Policy Administration & Enforcement

Problem

More complex systems are being assembled, in shorter time frames, with increasing business dependence on less understood technologies. New guardrails are needed to protect people and the company from mistakes or unsanctioned behavior.

Solution

As the third Security step with the Network Blueprint* layer as a foundation, policy enforcement can also be deployed and applied in edge nodes for improving boundary controls and preventing mistakes or malicious actions within the inspection zone. Leveraging monitoring capabilities, event processing can detect and take action in real time for a variety of scenarios that would otherwise not be possible. A developer accidently runs a test against a production database, an employee tries to send a file link but sends access to the folder (containing competitor information) — since all business traffic traverses the edge nodes, distributed control points operate at every intersection point.

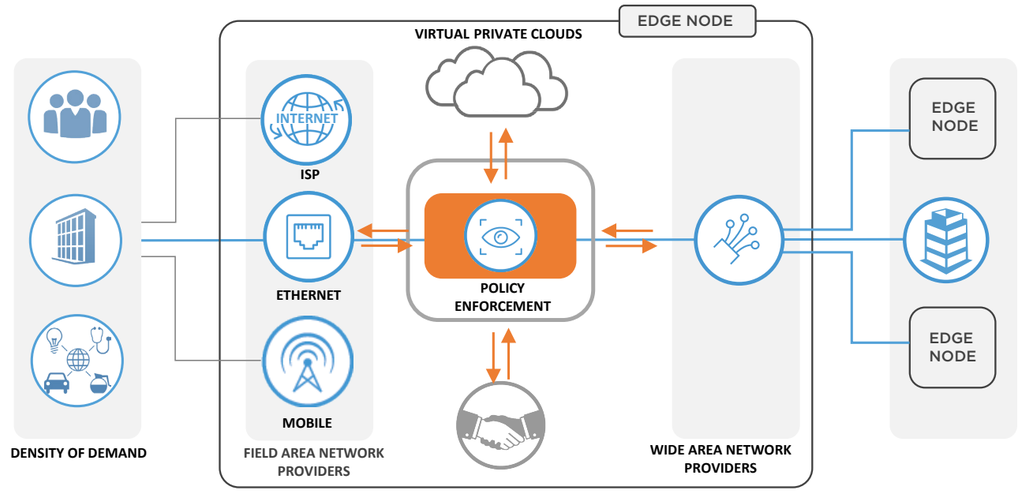
Constraints

1. The ability to establish policies is mostly unlimited within any organization, yet most organizations do not have the ability to enforce policies.
2. In order to enforce policies, you need to implement in a way that cannot be circumvented. Doing so is generally difficult to achieve.
3. Many of the activities to which firms need to apply policies are outside their boundaries (perimeter) and not visible. It may be known that it is occurring, but there is no broad enforcement capability (other than manual processes).
4. Without basic event processing and monitoring, determining what policies are needed is difficult.
5. You cannot manage an automated environment without automated controls. As a result, governance and risk management are severely limited.

Steps

1. Establish which flows require what kinds of policies. In doing so, determine what is available in your security ecosystem that can be leveraged in your edge node.
2. Install the interception appliance and configure it to be part of the flow with a dedicated path to SaaS services.
3. Consider a SaaS service that maintains polices and registries of already prescribed and mature execution/remediation steps.
4. Monitor and log policy actions as another source of data for later analytics.
5. Tailor the policies over time for the most effective coverage.

Reference View



Forces

- The digital economy is driving exponential increases in types and sources of requests that require policy approval (e.g., APIs, mobile apps, partner and ecosystem connections).
- Policy enforcement decisions are real-time in nature, and as such, user experience and scale are driving enforcement decisions closer to the edge.
- Automated businesses need equally capable guardrails in place to mitigate risk and protect boundaries and employees from mistakes amid the automated chaos.
- Through software-defined infrastructure (technology APIs) and digital services (business APIs) come tremendous power and capability. You didn't hear about millions of people's private information being lost, or leaked, 10 years ago.

Results

- Know that firm policies, like cloud usage, are being adhered to.
- Avoid the most common mistakes and an ecosystem full of lessons learned (the hard way) with subscription(s) to security services.
- Another hybrid design allows offloading into clouds to shifting to cloud-delivered, from cloud-assisted.
- Capitalize on the latency advantages and implement more security, governance and controls, which would have otherwise negatively impacted user experience or scale.

* Network Blueprint — IOAKB.com