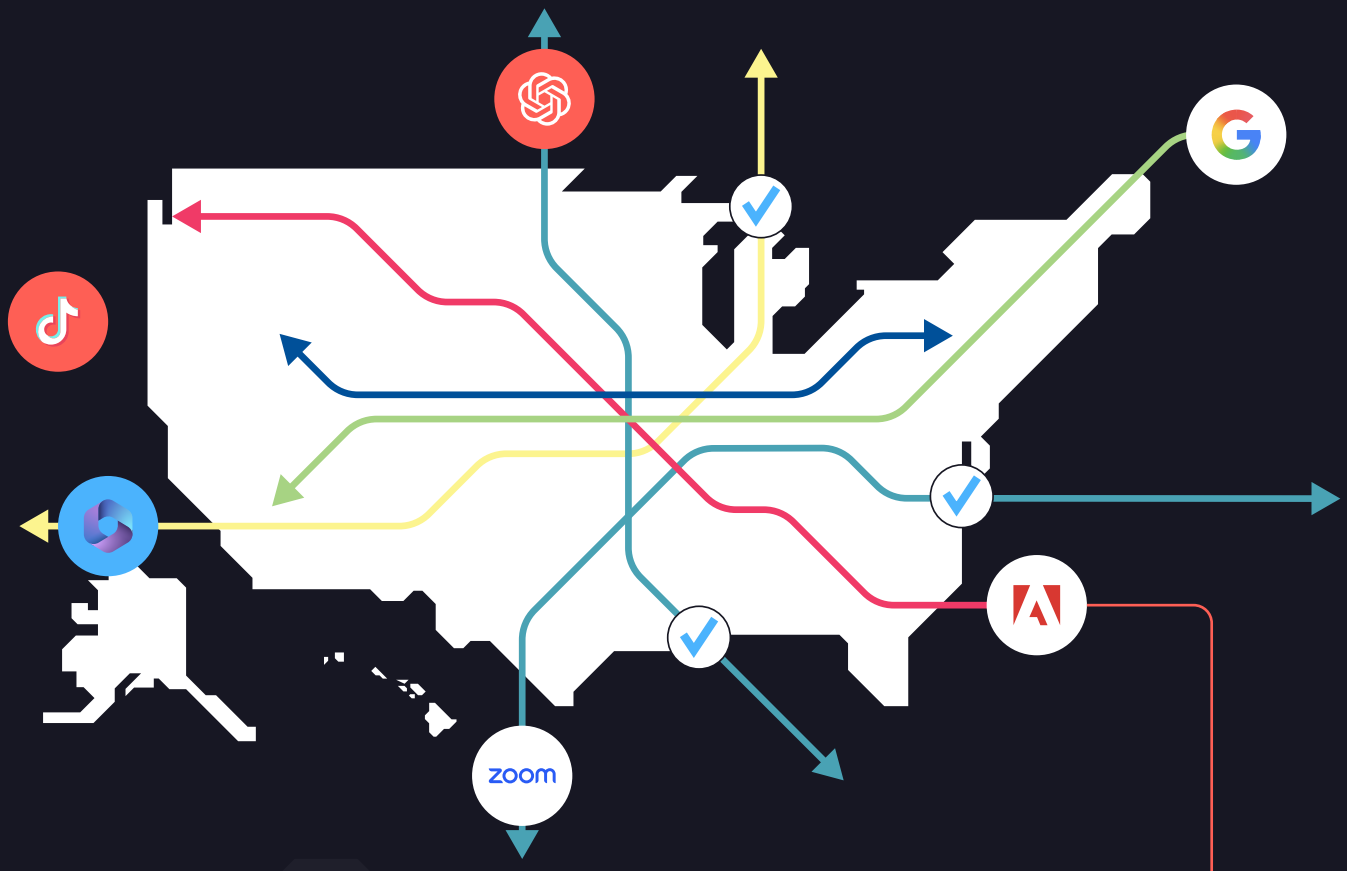
graphiant



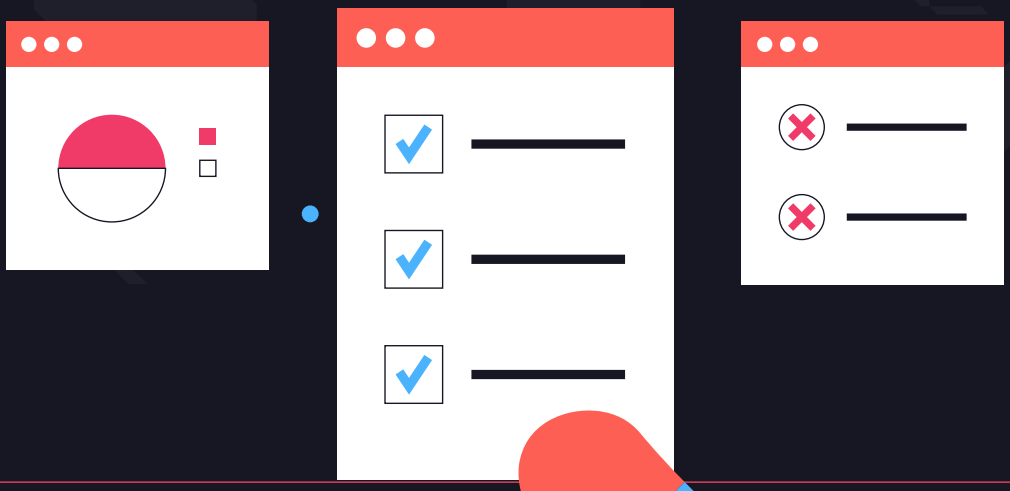
Understanding How A Graphiant Telecom Provider Delivers Multi-Cloud Services

Multi-Cloud Challenges, Solved

Graphiant provides telecom providers with a next-generation network service built for multi-cloud environments using SDN principles with specific advancements in areas like encryption and data-plane management. Our stateless core adapts to modern business requirements, combining security, scale, and performance.

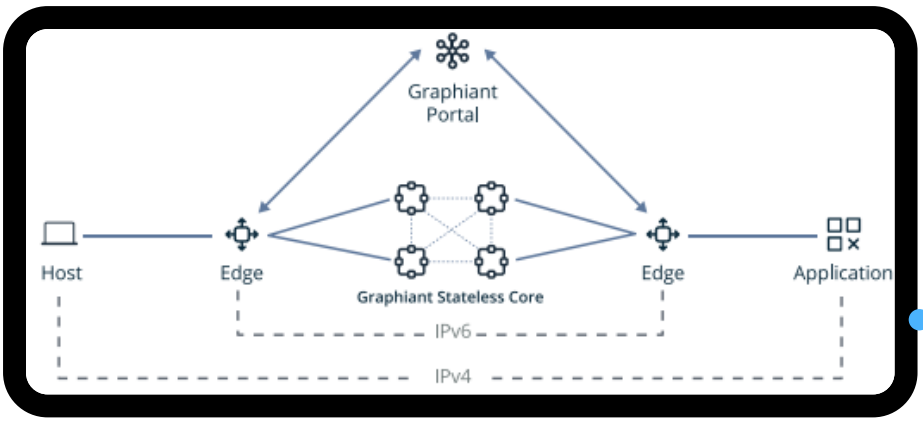
Every encryption and decryption cycle consumes processing power. During transfer, each point temporarily sees unencrypted data, which requires extra checks before re-encryption. Traditional solutions tie control and data planes together and stack on an encryption layer. This creates major challenges for both security and scalability.

The Graphiant edge is designed to be “any” x86 platform either in hardware or virtual form factors. **These are the types of edges that are available for customers to choose from:**



Graphiant Network

From the customer perspective, deployment is simple and automatic, with only standard LAN and WAN routing configured.

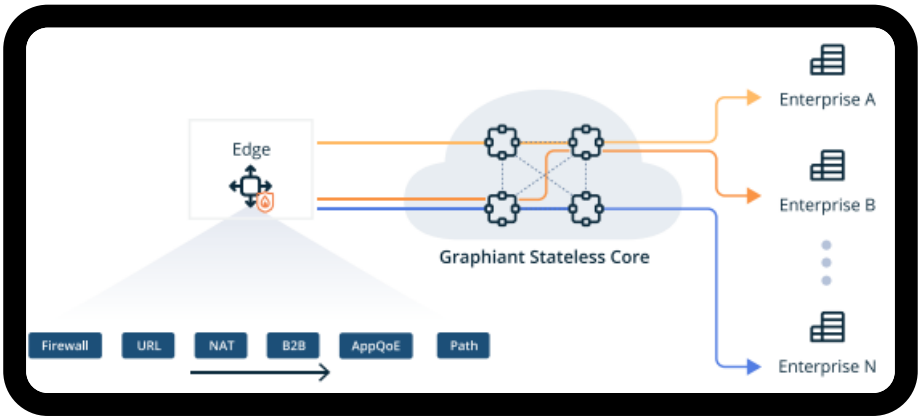


Simple & Granular Policy Controls

Through the Graphiant Portal, all networks tied to a location can be accessed and configured on the Edge. Modern networks demand flexibility: traffic can move across multiple circuits, go directly to the internet and be inspected locally with a Next Gen Firewall, or route through third-party tunnels to the SSE vendor of choice.

At the Edge, metadata labels are encoded for the Stateless Core. This gives users full control to program traffic through the Portal and direct it to the Edge. They can set QoS policies, define segment membership, guide path selection, and map B2B traffic flows.

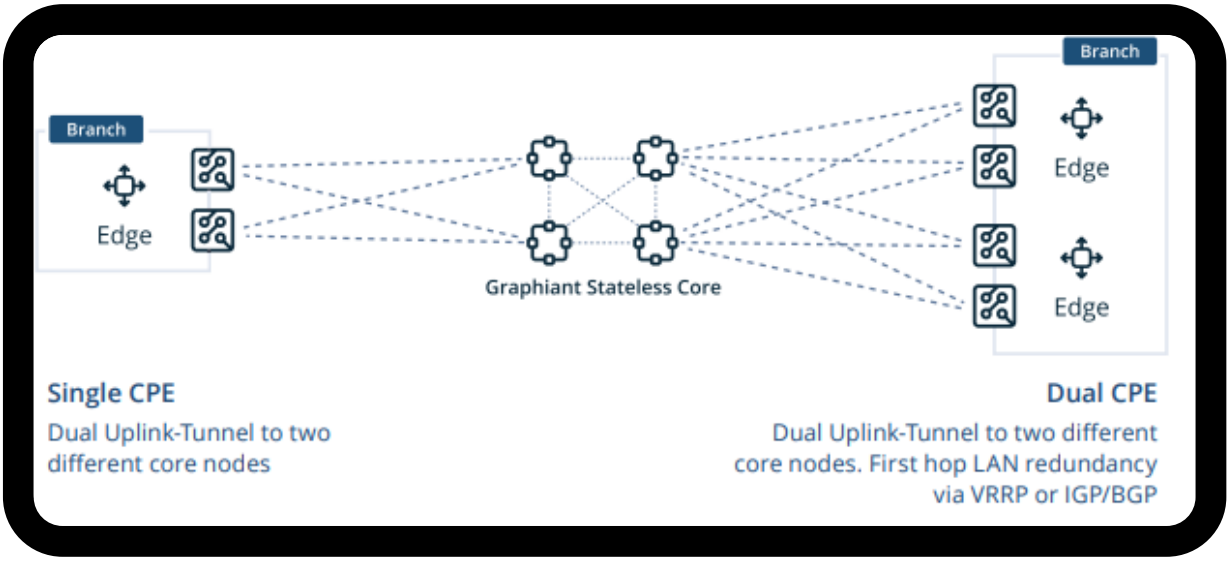
This design makes the Graphiant Edge intelligent, while allowing the Stateless Core to do what it does best, forward packets at scale. All traffic between Graphiant Edge nodes is encrypted end-to-end, with no decryption required in transit.



Branch Redundancy

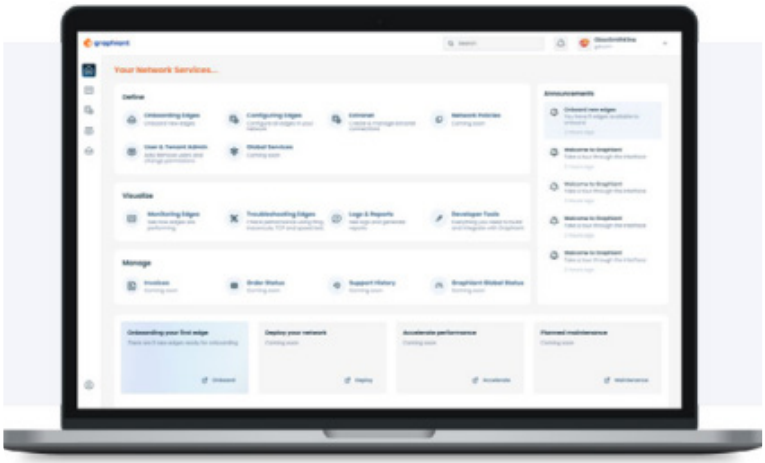
Branch circuit redundancy is achieved using multiple WAN circuits, while Edge CPE redundancy is achieved using multiple Edge devices. High Availability (HA) requirements can be met by multiple configurations, depending upon overall site design standards. The Graphiant Edge device uses Virtual Router Redundancy Protocol (VRRP) with object tracking in a Layer 2 failover scenario. Failover in a Layer 3 scenario can be achieved using either OSPF or BGP, in an Equal Cost Multi-Pathing (ECMP) and/or HA design. The Graphiant Stateless Core solves for return traffic symmetry, removing a layer of complexity from the end user configuration requirements.

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



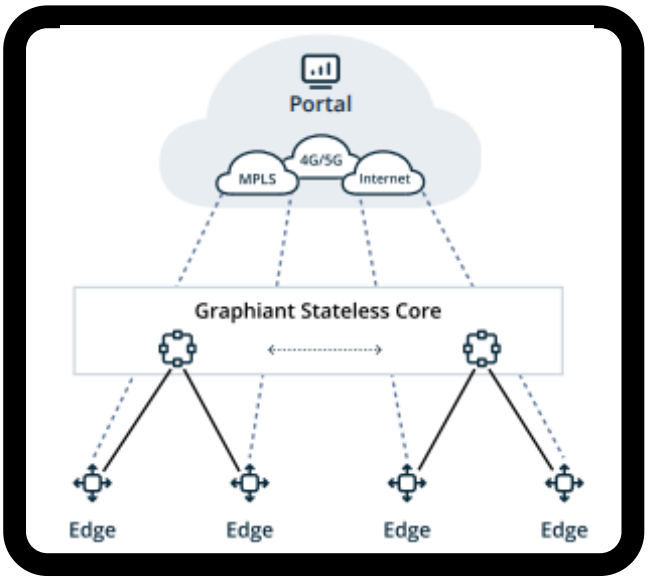
The Portal

Graphiant Portal is the 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.



Control & Management Plane

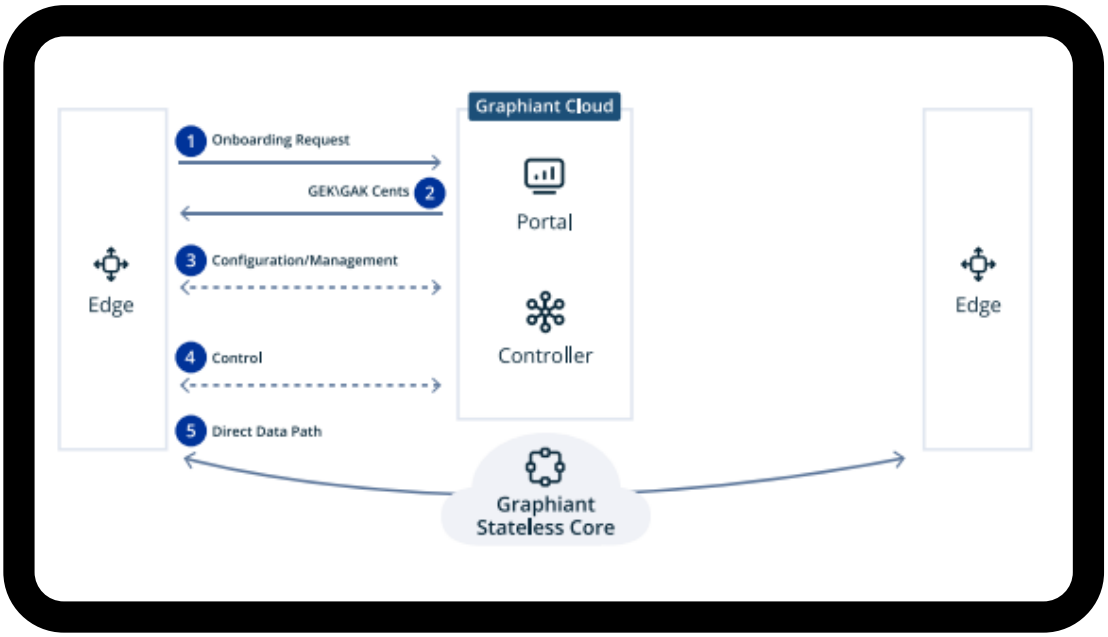
The Graphiant Portal maintains constant connection with Edges via a secure tunnel. This connection allows real-time monitoring, troubleshooting, configuration adjustments, and enables use cases provided by Graphiant. The Portal is multi-tenant and runs on micro-services across various multiple regions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



Control Plane

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

Graphiant is designed to comply with all major security regulations (SOC2, HIPPA, PCI-DSS, etc.). We ensure that hardware devices approved for our service include Trusted Platform 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.



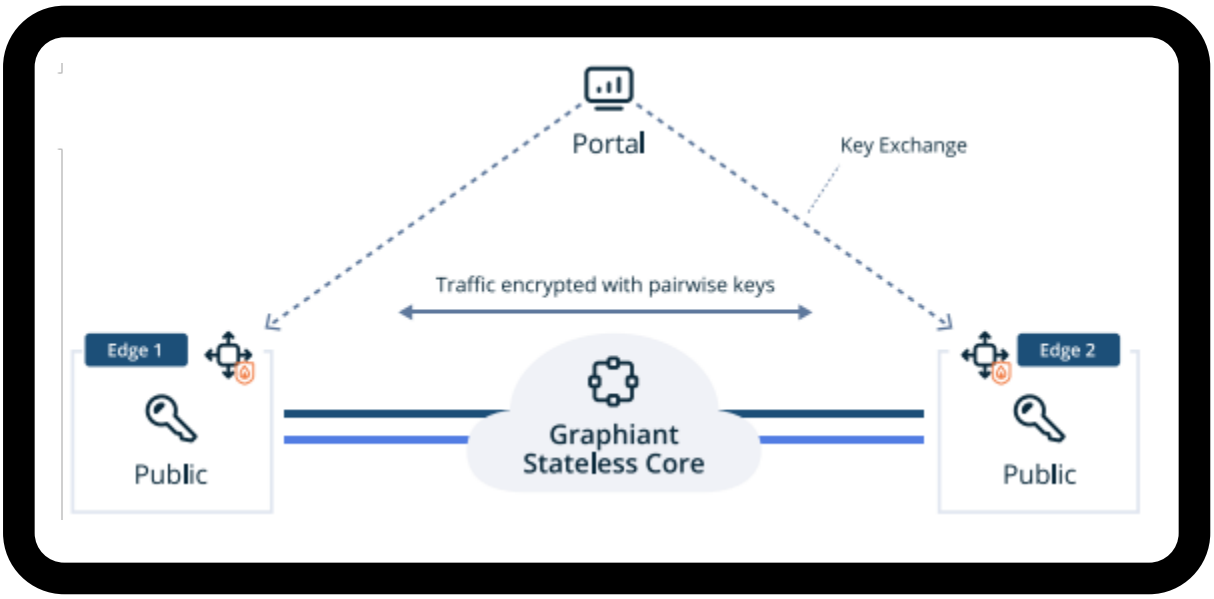
Our software never generates keys. Instead, we rely on TPM or HSM and use private/public keypair for setting up primers and symmetric encryption keys. The keystore resides on the device HSM and is under the customer control. Graphiant never accesses the private keys and doesn't use pre-shared keys.

Graphiant uses the public key from the TPM or HSM keystore to set up encrypted connections to the Graphiant Service. Diffie-Hellman is used, via the controller, to set up symmetric pairwise 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 keystore, it then establishes a connection to the Portal. Once this control plane is established, the edge device doesn't need another exchange with the Core network. It relies on the metadata information delivered by Portal. The Portal instructs the Edge on what metadata to use when communicating with the Core.

Encryption

Keys must never be exchanged over the data plane. Instead, we use the public key information on the Edge HSM to generate Diffie Hellman primers, which are 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, many tunnels terminated on each edge increases this time exponentially.

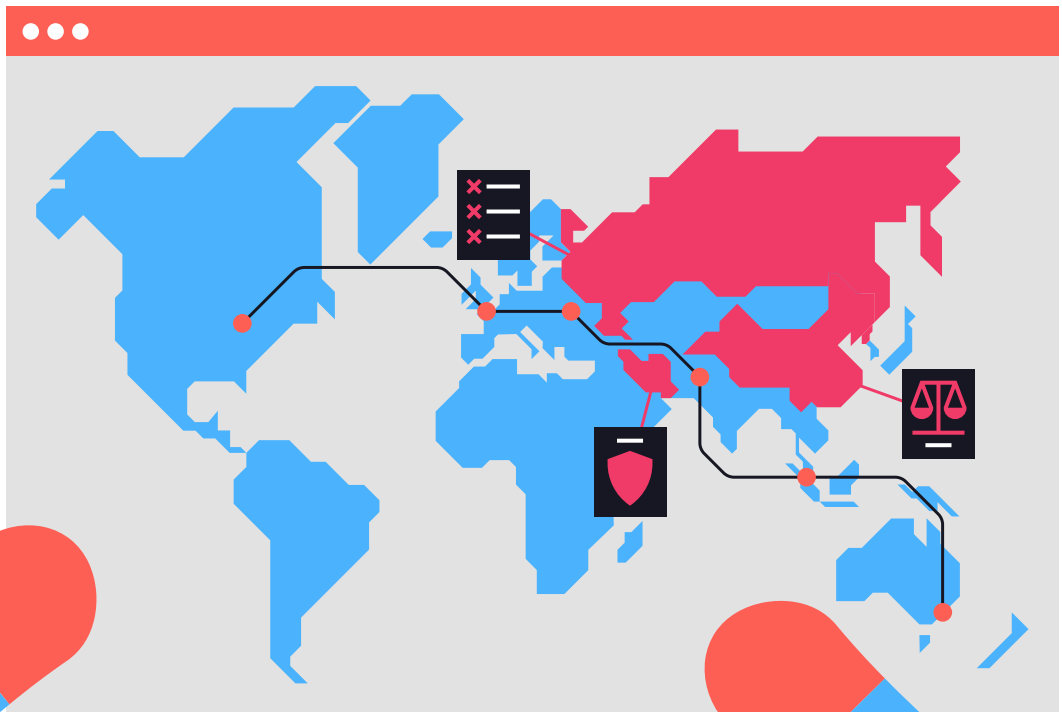
Our advantage lies in the absence of end-to-end IPsec tunnels. Edge nodes only establish a data plane connection to the Core. The security association key exchange doesn't require a full session state handshake, taking only a couple of seconds depending on the latency between each Edge and the cloud 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.

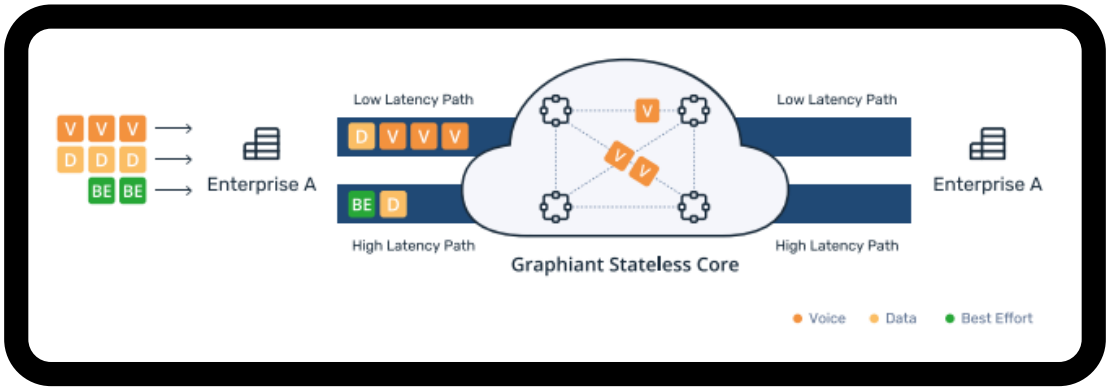
Graphiant's Stateless Core & Data Plane

Because of 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 can 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.



Metadata Labels for Policy & SLA

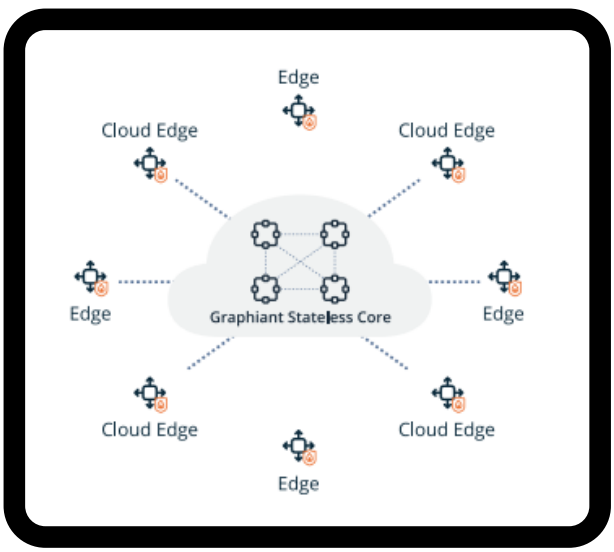


Graphiant has developed a new protocol and BGP extensions that propagate additional information beyond currently available address family attributes. For instance, extended segment information regarding application characteristics is handled in the routing protocol itself. The combination of our new 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.

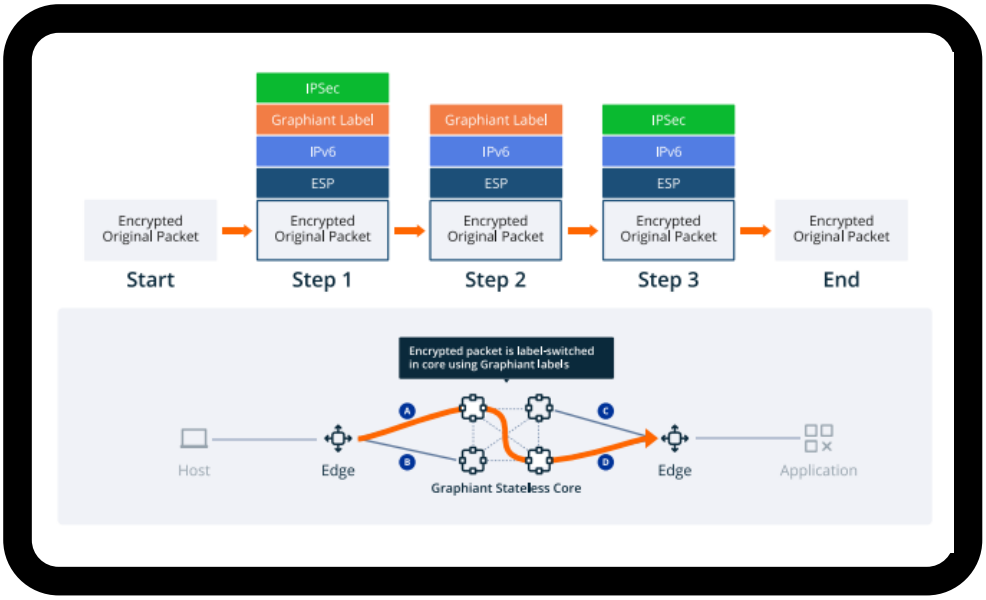
Due to reduced tunnel overhead and removal of customer config, our Stateless Core nodes have a significantly smaller footprint than traditional carrier backbone routers or MPLS P or PE devices. The lower power draw and smaller physical footprint allow rapid deployment (usually contract +60 days) as per 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

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.

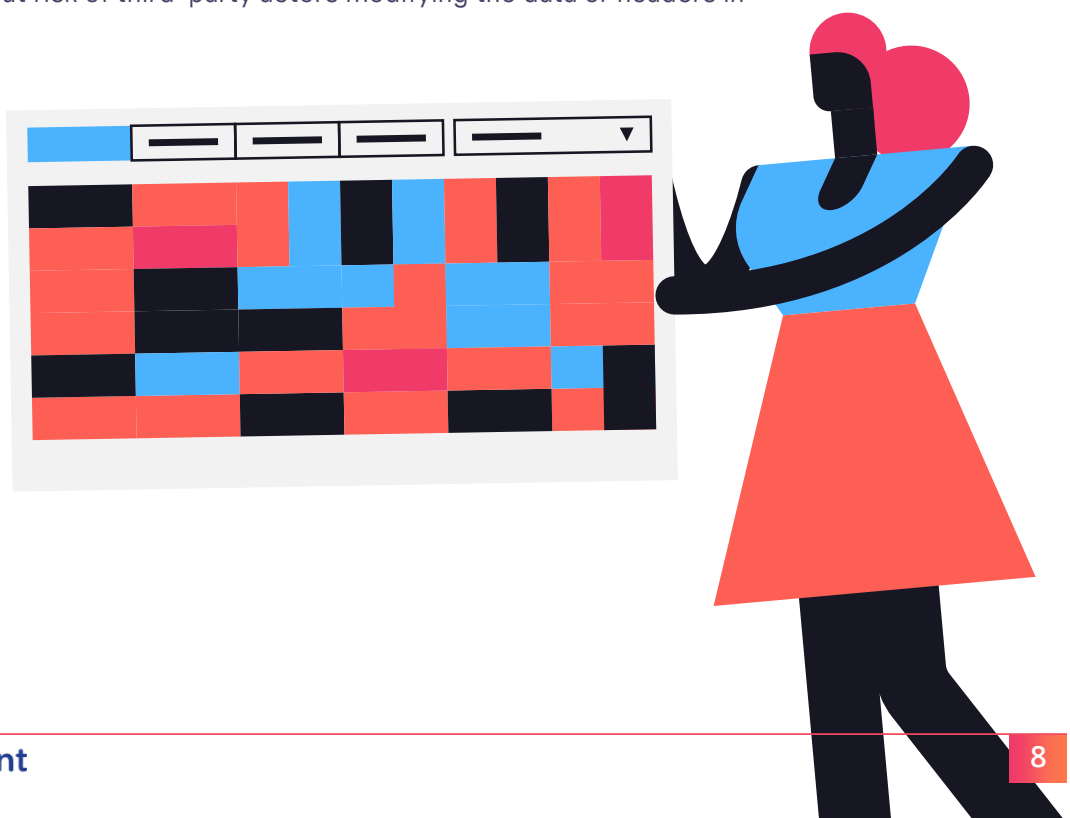


Metadata Based Forwarding



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 the Graphiant Core

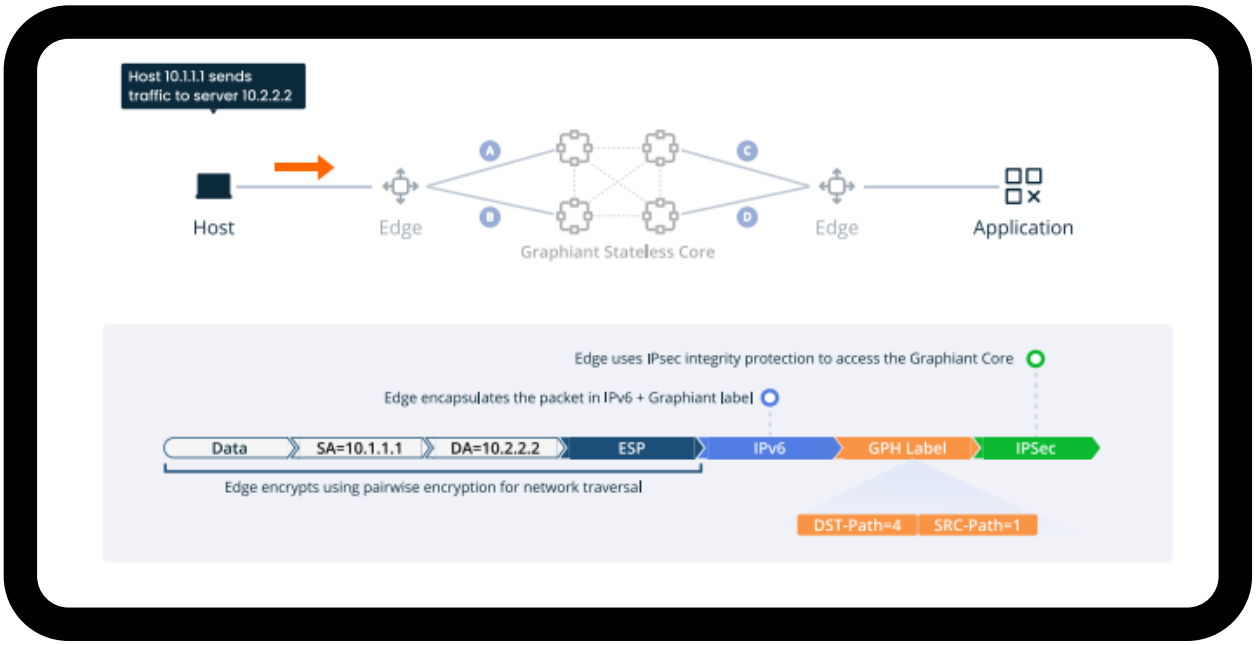
By arranging the packet header in this specific way, we ensure traffic is encrypted only once, maintaining edge-to-edge encryption. This method prevents tunnel sprawl and enables us to transmit customer data without revealing their IP information. In essence, our unique use of ESP, IPv6, and AH ensures 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.

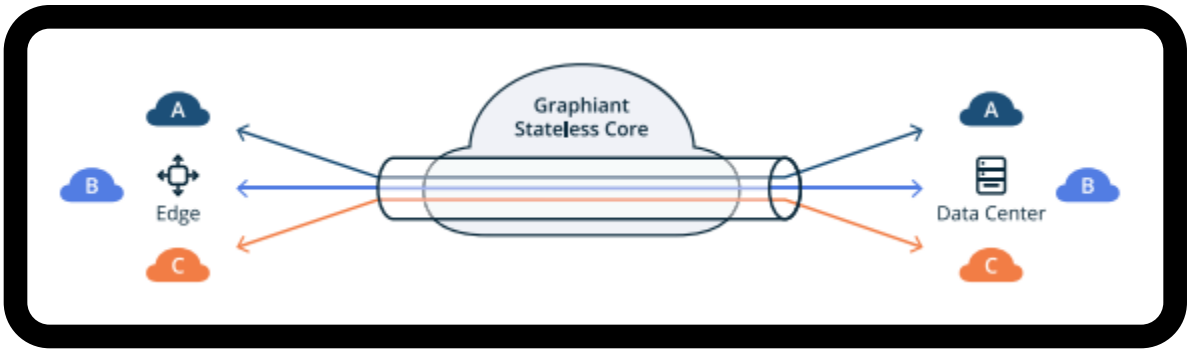
One major issue we're addressing with this approach is the intermittent fluctuation of frame size at intermediate points across the public internet. With our service, this probability is significantly reduced, limited only to the last mile segment where it's extremely unlikely to occur. We know that 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



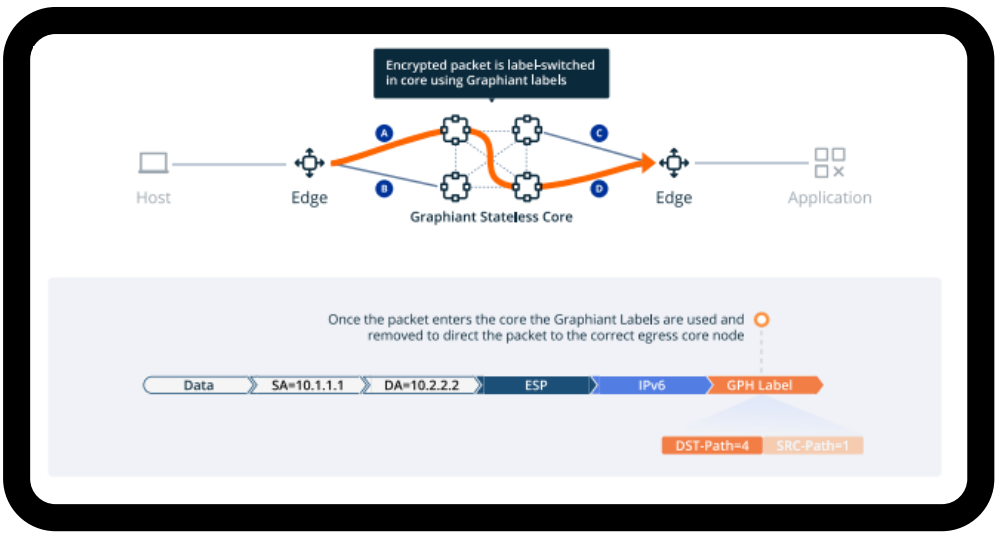
Once traffic reaches the Stateless Core, it removes the authentication header providing integrity protection. The Graphiant Core can't decrypt the packets since only the customer's edge has the pairwise encryption keys. Most importantly, the authentications headers ensure our metadata labels can't been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



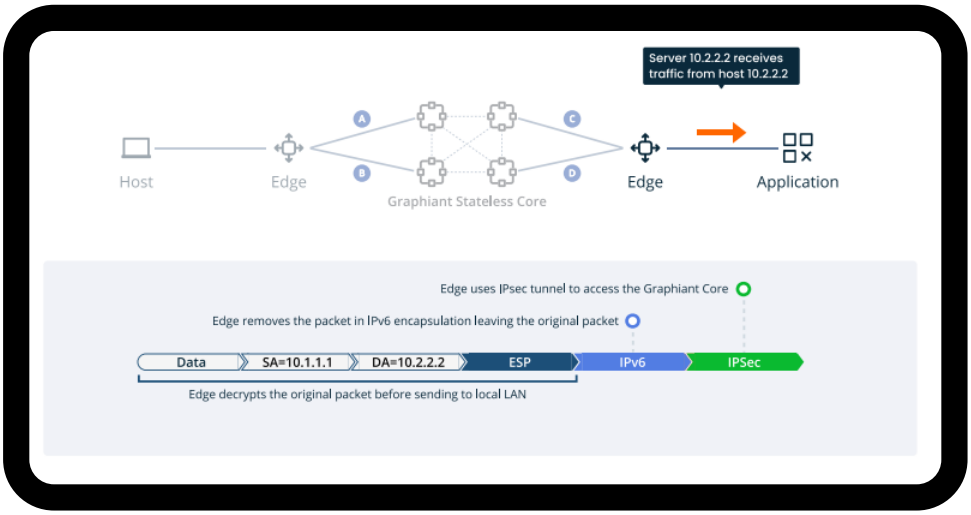
Segment information is encoded in the IPv6 Header, assuring that enterprise traffic remains separate unless all parties agree to share specific services and Graphiant authorizes this relationship. This offers the highest level of data protection and privacy for customers while giving them the flexibility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

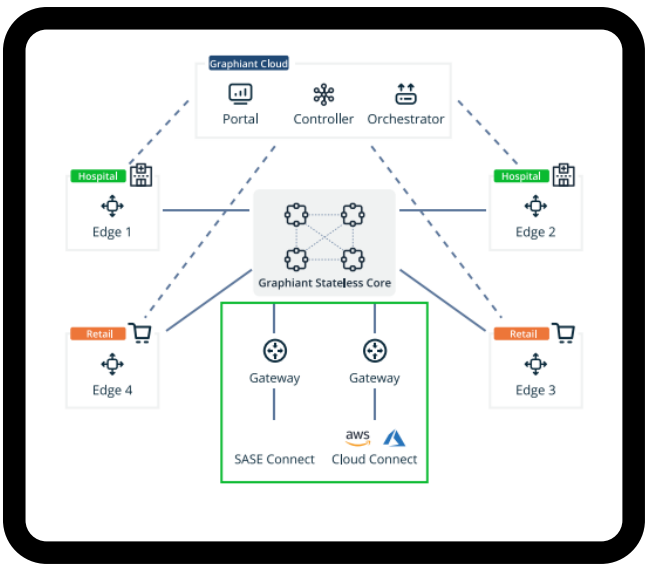
Step 3: Egress Core to Edge



Graphiant uses a combination of IPv6, MPLS, VPN, and SD-WAN capabilities in unique and innovative ways. By decoupling, we achieve peak efficiency from SDN. State abstraction means the 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 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 include:

- Internet Services (e.g., SaaS)
- SASE service providers (e.g., Zscaler, Netskope, 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 Gateways can be thought of as a Graphiant hosted multi-tenant Edge. Many of the functions of the GATEWAY are common with the Edge, including but not limited to

1. **Control/management plane**
2. **SLA-based routing and QoS**
3. **Edge redundancy/HA**
4. **Service side routing (BGP)**
5. **Control/traffic/FW policies**

Some aspects of the Gateways are different to what is delivered on the customer Edge. Some examples include segmentation, multi-tenancy, split horizon to avoid inter-enterprise and transit traffic, NAT on the Edge to a globally unique address before sending traffic to Gateways, 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 cases where Gateways 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.

Assured, Agile, Awesome.

Follow us on: