Locate Identity & Key Management

Problem

Tracking the bidirectional flow of users and services and requiring those services to constantly fetch credentials and decryption keys causes latency delays if those services are not colocated. However, in a multicloud environment, that can cause a proliferation of copies, which increases complexity and may be compromised.

Solution

Place critical infrastructure services in the edge nodes. These services should be both latency sensitive and risk sensitive (like security services such as identity and key management). They typically have high traffic volumes – and can be placed in proximity to clouds, digital ecosystems and user population centers in the edge nodes. This provides a federated service within the trusted security infrastructure. This way your company retains full control over the services, and if any of the clouds and/or partners become compromised, it is not a "shared fate" scenario (they don't even have the data). Likewise, even within your firm, access to these systems must traverse the inspection zone, and policy enforcement points ensure attempts to steal or leak security data are detected and prevented. Not only does this simplify management and improve security, the results are far more efficient and beneficial.

Constraints

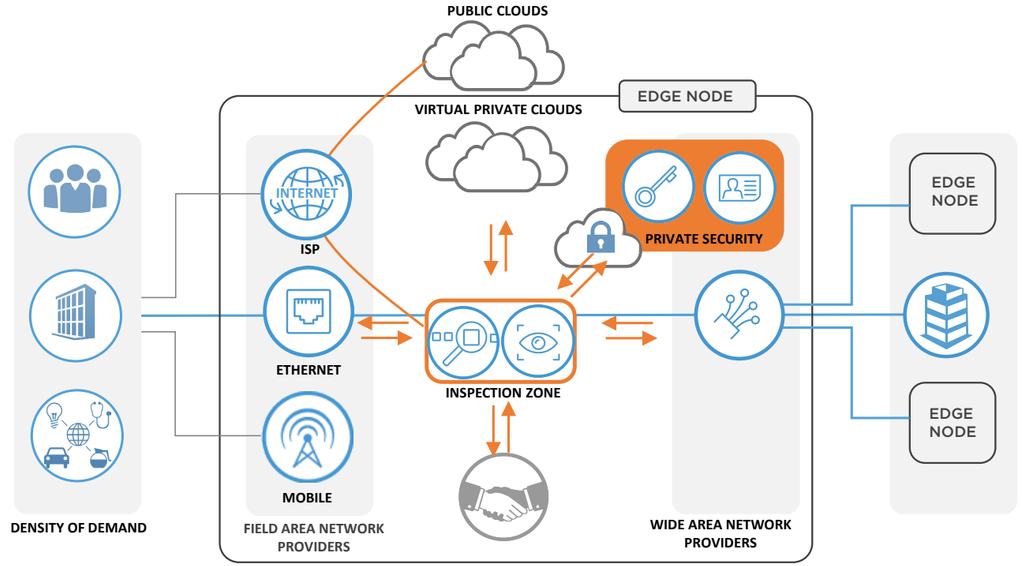
1. Having the security information stores like key management and identity services centrally located (HQ data center) forces all edge requests to backhaul and longhaul over the WAN. Whenever traffic does that, user experience and application performance suffer.
2. Likewise, security information has traditionally been centralized due to a natural resistance to proliferate sensitive data that, if compromised, could cripple the firm.
3. Cloud providers offer these services to alleviate the need for backhaul, and they get used because there are no viable alternatives.
4. If a multicloud environment is compromised or caught up in a government action (does cloud have a nationality?), as a shared infrastructure tenant your company's data could be involved.

Steps

1. Deploy security appliances (usually dedicated hardware appliances) and apply proxy/load balancing as needed.
2. Configure boundary roles and inspection zone policies to further protect access.
3. Leverage network segmentation to provide an isolated service replication/synchronization channel (closed circuit) across the edge node fabric.
4. Encrypt security service data with a separate mechanism and break-glass procedures.

Note: Public internet apps can also use the services over the ISP link. In addition, for services that are already established in a cloud, you can extend hosted service(s) to other clouds with a path through the edge node rather than duplicate them.

Reference View



Forces

- The balance between "trust-no one" security and reasonable performance is very hard to achieve with remote critical infrastructure services—but the risks need to be mitigated.
- Business is becoming heavily dependent on IT services and the impact of outages—especially for what is sometimes termed critical infrastructure (DNS, Directory, Identity, Key Management or even Network) equates to $/second in downtime and reputational damage.
- When private information is compromised, data is leaked, and/or worst case, slowly corrupted over time, the impact can take months to be fully understood and typically costs the firm hundreds of millions in remediation.

Results

- Security services remain in control of the firm at all times regardless of changes to cloud services' use.
- Multitenant service attacks (hypervisor core dumps) will not yield services or security data, as the information doesn't exist there.
- Capitalize on the latency advantages and implement more security, governance and controls, which would have otherwise negatively impacted user experience or scale.
- Overall performance and resiliency is improved with services federated across edge nodes and intersection points.
- Any disruptive event in a cloud or partner environments will not be a "shared fate" scenario.