netskope

SOLUTION BRIEF

Netskope Private Access for Mergers & Acquisitions

Day-one access to internal resources without the complexity of combining networks

Mergers and Acquisitions is a key strategy that many organizations adopt to gain competitive advantages, acquire new technologies, enter new or adjacent markets, and grow revenues. M&A activities are fast-paced, high-stakes, time-intensive events. For IT, networking, and security teams, M&A presents a unique set of challenges. The need to maintain business continuity must be balanced with protecting highly sensitive information. M&A success is driven by how quickly the integration of the two firms can be completed, so time-to-market is key for gaining synergies and ultimately achieving ROI.

COMPLEXITY, DELAYS, AND SECURITY CONCERNS

One of the greatest pain points for companies going through a merger and acquisition is meshing technology. IT teams are under immense pressure to deliver day-one access, connecting users from both companies to mission-critical internal applications and at the same time ensuring the security of sensitive data. In such high-stakes activities, teams are often working on a tight time frame, and any missteps can cause integration delays, inadvertently expose sensitive information, and result in serious consequences such as negative ROI or missed opportunities.

The traditional methods of connecting two disparate networks often require discovering every potential access path (and closing some of them), standing up a new infrastructure, and getting the network carriers of both firms involved. If the security postures of the two firms are substantially different, upgrading the posture of the less-secure firm can take months, which leaves users in both firms idle. Merging two networks is a costly, time-consuming, and complex process that often results in IP conflict and requires re-numbering of addresses. The firewall rules often cannot offer granular access control, making both networks vulnerable.

Additionally, with the trend towards digital transformation, today's private applications can be hosted in on-premises data centers, private cloud, or public cloud service providers such as AWS, Google Cloud, or Azure. Using legacy VPN technology for remote access requires complex routing, costly backhauling of traffic, and has a negative impact on performance and user experience. If the acquisition results in the exchange of only some assets, then the network segmentation and security policies separating divested assets from others present even more challenges.

EMBRACE ZTNA, SIMPLIFY M&A

M&A doesn't need to be a painful experience for the IT and Infrastructure teams. Successful IT leaders view this as an opportunity to drive business value. Leveraging cloud-delivered Zero Trust Network Access (ZTNA) can help these teams achieve critical objectives and support M&A activities in a timely fashion delivering quicker time-to-value, reduced risk, and revenue growth.

Cloud-delivered Zero Trust Network Access enables organizations to realize business value in M&A activities by providing a simple and efficient way to connect users to private resources. With Zero Trust Network Access, security is further enhanced because:

- Applications remain hidden and are not visible on the public internet
- Access is enabled for named users to a specific application and not the underlying network, thus minimizing the risks of lateral movement
- Implicit trust is replaced based on the user's network location (i.e. an IP address) with explicit, adaptive trust based on user identity, device identity, hygiene, and other context
- Security is independent of the underlying network designs and numbering schemes of both firms and eliminates the need to configure complex, inter-carrier routing
- End-to-end encryption
- Provide consistent user experience for accessing private resources

NETSKOPE PRIVATE ACCESS

Netskope Private Access (NPA) is a cloud-delivered Zero Trust Network Access (ZTNA) solution that is an integral component of the Netskope Security Cloud platform and is delivered through the global Netskope NewEdge network. NPA directly connects users to private applications running in public cloud environments or private data centers, reducing risk and simplifying operations.

NPA enables organizations to connect employees, contractors, and advisors to only the critical resources they need on day-one, without waiting for VPN infrastructure to be set up and eliminating the need for merging networks. The firms can immediately begin combining their businesses.

M&A doesn't need to be a painful experience for the IT and Infrastructure teams. Successful IT leaders view this as an opportunity to drive business value.

NETSKOPE PRIVATE ACCESS BENEFITS

ZERO TRUST NETWORK ACCESS (ZTNA)

ZTNA gives users the access to specific applications, but not the network, eliminating the reliance on cumbersome firewall rules for access controls. Private applications remain hidden and shielded from attacks. NPA combines user and group identity with the security posture of remote devices to provide strict application-level access, greatly reducing the attack surface that is otherwise present with traditional VPNs. By augmenting VPN usage, NPA reduces risks associated with VPN hardware vulnerabilities and protects private applications and other network assets from malicious insiders or compromised accounts.

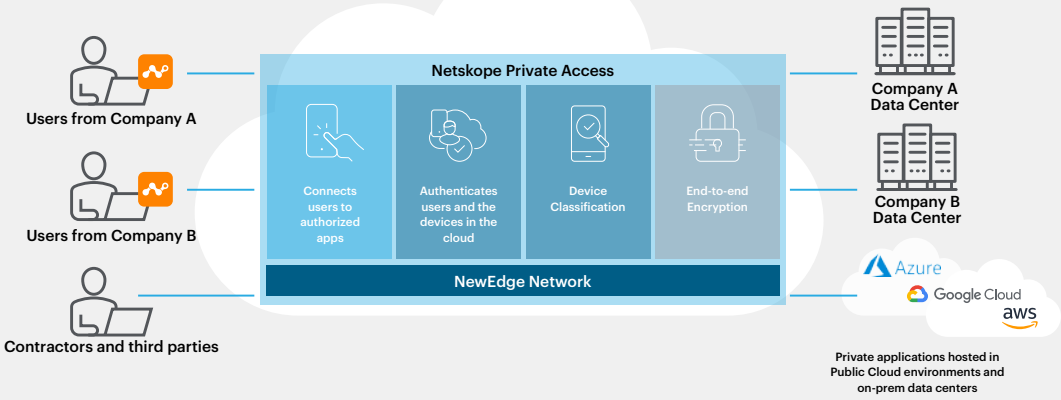

Figure 1: Netskope connects two entities and enables secure access to private resources in data centers and public cloud environments

OPTIMIZED, AND HIGH-PERFORMANCE CONNECTIVITY

NPA connects users directly to applications hosted in public cloud environments and private data centers using Netskope NewEdge Security Private Cloud—a high-performance, highly available, scalable global network infrastructure that is extensively peered with cloud providers. Netskope offers an always-on, end-user remote access experience by avoiding backhauling (or hairpinning) through the corporate network to access applications in public cloud environments. As a result, users gain a consistent experience, regardless of where the resources reside.

Cloud-delivered NPA can be easily deployed without provisioning hardware, providing day-one access, thus eliminating the need to merge networks, and associate pain and complexity such as re-numbering, and overlapping addresses.

REDUCE ATTACK SURFACE AND NETWORK VULNERABILITIES

With the NPA "inside-out" connectivity, there is no need to place services in the demilitarized zone (DMZ). Applications remain hidden and never exposed to the public internet, further reducing the attack surface and avoiding unauthorized access. In turn, Enterprises avoid introducing new network vulnerabilities following an M&A event by eliminating the risk of opening networks to the new organizations with uncertain security standards and granting network access to unknown devices.

BUSINESS AGILITY

Cloud-delivered NPA can be easily deployed without provisioning hardware, providing day-one access, thus eliminating the need to merge networks, and and the associated pain and complexity such as re-numbering, and overlapping addresses. This speeds up integration and time to market.

ENHANCED VISIBILITY AND CONTROL

With Advanced Analytics, and app discovery, IT and security teams get clear visibility on the traffic and access information. Application owners can then decide who gets what level of access. NPA allows IT, security, and lines of business to have shared responsibility and controls.

POSITIVE USER EXPERIENCE

During an M&A event, both organizations want to ensure that all employees have a positive experience and feel valued by the new organization. With Netskope NPA, IT can ensure employees have a seamless access to necessary resources to be productive. With a single steering client, users gain a consistent and superior experience in accessing resources, whether it is SaaS or private applications, without the latency and frustration of a legacy VPN connection.

FLEXIBILITY

With both client-based and clientless options, NPA gives organizations the flexibility to extend secure remote access to employees and third-parties, regardless whether the device is managed or unmanaged.

BEGIN YOUR NETWORK AND SECURITY TRANSFORMATION

The Netskope cloud-native architecture ensures scale, agility, and elasticity and provides a single administrative console for simplified security policies, analytics, and incident investigation for employee use of web, cloud, and private applications. Netskope takes you to the cloud-based future of network security, combining ZTNA with secure web gateway (SWG) and cloud access security broker (CASB), and aligning with the Gartner-defined secure access service edge (SASE) architecture—www.netskope.com/about-sase

Click here for more information about Netskope Private Access.

netskope

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope.

©2021 Netskope, Inc. All rights reserved. Netskope is a registered trademark and Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks are trademarks of their respective owners. 06/21 SB-471-1