach has significant issues regarding security and scalability.

Introducing the Graphiant Network Edge

The Graphiant edge was designed to be "any" x86 platform either in hardware or virtual form factors. There are three types of Edge's that will be available for customers to choose from:

Graphiant Edge

Virtual Edge
Generic Virtual Edge on ESXi, KVM,

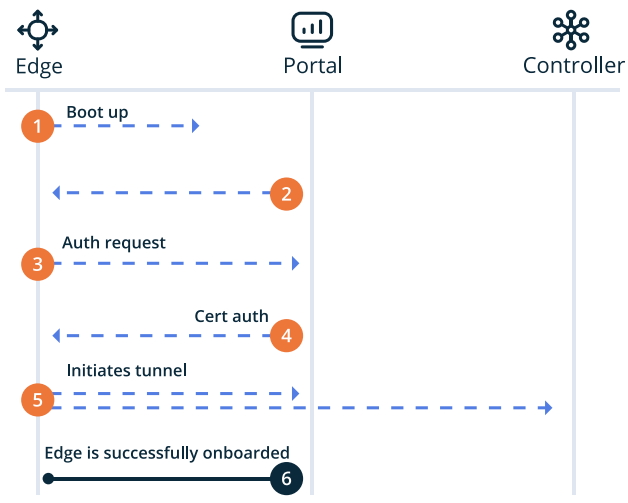
Cloud Edge
on AWS, Azure, GCP

Hardware Edge

Supported form factors and associated software will be managed by Graphiant and our partners. Installing virtual form factor options at customer site will involve booting a KVM or OVA file, scanning a QR code, and logging into the Graphiant Service Portal where everything else will be configured.

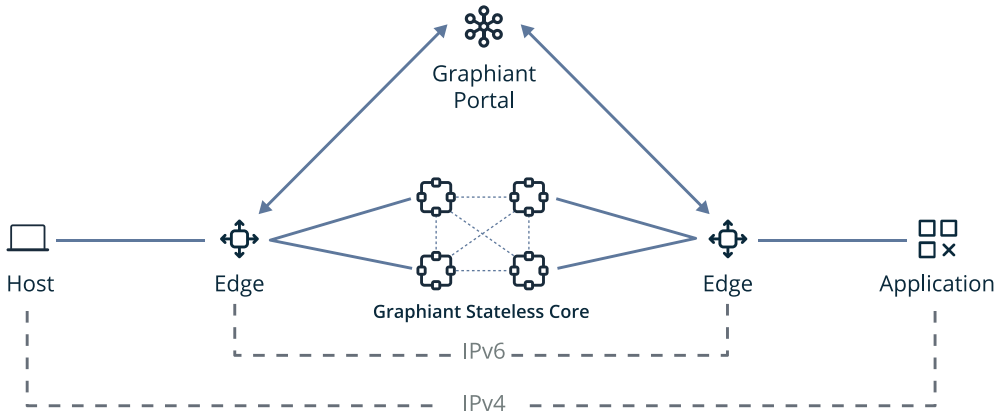
Edge Onboarding

1. **Platform boot up & bring-up Connectivity to Portal**
   - UEFI BIOS, Secure Boot ensures to only boot images signed by the Graphiant key in the firmware
2. **Portal validation**
   - Admin authorization needed for VM & Cloud platforms
3. **Edge authentication by requesting Graphiant certificates**
4. **Portal provides GEK & GAK certificates for the Edge**
5. **Edge initiates tunnel to Portal & Controller**
6. **Upon admin authorization, Edge onboarded successfully into the Graphiant network**



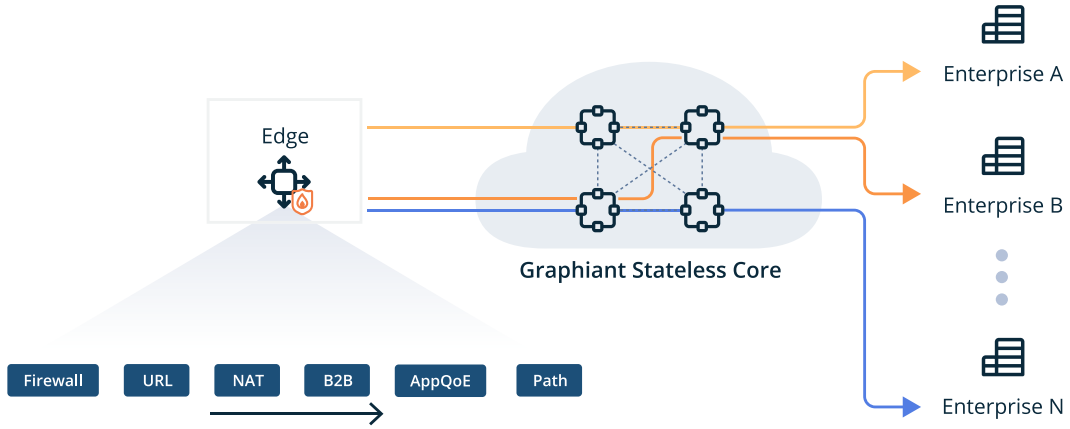
Hardware Edges will come pre-loaded with the Graphiant Edge Operating System, and will register automatically using certificate's present in the Tamper Proof Modules (TPM) to authenticate with the Graphiant Portal where customer configuration will take place.

Graphiant Network



This process happens automatically and transparently from the end user perspective so that only traditional LAN and WAN interface routing is configured on the Edge by the customer.

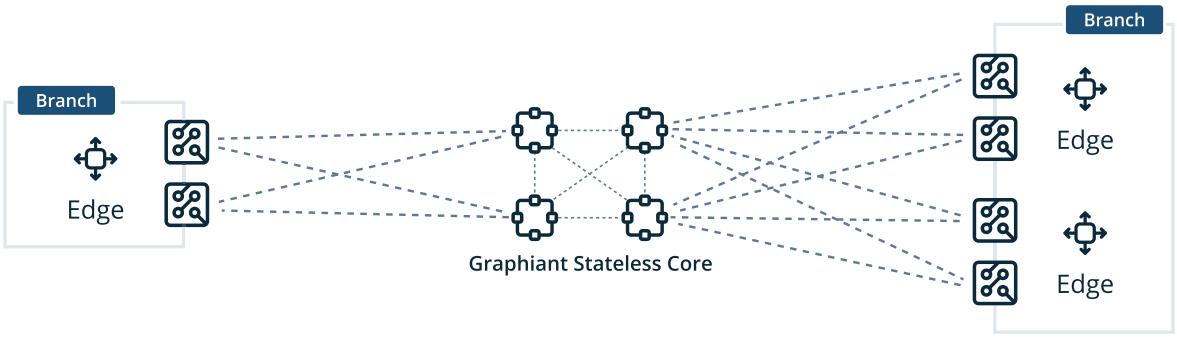
Simple & Granular Policy Controls



Through Graphiant's Cloud-hosted Portal, all network typically associated with the enterprise edge will be accessible and configurable on the Edge. In modern networks, being able to utilize multiple circuits, sending traffic directly to the Internet and be inspected either locally via Next Gen Firewall (NGFW), or via 3rd party tunnels to the SSE vendor of choice are considered table stakes.

In addition to standard services, the Edge will encode metadata label information for the Stateless Core. This allows users to program traffic routing via the Portal and send it to the Edge. Users can decide how QoS is applied, define segment membership, influence path selection, and map B2B traffic as needed. This makes the Graphiant Edge smarter and enables the Stateless Core to focus solely on packet forwarding. Crucially, all traffic between Graphiant Edge nodes will be encrypted end-to-end, with no decryption in transit.

Branch Redundancy



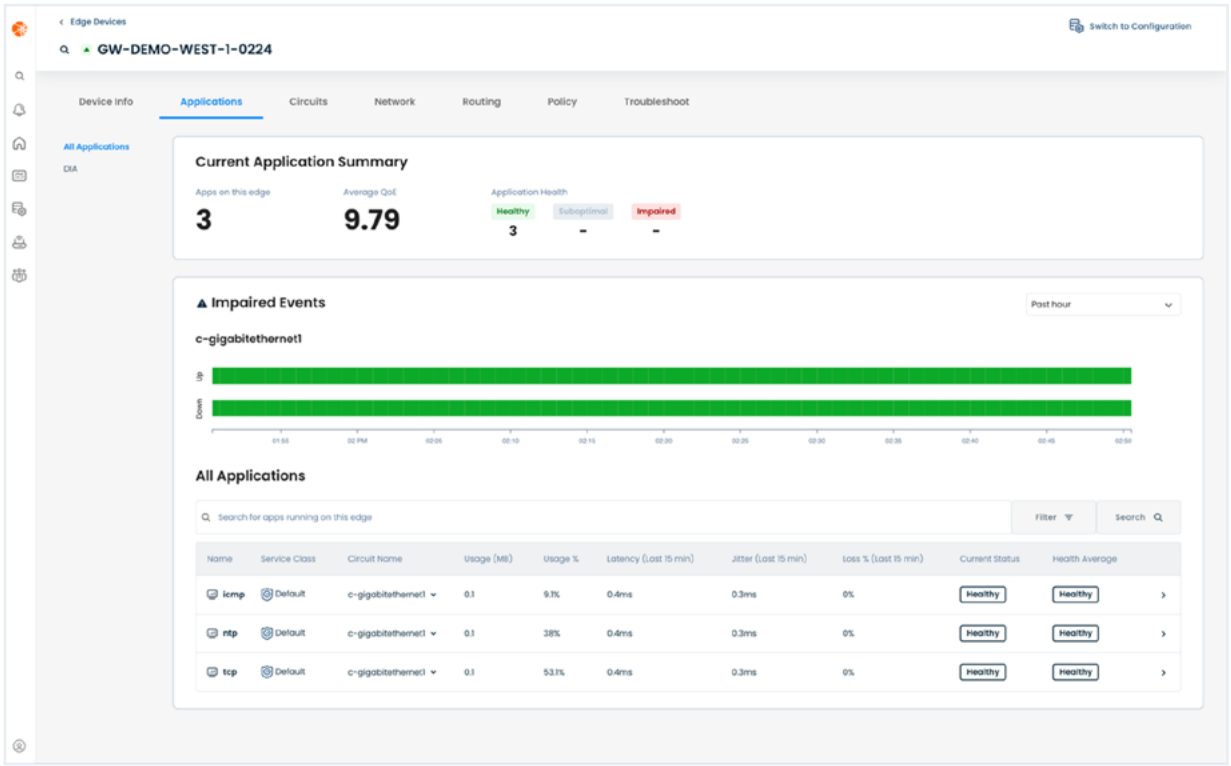
Single CPE

Dual Uplink-Tunnel to two different core nodes

Dual CPE

Dual Uplink-Tunnel to two different core nodes. First hop LAN redundancy via VRRP or IGP/BGP

Branch WAN circuit redundancy can be achieved through the use of multiple WAN circuits, and Edge redundancy can be achieved through the use of multiple Edge devices. In a high availability (HA) scenario, depending on the local site network configuration, the Edge can use VRRP with object tracking for quick L2 failover, or for L3 sites, use OSPF or BGP to achieve ECMP as well as HA. The Graphiant Stateless Core also solves for return traffic symmetry, removing a layer of complexity from the end user configuration.



Finally, Graphiant Edge provides Deep Packet Inspection (DPI), recognizing thousands of common applications. The Graphiant Portal offers visibility, reporting, and the ability to program application routing and prioritization across the Stateless Core. Users can also define custom applications based on attributes like source/destination IP, DNS, and more via the Portal. Where possible, the DPI engine will classify traffic using first-packet matching for well-known resources.

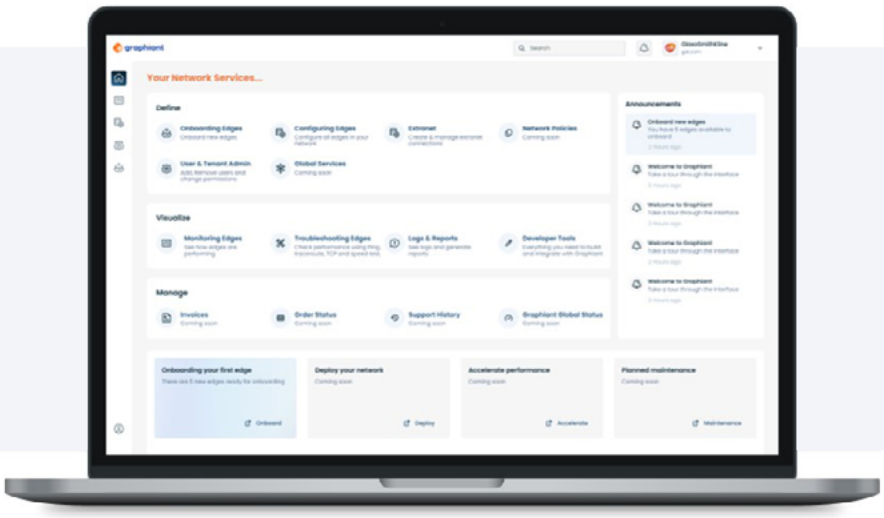
The Portal

The Graphiant Portal, accessible at https://portal.graphiant.com, is a one-stop platform for users to engage with the Graphiant solution. It enables users to deploy, configure, upgrade, monitor, and troubleshoot their network. The portal also hosts an API gateway, allowing customers to interact with the service programmatically.

Admin Visibility & Troubleshooting

Intuitive Management

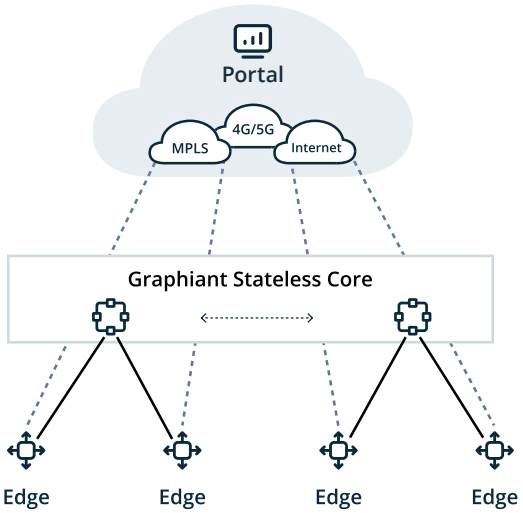
- Administration
- Configuration
- Monitoring
- Analytics
- Reporting
- Troubleshooting



Control & Management Plane

Graphiant Cloud Services

- Natively multi-tenant
- Handles reachability for Graphiant Service
  - Data Plane Connectivity
  - Transport Network Connectivity
  - Subscriber Services
  - HA and Redundancy
- Multi-operational modes for deployment flexibility



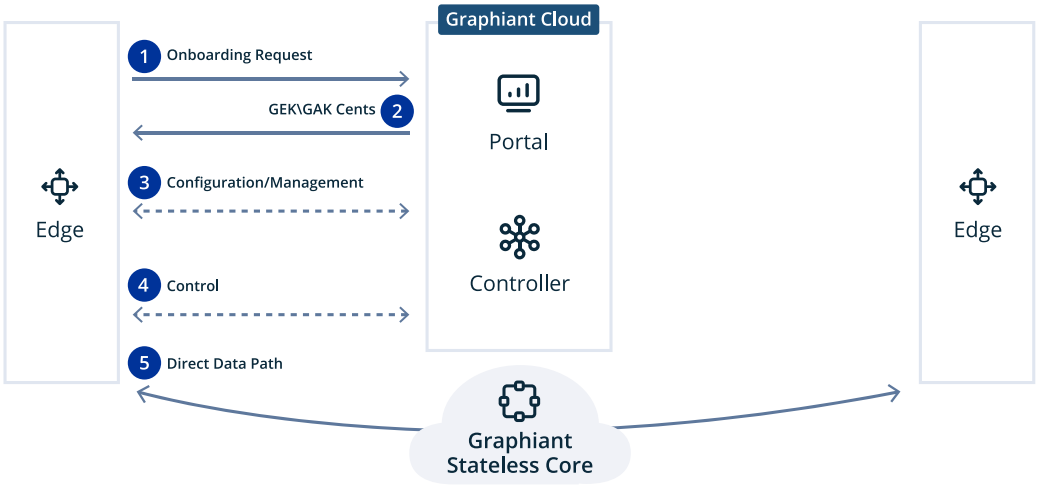
The Graphiant Portal, residing in both the Control and Management Plane, maintains constant connection with Graphiant Edges via a secure tunnel. This connection allows real-time monitoring, troubleshooting, configuration adjustments, and enables all use cases provided by the Graphiant Service. The Portal is natively multi-tenant and runs on micro-services across various multiple regions in the Cloud for guaranteed availability. As it's included as part of the Graphiant service and delivered via the cloud, customers don't need to maintain their own control and management plane.

Control Plane - What does it mean?

Legacy solutions tightly couple the encrypt/decrypt boundary with the data plane; encrypting/decrypting traffic at every hop. Graphiant's control plane separates this encryption issue from the data plane, while ensuring that:

1. Security associations must be edge to edge
2. There can be no decryption in transit

Bring Up Overview



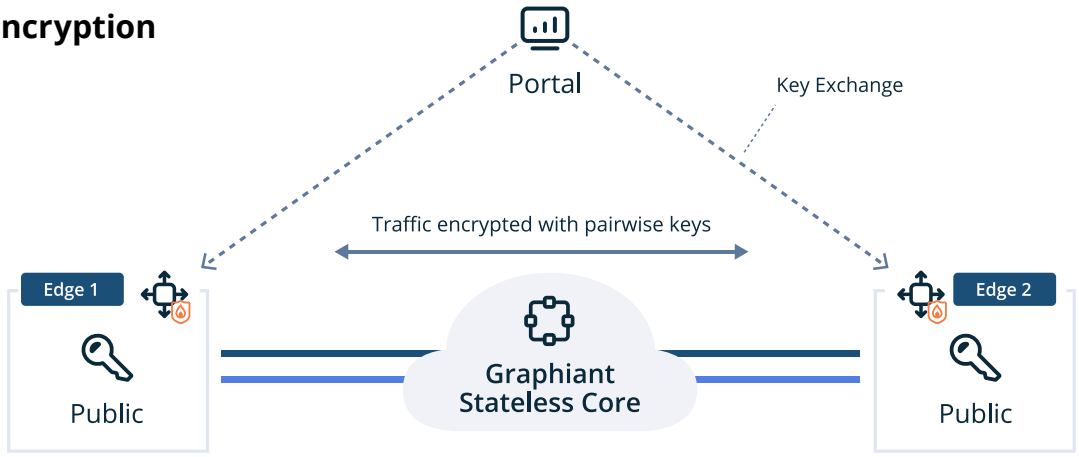
The Graphiant Architecture is designed to comply with all major security regulations regulations (SOC2, HIPPA, PCI-DSS, etc.). We ensure that hardware devices approved for our service include Tamper Proof Modules (TPM) or Hardware Security Modules (HSM). For virtual devices, we utilize HSM and TPMs available on platforms like KVM, ESXI 6.5+, AWS NitroTPM, Azure Confidential computing, and more.

Our software never generates keys. Instead, we rely on TPM or HSM and use their private/public key pair for setting up primers and symmetric encryption keys. The key store resides on the device's HSM and is under the customer's control. Graphiant never accesses the edges' private keys and we don't use pre-shared-keys.

We use the private/public key pair from the TPM or HSM key store to setup encrypted connections to the Graphiant Portal and Controller. We then use Diffie-Hellman, via the controller, to set up pair-wise keys for data plane traffic between each pair of edges. Our software never generates keys. The key store resides on the device's TPM or HSM and is under the customer's control. Graphiant never accesses the edges' private keys, and we don't use pre-shared keys.

Once certificates are exchanged and issued to the edge based on the key store, it then establishes a connection to our Portal. Once this control plane relationship is established, the edge device doesn't need another exchange with the Core network. It relies on the metadata information delivered by our cloud-based Portal. In essence, the Portal instructs the edge on what metadata to use when communicating with the Core.

Encryption



Keys should never be exchanged over the data plane. Instead, we use the public key information on the edge's HSM to generate Diffie Hellman primers, which are then exchanged over the control plane to establish an edge-to-edge security association. This is not a conventional "tunnel," but rather a security association that allows for data encryption and decryption between two edge endpoints. We've decoupled the relationship of tunnel and encryption key exchange.

The payload is encrypted edge-to-edge, with only the edges able to encrypt and decrypt it. With no edge-to-edge tunnel, there's no need for a full session state or running BFD or IP SLA probes. Compared to an IPsec relationship, our approach is quicker to set up. In a full mesh environment with transport flaps, a large number of tunnels terminated on each edge increases this time exponentially.

Our advantage lies in the absence of end-to-end IPsec tunnels. Edge nodes only establish a data plane connection to the Core. The security association key exchange doesn't require a full session state handshake, taking only a couple of seconds depending on the latency between each Edge and the cloud they're communicating with to exchange the Diffie Hellman primers. Key exchange and rotation have no relationship with the tunnel, and encryption is also decoupled.

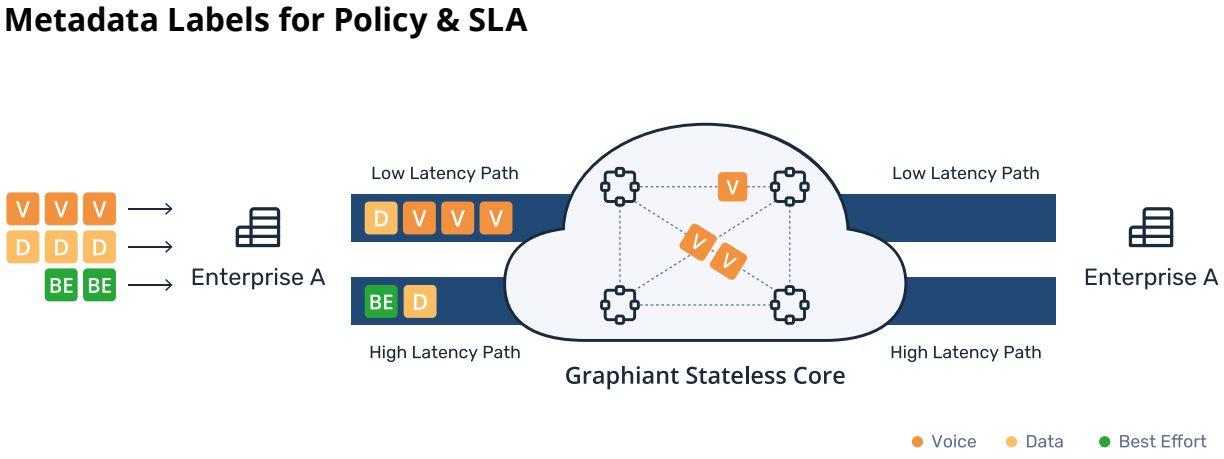
From a traffic perspective, when the edge sends traffic, it uses the security association of the destination. However, the next hop is the Core, which has no key pair association, eliminating the encrypt/decrypt event associated with the next hop. When the packet reaches the Core, it merely label switches the packet. Only the destination edge, with the security association, can decrypt the payload.

All other transport solutions and architectures include the state is in the Core. Not so with the Graphiant Stateless Core. Our design strategy focuses on making the Core as lightweight as possible, prioritizing efficiency and performance above all else.

Graphiant's Stateless Core & Data Plane

Because of the Graphiant Stateless Core's multi-tenant capabilities, it allows for management of connectivity to Graphiant services and provides dedicated bandwidth and high throughput in a stateless environment. As a result, enterprises are able to connect to the edges.

Our Stateless Core differs from MPLS VPN as it doesn't contain any customer information, routing state, or VRFs. Compared to SD-WAN, we reduce the number of tunnels and overhead associated with current SDN deployment models. Essentially, the Stateless Core is a pure packet forwarding space.



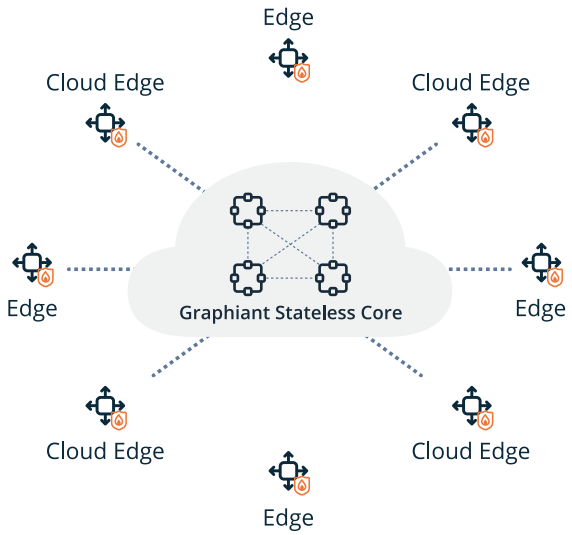
Graphiant has developed a new protocol and BGP extensions that propagate additional information beyond currently available address family attributes. For instance, extended segment information regarding application characteristics is handled in the routing protocol itself. The combination of our new protocol and label switching techniques allows for metadata label switching across the Graphiant backbone. This enables us to guarantee SLAs and allows customers to influence the types of connectivity their applications traverse across the Core. Our service aims to simplify operation without requiring specialized skills.

Due to reduced tunnel overhead and removal of customer config, our Stateless Core nodes have a significantly smaller footprint than traditional carrier backbone routers or MPLS P or PE devices. The lower power draw and smaller physical footprint allow rapid deployment (usually contract +60 days) as per customer demand. This ensures the customer edge is never more than 15ms from the nearest Core, reducing intermediate ISP peering points where most transit issues occur.

Data Plane

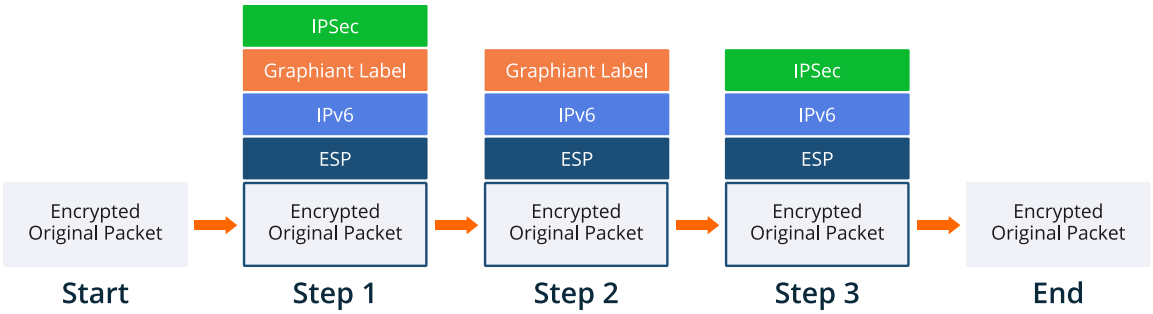
Graphiant Services

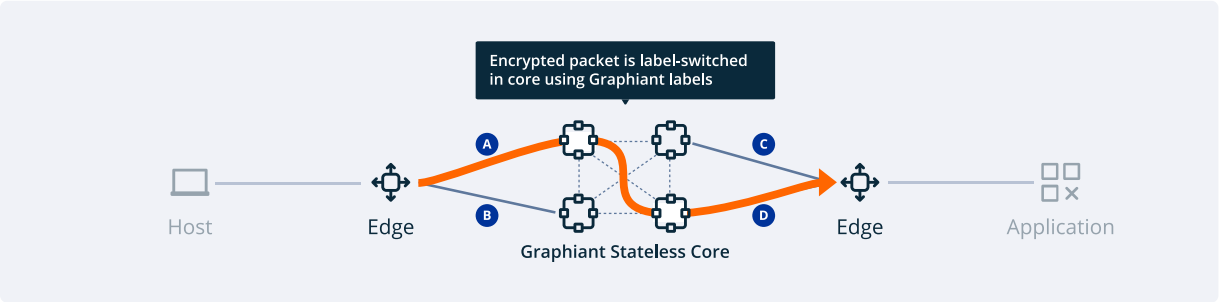
- Natively multi-tenant
- Handles reachability for Graphiant Services
  - Data Plane Connectivity
  - Transport Network Connectivity
  - Subscriber Services
  - HA and Redundancy
- Multi-operational modes for deplyment flexibility



In enterprise networks, security is paramount. That means traffic must be encrypted end-to-end without being decrypted in transit. Simultaneously, the need for each enterprise edge to maintain legacy IPsec tunnels to all other edges should be eliminated. To achieve both, we developed a new protocol stack. To understand this, let's look at the packet header.

Metadata Based Forwarding

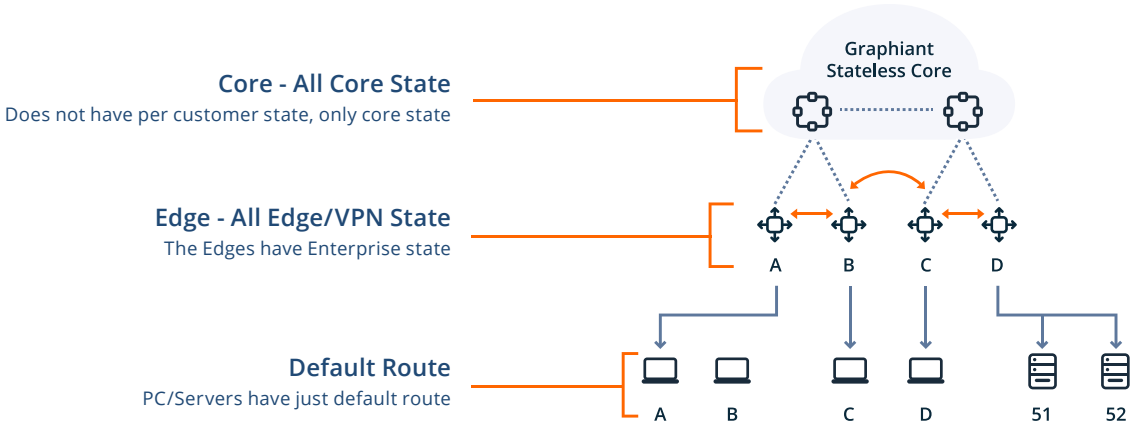




As packets from the LAN enter the Graphiant Edge, we first encrypt the packet and add ESPv3 header based on established security association (SA). The Edge does not build a full IPsec tunnel end to end; separating each is crucial.

The packet is now encrypted but not associated with a tunnel. Next, we add an IPV6 header assigned from our pool, not the customers. After IPV6, we add the Graphiant metadata labels, followed by an Authentication Header (AH) to protect the integrity of the traffic. This allows packets to traverse the public Internet without risk of third-party actors modifying the data or headers in transit.

Scalability of Graphiant Core



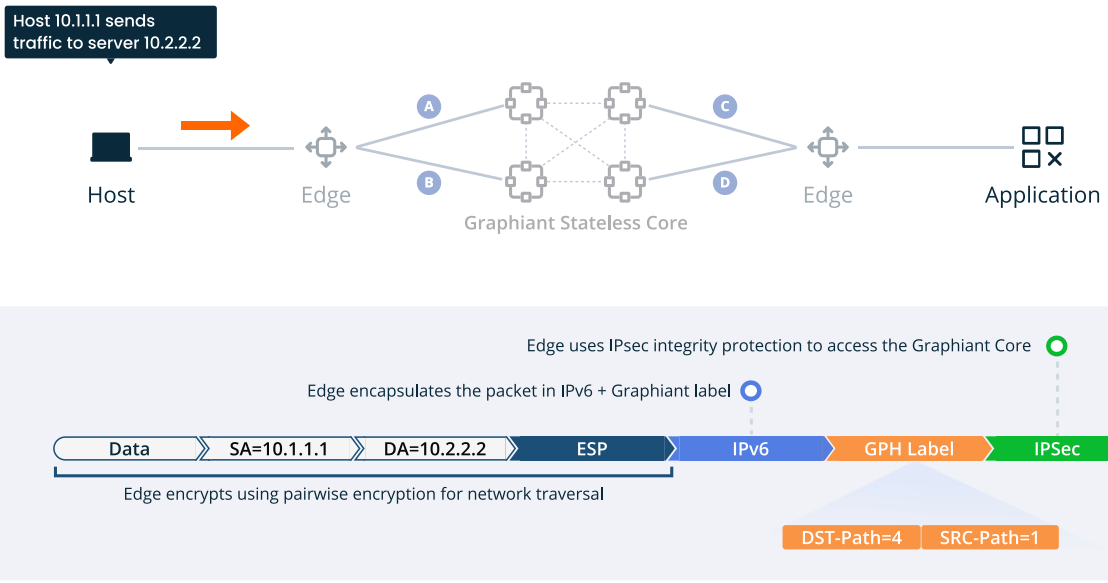
By arranging the packet header in this specific way, we ensure traffic is encrypted only once, maintaining edge-to-edge encryption. This method prevents tunnel sprawl and enables us to transmit customer data without revealing their IP information. In essence, our unique use of ESP, IPv6, and AH ensures that customer information, including their internal IP addressing, is never exposed.

From a forwarding perspective, when packets traverse our Stateless Core, there is no need for fragmentation or reassembly, enabling customers to benefit from the associated performance gain. If the last mile supports a 1,500-byte MTU size, we can maintain this (minus the Graphiant overhead) end to end. If the last mile supports a larger MTU size, the Graphiant Stateless Core can support that as well without the need for fragmentation.

There will be a pre-determined limit on frame size from the edge to the Core. This won't change in transit as the edge is only a hop away from the Core. Our header stack, including padding, will take no more than 92 bytes of overhead for a guaranteed transmission size of 1408 bytes, end to end.

One major issue we're addressing with this approach is the intermittent fluctuation of frame size at intermediate points across the public internet. With our service, this probability is significantly reduced, limited only to the last mile segment where it's extremely unlikely to occur. We know that the only overhead introduced will be our predictable packet header size. Our Core-to-Core connections are private, which allows us to ensure that what's set by your provider remains constant from edge to edge. Our guiding principle is simple: by reducing the number of hops with indeterminate behavior, we can provide our customers with better and more predictable performance over time.

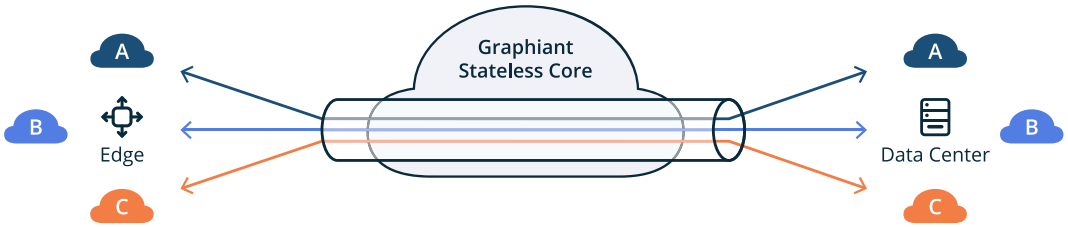
Step 1: Edge to Core



Once traffic reaches the stateless Core, it removes the authentication header providing integrity protection. The Graphiant Core can't decrypt the packets since only the customer's edge has the pairwise encryption keys. Most importantly, the authentications headers ensure our metadata labels can't been tampered with in the last mile.

The Core then examines the metadata stack and determines how and where to route the traffic, selecting the path that meets the SLA specified in the packet header's metadata label.

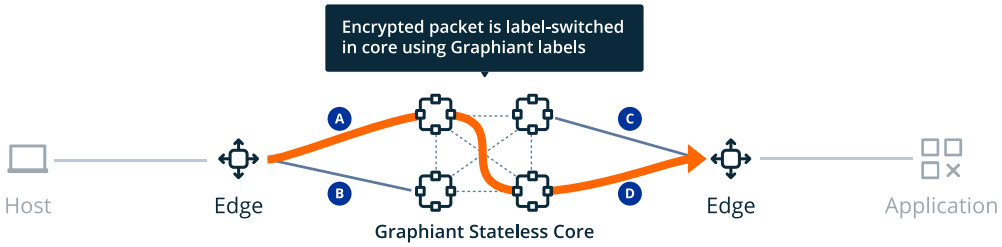
Segmentation

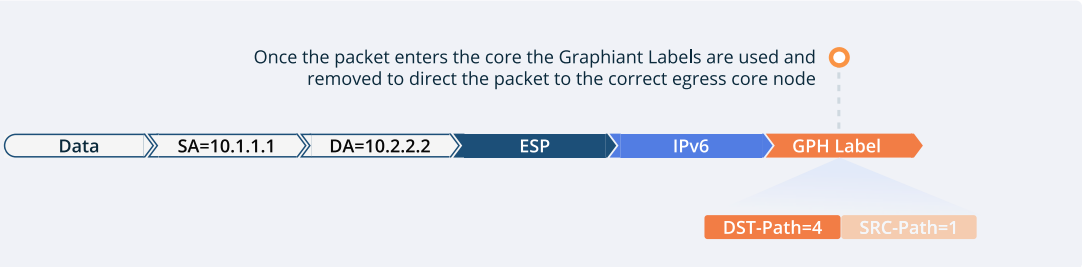


- As with MPLS, Enterprises are segmented from each other
- Segments are defined for connectivity
- Segment ID is encoded in the IPv6 address of the E2E path
- Edges can be part of multiple segments
- Using metadata labels for segments eliminates the segment specific information in the Core

Segment information is encoded in the IPv6 Header, assuring that enterprise traffic remains separate unless all parties agree to share specific services and Graphiant authorizes this relationship. This offers the highest level of data protection and privacy for customers while giving them the flexibility to share what they need, when needed, to meet business demands.

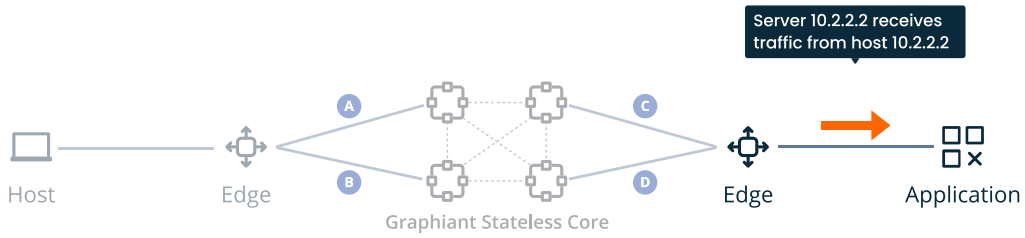
Step 2: Ingress Core to Egress Core

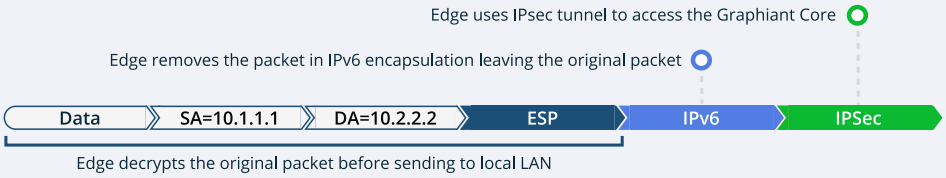




Once the packet arrives at the Core node servicing the destination edge, it adds an integrity protection header before forwarding to the final edge. The edge can then determine the source, understand the header information, and use its private pairwise encryption key to open the payload.

Step 3: Egress Core to Edge





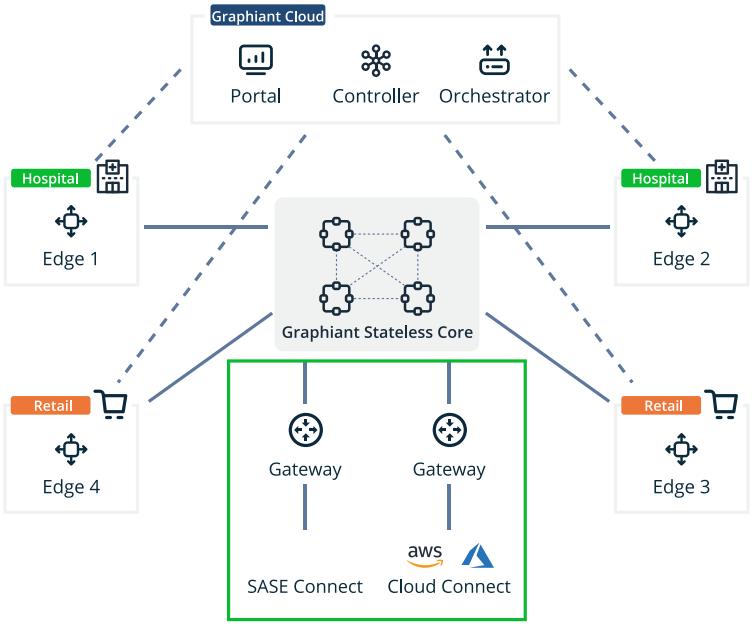
Notice, we are using a combination of IPv6, MPLS, VPN, and SD-WAN capabilities in a unique and innovative way. By decoupling these elements, we achieve the peak efficiency promised when SDN came into existence. State abstraction means the Graphiant Core doesn't need to carry customer state information in the data plane. We can split up state and abstract control plane and data plane. We are applying a scalable microservices control plane, provider and SDN models in our design. These proven techniques allowed us to evolve and provide a service that is a more secure and efficient way to accomplish private any-to-any connectivity. In addition, our customers have dedicated bandwidth allocation and are not subject to the constant performance fluctuations of the internet.

Gateway Services

The Gateway in the Graphiant architecture serves as an intelligent onboarding point for external resources and services into the Graphiant domain. It's a core element that functions as an extension of the edge, offering external services to all customers. Interaction with the Gateway is facilitated via the Portal, simplifying configuration and management by abstracting complexity.

Gateway Services functions as an extension of the edge

- Internet Services
- SASE service providers
- Cloud Connectivity (public and private)
- NNI interconnects
- 3rd Party IPsec Tunnels to partner networks



Gateway Services include:

- Internet Services (e.g., SaaS)
- SASE service providers (e.g., Zscaler, Netskope, Skyhigh, etc.)
- Cloud Connectivity (public and private, Azure express route, AWS direct connects, etc.)
- NNI interconnects with 3rd party service providers (e.g., Verizon, ATT, etc.)
- 3rd Party IPsec Tunnels to partner networks not yet connected or published to the Graphiant service.

Graphiant Gateways can be thought of as a Graphiant hosted multi-tenant Edge. Many of the functions of the GW are common with the Edge, including but not limited to

- Control/management Plane
- SLA-based routing and QoS
- Edge Redundancy/HA
- Service Side routing (BGP)
- Control/Traffic/FW Policies

Some aspects of the GW are different than what is delivered on the customer Edge. Some examples include segmentation, multi-tenancy, split horizon to avoid inter-enterprise and transit traffic, NAT'ing on the Edge to a globally unique address before sending traffic to GW, SLA negotiation between the service provider and enterprise consumer, etc. Graphiant gateways are typically deployed next to the Stateless Core nodes in the same POP. However, there are some use cases where the GW might be deployed in a partner location and connect to the Core via internet tunnels or private connectivity.

As an integral part of the Graphiant service, Gateways allow enterprises to eliminate the need to architect, design, build, provision and deploy (or procure) advanced connectivity use cases. Including the gateway as part of our Service provides tremendous value and flexibility in the way customers can migrate to and consume the Graphiant Service subscription.

Use Cases

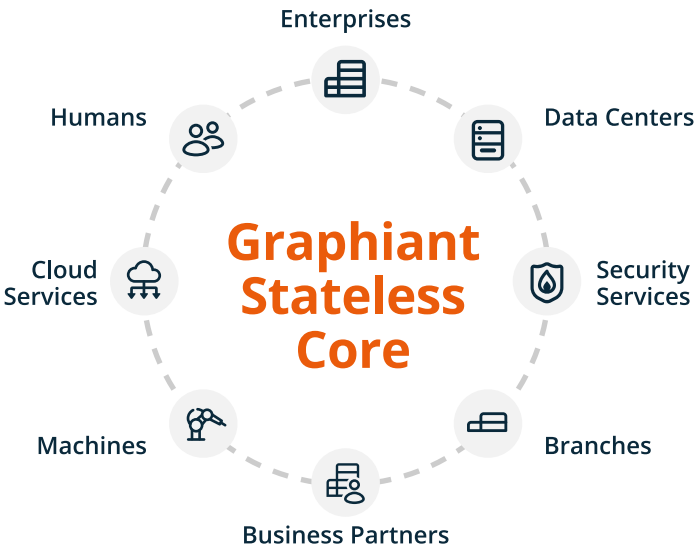
Enterprise Networking

Networks are expanding from core datacenters to include edge locations, branch offices, work-from-home employees, and partner/customer networks. There are orders of magnitude more nodes to connect, and the pace at which nodes must be connected has increased rapidly. Traditional connectivity solutions (MPLS and SD-WAN) no longer work – they are too expensive, take too long to provision, and massive amounts of tunnels between nodes.

The enterprise needs connectivity that is simple, consumable, and available as a service. Graphiant delivers this networking service by blending the scale and security of private MPLS networks with the agility and last-mile flexibility of SD-WAN and public internet. Our Network-as-a-Service (NaaS) presents a new architecture for the service economy.

Network Edge

A next-gen solution with the performance to replace MPLS + SD-WAN



Problem

Networks connect the edge, multiple clouds, customers, & partners together, but existing solutions don't support today's digital transformation

With Graphiant

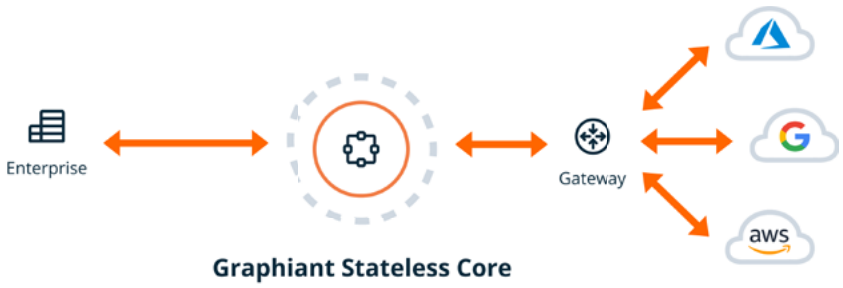
Simple provisioning in minutes, cost-effective, enterprise-grade privacy and secure connectivity to meet business needs

With Graphiant, the enterprises no longer need to provision and build the WAN; it's already built. The only decision is the edge device. Whether this is a virtual machine running as KVM or ESXi, or software running on certified bare metal, the customer can choose the functionality, performance, multi-device redundancy they require, and deploy that edge through an intuitive cloud-delivered Graphiant Portal - a single dashboard that provides administration, configuration, monitoring, analytics, reporting, and troubleshooting.

All points on the enterprise network connect to the Graphiant Stateless Core through edges. Any edge can connect to any other edge on the Graphiant network. Edges operate in multi-VRF segmentation and seamlessly integrate with the customer's LAN side routing protocols such as OSPF and BGP. All traffic is encrypted edge-to-edge automatically, without decryption or tunnels in the Graphiant Core. This results in a highly scalable architecture, free from tunnel management overhead.

Cloud Connectivity

Simplify hybrid & multi-cloud connectivity at a lower cost, and faster time to production with guaranteed security



Problem

Multi and hybrid-cloud connectivity is a complex process. Current solutions are cumbersome, expensive, & operationally intensive.

With Graphiant

All the enterprise needs to do is connect its locations and cloud workloads to the Graphiant Stateless Core. The benefit is lower cost, faster time to productivity, and a more secure connection.

Today, there are no robust, secure, and agile solutions for multi-cloud, B2B, and IoT cloud networking. Existing solutions are complex, expensive, and lack scalability. As a result, enterprises must choose between the costly and inflexible MPLS, the expensive and static Colo to cloud connections from CSPs, or deal with the tunnel issues of SD-WAN over an unreliable and insecure internet.

The Graphiant service dramatically simplifies cloud on-ramp and hybrid cloud connectivity, making it more affordable and easier to operate.

There are several ways to integrate:

1. Graphiant Gateways enable high-performance interconnect to the Cloud Service Provider (CSP) through carrier-neutral facilities (CNF) in multiple regions and to various clouds. These gateways, which are multi-tenant capable, are typically connected in colocation with the Graphiant Cores. Since an enterprise customer's WAN is already connected to the Graphiant Stateless Core, and because there's inherent any-to-any connectivity, any site can map directly to the multiple cloud services connected via the Graphiant Gateways through the private connection.

2. The Graphiant Edge can be provisioned directly via the CSP's marketplace within the enterprises' Cloud Portal. Deploying Cloud Edge instances offers the simplest way to extend our Graphiant-connected network directly into a VPC or VNET using only a single tunnel connection to the Graphiant Core, gaining access to and from the entire enterprise network.

Business to Business

The business landscape is transforming fundamentally, driven by the desire to deliver modern, cloud-like experiences that reshape customer engagement. As seen in consumer markets, business-to-business sectors are shifting from traditional product manufacturing and sales towards service-based models.

In this service-model economy, business-to-business (B2B) connectivity is becoming the norm rather than the exception. Provisioning and managing B2B connectivity must be swift and straightforward, while the resulting B2B networks need to be secure, respect data sovereignty, and scale effortlessly.

However, current extranet solutions fall short. Extranets based on MPLS networks are labor-intensive to provision, change, and secure, besides being extremely expensive. While public Internet extranets are less costly, they inherently lack security and reliable performance. Moreover, provisioning, securing, and maintaining public Internet-based extranets are labor-intensive tasks.

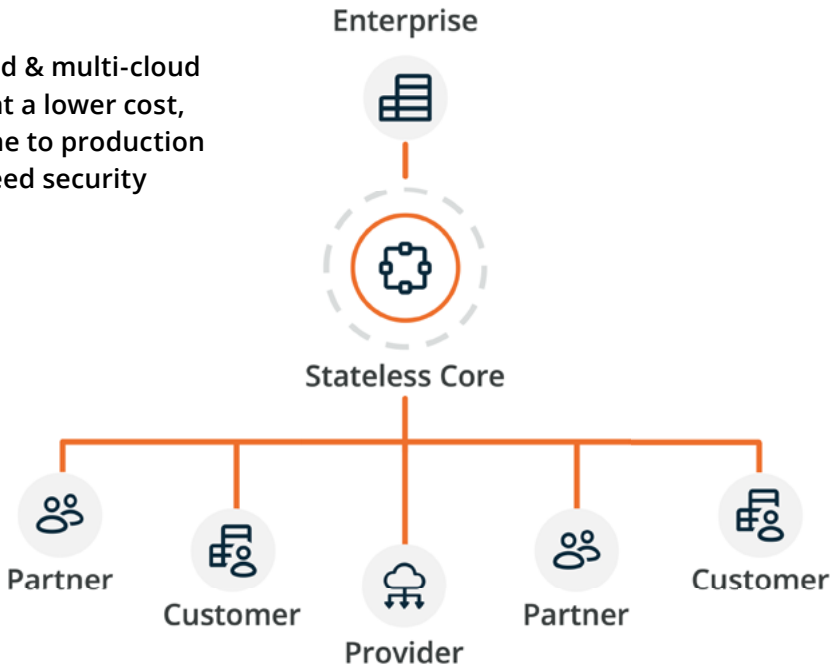
Graphiant offers a solution for this new B2B connectivity using a multi-tenant Stateless Core. We

leverage metadata tags that enable businesses to programmatically map permitted connections to services offered by other businesses or vice versa. This allows them to publish a service and enable others to subscribe to it.

Services are published through a Marketplace and consumed via a subscription. The underlying B2B connections are provisioned through policies and automatically secured with high-performance encryption, end-to-end, with built-in resilient connections to multiple Graphiant Cores. This process eliminates the need for manual CLI configurations or the construction of numerous IKE based tunnels using insecure pre-shared keys.

B2B Connectivity

Simplify hybrid & multi-cloud connectivity at a lower cost, and faster time to production with guaranteed security



Problem

Businesses increasingly need to connect with customers and partners, but current solutions are broken

- Expensive to maintain
- Complex operations
- Requires static DMZs

With Graphiant

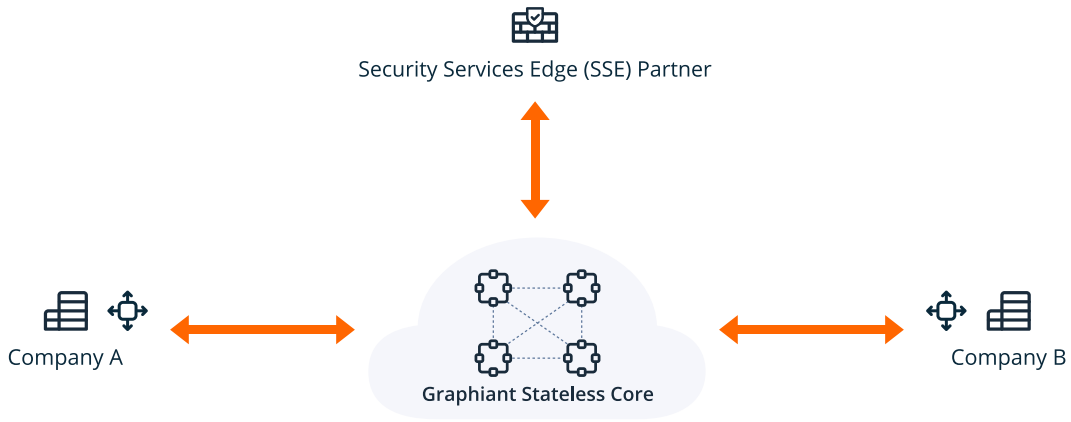
Connect your enterprise to customers + partners using the Graphiant service. Use simple business policy to enable connections & decrease time to market.

From a security perspective there are multiple options available:

1. The Graphiant Edge serves as a full-service stateful firewall, providing robust NAT services, which are often needed in business-to-business connections.
2. If a customer opts to integrate a Secure Services Edge (SSE) provider, the Graphiant service can use metadata tags to route the identified traffic to the SSE partner for inspection based on the customer's policy. The traffic is then directed to its final destination.
3. Traditional models still employ an enterprise DMZ with firewalls and a complete security stack on the customer's side. In these cases, few changes are needed on the security stack side, but all middle-mile connectivity and security requirements are provided via the Graphiant service.

Brownfield Deployments

B2B with Graphiant & SSE



Customers and partners who are not yet part of the Graphiant Core and still using traditional IPsec tunnels can terminate these tunnels into a Graphiant gateway within the region, facilitated by the Graphiant Portal. We then attach the appropriate metadata tags to the traffic at that point and map it across the Core to the customer, service, or destination. This results in a simpler operational model for the customer to maintain.

Summary

Summary of the value that Graphiant service offers:

- **Guaranteed SLAs**
  Unlike SD-WAN which relies entirely on the internet, we guarantee service levels for the middle mile.
- **Any-to-Any Connectivity Without Tunnels**
  Without the need to manage tunnels, we address the tunnel proliferation issue seen in SD-WAN.
- **Multi-tenant**
  Unlike single-tenant SD-WAN, we allow for multi-tenant and B2B connections.
- **True Network-as-a-Service (NaaS) Model**
  No more building and managing the network.
- **Support**
  Unlike SD-WAN, we have a dedicated support expert ready for your call. Because the Graphiant Service is delivered "as-a-Service," we provide support for the end-to-end solution. There is no need to bounce between vendor and provider.
- **Visibilty and Control**
  Unlike traditional technology where the enterprise has neither control nor visibility, Graphiant owns, controls and manages the middle mile.
- **Gateway Services**
  We include this so there's no hidden fees unlike most SD-WAN services which require cloud-hosted routers, incurring egress fees.

We predict our technology and protocol stack will be adopted by telecommunications carriers and cloud service providers. Our design is not just a novel way to evolve the industry but also promises significant savings in support, hardware, and power costs due to our efficient solution for private carrier-grade backbone connectivity.

The next layer we plan to add to our service is the Graphiant Marketplace. Technology has fundamentally altered how brands and marketplaces collaborate. B2B marketplaces allow organizations to network with other companies and provide all services in one place. However, connecting network infrastructure is complex, and enterprises struggle to launch consumable services and find easily integratable solutions. Our service guarantees private connectivity, faster deployment, cost optimization, and enables subscription-based modeling.

The Graphiant Marketplace aims to facilitate connectivity between enterprises, simplify the service consumption experience, and accelerate business growth. The Gateway and Marketplace will let us incorporate product and customer-led value creation into industries that urgently need standardized B2B connectivity. Our vision is to replicate what cloud service providers have done for computing in the networking realm.

This is just the beginning – we envision a world where applications themselves can program the network landscape to suit our needs. Deploying the Graphiant Edge in containers, kernel modules, and endpoint agents is on our roadmap. We view these steps as crucial in the evolution of networking to the point where our next-gen protocol stack is included in applications supporting IoT and other emerging industry verticals.

It’s Time for a New Network Edge Service

Schedule a Demo

graphiant

Graphiant is a Silicon Valley-based provider of next-generation Edge services. Graphiant has developed the Graphiant Network Edge, an “as-a-Service” solution that provides connectivity between the enterprise WAN, hybrid cloud, network edge, customers, and partners. Graphiant’s Network Edge combines MPLS-like performance (guaranteed delivery and privacy) and Internet-class agility to enable network architects to build enterprise-grade networks at the speed of business. Khalid Raza, also known as the “Father” of SD-WAN, is the founder of Graphiant and is completing his vision for next-gen connectivity with Graphiant.