The network architect's guide to accelerating mergers & acquisitions with a zero trust network access service

Written by

Nathan Howe

ZPA Architect, Zscaler

zscaler™

Mergers and acquisitions (M&As) can be some of the most stressful situations for business leaders, CIOs, and network architects responsible for a successful IT integration. M&As are often high-profile events and must be implemented as quickly as possible so that the business can realize a return on its investment. But an M&A also serves as a catalyst for modernization within any enterprise as it opens the door to considering new technologies for standardizing security across multiple entities, ensuring a seamless experience for all users and determining the best infrastructure to use.

As teams look to embrace modern, cloud-based technologies, it's often up to the network architects to seek out new ways to connect users to business applications, ensure that products integrate well within the existing system, and accelerate the M&A process. Determining the right approach is not easy given the overload of relatively new solutions out there and the need to ensure that their implementation does not disrupt user productivity or hinder operations.

To achieve this modernization, many network architects have begun to leverage zero trust network access (ZTNA) services to connect users to apps. ZTNA technologies serve as a faster and more secure alternative to the incumbent, network-centric processes that involve converging disparate networks and dealing with overlapping IP addresses through NATing—a process that can take between nine and 12 months on its own.

Within this architectural guide, we will cover the following:

- Architectural differences between incumbent access technology and ZTNA
- A look at a reference architecture for deploying ZTNA during an M&A
- The phases to consider when adopting ZTNA across multiple entities
- Pro-tips and considerations for accelerating the IT integration process during M&A with ZTNA

Before we begin, please take a few moments to read "A Tale of Two M&A Journeys." The blog provides a quick overview of incumbent methods of IT integration during M&A vs. an ZTNA-based implementation.

In this guide, we will use a typical enterprise scenario as an example. Mother Company SE, a manufacturer based in Frankfurt, Germany, is acquiring Child Company PA and needs to scale seamlessly to empower and connect users in each environment to key applications in the environment. Historically, this would mean overlapping RFC1918 address space, which complicates interconnection of the two networks. Additionally, Mother Company anticipates further acquisitions and will need a unified solution to address user access across the disparate environments.

Mother Company SE's current M&A architecture

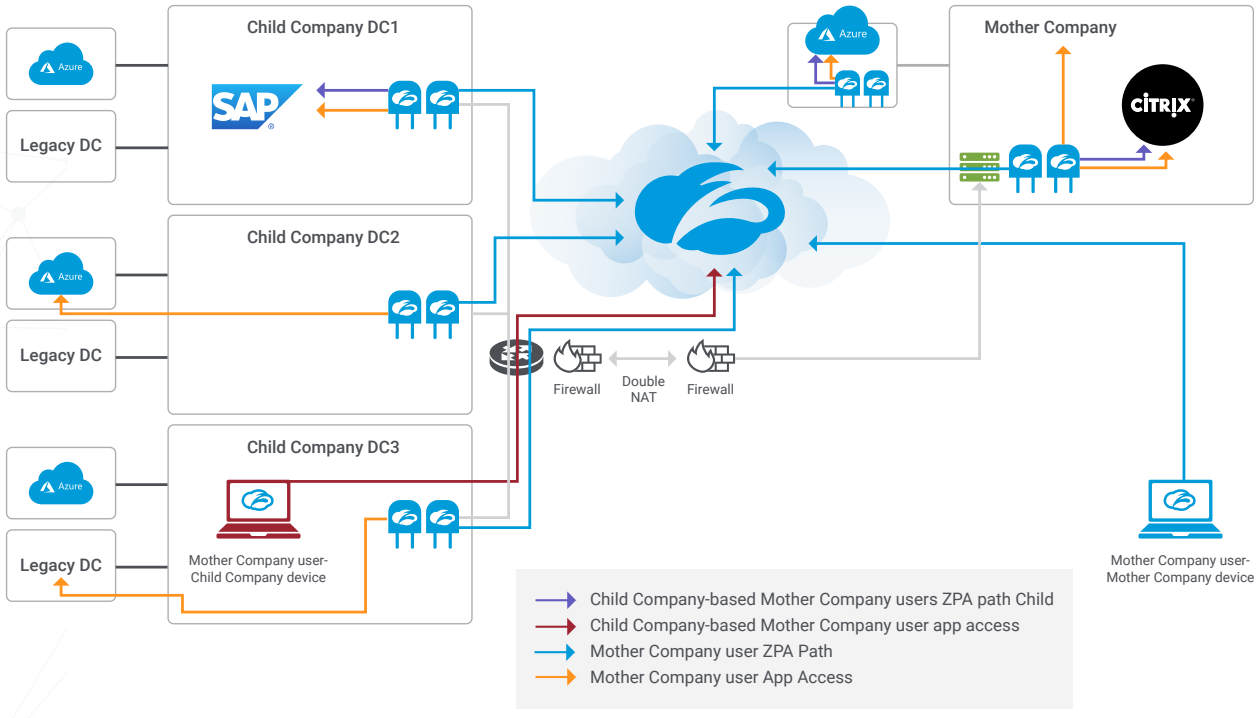
Mother Company is beginning to address how to enable access for its new requirements. Each PA is isolated and does not share any resources, but they all leverage the data center infrastructure as well as Microsoft Azure. The long-term goal is to migrate the applications from within these legacy locations, both DC and Azure, to the Mother Company Corporate Network (BCN).

The access path today for Mother Company devices to the PA regions (and subsequently the inverse for PA users to Mother Company applications) is through a traditional M&A architecture of interconnected firewalls with double NAT and DNS controls at the network boundary. This complex process is time-consuming and costly, especially for networks with significant internal IP overlap or different levels of security hygiene.

Mother Company SE desires a simpler architectural model to quickly and easily provide granular cross-company access. Mother Company will test this model by building out a cloud-based environment and pretending that this is an M&A ecosystem. They are considering using Zscaler Private Access™ (ZPA™). ZPA is the Zscaler™ software-defined perimeter service that provides secure connectivity to private apps running in any data center, hybrid, or multi-cloud environment without placing users on the network.

Mother Company's vision for its architecture of tomorrow

Increases in remote users and in the number of apps they are consuming have placed pressure on the network infrastructure at Mother Company. ZPA will relieve some of this pressure and empower employees and partners to perform their job functions in the most efficient way possible, without compromising security. IT will also benefit from increased visibility, agility, and simplification enabled by ZPA.



High-level proposal for M&A access at Mother Company

At Mother Company, it's not only road warriors who need secure access to applications; office-based employees need to connect directly to cloud-based applications as well. An ZTNA service like ZPA will provide Mother Company with:

Global, unified, secure, and simple access: The ability to access applications regardless of their locations is critical to business. Because apps reside in diverse locations, security and access controls for all users should be applied globally.

Increased security, visibility, and control: All traffic flows to internal applications have controls to ensure that only authorized users can access applications. Teams now have visibility into what users are accessing and can identify previously unknown apps, then apply the appropriate controls.

Cost avoidance: Security and network infrastructure that was once set up to enable your remote users to access—and thus expose—your infrastructure can be eliminated as part of this project. At the same time, VPN, network infrastructure, and software management costs can be minimized.

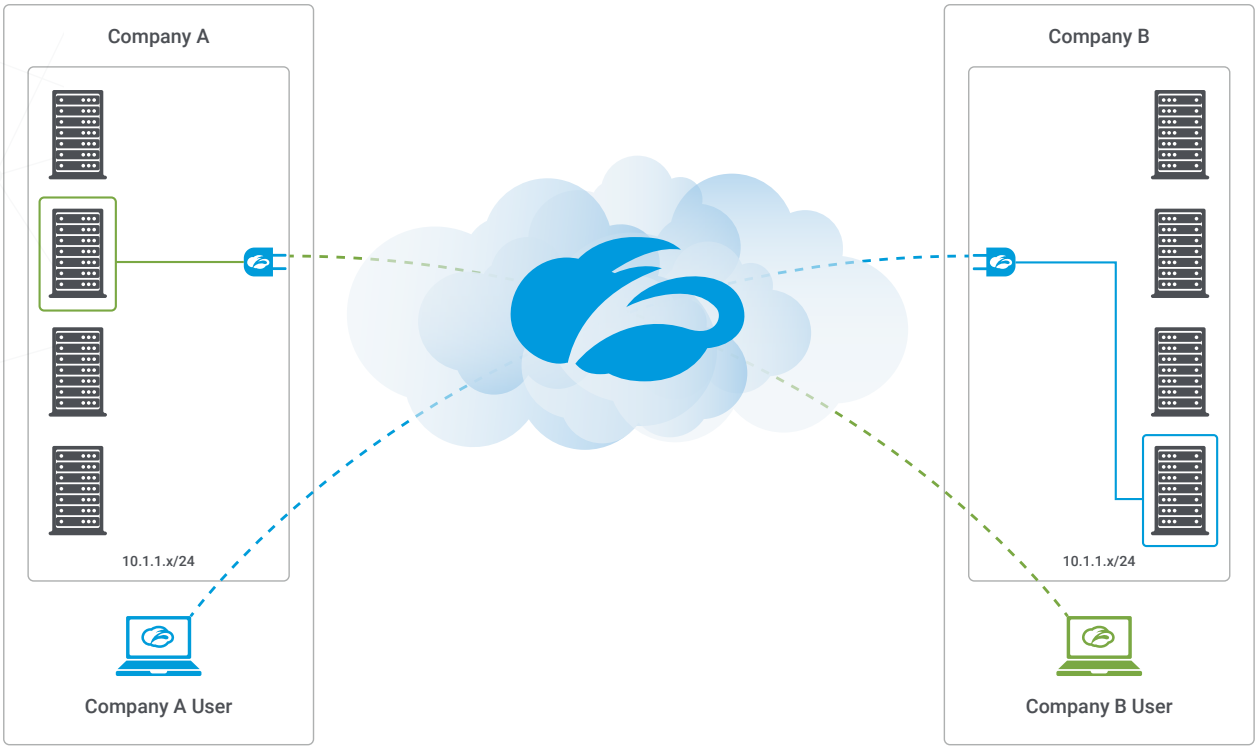
Cloud readiness: As applications shift to the cloud and users shift to mobility, the only way to apply security is either at the endpoint or in the cloud. Leveraging an ZTNA, Mother Company will be ready to adopt cloud applications without infrastructure strain.

Decoupled application access from the network: Shift to a model of application access that uses identity and posture to provide access, rather than network connectivity.

Mother Company's intended end-state

As the diagram shows, Zscaler provides an optimized path to private applications in data centers or cloud environments across a global cloud footprint. Mother Company users will connect to the Zscaler global cloud platform, and Zscaler then becomes the one path for all private application traffic. The Zscaler approach brings all policy controls, reporting, and visibility into a single, unified platform. Diversity and failover are provided by the distributed Zscaler cloud as well as App Connector groups and redundancy. The key is that during this transition, Zscaler provides the consistent end-user experience and policy controls required by the business.

We will explore the recommended phases for Mother Company's ZTNA rollout to the Child Company and how it will allow all users to access private apps running across their environment. In the end, all traffic intended for internal apps will be routed to the Zscaler cloud via ZPA across the combined organization's data centers and cloud environments.



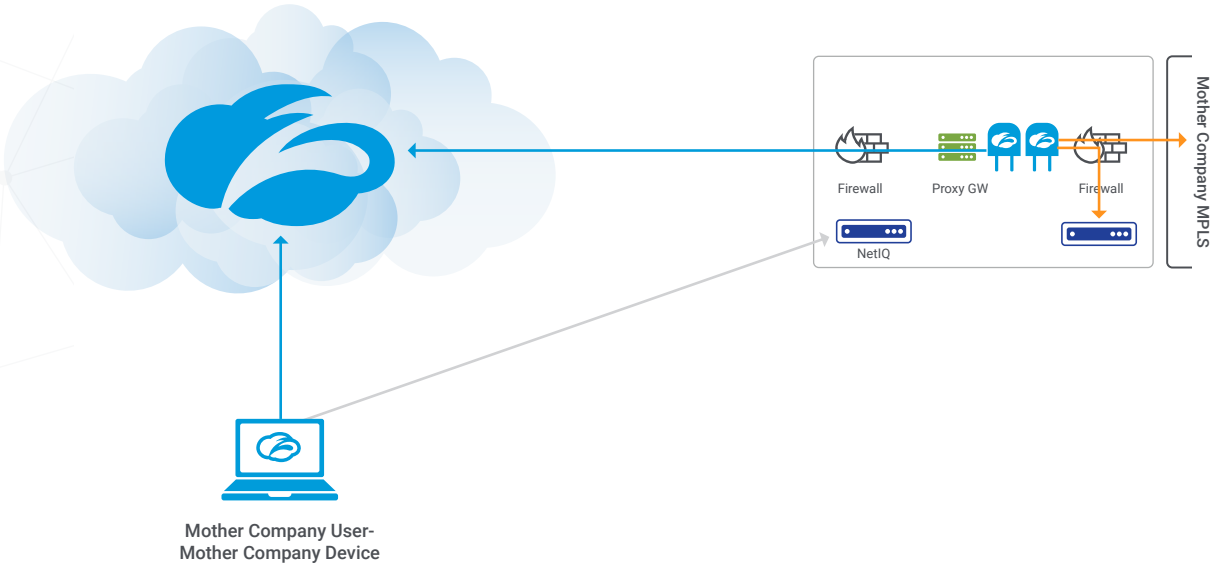
Rather than placing users on the network and delivering connectivity via a remote access service like VPN, ZPA enables Mother Company to leverage the software-defined perimeter (ZTNA) solution.

The ZPA service enables applications to connect to users via inside-out connectivity without extending the network to users and regardless of where the application is running. Applications are never exposed to the internet, as they do not listen for inbound pings, so they're completely invisible to unauthorized users, all of which prevents DDoS attacks. ZPA can also discover previously unknown applications running either in Mother Company or Child Company and then apply granular controls to them.

A phased approach to adopting ZTNA for accelerated M&A

Phase 1 Prioritize accessibility

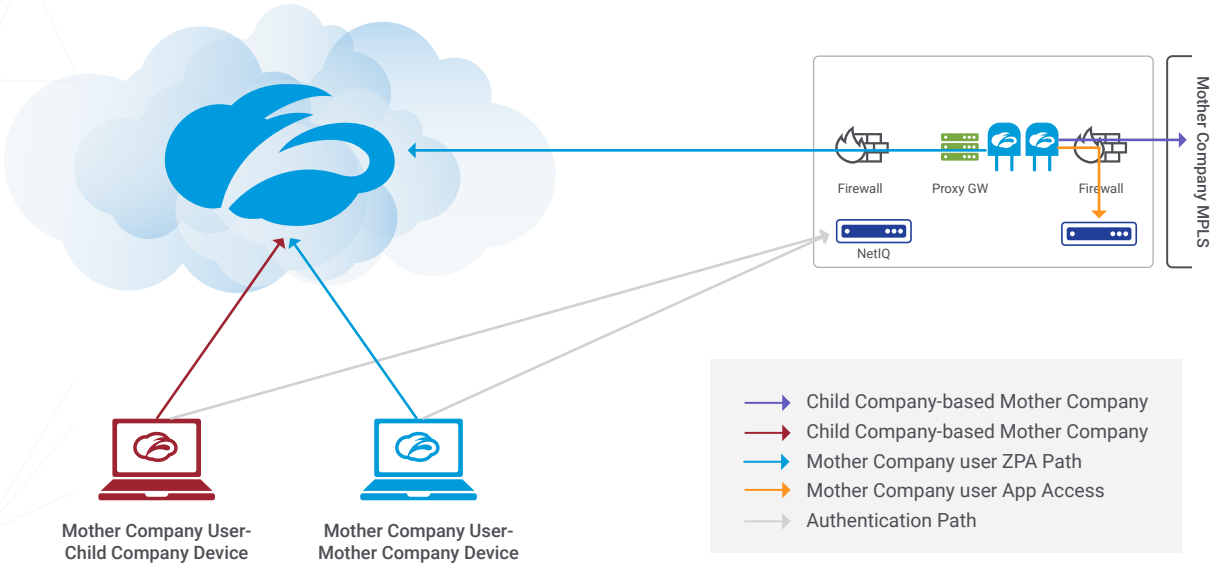
The first stage in this journey should be to establish multiple application connectors within the Mother Company site in Frankfurt, Germany. Mother Company will have failover and load balancing for the Mother Company side of the access path. This pair of connectors will continue to establish the connectivity for the existing Mother Company users, thus providing continuity for the next phase of the testing. The connectors here will establish their connection to the ZPA cloud through the corporate proxy server. This proxy is one of three main internet gateways used by Mother Company, and a specific rule has been established for the connector. All TLS tunnels to Zscaler are passing through a bypass rule (auth and SSL) through the *serverproxy.MotherCompany.net:8080*.



Authentication will continue to leverage the company's SAML identity provider. Once users are authenticated, their private application traffic will be sent via the ZTNA service and connected to applications via the Frankfurt-based connector. Once policy controls are configured to Mother Company standards, more users can be moved from the legacy VPN (Juniper, Pulse, Cisco AnyConnect, etc.) platform over to ZPA.

Phase 2 Address additional M&A users

The second stage in Mother Company's journey with ZTNA should be to enable access for a set of test users utilizing the Child Company devices. These devices will connect to applications running within the Mother Company ecosystem. When complete, this test will demonstrate the successful and secure connectivity between newly acquired users and existing internal applications in the Mother Company ecosystem via the ZTNA service.



Phase 3 Full M&A execution

In this phase, you should look to define granular access to Mother Company users and Mother Company users with Child Company devices to internal applications, so that only specific users are able to connect to specific applications. These granular access definitions will be the first stepping stone to building out a full zero trust security model that can power Mother Company's future IT operations.

Delivering granular access to applications, visibility, and control is fundamental to ZTNA services like ZPA. Plus, its setup is simple and can be divided into three key areas:

01 Application definition and granular policy definition

The criteria for access is based on user attributes that are assigned via the directory services at Mother Company. Aligning these memberships, attributes, and assignments means that the access policy can be used to enforce controls for exactly who is authorized to access Mother Company applications.

Examples of such controls could be:

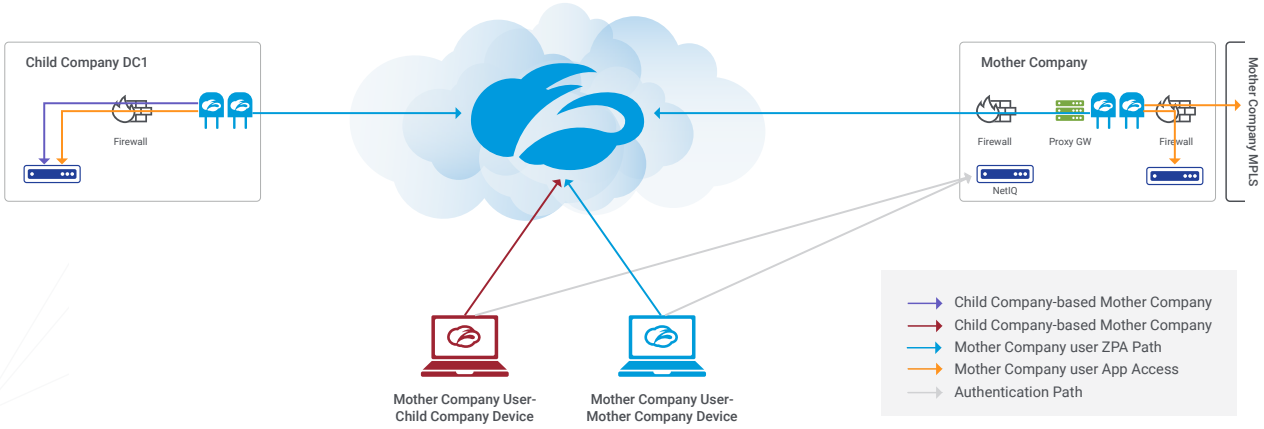
- Defining specific employee access to application segments, where the user identity is the control
- Enabling third parties to access specific applications, in which the controls define both who is accessing and what they are accessing

02 App discovery

Reviewing the applications that have been identified as part of the discovery process means that Mother Company will have the ability to "weed out" specific applications and then assign policies to either block or enable access to these apps. Zscaler recommends sorting discovered applications into categories that allow Mother Company to take actions based on its priorities, such as critical, medium, and low priority.

03 Analyze diagnostics to gain insights

The content of the diagnostics within the ZTNA service will give Mother Company the ability to analyze, review, and understand challenges within the network infrastructure. Focusing on error and policy blocking will allow the Mother Company team to identify misconfigured applications, networks, and even the latency of application access.



In addition to the centralized control of the ZTNA environment, which allows for the definition of who can access what, Mother Company has the ability to isolate and define access at the network level by leveraging firewall or ACL controls within the Mother Company network (the exact design needs to be addressed by the Mother Company security and network teams). The ZTNA service allows Mother Company to build out hyper-secure isolation by enabling a connector to be the sole inbound path to applications.

As the ZPA App Connector can exist anywhere within the Mother Company network and route outbound traffic through the proxy service, Mother Company can decide how granular, at a network level, the connectors are rolled out.

Phase 4 Cloud inclusion

Once the Zscaler service is in production within the main app locations at the Mother Company and the Child Company locations, the ZTNA service will enable access, directly and securely, to the public cloud location. Using Azure as an example, access is accomplished by rolling out the App Connectors within the necessary Microsoft Azure regions or resource groups, depending on the Mother Company architecture. In the case of ZPA, by leveraging its default function, application access will dynamically find the most direct path for the user to the application, thus steering the Azure access traffic via the available connector.

As Mother Company continues to leverage Azure in the future, its network teams can simply deploy more ZPA App Connectors within the relevant Azure regions. Subsequently, the cloud objectives for flexible, seamless, granular application access would then be delivered, now and into the future.

Final thoughts

Adoption of ZTNA will allow Mother Company SE to transition to a model in which client machines are not on the same network as production services. User identity and device context become the controls by which access is granted to applications, rather than network residency. Such controls align with any efforts to segment the services network from the user network.

We hope the guidance outlined within this architectural document has been helpful to you. ZTNA has fundamentally changed the way teams are delivering security, allowing them to accelerate IT integration during M&A from nine to 12 months to just a matter of weeks. We urge you to consider ZTNA during your new M&A transaction.

Zscaler has helped many enterprise architects successfully design and implement ZTNA as a way to redefine how they secure access to their applications when in the midst of an M&A process. The Zscaler ZTNA solution enables architects to simplify activities and deliver standardized security practices across all apps and assets in the process.

To learn more about Zscaler and how it's being used to accelerate mergers and acquisitions as well as the divestiture process, visit zscaler.com/solutions/MA-divestitures.

You can also experience ZPA with a free 7-day test drive by visiting zscaler.com/zpa-interactive

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com