Boundary Control

Problem

Effective boundary control proves difficult when the edge has been redefined across mobile, cloud, B2B and traditional networks. The majority of traffic is shifting out into the untrusted side of the traditional perimeter. For some, the perimeter has ceased to exist.

Solution

Based on the IOA Network Blueprint* as the foundational layer, implement new boundary control inside your geographical edge nodes at the ingress and egress points of segmented traffic flows. This is the closest point to users, clouds and business partners, and the ideal location for a standardized set of hybrid boundary services (i.e., that leverage Security SaaS, over multicloud connectivity, by design). The primary objective is to solve boundary control locally. Using airport security as an analogy, in this solution we are establishing the first checkpoint to determine if the actor has a valid reason to continue inside the security zone, with the exception that we are following a “zero-trust model” and challenging both ingress and egress. The types of things to block, or redirect, are not functionally different (if security is current); they are just now applied in distributed intersection points, with hybrid capabilities, and tailored according to what you need in each metro location (e.g., if its an IoT edge — tailor for that).

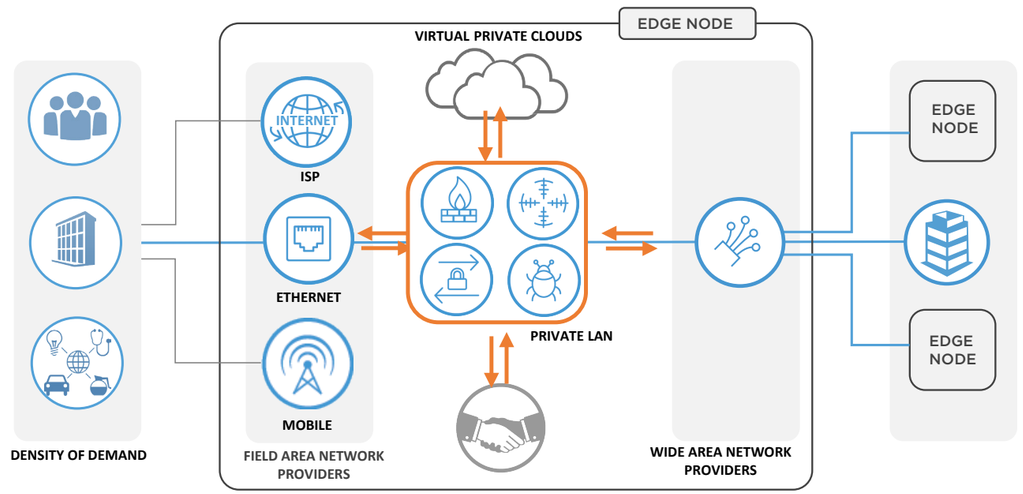
Constraints

1. While network defense has always been concentrated on securing "the edge," with the advent of mobile, cloud and digital ecosystems, the “edge” has been redefined.
2. For those still living with the traditional perimeter model, there effectively is no single edge anymore. There are many edges. This makes traditional protection methods increasingly ineffective yet still expensive.
3. Much of what security needs to protect against is occurring closer to the user, and so the protection also needs to be close to the user. Centralized protection is far from everyone.
4. Backhauling and converging traffic is creating bottlenecks, impacting performance and requiring very large and expensive security equipment that ultimately provides a questionable return on protection.

Steps

1. Determine the security policies and filters for each flow of traffic segmentation (Network Blueprint*).
2. Next determine the local volumes and arrival rates of each flow to size the boundary services.
3. Qualify the expected latency overhead. Note, you can add more security as your starting latency was already exceptionally lower than before.
4. Size the services and review placement options. Use physical/virtual appliances in the node and/or potentially extend with Security SaaS. Overall demands are typically lower in a distributed model vs. centralized.
5. Apply the boundary stack across all network types: Field Area Networks, Internet Peering, Multicloud, Digital Ecosystems (B2B) and Metro WAN links to other hubs/corporate data centers.
6. Log everything for later pattern analysis.

Reference View



* Network Blueprint — IOAKB.com

Forces

- Cyber attacks are on the rise, and with the shift to digital business models and increased business dependency on technology, the impact of those cyber threats is also increasing.
- New forms of digital engagement with customers, employees and partners are being adopted every day and are becoming the dominate forms of business communication and processing.
- Likewise, digital services and ecosystems are connecting to transact (messaging). Applications are being assembled from a set of networked APIs from different sources. How do you know any of those have not been compromised?
- Lastly we have the advent of IoT. Millions of mobile and stationary ‘things’ try to report in.

Results

- You have localized security controls by placing security boundaries as close to where business is executed as possible (same data center).
- Field network traffic only crosses the internet locally, and all other traffic is on private networks (dramatically reducing attack vectors).
- Capitalize on the latency advantages and implement more security, governance and controls which would have otherwise negatively impacted user experience or scale.
- The distributed edge nodes, with load-balanced traffic across the mesh, already minimize impact of attacks in any one location.
- This alleviates the impact on user experience (which is how companies usually find out they are being attacked).