Inspection Zone

Problem

Applications and business processes are becoming more distributed, more granular (services), more mobile and more automated. With increasing business impacts and dependencies, the need to observe interactions and flows has greatly increased, but the ability to do so has not.

Solution

Having applied the IOA Network Blueprint* as the foundational layer, and boundary control in the edge nodes, the solution to monitoring digital engagement and traffic is to create an inspection zone in each of the edge nodes, positioned at the intersection point of all networks, flows and traffic. This puts your controls back at the center of the network (in order to improve intrusion detection and prevention, or stop data leakage, etc.) and provides the perfect location to capture data for later analytics—not just for security, but for many analytic use cases. Extending our airport security analogy, border control allows entry into the security zone, but then what is being carried needs to be inspected before it can be allowed through (again regardless of arriving or departing in this case).

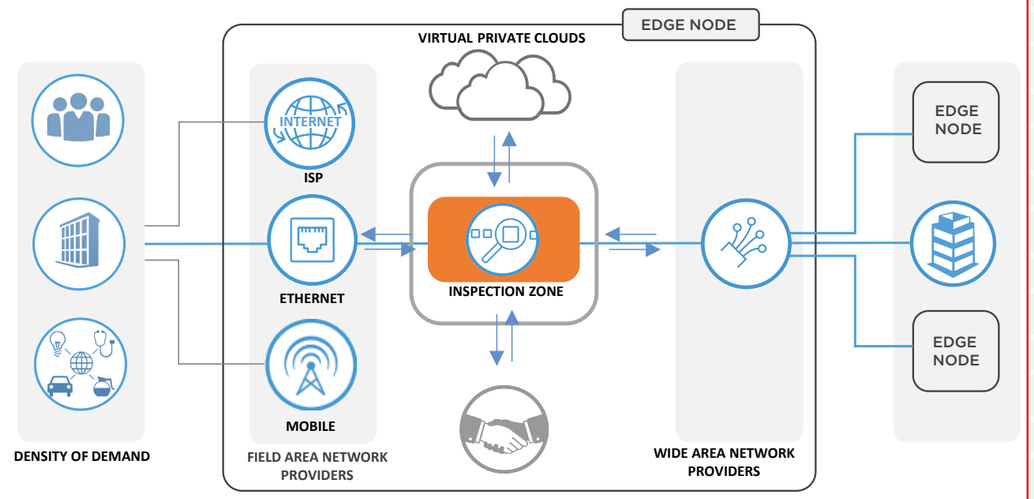
Constraints

1. Integrating ecosystems in today's multicloud and multinetwork environment requires a zero-trust model that goes well beyond the capabilities of a traditional perimeter model.
2. There are various techniques to observe network traffic in order to monitor interactions and flows. However, traffic is shifting to the edge and with trends such as the consumerization of IT and direct cloud access occurring, inspection points are not available or are being bypassed.
3. Even if you could backhaul all the traffic, the volume continues to increase and centralizing that volume quickly overwhelms the inspection point.
4. As customers and employees become more mobile, security needs to be able to follow the user no matter the location or device. Traditional models are static and more limited.

Steps

1. Determine what levels of monitoring will be applied to each segmented network flow, the amount of data captured or generated per event being processed, and what the expectation on arrival rates and projection of growth will be.
2. Size and deploy the appliances into the edge node and route authorized and authenticated traffic from boundary control into the inspection zone.
3. Apply real-time traffic analysis in this way across each of the distributed edge nodes — logging and aggregating the data for global monitoring and analysis.
4. Leverage the inspection zone to help follow the user and apply user-centric security models.

Reference View



Forces

- We are developing more complex systems, in shorter time frames, with increasing business dependence on less understood technologies, that all require greater partner and provider trust. The need for control is increasing disproportionally to the ability to control.
- More dynamic and adaptable approaches are needed to monitor traffic (which is becoming synonymous with business and commerce).
- To build advantage in the digital economy, algorithms are needed to provide insights that help decision support – like improving security, detecting intrusion, and automating efficient responses to our pace cyberbots. This starts with having useful data about traffic and interactions.

Results

- Now all traffic and interactions across network segments can be monitored and logged.
- Distributed inspection zones at high-bandwidth and lowest-latency intersection points allows this service to efficiently scale.
- The ability to leverage cloud ecosystems (and security service innovation) with a low-latency cross connect presents opportunity.
- As new cloud services are added, they can automatically be monitored. In addition, interactions between cloud services can be routed through the inspection zone (even from the internet).

* Network Blueprint — IOAKB.com