Secure Collaboration Channels

Problem

Compliance regulation software and data have traditionally been kept in the core data center, but in a widely dispersed enterprise, regulations often change, reflecting local needs including a growing mobile workforce. Compliance must not impede the ability to conduct business effectively.

Solution

Control transactions and interactions with locally enforced policies reflecting geographic limitations and protections which change most often. Ensure that regulation polices 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., video conferencing calls) and transactions required by regional compliance. Ensure localized regulations are applied to inter-cloud interactions.

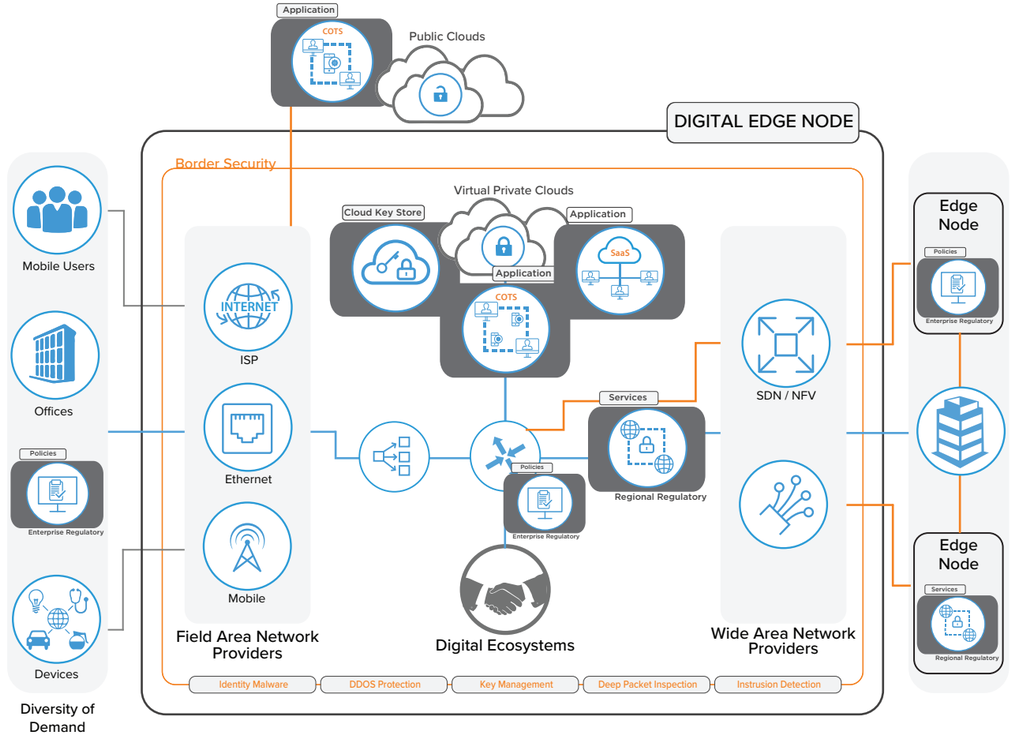
Constraints

1. Regulation software is often considered too important to be distributed outside company firewalls, but keeping it centralized inhibits collaboration due to significant delays associated with backhauling all regulation checks to a centralized data center.
2. Some compliance services (e.g., recording video conference calls) present performance problems in multicloud interactions if they are not enforced at a regional level.
3. The traffic volume entering the digital edge in a large population center from the public internet creates a significant threat vector.
4. Regulation mandates must be balanced with the need for exceptional performance, as certain collaboration workloads are highly sensitive to jitter and latency.

Steps

1. Expand security service chaining at the edge by leveraging ecosystems to include recording 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) to enable cloud-based solutions.
4. Ensure that local BYOD policies are enforced.
5. Install auditing features at the digital edge to ensure comprehensive security and user confidence.
6. Control traffic across the mesh connections with appropriate segmentation at the edge.

Reference View



Forces

- Control must be asserted to protect against theft, attacks and information loss.
- Regulations change rapidly across a global enterprise, but most regulation changes occur regionally and should be enforced locally.
- Some regulations require transactional recording and can 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 in a cross-value-chain collaboration community must be balanced with the need for exceptional performance.

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.
- Compliance services (such as end-point auditability and security analytics) are easier to maintain and enforce because of improved response time.

Business

- Costs and reputational risk are better controlled using local services at the edge.
- Expand cloud services that were previously held back due to local regulation issues.

Potential New Challenges

- Unplanned volume growth can still affect the performance of security services.