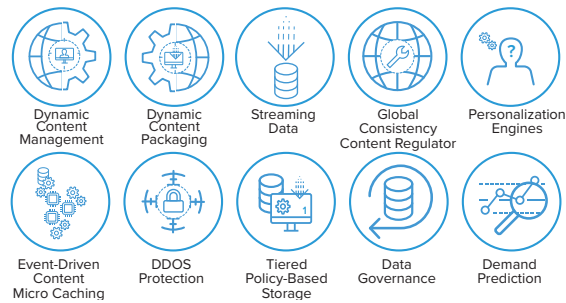




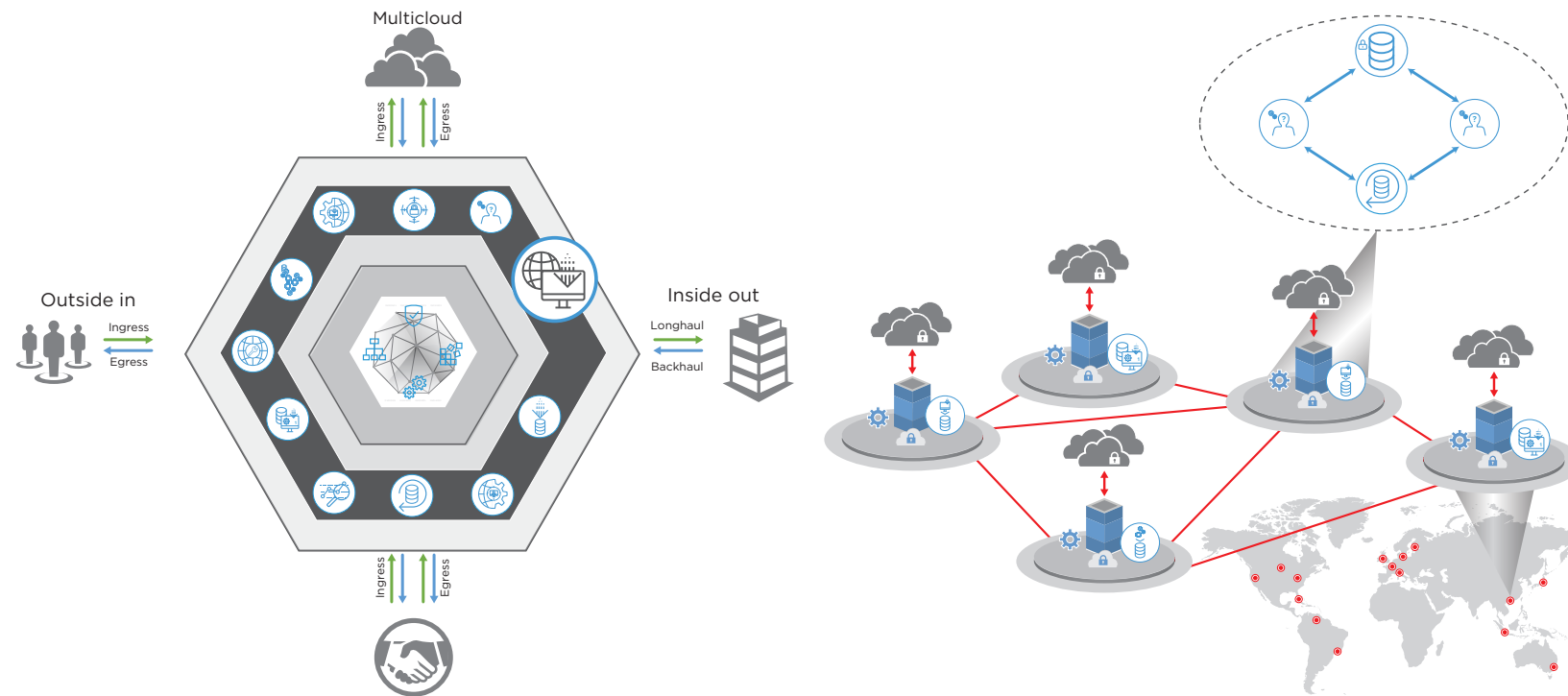
Design Principles

- Mobile devices are increasingly the main target for content consumption.
- Highly personalized and tailored content is a value differentiator, so it must be created and delivered at the digital edge, adjacent to the consumer.
- Content delivery is not hierarchal and central; it has bi-directional flows.
- Content creation is transforming to a global community of contributors collaborating on digital assets in all phases of production and post-production.
- Event-driven content requires edge distribution for high-quality user experience.
- Data analytics at the edge is a requirement for adaptable advertising monetization, tailored content and product improvement.

Edge Node Components



Content delivery and contribution have changed, becoming multisourced and altering network architecture assumptions inherent in traditional hierarchical content push services. Content creators, collaborators, distributors and consumers all experience the same problem across a global ecosystem which is optimized for high-quality consumer experience with minimal latency. With the increasing shift of users and enterprises consuming content on mobile devices, the enterprise must transform the content delivery paradigm to embrace a network design that shortens the distance between all parties in the creation, distribution and consumption digital workflow—employing an Interconnection Oriented Architecture® (IOA) strategy that drives content to a mesh of interconnected digital edge nodes to deliver content locally, enabling responsive personalization, local compliance enforcement and guaranteed consistency.



Capabilities

- Multicloud access to data: distributors and users demand that applications pull from many sources in a timely manner.
- Event-driven content support: dynamic user experience assumes that content distribution is bi-directional and allows for extremes in demand.
- Global, near-real-time replication: application success depends on consistency, content availability and security.
- Micro-caching: optimizes simultaneous local requests for high-demand content.
- Data and logic colocation: enables APIs to interact with data at the edge.
- Secure data traffic with traceability and DDoS: attack prevention is improved for mobile applications.
- Regulatory requirements: meet local compliance needs.
- Personalization engines: localized and timely enactment enhances user experience and monetization of content.

Edge Node Deployment

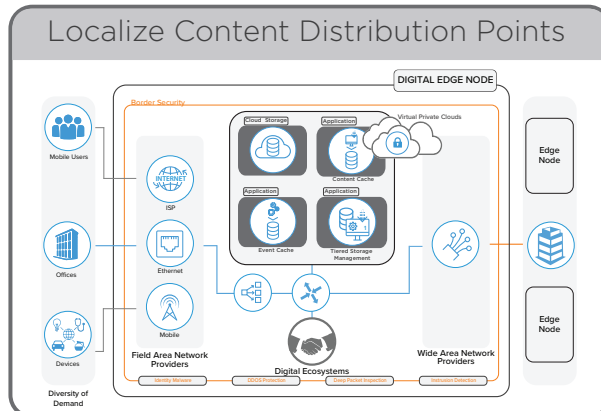


Implementation is a mix of physical devices and virtual appliances that support SaaS services for network, storage, compute, cache and security, typically 1 cabinet. The cabinets required for applications and data depends on an analysis of app characteristics and PBs of data, with 1PB requiring 5 cabinets.

DESIGN PATTERNS

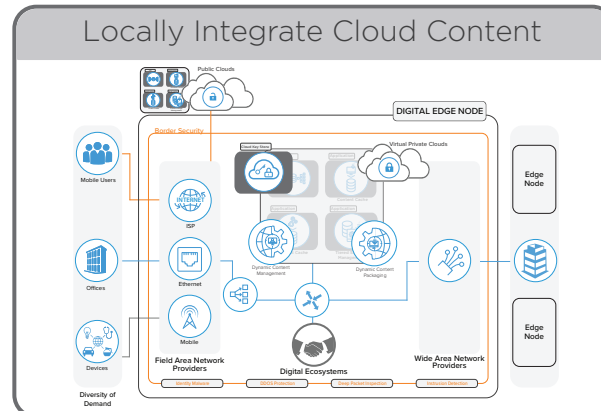
1 STEP 1

Control and enhance user experience by shortening the distance to a secure digital edge. Improve content creation, contribution and distribution by rerouting local traffic within dense user clusters.



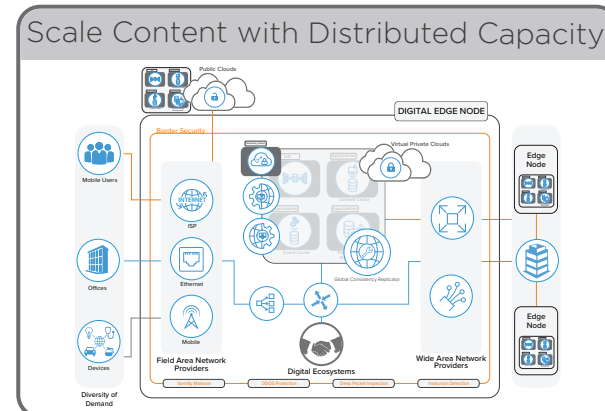
2 STEP 2

Enhance responsiveness of growing multicloud-based workloads by securely integrating them at the edge, lowering latency, leveraging data gravity and improving delivery and user engagement.



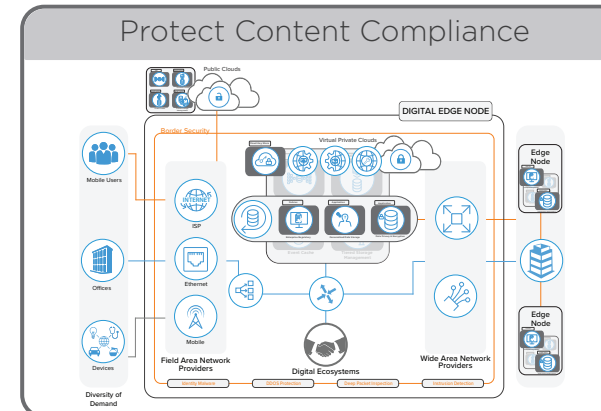
3 STEP 3

Improve reliability and efficiency of content service growth via distributed scaling to meet demand. Distribute content and workload to an interconnected mesh of digital edge nodes, adding services from the enterprise and third-party MSPs as needed.



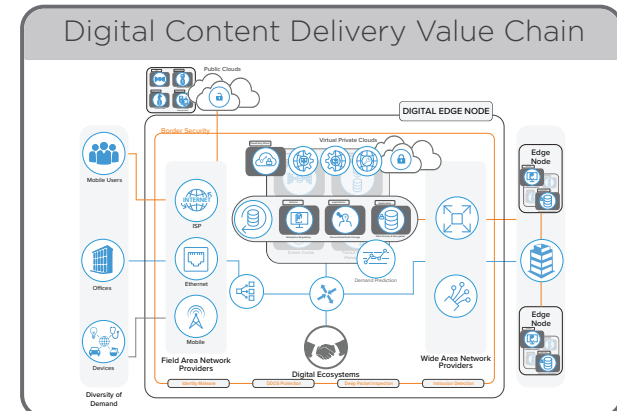
4 STEP 4

Guarantee timely, relevant regulatory compliance and brand-enhancing personalization, driving policy enforcement decisions to local regions through edge-based service chaining and bi-directional interactivity.



5 STEP 5

Adapt to changing business needs across unpredictable events, new regulations, partners and technologies by dynamically rerouting traffic through the mesh, enabling the addition of new services at local edge nodes in a 24-hour global cycle.





Problem

The accelerating demands for higher bandwidth and the increasing and ubiquitous nature of mobile high-quality content consumption (anywhere, anytime) will continue to create congestion and inject latency into content distribution across traditional centralized network topologies.



Solution

Content delivery must change from a centralized distribution model to one that places content closer to the population centers that consume and create it to improve user experience. Control and enhance user experience by shortening the distance to a secure digital edge where users are. Push content to the edge while rerouting local traffic within dense user clusters to speed access. Install repositories at the edge to vastly improve the user experience of content consumption and contribution, while ensuring secure, authorized access. Install policy-based, tiered storage to manage the cost and performance of expanding content volumes and demand. Deploy distributed denial of service (DDoS) protection and encryption to ensure data access is protected against attacks and theft. This movement of data and services to the edge is the first step to re-architecting to an IOA.



Constraints

1. Content volumes are growing, exhausting network capacity and making user experience requirements harder to achieve.
2. Investing in centralized network resources does not meet the needs of the changing content delivery environment.
3. Long-haul streaming to multiple sites does not scale in a hierarchal network, causing delays in delivery and poor user experience (i.e., latency and jitter).
4. More content is being created non-centrally, which requires backhauling to a central site for distribution in traditional network architectures.
5. Metro traffic continues to grow faster than long-haul traffic, which traditional centralized network infrastructures are not designed for.



Steps

1. Simplify the network topology by deploying a digital edge near large population centers, reducing latency by shortening the distance to users.
2. Consolidate endpoint management for all traffic sources and types, including the internet.
3. Segment and control regional traffic at the edge, minimizing latency and response time.
4. Introduce security services (including encryption) at the edge to optimize regional access and keep data safe from attacks and theft.
5. Leverage network provider choices for optimal delivery.
6. Install caching at the edge, enabling fast access to consume or contribute content.
7. Introduce policy-based, tiered storage management to effectively retain the rapid growth of content types and usage.
8. Introduce event-based micro-caching to generate update alerts for mostly static content.



Forces

- Traffic from wireless and mobile devices will account for 66% of total IP traffic by 2020, most carried by content delivery networks (CDNs) as video.
- The global CDN market is projected to grow to \$23.22 billion by 2021, at a CAGR of 30.9%.
- Globally, metro traffic will grow nearly twice as fast as long-haul traffic through 2019.
- Global OTT devices and services market growth is at a CAGR of 20.6% (2016-2020).
- User experience expectations are more demanding, stressing available bandwidth and driving up network costs.
- Production and post-production workflows are moving to ecosystem-based hybrid cloud and multicloud-based technologies for compute, storage, archive, encoding, distribution.
- Digital media businesses require greater interconnection to drive global IP traffic growth.



Results

Technical

- Localizing traffic in the hub shifts latency from ~20 ms/~20 hops to <1 ms/hop (or wire speed) with unlimited local bandwidth.
- Communication end points are aggregated and interconnected in a secure digital edge, reducing attack surfaces.
- Visibility into potential attacks and threats at the edge is achieved, making it easier to craft access tunnels and policies.

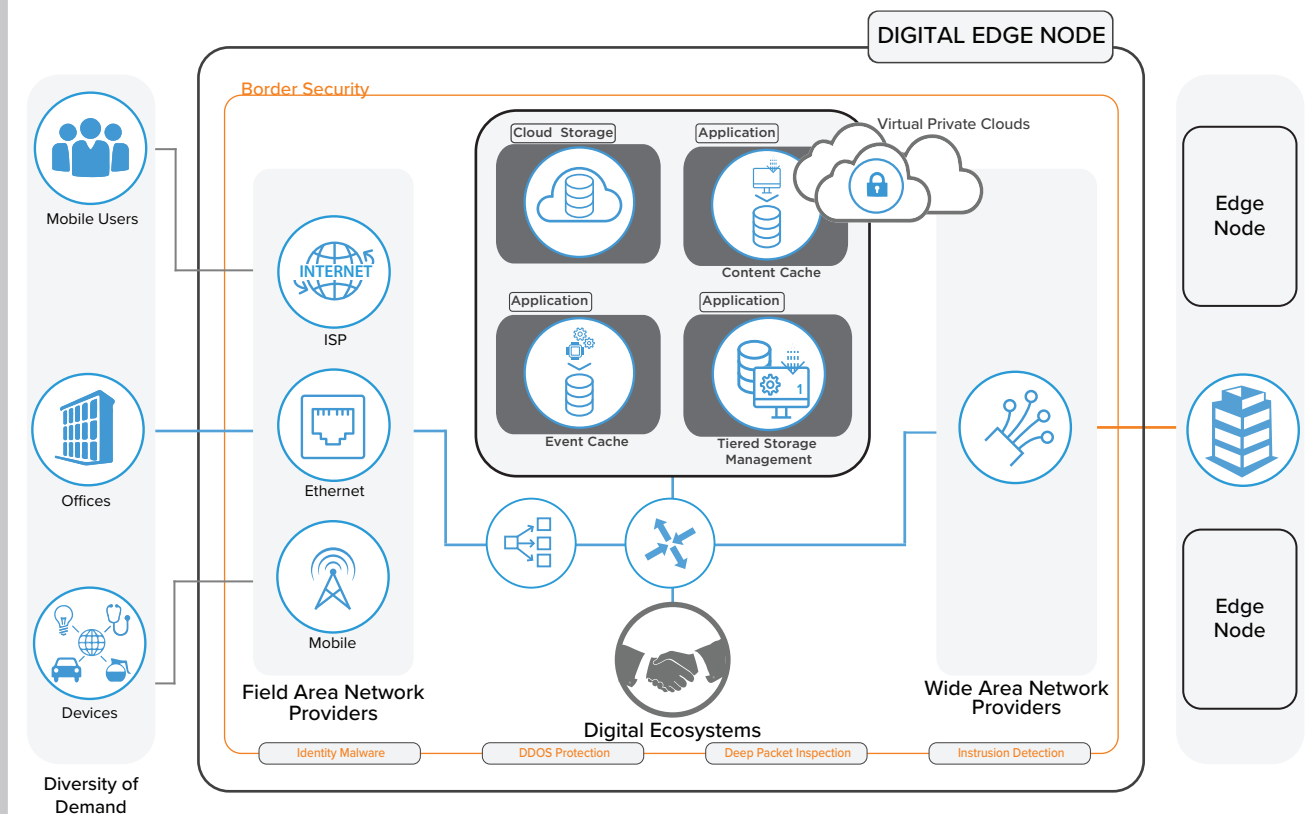
Business

- Consistent and optimal user experience that minimizes jitter and reduces content contribution and distribution delays.
- More WAN and metro Ethernet choices reduce costs.

Potential New Challenges

- Managing content delivery and contribution growth globally across multiple cloud environments.

Reference View





Problem

The growing pace of distributed content creation and consumption drives multicloud and hybrid cloud deployments in multiple regions. This creates user experience and security issues as cross-cloud application integration is required to fulfill delivery service expectations and Service Level Agreements (SLAs).



Solution

Enhance responsiveness of growing multicloud-based application workloads by securely integrating them at the edge. Lower latency and leverage data gravity to improve user productivity and engagement. Use the digital edge to interconnect all cloud deployments in a region, localizing cloud key stores and greatly improving performance, while reducing the complexity of inter-cloud connectivity. Safely interconnect to digital ecosystems for greater partner choice and lower network costs. Place a distributed cache to enhance inter-cloud response time. Improve content delivery across hybrid and multicloud environments by leveraging dynamic content packaging services at the digital edge near user populations so that multisource content is delivered rapidly as a consistent whole. These actions drive more applications and content to the edge, leverage data gravity, and are consistent with the growing trend to send local content updates via metro links instead of backhauling them through a centralized hub, saving time and reducing costs.



Constraints

1. Delivering large, rich content to a local population with high QoS is difficult because endpoint devices and paths have varying bandwidth and format requirements.
2. Services to tailor formats for delivery may not be in the same cloud as the content, causing processing delays between cloud platforms.
3. Content contribution and repurposing processed at the local level is not addressed by traditional long-haul network architectures. Investing more capital in MPLS long-haul networks will not solve this problem.
4. Multicloud deployments of content are inevitable, but cross cloud integration is complex and requires extra safety measures.
5. SaaS-based collaboration services do not solve for distance to the edge, creating response delays.



Steps

1. Use digital ecosystems to interconnect to multiple cloud deployments at the edge where content resides.
2. Control the flow of application integration at the edge across clouds, reducing response time and latency.
3. Install a cloud key store to ensure safe inter-cloud exchange within the edge.
4. Inter-cloud security is enhanced by expanding in-band security services at the edge (deep packet inspection, cloud key management).
5. Enhance caching to include storage for inter-cloud workloads and faster user uploads.
6. Recalibrate storage tiering policies to account for multicloud.
7. Use service chaining to include dynamic content packaging that aggregates multi-sourced content before delivery.
8. Employ content replication between clouds.



Forces

- Enterprise content applications and services are being replaced with or pushed to cloud-based SaaS platforms to cut costs and improve time to market, but resulting unpredictable latency and response times affect user experience and results.
- Support needed for the delivery of heterogeneous, mobile end-point devices in multiple formats with superior scale and performance along with increased expectations of interactivity.
- Higher density of information streams needs to be tailored to local population needs as inter-cloud communication delays hurt user experience.
- Guarding against theft across multiple clouds is a critical concern.
- Responsive content consumption and contribution require applications to run and access data at the edge, not just the cloud.



Results

Technical

- Multicloud application workloads have secure, low-latency access to data.
- Data loss, leakage and theft are minimized without compromising accessibility or user experience.

Business

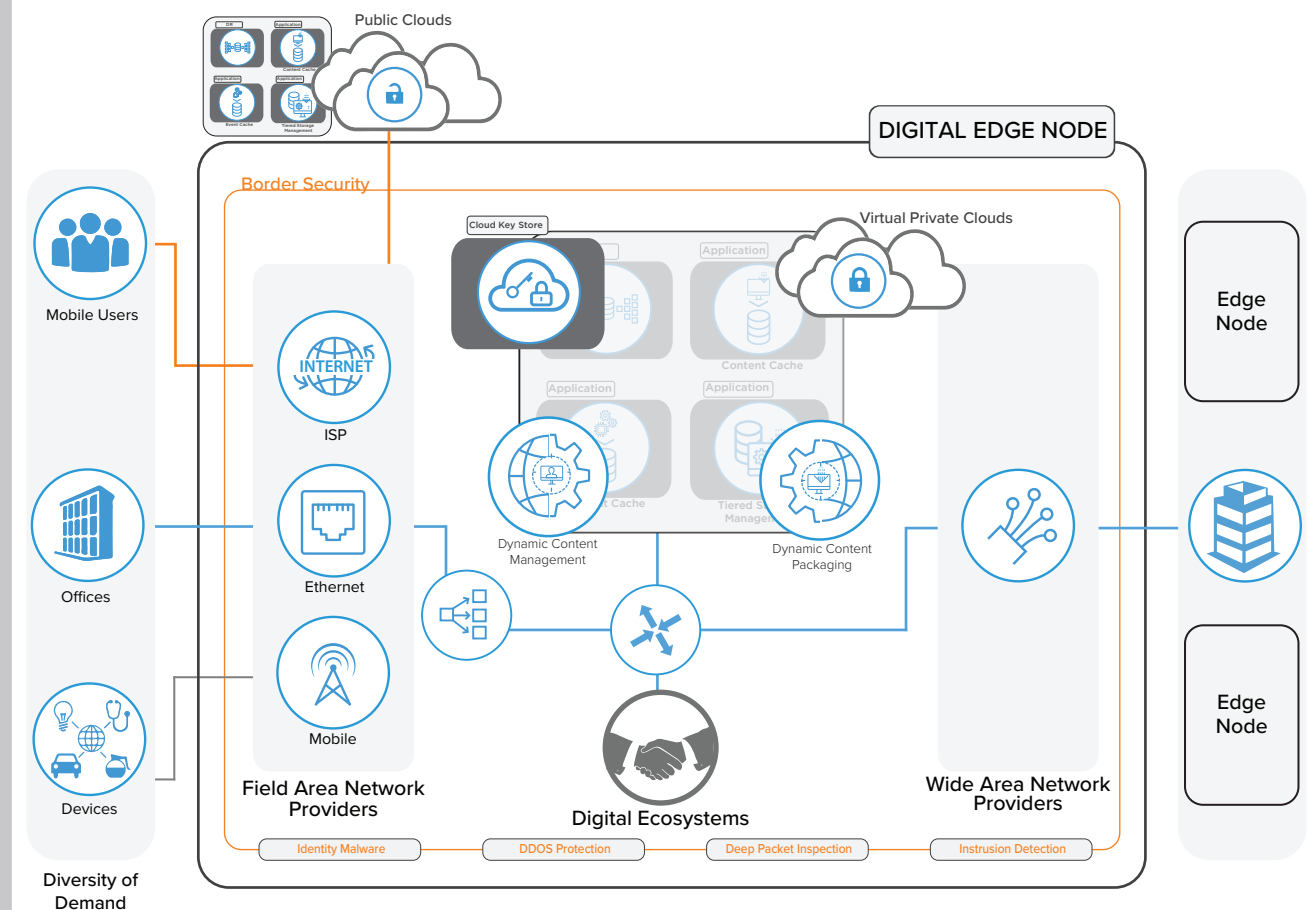
- More content is driven to the edge, improving user experience and engagement.
- User experience for mobile devices is enhanced.
- Investment is in line with data growth, and IT can leverage multiple cloud choices.

Potential New Challenges

- Growth to new locations with new users, and more devices with richer content and greater volumes, will stress any one cloud-based content delivery service.



Reference View





Scale Content with Distributed Capacity



Problem

Content volume continues to grow across new regions with additional devices and richer content types. Network choke points occur when driving content down to key population centers over long-haul lines. This degrades user experience and limits ability to scale the business.



Solution

Control the reliability and efficiency of network capacity as traffic volumes increase exponentially. Strategically add capacity and redundancy by distributing growing content workload volumes across geographically dispersed and secure digital edge nodes near dense user populations. Mesh these nodes so they interconnect directly, providing secure, dynamically routed, resilient paths that adjust to spikes in demand and congestion in supply. Localize data requirements in the digital edge node, balancing protection and scale with accessibility. Deploy a single namespace data service that is available in all edge node locations, optimizing for high availability and data protection. Each node is tailored for local services at that location, providing performance that scales on demand. Data services are also optimized for integration, supporting multiple interfaces (web, APIs, file system, etc.).



Constraints

1. With few distribution points, the delivery of content to a dispersed network will cause bandwidth consumption and costs to scale linearly, even if performance does not.
2. It is impossible to tailor the widespread delivery of local content from just a few central points.
3. The proliferation of devices and their expanding capabilities per user in an expanding mobile workforce and consumer base is unsustainable using traditional centralized network architectures.
4. Planned capacity management cannot meet demand.
5. The increase in metro-centric traffic cannot be solved by centralized network architectures.
6. Content delivery traffic is multidirectional, with real-time messaging and localized contribution.



Steps

1. Deploy edge nodes in new population centers as needed, adding more cloud interconnections and increasing points of presence.
2. Mesh nodes together, and install replication services in the nodes, expanding edge-to-edge volume and reducing traffic back to the centralized data center.
3. Expand interconnections to new digital ecosystems leveraging service chains (e.g., utilizing replication) and SDN/NFV to enable scale and manage volume distribution across the edge-to-edge mesh.
4. Implement dispersed, self-healing content replication where every digital node has multiple connections, preventing a single point of failure.
5. Add caching repositories to optimize data transfer based on policies, employing a single namespace.
6. Globally deploy event-based content updates.
7. Reassess tiered storage management strategy along with cloud storage policies to meet unpredictable demand.



Forces

- By 2020, there will be 4.1 billion internet users, 26 billion networked devices and IP video that comprises 82% of all internet traffic.
- By 2020, the projected global aggregate household data consumption will be 44 zettabytes.
- More users with multiple devices at more locations create exponential growth in demand which consumes all available and planned-for network bandwidth.
- Greater demand in more regions stresses conventional network cost models.
- Content consumption is accompanied by large interactive social media traffic (e.g., Twitter or Snapchat). This data has very different traffic characteristics that must be handled to support the business model.



Results

Technical

- Demand is managed at the local level, alleviating global network congestion.
- Dynamic routing enables self-healing for DR and replication in case of local bottlenecks.
- Replication and disaster recovery is more efficiently processed across the dispersed mesh.

Business

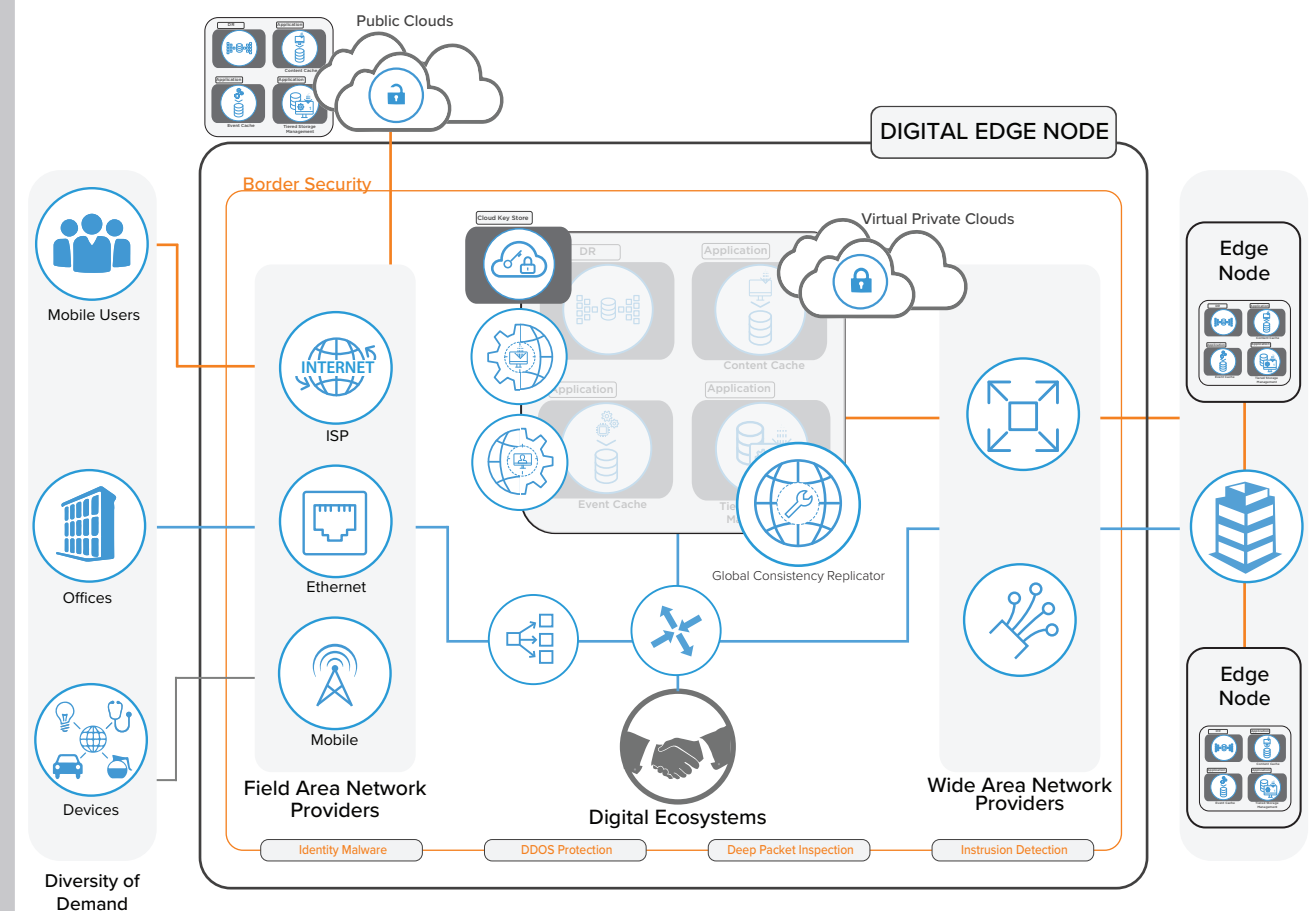
- Local services driving bandwidth via the interconnected mesh reduce communication costs while improving user experience and meeting growth needs.
- Replication scalability becomes more feasible.

Potential New Challenges

- Local dispersion of volumes will need timely, regionalized regulatory compliance.
- Localized personalization is critical to superior user experience.



Reference View





Problem

Compliance regulation software and data have traditionally been kept in the core data center. In widely dispersed enterprises, regulations often change, reflecting local needs including a growing mobile workforce. Regional personalization requirements cannot be managed centrally as user experience requirements are not met.



Solution

Guarantee timely and relevant regulatory compliance and brand-enhancing personalization services by driving policy enforcement decisions to local regions through edge-based service chaining. Control data sovereignty and access with locally enforced policies reflecting geographic limitations and protections which change the most often. Ensure that regulation policies are pushed to the edge through expanded compliance services. Leverage deployed edge security services (e.g., deep packet inspection) to enforce local compliance regulations. Deploy edge repositories that retain the latest compliance policies, protect all users from theft and attacks and log all required events (e.g., auditable file changes) required by regional compliance. Ensure localized regulations are applied to inter-cloud interactions. Enable dynamic changes to personalization for content delivery. This allows for shifting business needs and changes that can be extended as needed to business value chain partners.



Constraints

1. Regulation software is deemed too important to be distributed outside company firewalls, but keeping it centralized delays file access and delivery. Backhauling all regulation checks to a centralized data center creates a poor user experience.
2. Traditional centralized compliance is unsustainable in a global dispersed network where many of the enforcement policies reflect regional concerns.
3. Some compliance services (e.g., data sovereignty checks) present performance problems in multicloud interactions if they are not enforced at a regional level.
4. The traffic volume in a large population center from the public internet creates a significant threat.
5. Most compliance changes originate regionally, making timely enforcement a complex challenge.
6. Application interaction for content creation across the value chain will suffer from critical response time issues.
7. Regional personalization requirements cannot be effectively managed centrally.



Steps

1. Expand security service chaining at the edge by leveraging partner ecosystems to include encryption services and data repositories that hold all local compliance policies, including auditing.
2. Install repositories to meet local/regional audit and logging compliance regulations.
3. Invoke policy-driven segmentation at the digital edge (an extension of the company firewall), where a cloud-based solution would be prohibited.
4. Ensure that local BYOD policies are enforced.
5. Control traffic across mesh connections with appropriate segmentation at the edge.
6. Install repositories and leverage service chaining to provide nuanced, scalable and localized personalization services.



Forces

- Regulations change rapidly across a global enterprise, but most regulation changes occur regionally and need to be enforced locally.
- Control must be asserted to protect against theft, attacks and information loss.
- Some regulations restrict viewing of data at a regional level.
- Audit features are critical for holistic security and user confidence, but can hurt user experience by introducing latency.
- The need for non-repudiation (e.g., buying content) needs to be balanced with the need for exceptional performance.
- Regionalized personalization is a critical success factor in content delivery.
- Content creation drives new business value chain partners and opportunities.



Results

Technical

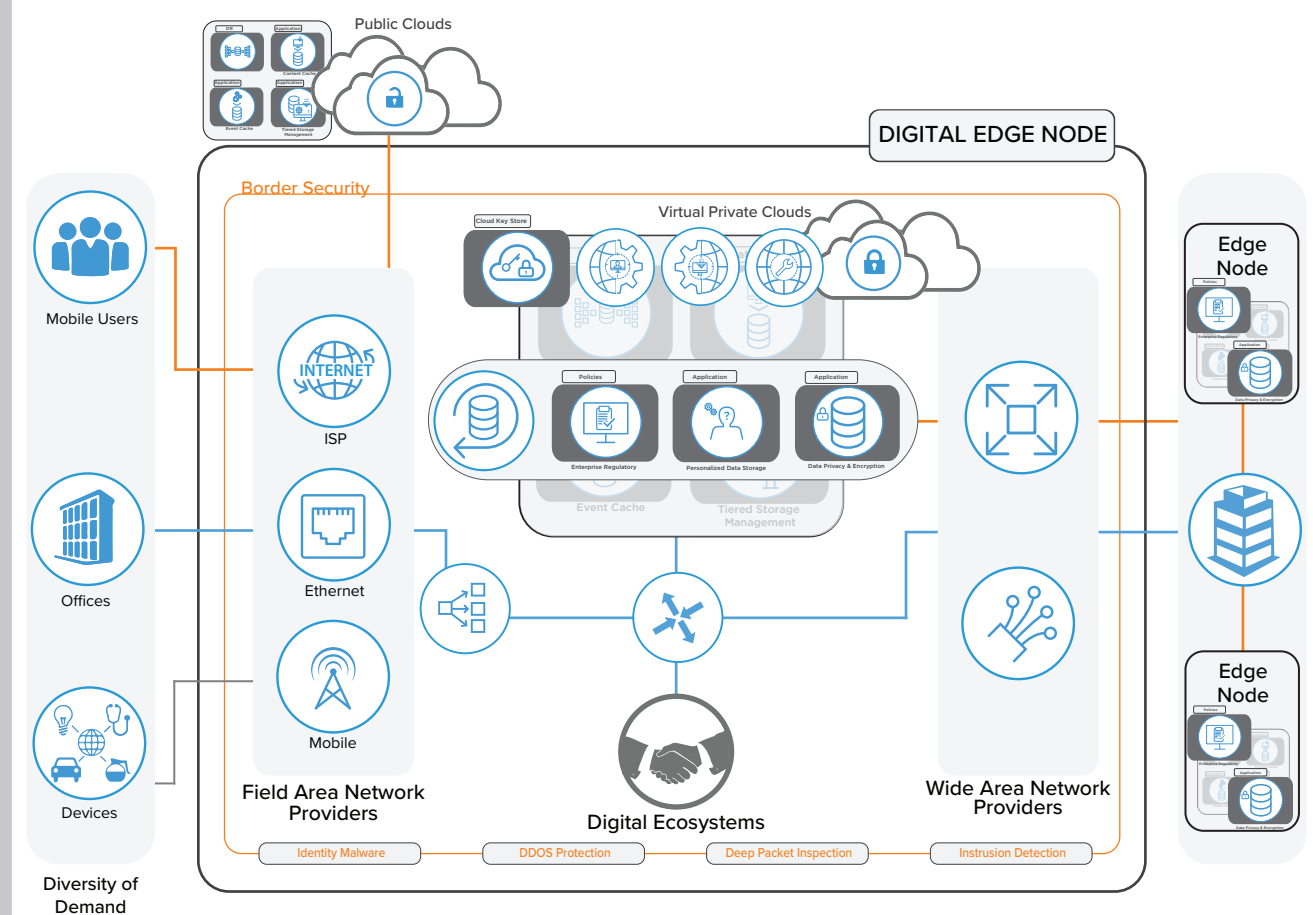
- Regional regulatory compliance can be tailored and kept timely without performance delays.
- Privacy can be better protected by ensuring secure edge-to-edge connections over the mesh.
- Automated workflows and compliance services (such as end-point auditability and security analytics) are easier to maintain and enforce because of improved response times.

Business

- Costs and reputational risk are better controlled using local services at the edge.
- Cloud services that were previously rejected due to local regulation issues can be utilized.
- Business value chain partners can be safely and quickly added and removed.
- Personalization services can be administered and applied locally for optimal user experience.



Reference View





IOA® KNOWLEDGE BASE

Digital Content Delivery Value Chain



Problem

Content delivery models are changing to a multidirectional, multimedia volume mix that becomes less predictable as users grow and technology advances, requiring a more flexible, resilient architecture that can add bandwidth as needed and survive local outages cost-effectively.



Solution

Leverage an ecosystem of service providers that can expand and contract based on business-driven policy decisions enacted through real-time configuration control. Adapt to changing business needs across time zones, business and partner acquisitions, content contribution trends, traffic patterns, new regulations, unpredictable events, technical innovation and new capability requirements to support new business value chain models. Store the policies in local data repositories at the edge. Drive most traffic volume to the interconnected edge node mesh where digital ecosystems can route the traffic most efficiently. Leverage predictive analytics to inform policies about real-time changes to demand across the distributed enterprise. Assess user trends and traffic analysis that will enable you to dynamically rewire services and connectivity to continually adapt.



Constraints

1. Fears of being caught without sufficient bandwidth cause firms to over- or under-provision in a fixed-price architecture, while demand remains dangerously unpredictable.
2. Volume and bandwidth policy management are not considered feasible or strategic, given historical experiences in IT.
3. Dispersed, policy-driven volume management is unfeasible in a traditional hub-and-spoke network architecture with a few central hubs.
4. Service connections are often fixed, limiting the responsiveness required in a crisis.
5. A mindset change is required to architect a network and its services as a fluid set of interconnections.
6. The mix of file types and sizes requires increasingly sophisticated QoS transmission policies.



Steps

1. Install business policies at the edge for dynamic responses to spikes in demand by leveraging local vendor and business ecosystems via interconnection.
2. Drive traffic volume to the inter-node mesh, allocating resources where they are needed while meeting user experience requirements.
3. Leverage a global ecosystem of digital services as and when needed, managing costs more effectively.
4. Employ policy-based acquisition of content delivery and contribution service chaining in real time.
5. Leverage cross-regional digital ecosystems to find the optimal service chain across clouds by driving traffic through the interconnected edge mesh.
6. Leverage predictive analytics to inform policies about real-time changes to demand across the distributed enterprise.



Forces

- Meeting unpredictable demand must become a strategic asset, not a liability.
- Planning for periodic shifts in demand is a policy issue, not an engineering project.
- Real-time, flexible, purpose-built infrastructure is a strategic enabler of a global digital enterprise.
- Demand will fluctuate sufficiently to challenge most assumptions about capacity management in traditional architectures.
- Technology change rapidly accelerates increased file sizes and rich content, with live events requiring increased infrastructure/mission-critical support.
- User mobility across regions creates challenges for personalization.



Results

- Technical**
- Utilize real-time analytics and predictive models to inform business strategies and link marketing to results.
 - Expand services and bandwidth without re-architecting every few years.
- Business**
- A dynamic, real-time enterprise that responds to changing needs in demand, flexibly increasing infrastructure supply to match user experience needs while saving resources when demand drops, without re-architecting the network.
 - Consistently enhance local user experience based on local needs, regulations and customs.
 - Add or subtract business value chain partners as needed.
 - Improve and drive business strategy, operations and execution in real time.



Reference View

