Control Digital Communications

Problem

Dispersion of processing and data, combined with increasing ingress/egress points (to internet, clouds and partners), in more locations globally, with changing regulations, and increasing attack surface and sophistication – begs the question, how do you retain control? Especially at an increasing rate of change?

Solution

What is needed is not a "perimeter", but a series of security checkpoints (a.k.a. control points). In an IOA these checkpoints are like airports, and like airport security, you challenge and inspect all traffic from multiple source and destination locations. In a zero-trust environment you are checking both inbound and outbound traffic equally. These checkpoints are geographically located where you need them, near clouds, customers, employees, etc. Together they form a distributed security mesh. By placing a control stack (or physical and virtual/SaaS functions) in each control point and routing all (important) traffic through it, you not only can control isolation, segmentation and inspection; but verify identity and enforce policy as well (who are you? where are you going? which airline or flow? what are you bringing with you? are there any red flags?). All of this happens locally and overall acts like a spider's web. As a result, when new cloud environments or partner connections are created, the new endpoints and traffic are discovered (auto update and verify), and base controls/policies are automatically applied. These permissions can be elevated or the traffic is quarantined. With this approach you can effectively track and govern all digital communications.

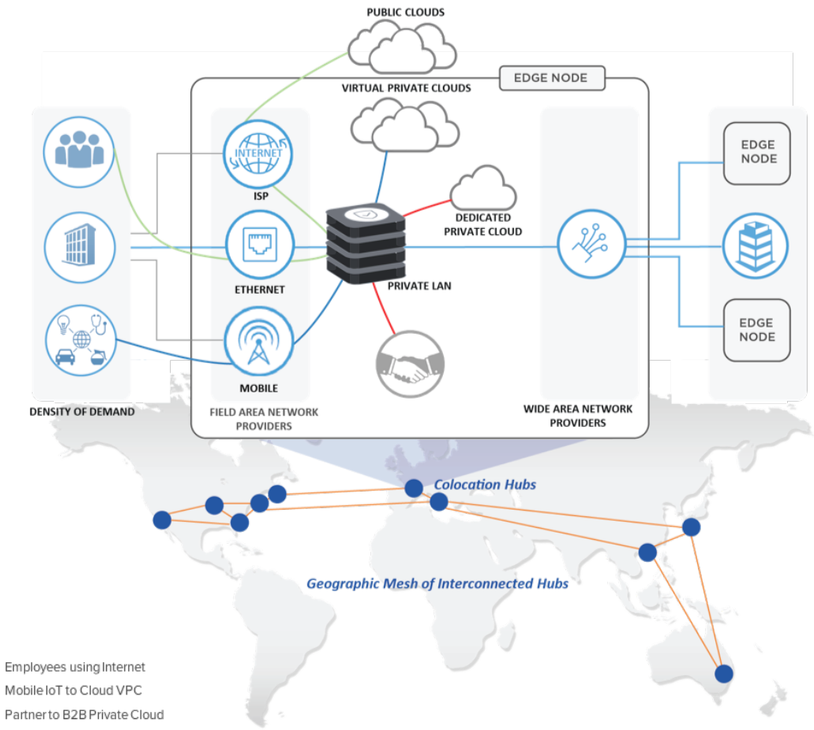
Constraints

1. It's difficult to establish, let alone enforce, a global standard set of controls across disparate networks, clouds, partners and endpoints — especially in a way that cannot be circumvented and is able to keep up with dynamic change.
2. Backhauling all digital communication traffic to a traditional centralized security stack is impractical with the exponential growth of traffic, and data and response time and performance impacts are too high. Bypassing the security stack would be the preferred choice.
3. Storing security information like identity and key management in multiple cloud locations alleviates the backhaul problems but creates new kinds of risk. If one is compromised, they could all be compromised, and any keys or data that get caught up in a government action may expose your data as well (and you wouldn't be notified).

Steps

1. Deploy strategic fortified control points: Select colocation hubs that meet security, availability and regulatory compliance requirements. Ensure that the networks, clouds and partners that you need to interconnect with are available.
2. Apply zero-trust boundary with dynamic interconnection: Isolate networks (e.g., corporate, commercial and third party), define primary traffic flows and interconnect the counterparties, internet circuits and SD-WAN to each.
3. Localize traffic management and transport security: Deploy global secure dynamic DNS with load balancing for planned use with multiple public/private network address spaces, including clouds. Deploy key management for encryption/certificates and global secure uptime.
4. Segment network access with inspection zones: Segment traffic flows into security zones and rules. Place device, actor, role, location — access controls and DDoS.
5. Position threat detection and policy enforcement: With guardrails that correct for insecure services (e.g., instead of blocking insecure actions, contact their APIs and secure 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.
- As companies adopt dozens of cloud services, users are being confronted with new apps. SSO integrates that, but it's both a blessing and a curse. It only takes one fake SaaS site to capture an employee's SSO credentials, and they would have access to all that employee's SSO-based SaaS apps. That entire scenario is out of your control.

Results

- You now have distributed critical infrastructure services near customers, clouds and ecosystems — in some of the most secure, resilient and compliant facilities in the world.
- Your security stack is now colocated in ideal locations—the intersection points of networks, clouds, partners and ecosystems with the highest security and bandwidth and lowest latency.
- The majority of business traffic crosses private dedicated links and typically stays within the colocation facility and metro area.
- Because of the huge performance gains and low latency, a much greater level of security can be applied and all traffic can be routed through the stack with minimal penalty (limiting lateral attacks). Your security stack will actually be the preferred route to alternatives.
- Gain bidirectional visibility and control over all mobile, IoT, cloud, partner and data center communications — including shadow IT.

Controls

- Access control and segmentation.
- Secure global DNS load balancing.
- Distributed Denial of Service.
- Transport encryption and secure access.
- Key management and tokenization.
- Security proxy.
- Advanced threat detection.
- Secure messaging and exchange.
- Global secure time.