appgate

A Return on Investment Analysis of Universal Zero Trust Network Access

This white paper provides an analysis of the difference between direct-routed and cloud-routed architectural approaches, key considerations and the potential direct and indirect return on investment (ROI) for universal Zero Trust Network Access (ZTNA).

ZERO TRUST NETWORK ACCESS **WHITE PAPER**

ROI Analysis of Universal ZTNA

Table of Contents

INTRODUCTION

With remote and hybrid working environments established as the new enterprise model, traditional network security solutions have demonstrated their ineffectiveness in providing secure access to users. This shift is driving escalating demand for Zero Trust Network Access (ZTNA), initially deployed as the modern, highly secure remote access replacement for risk-prone, obsolete VPN technologies. The concept of universal ZTNA expands beyond the primary use case of VPN replacement to offer secure access across complex hybrid IT environments for any user, from any device, whether on-campus or remote, with a unified policy model.

On-campus
UNIVERSAL ZTNA
Remote

Universal ZTNA facilitates the consistent enforcement of Zero Trust security principles to secure access for every identity and to every protected resource irrespective of location. Embracing universal ZTNA presents an opportunity for vendor and tooling consolidation, enabling organizations to balance fiscal responsibility while maintaining a strong security posture. This white paper provides an analysis of the difference between direct-routed and cloud-routed ZTNA architectural approaches, key considerations and the potential direct and indirect return on investment (ROI) when applied only to VPN replacement for remote access or extended universally across all enterprise use cases. The document demonstrates how organizations can unlock business-critical use cases and achieve substantial cost efficiencies at scale through the adoption of a purpose-built universal ZTNA solution.

> **"Universal ZTNA extends existing ZTNA technologies to use cases beyond remote access in order to support local enforcement in on-premises campus and branch locations. ('Universal ZTNA' is a marketing term, as the original definition of ZTNA was not limited to remote access use cases.) Universal ZTNA centralizes device and end-user zero trust access policy to enable a single access policy definition."**
>
> ***– Gartner 2023 Market Guide for ZTNA***

Use Cases Driving Universal ZTNA

- **Full VPN replacement:** Transition from traditional VPNs to ZTNA for all use cases
- **Third-party access:** Ensure external entities can connect without compromising the integrity of the network
- **Transition traffic off MPLS to the internet:** Migrate network traffic from costly MPLS connections to the public internet
- **Eliminate software-defined wide area network (SD-WAN):** Provide secure access to resources without relying on traditional SD-WAN complexities and potential vulnerabilities
- **Network access control (NAC) replacement:** Replace expensive NAC solutions with consistent access control mechanisms for all users, devices, and locations
- **Zero Trust branch connectivity:** Ensure continuous verification and authorization for all users and devices accessing corporate resources from branch locations

Critical Capabilities for Universal ZTNA

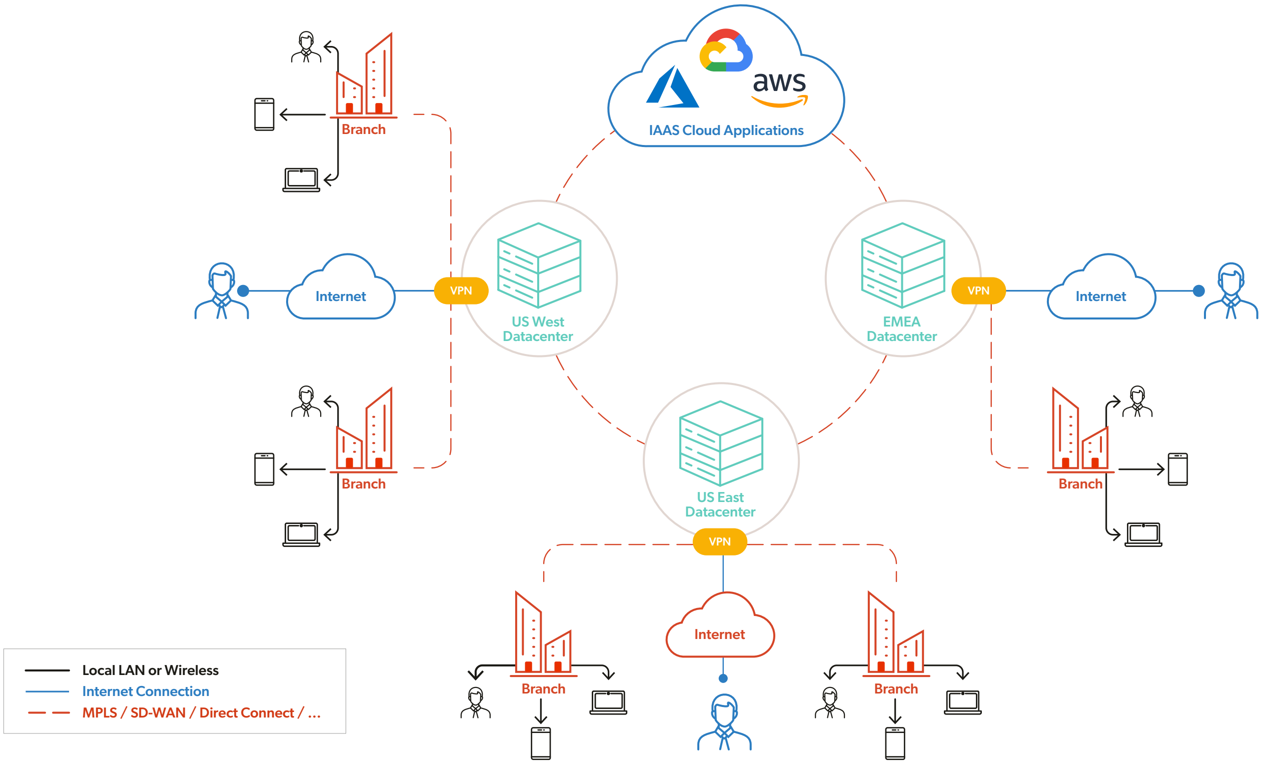
- **Identity-centric security:** Guaranteeing only authorized and authenticated entities can access specified network resources
- **Application layer access control:** Ensuring users have the minimum necessary access required to perform their tasks
- **Dynamic access policies:** Granting access based on the specific context of the user and device
- **Adaptive authentication:** Responding to changes in user behavior or contextual factors to ensure access privileges are appropriate for the current security posture
- **Scalability and high performance:** Extending dynamic scalability to accommodate additional users and devices, while maintaining optimal performance branch locations

ZTNA: VPN REPLACEMENT FOR REMOTE USER ACCESS

Replacing VPN technologies to support remote user access is often an initial use case for ZTNA adoption. Traditional VPN technology extends the enterprise perimeter all the way to a remote device. However, if that device is compromised, an attacker can breach the perimeter, establish persistence, perform reconnaissance, and move laterally throughout the environment to successfully carry out their attack. Many examples of either via a VPN a VPN account or an exploit on the VPN concentrator have proven that VPNs no longer meet modern security standards.

An enterprise perimeter network typically exists out of one or more regional data centers or locations where core applications and security stacks are hosted. That location can be a local server room, a commercial data center or even in the cloud via infrastructure as a service (IaaS). These locations are typically interconnected by secured, dedicated connections (i.e., MPLS, SD-WAN, direct connect and leased fiber) provided by a telecommunications service. These connections are significantly more expensive than traditional internet bandwidth. However, the connection is encrypted, dedicated and invisible to any nefarious characters on the internet.

STANDARD VPN ARCHITECTURE



Recent CVEs Emphasize VPN Vulnerabilities

June 2023: Fortinet confirmed the existence of a critical zero-day vulnerability impacting Fortinet FortiGate SSL VPNs, tracked as CVE-2023-27997 (CVSS: 9.2). Exploitation allowed a remote and unauthenticated threat actor to execute code on vulnerable devices. As the vulnerability was pre-authentication, attacks bypassed multi-factor authentication (MFA).

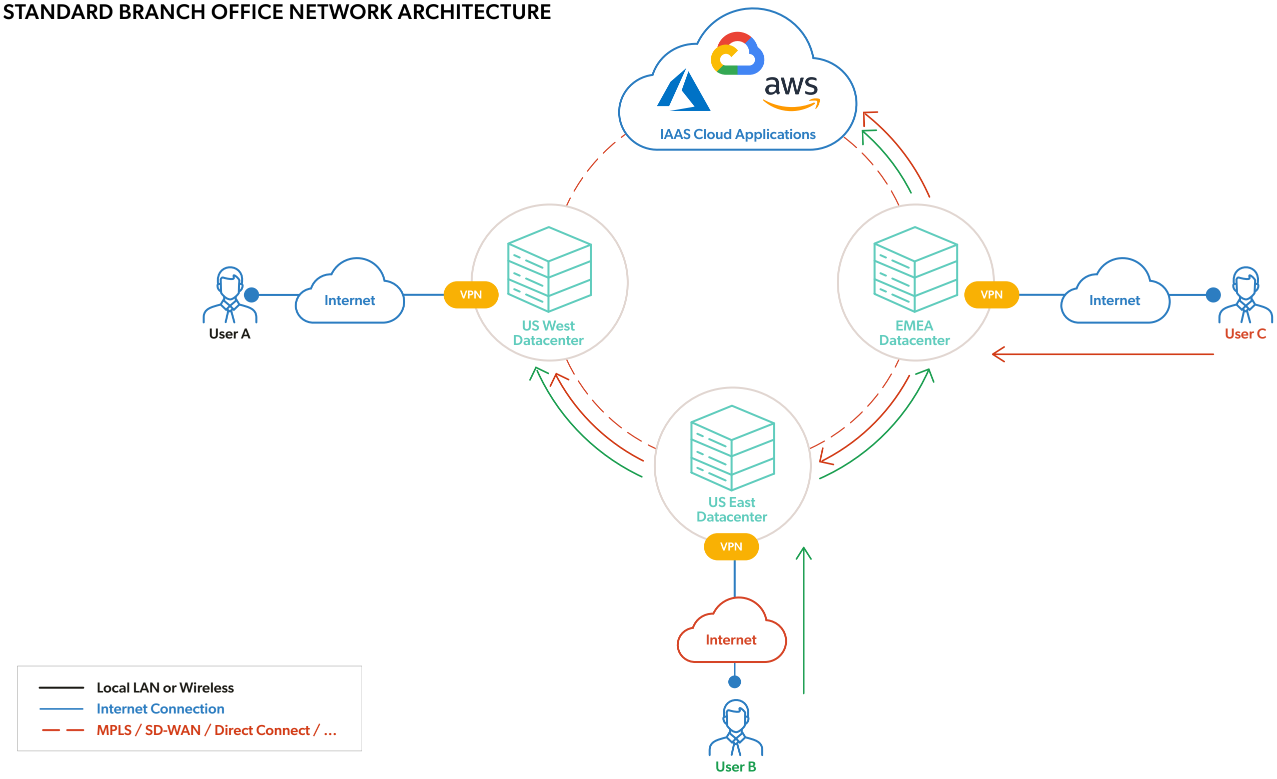
September 2023: Cisco confirmed a zero-day vulnerability in the remote access VPN feature of its Adaptive Security Appliance Software and Firepower Threat Defense Software, tracked as CVE-2023-20269. Exploitation allowed an attacker to identify valid credentials that could then be used to establish an unauthorized remote access VPN session, as well as a clientless SSL VPN session.

January 2024: Ivanti confirmed two zero-day vulnerabilities being exploited in the wild, tracked as CVE-2023-46805 and CVE-2024-21887. The first was an authentication bypass that allowed remote access to restricted materials. The second was a command injection vulnerability that allows authenticated admins to send unique requests and execute arbitrary commands. More CVEs were published in February 2024.

Branch offices or campus networks are typically linked to one or more of the regional data centers or cloud locations using similar dedicated connections. It is common practice for the regional data centers to be the internet ingress and egress points for the enterprise. The VPN concentrators are oftentimes hosted here and typically provide regional access for remote users, and then route the application traffic over the internal network to the different locations if required.

Visualizing the remote user VPN traffic, all traffic from a user enters the enterprise network in one location, typically the regional VPN concentrator. For example, User C connects their VPN to the regional EMEA data center and all VPN traffic arrives in that location. They also might connect to local applications in the US East data center or applications in other regional data centers. In this case, the remote user consumes bandwidth of the different private connections between those data centers. Bandwidth consumed over a private connection is significantly more expensive than internet bandwidth. Moreover, if the user must pass multiple links to reach an application, the associated cost as well as the latency would be even higher.

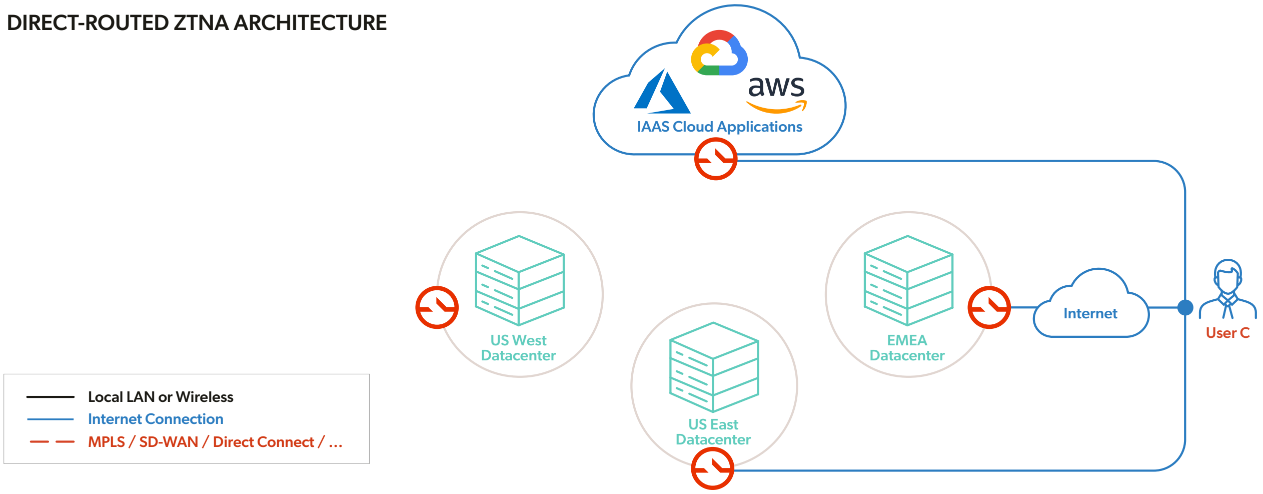
STANDARD BRANCH OFFICE NETWORK ARCHITECTURE



REPLACING VPN WITH DIRECT-ROUTED ZTNA ARCHITECTURE

Let’s take this same example but replace the VPN solution with direct-routed ZTNA. Instead of a single entry point into the enterprise network, we now have a gateway in each location. The user will create a mutual TLS (mTLS) tunnel to each location for which they have application or network entitlements. The gateways are invisible on the internet by using single packet authorization (SPA), which requires the client to send a special packet before the network socket can connect from that client to the gateway. This technique mitigates the risk of distributed denial-of-service (DDoS) and zero-day attacks, which cannot be supported with VPN technologies. User C in this example has established direct mTLS tunnels between the three data centers, leveraging standard internet bandwidth. As shown in the image below, remote User C is completely offloaded from all MPLS/SD-WAN connectivity, of which VPN technologies are not capable.

DIRECT-ROUTED ZTNA ARCHITECTURE



Direct ROI: Replacing VPNs With Direct-Routed ZTNA

Reduced MPLS/SD-WAN connectivity costs:

The amount of MPLS/SD-WAN bandwidth consumed by VPN users depends on where VPN concentrators are located and how distributed applications are on the enterprise network. If the organization is very cloud-centric, but still leveraging an on-premises VPN to connect to cloud environments, there will be immediate savings for all remote users by moving from expensive MPLS/SD-WAN bandwidth to standard internet connectivity. By shifting VPN users over to direct-routed ZTNA for remote access, organizations should generally expect to see a 10% to 20% drop in overall MPLS/SD-WAN connectivity costs.

Reduced hardware costs:

Direct-routed ZTNA replaces VPN concentrators with a pure software solution, making it easier to add more entry points without buying or maintaining additional expensive hardware VPN appliances. In addition, it facilitates automated cloud-scaling, enabling provisioning and deprovisioning of resources in response to fluctuating demand. Moreover, during significant events such as a global pandemic or severe weather impacting specific regions, a sudden shift to remote work for all users can be supported without any disruption. It’s important to consider that hardware-based VPN bundles can range from $4,700~ for 75 users to $300,000~ for 10K users, for example as evidenced by this Cisco pricing structure. For enterprises that are more network-centric with load balancing and redundancy considerations, the capital expenditure for hardware could be even higher with added appliance maintenance costs.

What is Direct-Routed ZTNA?

Direct-routed ZTNA architectures provide a purpose-built and flexible approach to accommodate the unique set of private applications and network infrastructures within an enterprise. This model ensures full control over how data traverses the network; providing secure access to all user-to-resource and resource-to-resource connections from anywhere across hybrid infrastructure located everywhere. A key advantage is the scalability and performance of direct-routed architectures, allowing enterprises to scale their business while maintaining optimal network performance. The pricing model associated with direct-routed ZTNA is transparent, easily comprehensible and devoid of hidden charges, providing enterprises with a predictable and manageable cost structure.

Indirect ROI: Replacing VPNs With Direct-Routed ZTNA

Reduced risk of breaches and preserved business continuity:

With single packet authorization (SPA), standard internet for critical enterprise network traffic can be leveraged. SPA makes edge points invisible, so the potential for DDoS attacks, VPN vulnerability patching and zero-day attacks are eliminated. As reported by SecurityWeek, downtime due to a successful application DDoS attack costs organizations an average of $6,000 per minute. As a result, savings on DDoS management and operational costs and risks can be realized and business continuity maintained with a direct-routed ZTNA solution.

Minimized attack surface:

The fine-grained policies of universal ZTNA ensure users are not granted broad network access, significantly reducing the attack surface, especially if a malicious user or device attempts to connect from a remote location. Additionally, fine-grained policies allow for tailored access privileges based on contextual factors, enhancing an organization’s ability to provide secure access to users while preventing unauthorized access attempts from malicious actors.

Increased productivity:

Universal ZTNA streamlines the process for authorized users to access necessary resources, enabling business owners to expedite the deployment of applications into production. It also allows IT security teams to provide third-party entities with precise access to critical systems, such as HVAC systems or manufacturing robots, effectively reducing the risk of third-party attacks. The ROI is reflected in the improved productivity and efficiency of employees or contractors who need secure access to company resources.

Simplified compliance:

Direct-routed ZTNA can help organizations comply with various regulations and standards and provides identity-based policies, which are easier to audit when compared to traditional network firewall rules and logs. ROI can be measured through the automation of data collection and reporting, which often requires a manual approach with traditional secure access solutions. ZTNA can aid in reducing compliance reporting scope and avoid non-compliance with industry regulations.

Proven ROI of Appgate SDP for Transitioning Traffic off MPLS to the Internet:

A Fortune 500 global IT services provider implemented universal ZTNA across its 130,000 user base. The adoption of a direct-routed architecture enabled every user to establish individual encrypted internet tunnels connecting to the organization’s six primary data centers, replacing previously utilized shared private MPLS connectivity. Prior to this, 10 Gbit MPLS connectivity was required as interconnection between six main data centers worldwide. The company removed MPLS from over 600 sites, reducing overall connectivity costs by 67%, enabling them to contract lower bandwidth commitments. This resulted in annual savings in the tens of millions, 10x what the company pays annually for the universal ZTNA solution.

The Proven ROI of Appgate SDP or Zero Trust Branch Connectivity:

A global food and health company embraced universal ZTNA to provide secure access for all users within its expansive network. Once in place, users inside branch offices could operate from the guest Wifi network, enabling the company to remove most traditional network security equipment. The company saved $750,000 in equipment renewal costs for their 14 branch offices globally. This streamlined their operational expenses and eliminated the need to maintain and update disparate security solutions at each location. The implementation of universal ZTNA ensured a consistent and uniform user experience for employees, regardless of whether they worked on campus or remotely.

REPLACING VPN WITH CLOUD-ROUTED ZTNA ARCHITECTURE

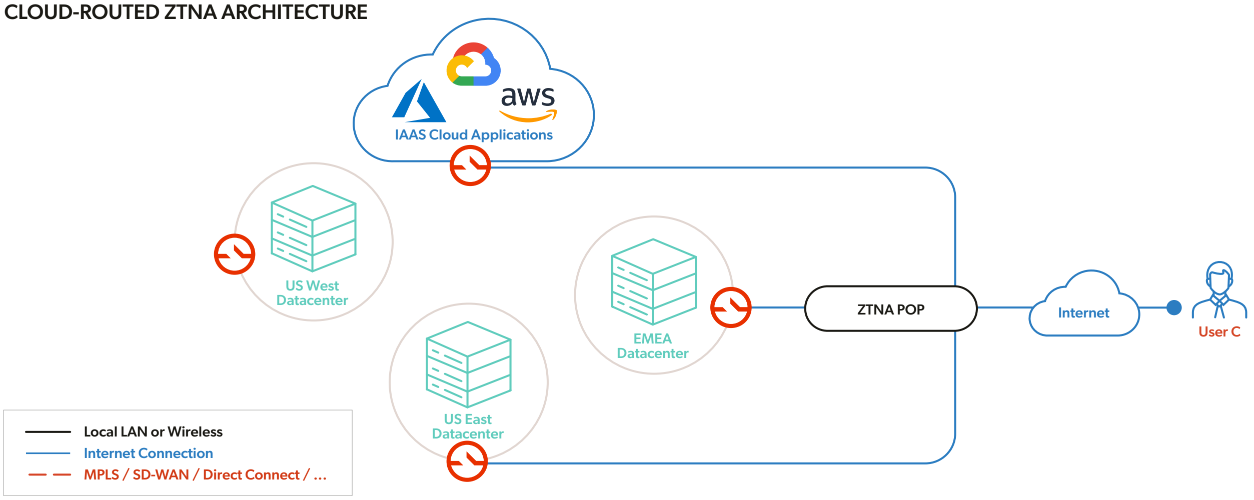
When replacing VPN technologies with a cloud-routed ZTNA architecture, similar cost savings and benefits as the direct-routed architecture apply. However, this architecture features twice the internet bandwidth cost and additional latency because connectivity is required between the user and the closest ZTNA point of presence (POP) and between the POP and the regional data centers. The connection between the cloud-routed ZTNA POP and each data center is typically a shared encrypted connection that significantly impacts the system's overall performance. Traffic enforcement occurs in the cloud and utilizes a shared open tunnel within the organization's data centers. If the cloud becomes compromised, there is an open back door to all of the organization's critical sites.

Additionally, cloud-routed ZTNA architectures often have limitations in supporting all protocols or handling downward-initiated traffic, which is critical to address Voice Over Internet Protocol (VoIP) use cases and IT operational toolsets that require device patching, management and support. This limitation can potentially force customers into challenging post-purchase decision-making to determine what can be included and what will not work with the acquired cloud-routed ZTNA solution. The organization then must bifurcate their applications into those protected by cloud-routed ZTNA solutions and those that are not, leaving them vulnerable to compromise.

What is Cloud-Routed ZTNA?

Cloud-routed ZTNA architectures, commonly referred to as identity-aware proxies (IAPs), are common in the market due to their quick development and speed to market. In this model, data traffic is funneled through multi-tenant cloud environments. These architectures can have many drawbacks, including limited network protocol support, on-premises resource constraints, latency and hairpinning limitations, as well as an inability to scale efficiently. Moreover, there's an implicit trust placed in the security, availability and scalability of the vendor's multi-tenant cloud. Enterprises seeking comprehensive control and predictability often find direct-routed ZTNA solutions to be more advantageous.

CLOUD-ROUTED ZTNA ARCHITECTURE



UNIVERSAL ZTNA: SECURE ACCESS FOR ALL USERS

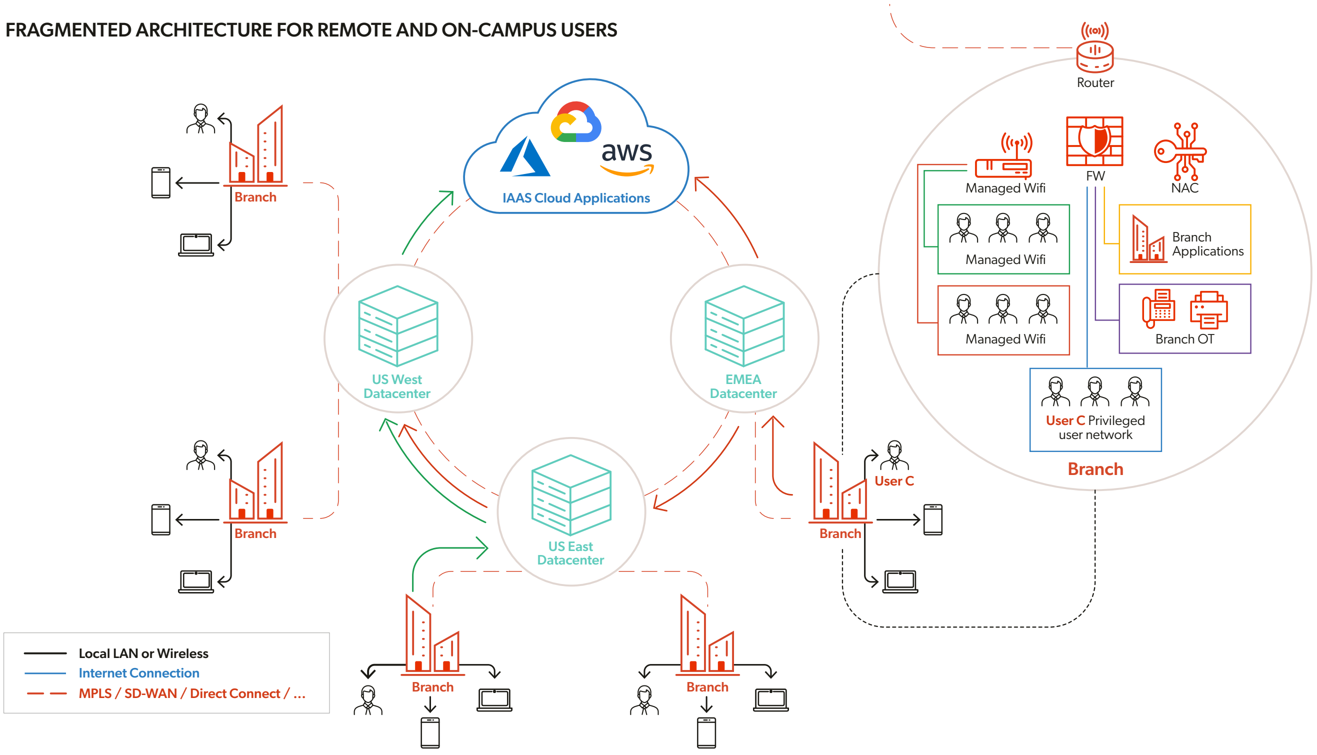
When ZTNA is limited to replacing VPNs to enable access for remote users, the IT admin team is often forced to manage security rules separately for remote and on-campus users. This fragmentation in security protocols can lead to increased complexity and potential vulnerabilities within network infrastructure. Shifting to universal ZTNA eliminates the distinction between remote and on-campus users, ensuring consistent security protocols and guaranteeing uniform latency and performance for all users. Let's review an example of why this adds complexity, and then highlight both direct-routed and cloud-routed architectures.

Take User C, which in this case is a privileged user (IT admin/operations) that needs to work from a branch office in EMEA using their desktop. Due to their status as a privileged user, they require broad access to numerous sensitive systems and applications. To protect privileged users from the rest of the office users, they are often placed in a privileged user network. To achieve this, the enterprise requires a network access control (NAC) solution, a wireless management system and special ethernet switches to identify the device of a privileged user.

This segment has access to critical systems in the entire enterprise network. As a result, they are isolated from standard users and from guest employees (i.e., contractors and third-party vendors) whose access typically is restricted to just internet connectivity. Advanced, complex firewall rules are put in place in all branches and typically pushed from a central firewall management system. Each new user segment added in an office to distinguish user groups creates exponential work on firewall firewall rules, the NAC solution and the wireless management systems. Therefore, segregating users and devices typically comes down to four to six different segments, making enterprise network segmentation very coarse grained.

> **"Enterprises spend billions to secure campus networks via a combination of switching features and NAC—an approach ripe for disruption with the shift to hybrid work. Product leaders should extend ZTNA products to campus environments to drive revenue and enterprise value, but they need to act fast.**
>
> ***— Gartner Campus Network Security and NAC are Ripe for Market Disruption***

FRAGMENTED ARCHITECTURE FOR REMOTE AND ON-CAMPUS USERS



When User C connects from their branch office to all the different applications in US West, US East, EMEA and the enterprise IaaS cloud environment, they are using MPLS/SD-WAN bandwidth on each of these links. All that bandwidth for private applications and internet browsing traffic is also consumed over the branch office private connection to the closest enterprise data center.

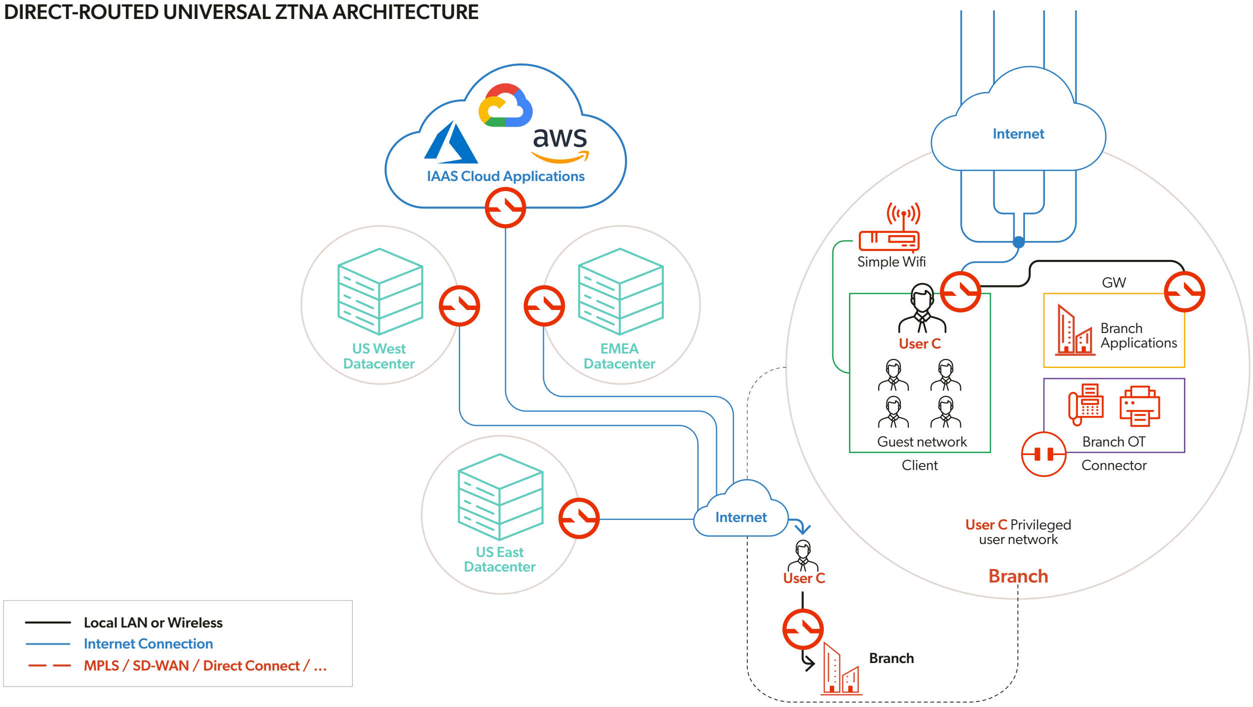
In addition, enterprise networking and security becomes significantly complex in the event of a merger or acquisition. New MPLS/SD-WAN connections would be required and overlapping subnets must be handled to extend the enterprise routing table. In most every case, the core firewall and branch security equipment are different solutions, making it challenging to integrate or costly to replace by enterprise standards.

UNIVERSAL ZTNA WITH A DIRECT-ROUTED ARCHITECTURE

Let's now review the universal ZTNA approach. This approach will apply to all remote and on-campus users who connect to enterprise applications through ZTNA connectivity. This use case can then be expanded to IoT devices, servers, or devices where a ZTNA client could not be installed.

It is crucial to select a solution that offers comprehensive universal ZTNA functionality, coupled with direct-routed architecture. Typically, the protocols and number of supported devices are much more complex when attempting to address all enterprise use cases, not just remote user access. Therefore, it is key to keep these potential hurdles in mind when selecting a ZTNA solution to protect all user-to-resource and resource-to-resource connections. Since ZTNA is a software solution that works as a secure, individual network overlay, there is an ability to migrate user-by-user and branch office-by-branch office making it relatively easy and non-disruptive to implement for most enterprises. The only requirement is to remove or diminish the remaining dedicated interconnections and eliminate certain branch security tools once all users or the entire office has completed the migration.

DIRECT-ROUTED UNIVERSAL ZTNA ARCHITECTURE



Direct ROI: Universal Direct-Routed ZTNA

Cost reduction and unlocked use cases:

Once fully deployed, user traffic no longer travels over the MPLS/SD-WAN connections between the data center and branch offices (via private links). Instead, all user traffic from branch offices to the nearest data center will use regular internet connections. In addition, if IoT devices or local servers in the office are protected by universal ZTNA, the entire connection can be replaced by a simple internet connection that is significantly more cost efficient.

As previously noted, VPN concentrators are replaced with a pure software solution making it easier to add more entry points without buying or maintaining additional expensive hardware VPN appliances. In addition, it facilitates automated cloud-scaling, enabling the provisioning and deprovisioning of resources in response to fluctuating demand. Moreover, during disruptive geopolitical conflicts, epidemics or natural disasters impacting specific regions, a sudden shift to remote work for all users can now be supported without any disruption.

Additionally, branch office security tool costs are significantly reduced. Taking all users into account, they can all work from a café-style wireless (or wired) internet guest network. Only internet access is required, and the branch office network does not have access to enterprise applications. When the user utilizes their device, the ZTNA client will connect to all locations they have entitlements for, which could even be a local area network (LAN) connection inside the branch office to use local applications (i.e., local printer or VoIP server). When the user connects, their local device can be ringfenced to prevent other users from seeing the device on the local network. This removes the need for different user network segmentation, NAC solutions, complex managed wireless settings and the complex firewall rules required to guarantee appropriate user access.

With mergers or acquisitions, additional gateways for new data centers or cloud locations are the only requirement. Onboarding new users utilizing an existing identity and access management (IAM) solution is accomplished by deploying ZTNA client software to those respective users. Direct-routed solutions do not require a central enterprise routing table as every user's network is built to specifications dictated by the policy engine, thereby eliminating any issues with overlapping IP subnets. This streamlines merger and acquisition integration, allowing for the first users to connect to the acquired company within hours or days, rather than months or quarters.

Expanding use cases to encompass IoT or other devices using connectors also leads to cost savings and security benefits, enhanced operational efficiency and more comprehensive network management. By integrating IoT devices into the ZTNA framework, organizations can extend robust security and access control measures to a broader range of connected devices. This integration allows for centralized policy enforcement, simplified access management, and consistent security protocols across diverse device types, reducing the complexity of managing security for many endpoints.

Proven ROI of Appgate SDP for NAC Replacement:

A managed hosting solutions provider, evolving beyond basic hosting, embraced universal ZTNA for comprehensive control over network communications and access points. The implementation resulted in a notable 98% reduction in user provisioning and access modification times. Formerly taking three days, cloud user provisioning now requires only 10 minutes and hour-long account modifications are completed in 30 seconds. With ZTNA adoption, the organization shifted 30% of its systems to better align with the principles of Zero Trust. The organization improved network and system access while concurrently enhancing visibility into network access events, resulting in a significant decrease in security incidents. Future plans involve phasing out a standalone NAC that protects 60% of their endpoints, reducing that number to zero.

Indirect ROI: Universal Direct-Routed ZTNA

Reduced risk of breaches:

With SPA, standard internet for critical enterprise network traffic can be leveraged. As the edge points are invisible, the potential for DDoS, VPN vulnerability patching and zero-day attacks are eliminated. As reported by SecurityWeek, downtime due to a successful application DDoS attack costs organizations an average of $6,000 per minute. As a result, savings on both DDoS management and operational costs and risks can be realized and business continuity can be maintained.

Implementing fine-grained policies ensures that users are not granted broad network access, significantly reducing the attack vector especially if a malicious user or device attempts to connect from a remote location. Additionally, fine-grained policies allow for tailored access privileges based on contextual factors, enhancing the organization's ability to provide secure access to users while preventing unauthorized access attempts from malicious actors.

Increased productivity:

Universal ZTNA streamlines the process for authorized users to access necessary resources, enabling business owners to expedite the deployment of applications into production. It also allows IT security teams to provide third-party entities with precise access to critical systems, such as HVAC systems or manufacturing robots, effectively reducing the risk of third-party attacks. The ROI is reflected in the improved productivity and efficiency of employees or contractors who need secure access to company resources.

Simplified compliance:

Universal direct-routed ZTNA can help organizations comply with various regulations and standards and provides identity-based policies that are easier to audit when compared to traditional network firewall rules and logs. The ROI can be measured through the automation of data collection and reporting, which often requires a manual approach with traditional access security approaches. ZTNA can aid in reducing the scope of reporting compliance and avoid non-compliance with a variety of industry regulations.

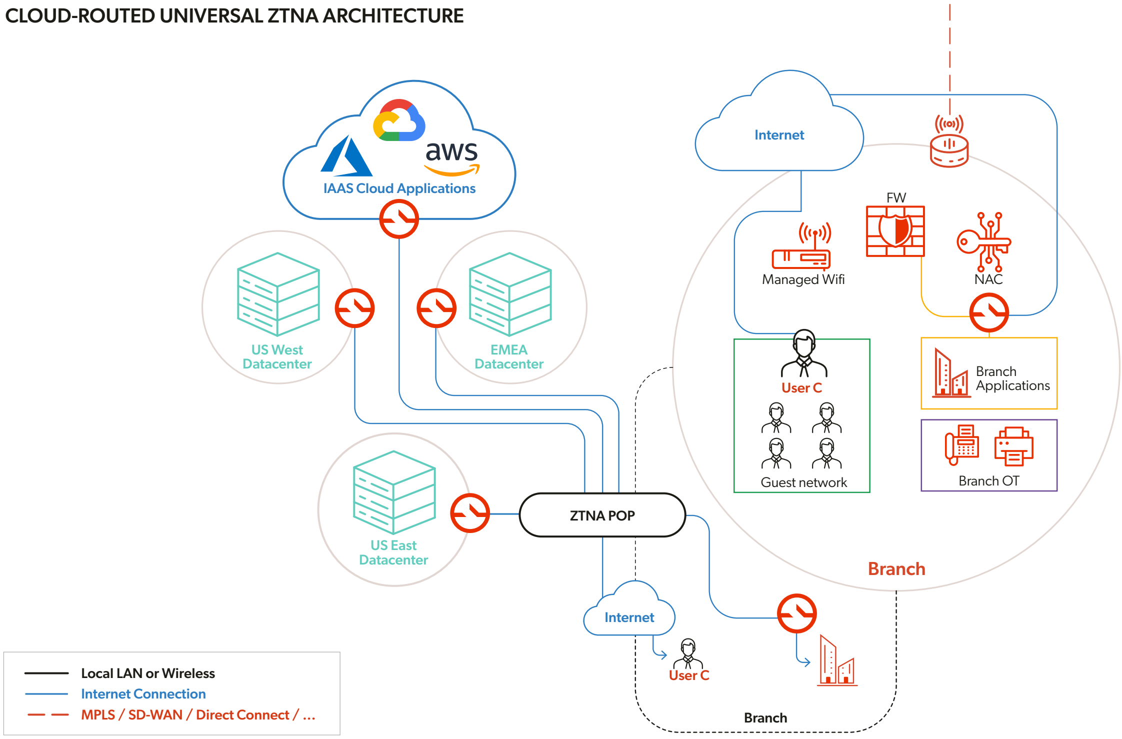
UNIVERSAL ZTNA WITH CLOUD-ROUTED ARCHITECTURE

Deploying a cloud-routed ZTNA solution can introduce several challenges that negatively impact ROI. These architectures present numerous protocol restrictions, many of which do not support downstream traffic or fail to offer clientless options that accommodate IoT scenarios. Because of this, local branch security tools cannot be replaced. Furthermore, cloud-routed ZTNA solutions often cater exclusively to web-based applications, excluding non-web local branch resources like file servers, printers and VoIP systems.

This limitation requires all traffic to be redirected to the cloud and back to the local branch, leading to increased latency and a doubling of internet bandwidth costs, which increases operational expenses.

Moreover, the shared connection from the cloud-routed ZTNA POP to the branch is used collectively by all users and devices, resulting in substantial performance degradation. While some vendors offer a local POP to mitigate this issue, they require extra computing resources and incur high licensing fees for each branch, further impacting ROI. In a cloud-routed ZTNA model, traffic enforcement is managed in the cloud, posing an additional risk. If a ZTNA POP is compromised, it could serve as a gateway for attackers to infiltrate the network.

CLOUD-ROUTED UNIVERSAL ZTNA ARCHITECTURE



CONCLUSION

The adoption of universal ZTNA enables enterprises to attain substantial ROI and become more operationally efficient, especially with direct-routed architectures. Consolidating Zero Trust access policies for all users and devices provides a unified, consistent access policy definition across the enterprise. This approach ensures a more secure and consistent user experience for employees regardless of their work location, while enabling security teams to streamline deployment and management of access controls and policies across the full network. Through careful planning and partnering with the appropriate vendor, the adoption of universal ZTNA offers a cost-effective approach to bolstering security across the most complex enterprise networks.

About Appgate

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises and hybrid environments. Appgate helps organizations and government agencies worldwide start where they are, accelerate their Zero Trust journey and plan for their future. Learn more at appgate.com.