Instant Zero Trust Access for Merger & Acquisition
Powered by Overlay Zero Trust Networks

Acquisitions Lead to Infrastructure and Access Challenges

With companies looking to acquire technologies and businesses through M&A, some combined operations frequently require crossing the traditional boundaries, almost immediately. For example, new employees from the acquired party need to register on a new HR and admin system. Users need to access some libraries and databases, owned by the other party, to support newly integrated business and developments. Selected critical data in the remote datacenters may need to upload to local services immediately. However, the integration phase of the M&A presents a series of infrastructure and operations roadblocks. Connecting IP networks from both parties (e.g. using a VPN) often lead to a network collision problem. Re-IPing those resources is not an option, since many existing operations are already using those resources in production. It's like trying to renovate a kitchen while cooking at the same time. Network re-engineering is also very expensive and is therefore not a preferred option.

As a result, the need to access selected resources, due to M&A, leads to 6-18 months of infrastructure customization. Enterprises are taking a risk of losing productivity and compromising the business value of the acquisition. Enterprises need an agile and secure solution that provides instant access to resources without going through all the infrastructure hassle.

Zero Trust Network Flexibility and Agility

- Instant Zero Trust Access across corporate security boundaries

- Overcomes network collision issues

- Strong authentication and end-to-end encryption

- Overlay network deploys without touching existing corporate infrastructure

- Faster time to market for LOB's business needs

Zentera's Zero Trust Network across Boundaries Enables Instant Secure Access

One of the promising solutions to address M&A challenges is to implement Zero Trust Access for the selected resources for immediate access, without altering infrastructure. Zentera's Zero Trust Network (ZTN) uses overlay technology to establish end-to-end direct tunnel connections for specific resources. Because of its overlay network technology, Zentera's ZTN is added on top of the existing IP network with total transparency.

With an overlay routing plane, the ZTN can connect specified workloads and users between parties almost instantly – this deployment completely avoids the underlay network collision and re-IP issue. Zentera's ZTN is able to run across network domains. As a result, it helps enterprises to avoid reconfiguring perimeter firewalls.

zentera™

Furthermore, Zentera's ZTN supports fundamental Zero Trust Security requirements including strong authentication as well as micro-segmentation.
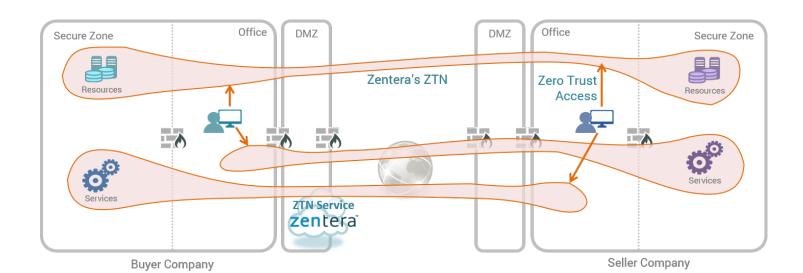
With Zentera's ZTN, enterprises can immediately overcome operational hurdles.
- New employees can immediately access selected resources hosted by remote parties in an M&A
- New employees can log in from remote corporate locations, home offices, and even a Starbucks
- Multiple parties and corporate sites with overlapping subnets can still connect without changing any network and security infrastructure

How is Zentera's Zero Trust Network Deployed?

Zentera supports both product and SaaS business models for enterprise deployment. Zentera's ZTN is a software-based computing solution running on top of existing IP networks. Zentera's ZTN is composed of a few software components listed in the table below. The ZTN core service and the ZT Access for selected resources can be implemented very quickly without any IT ticket for infrastructure change.

- **zCenter** – A centralized controller that hosts connectivity and security policies and enforcement
- **ZNS Switch and Cluster** – A virtual switch that connects overlay tunnels. Multiple switches form a cluster
- **Edge Gateway** – A gateway connecting overlay ZTN and IP network, acting as a proxy for remote access
- **Endpoint Gateway** – A host-based agent that connects to ZTN, without any modification to the application or OS kernel. It supports various popular Linux and Windows operating systems.