Next Generation Post Merger Integration with Zero IT Footprint

Solution Brief

Utilizing the Zscaler Zero Trust Exchange to rapidly provide cross company access in a secure and reliable fashion, with no business impact, nor physical deployment.

I. Streamlining Mergers and Acquisitions with the Zscaler Zero Trust Exchange

Mergers and acquisitions (M&A) remain a critical growth strategy for many organizations. However, realizing their full potential often requires navigating time-consuming, costly, and complex integration processes. A key challenge lies in providing cross-company access to employees and applications promptly, enabling both entities to focus on value creation from Day 1 of the integration process (sign-and-close).

The Zscaler Zero Trust Exchange (ZTE) revolutionizes M&A integration by eliminating the complexities of physically connecting the IT environments of the acquirer and acquiree. By securely enabling seamless integration, ZTE eliminates the need for traditional network and security infrastructure integration, significantly reducing both one-time and ongoing costs. This innovative cloud-delivered approach ensures secure connectivity between designated resources while preserving user experience—without requiring physical deployments or endpoint modifications.

The Zscaler Zero Trust Exchange empowers organizations to accelerate value creation, maximize synergies, and mitigate risks, enabling a transformative integration experience that prioritizes business outcomes.

II. Expanding Your IT Footprint During M&A Integration

M&A integration demands IT infrastructure deployments at the acquired company's location (i.e., network, security, desktops) in order to enable users to have cross-company access to IT resources. This approach, is fraught with risk and complexities:

- Disruptive to end user productivity
- Talent limitations required prioritization of resources and projects
- Technological compatibilities and complexities often understated
- Varying levels of security, regulatory, and policy compliance requires mitigations/remediations
- Geopolitical and geographical challenges in both supply chain and logistics

These challenges are indicative of why integrations rarely meet the deal thesis, and missing the intended business outcomes of the acquisition:

- Unintended time/cost intensive integration programs
- Blocked or significantly delayed value capture activities and objectives
- Elevated risk to the business by permitting connections between the acquirer and acquiree, permitting malicious behavior, insider threats, unauthorized third-party access and ransomware to spread between both companies

III. Zscaler Next-Gen M&A: Minimizing Your IT Footprint for Integration

To simplify M&A complexities, an M&A Integration Proxy, enables the acquired entity to securely access buyer IT/OT assets via a Zero Trust Exchange, by redirecting edge traffic through an encrypted tunnel. This eliminates the need to deploy technology on the endpoint, while reducing the need for installing additional IT assets (i.e., routers, switches, firewalls) at each of the acquired facilities.

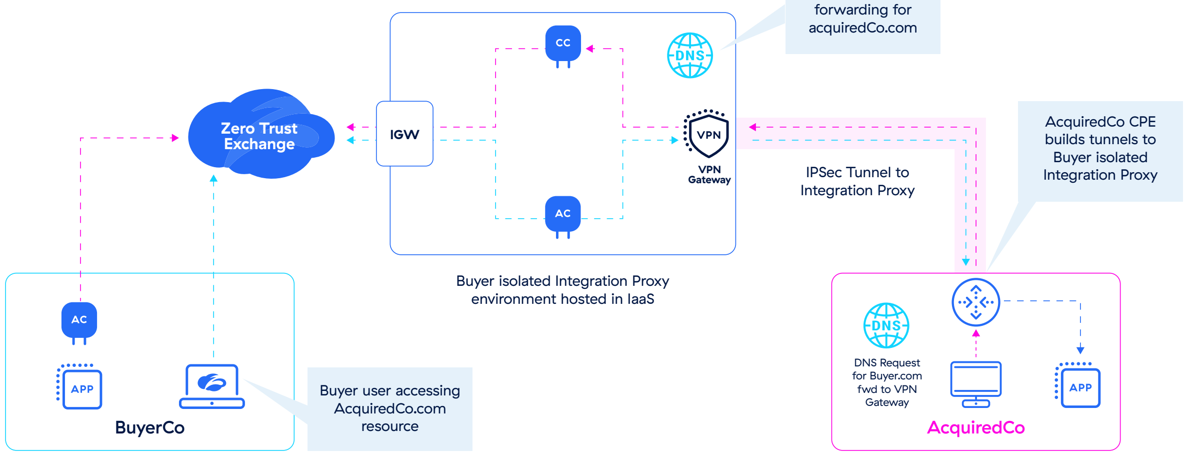
What Is an M&A Integration Proxy?

The Integration Proxy is a secure, isolated environment hosted on the cloud. It utilizes the buyer's Zscaler Cloud Connector and App Connector pairs to broker connectivity between the Buyer's environment and shared applications. Additionally, the Integration Proxy can facilitate connectivity between the Buyer's environment and the Acquired environment, enabling seamless integration and collaboration.

Architectural approach and design:

High Level Integration Proxy Architecture

The Integration Proxy environment is a secure, isolated and separated from BuyerCo's internal systems. It establishes connections to BuyerCo applications exclusively through Zscaler's ZTE (Zero Trust Exchange) technology, ensuring a policy based, secure and controlled interface between the two environments.



Conditional DNS forwarding for acquiredCo.com
CC
DNS
Zero Trust Exchange
IGW
VPN
VPN Gateway
AC
IPSec Tunnel to Integration Proxy
AcquiredCo CPE builds tunnels to Buyer isolated Integration Proxy
Buyer isolated Integration Proxy environment hosted in IaaS
AC
APP
BuyerCo
Buyer user accessing AcquiredCo.com resource
DNS
DNS Request for Buyer.com fwd to VPN Gateway
APP
AcquiredCo

1. Cloud-hosted isolated Integration Proxy (located in a data center, colocation, cloud VPC/VNet) with no direct routes to buyer assets
2. Integration Proxy only has access to Zscaler ZTE
3. Deploy Cloud Connectors and App Connectors, acting as proxies for the Zscaler Zero Trust Exchange
4. Acquired company connects branch locations to the Integration Proxy via IPSec tunnel
5. Route DNS requests for "buyer.com" over the IPSec tunnel

M&A Integration Proxy Overview

The M&A Integration Proxy enables seamless connectivity between companies and buyer applications from day one. Leveraging cloud connectors via Zscaler Zero Trust Exchange, it facilitates effortless integration.

IV. Technical Design Requirements

Prerequisites (Buyer Side)

1. VPC/Vnet
   - Transit Gateway (VPN Termination)
   - Transit Gateway Attachment (Routing to CC)
   - Gateway Load Balancer Service and Endpoint (Load-balancing traffic to Cloud Connector pair)
   - NAT Gateway (Routing traffic to Zscaler Zero Trust Exchange)
   - Cloud Connector Pair
   - App Connector Pair
2. IPSec credentials
3. DNS Conditional forwarders
4. DNS entries (Access to Acquired assets)
5. ZPA App Segments
   - Acquired ecosystem (Wildcard for acquired.com, or specific FQDN)
   - Buyer's shared applications
6. ZPA Policies for only allowing traffic from Acquired ecosystem IP Range.

KEY BENEFITS

Ease of deployment/improved user experience

- No agent required on endpoints
- Minimal IT footprint change in the acquired company's environment (no new hardware required)
- IPSec tunnels established from most on-premises network edge devices

Scalability and speed

- Integration proxy/broker environment can be easily spun up or down based on M&A activity
- Rapid deployment enables acquired end users to reach buyer IT assets, right after sign 'n close

Secure access

- Acquired end users can access shared applications through browser-based access

Finely grained control

- Acquired company can efficiently deploy Zscaler's Client Connector and Cloud Connector solutions, with implementation possible as soon as Day 2, ensuring seamless integration and minimal disruption.

Prerequisites (Acquired Side)

1. Local DNS entries to route Buyer.com traffic to IPSec endpoint (Transit Gateway)
2. Routing DNS traffic via IPSec tunnels to Integration Proxy

System architecture and design

Buyer Side – Integration Proxy
Designed and implemented a secure isolated integration Proxy architecture using Amazon Web Services (AWS).

- Virtual Private Cloud (VPC) with a Transit Gateway to terminate VPN connections from the Acquired ecosystem
- Transit Gateway attachment to route traffic to the Gateway Load Balancer (GWLB), which load-balances traffic towards the Cloud Connector cluster
- Cloud Connector intercepts and routes traffic via NAT Gateway to Zscaler Exchange, seeking the app segment traffic belongs to, thus enabling app segmentation and Zero Trust security
- Established secure connections between the Acquired ecosystem and the buyer's shared assets, utilizing App Connectors and Zero Trust Exchange for outbound connectivity
- App Connector deployed for routing traffic from Buyer ecosystem to traverse over the IPSec tunnel for discovering and accessing acquired assets
- Conditional Forwarding with Route 53 to route acquired.com DNS traffic over the IPSec tunnel
- Transit Gateway attachment routes to forward traffic destined for Acquired.com over IPSec tunnel.

Acquired Side
IPSec connections are built from Acquired Ecosystem towards the Integration Proxy.

- Build IPSec connection from Acquired router/firewall towards Transit Gateway
- Local DNS mapping to forward all buyer.com traffic to Transit Gateway IP
- Supported routing to forward the buyer.com DNS traffic over IPSec tunnel

Data flow and processing

Secure Connectivity between Acquired Ecosystem and Buyer Shared Assets

- **Buyer shared Asset Request:** The Acquired ecosystem asset requests access to app.buyer.com
- **Acquired ecosystem local DNS** resolvers point the resolution to the Transit Gateway over an IPSec tunnel
- **Acquired ecosystem local routing:** Acquired ecosystem local routing sends app.buyer.com traffic over the IPSec tunnel
- **Integration Proxy Transit Gateway Routing:** The Transit Gateway routes traffic to the Gateway Load Balancer (GWLB)
- **GWLB and Cloud Connector:** The GWLB forwards traffic to the Cloud Connector, which reaches out to the Zscaler Zero Trust Exchange (ZTE) via the NAT Gateway
- **Zero Trust Exchange:** The ZTE maps app.buyer.com traffic to the appropriate app segment
- **Buyer's Environment App Connector:** The Buyer's environment App Connector creates an outbound tunnel to the Zscaler ZTE
- **Secure Connection Established:** A secure connection is established between the Acquired ecosystem and the Buyer's shared assets

Secure access between Buyer Ecosystem and Acquired Ecosystem Assets

- **Acquired Ecosystem Request:** A user or workload from the Buyer ecosystem requests access to app.acquired.com
- **User Request (ZCC):** If the request comes from a user with Zscaler Cloud Connector (ZCC), ZCC intercepts the DNS request and establishes an outbound connection to the Zero Trust Exchange (ZTE)
- **Workload Request (DNS/Routing):** If the request comes from a workload, the DNS/ Routing forwards the request to a local Branch Connector or Cloud Connector, which establishes an outbound secure connection to the ZTE
- **App Segment Mapping:** On the ZTE, the app.acquired.com request is mapped to the appropriate app segment
- **Secure Connection Establishment:** The Integration Proxy App Connector creates an outbound tunnel to the ZTE via the NAT Gateway, establishing a secure connection between the Buyer ecosystem and the Acquired ecosystem

V. Streamlining Mergers and Acquisitions with Zscaler's Zero Trust Exchange

Zscalers ZTE M&A integration Proxy solution provides a secure, scalable, and reliable architecture for integrating the Acquired companies employees with the Buyer's IT estate. By leveraging a Cloud Service Providers hosted environment Zscaler Zero Trust Exchange, enables secure access to acquired assets, app segmentation, and zero trust security.

Key benefits of this solution include:

- Secure connectivity between the Acquired ecosystem and the Buyer's shared assets
- Zero trust security model
- Encrypted communication between ecosystems
- Scalable and reliable architecture
- Improved security posture and compliance

By implementing this solution, the Buyer can ensure a secure and clientless integration of the Acquired ecosystem, enabling business growth and success.

Zscaler's Zero Trust Exchange securely enables secure, cross-company collaboration with a zero IT footprint

VI. Appendix

Cloud Connector (AWS)

help.zscaler.com/cloud-branch-connector/deploying-zscaler-cloud-connector-amazon-web-services

App Connector (AWS)

help.zscaler.com/zpa/connector-deployment-guide-amazon-web-services

Glossary of technical terms

ZTE	Zscaler Zero Trust Exchange
ZCC	Zscaler Client Connector
VPN	Virtual Private Network
IPSec	Internet Protocol Security Tunnel
CC	Cloud Connector
FQDN	Fully Qualified Domain Name
DNS	Domain Name System
VPC	Virtual Private Network
GWLB	Gateway Load Balancer
TGW	Transit Gateway
PMI	Post Merger Integration

Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com