bsi.

The evolution of secure remote access

A unique alternative to traditional VPN in the cloud

01
Executive summary

Several high-profile breaches in recent years have been the result of attackers gaining access via a third party. By providing contractors, partners and third parties with Virtual Private Network (VPN) access, the potential for lateral movement by attackers and malware propagation across the corporate network is greatly increased as the credentials given to these users can be compromised or their devices can be carrying malware.

Zscaler's Private Access (ZPA) renders the corporate network invisible to these users, other than the subset of applications they specifically require. In doing so, organizations can limit the damage that can be done by attackers in the event of an incident.

This whitepaper looks at the difficulties encountered by organizations as they embrace cloud technologies and greater enterprise mobility while relying on traditional VPN infrastructure, and how BSI's cloud security partner Zscaler can help to address these difficulties and facilitate a new approach to remote access.

Most organizations have now adopted cloud services in some form with "Digital Transformation" listed as a key business objective for many organizations. Whether it is migration to Software as a Service (SaaS) solutions or moving on-premise applications to public cloud infrastructure, organizations are developing cloud strategies in order to take advantage of the benefits that cloud solutions can bring. These cloud applications, and the applications that remain on-premise and in private data centres, are being accessed by an increasing number of remote users as enterprise mobility continues to grow and become a reality for organizations. Because of this, some of the advantages organizations hope to gain from their cloud migration, such as an improved user experience, reduction in capital expenditure on hardware and upgrades, greater user productivity and improved scalability and reliability, are not always fully realized due to the limitations of traditional VPN technology.

We will now explore some of the limitations that VPN solutions can impose on organizations, how these can be addressed through Zscaler's Private Access (ZPA) offering and the additional security and operational benefits that ZPA can provide.

02
Potential vulnerabilities of VPN solutions

User experience and latency

The experience of using a SaaS application is a positive one for users. The user experience and latency are generally consistent regardless of the user's location or device which allows for greater user productivity. This is not generally true of internal applications that have been moved to public cloud infrastructure. While on-premise users will consume these applications as an extension of the corporate network, access for remote users will rely on the same backhauling of network traffic via VPN that was required when these applications were hosted on-premise.

This can create a negative user experience as users have to log on to a VPN client and experience the latency of routing through multiple on-premise point appliances in order to access an application that is hosted in the cloud. This problem is emphasized when users are travelling and find their traffic routed back to a VPN gateway across countries or continents. In addition, while users are more and more frequently working from approved mobile devices, a lack of cross platform support in VPN clients can become a limiting factor for enterprise mobility.

Appliance requirements

Depending on the size of an organization, VPN gateways can require multiple appliances to handle scalability, security and availability. Load balancers, Distributed Denial of Service (DDoS) protection, Intrusion Detection/Prevention Systems (IDS/IPS) and firewalls are all part of the appliance stack that will need to scale, be maintained and routinely upgraded in order to continue providing secure remote access to users. This is true for internal applications hosted both on-premise and in public cloud infrastructure as previously outlined. The cost and workload involved in procuring, deploying and maintaining this appliance stack is not trivial, while one of the primary reasons behind adopting public cloud infrastructure is to avoid this type of capital expenditure and appliance management.

Use case 1

VPN retirement

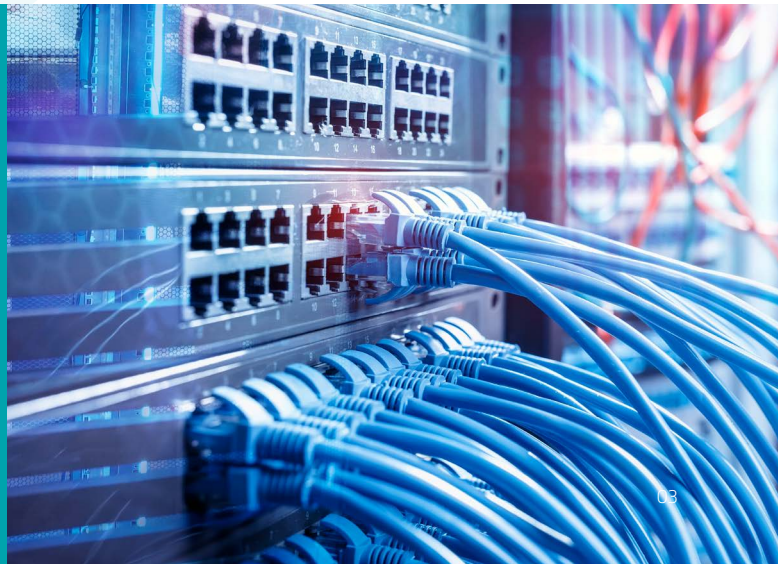
Most obviously, if a VPN refresh project is a present consideration for an organization, ZPA is an option to be considered. As an ever-increasing number of organizations begin to adopt cloud services as key assets, ZPA can ensure that the benefits of those services are not unnecessarily limited. As a replacement for a VPN solution, ZPA can facilitate a modern approach to remote access and allow remote users and branch offices to connect to applications securely over the internet. This is a positive change in approach that can benefit both users and administrators by enhancing experience and security while reducing complexity and cost.

Increased attack surface

By design, VPN's extend an organization's network to a remote user. This exposes the network and any available internal applications to potential compromise from malicious user behaviour or from malware being carried by user devices. In turn, this increases the requirements on the security appliances previously discussed and the administrators tasked with maintaining them. Whether users are connecting via a trusted, corporate device or an untrusted personal device, the attack surface and risk of a breach are greatly increased by extending the network to the user.

Occasionally, third parties and contractors can have a requirement to access an organization's internal applications. When this access is provided through a VPN, the access being given is to a network segment rather than the specifically required application. This does not conform to the principle of least privilege and opens up the possibility of unauthorized network discovery through lateral movement or network scanning tools.

Depending on the size of an organization, VPN gateways can require multiple appliances to handle scalability, security and availability.



03

A new approach to remote access

ZPA is a software-defined perimeter solution that enables a new approach to remote access. ZPA has been built around four key security tenets with the intention of addressing the limitations and risks of the VPN and allowing organizations to connect users to applications securely over the internet.

Connect users to applications without extending the corporate network

VPN's extend the corporate network to remote users by design. This increases the attack surface area and likelihood of a breach. By connecting users to applications rather than networks, the opportunity for attackers to propagate malware and probe for vulnerabilities is greatly reduced.

Do not expose applications to unauthorized users

While users should be connected directly with internal applications, they should only be connected with the internal applications they need to do their job. All other applications hosted within a data centre or public cloud should be invisible to that user. By making applications and internal IP addresses undiscoverable unless access is explicitly granted, organizations can mitigate security threats such as DoS and remove the risk of unauthorized network scanning and mapping.

Segment access to applications without segmenting the corporate network

Users should be given direct access to only the internal applications that they require. The Software-Defined Perimeter approach to doing this is to control access to applications based on policies rather than segment the network on which the applications are hosted. This simplifies the deployment and management of applications on the corporate network.

Provide remote access over the internet without requiring dedicated appliances

In providing the remote access described organizations can utilize local internet breakouts rather than hardware appliances. This will help organizations take full advantage of cloud technologies and enterprise mobility. By providing secure remote access to users over the internet, users can access their internal applications in the same way they interact with SaaS applications and avoid the latency and complication associated with backhauling through the network and hardware appliances.

If a user, third party or contractor can be given access to internal applications directly and in compliance with these four tenets, the principle of least privilege can be more truly applied to that access while providing users with a greatly enhanced user experience.

ZPA is a software-defined perimeter solution that enables a new approach to remote access.

04

ZPA benefits versus traditional VPN solutions

Improved user experience

Remote user access is provided directly to applications over the internet by deploying the Zscaler App (Z-APP) to the user's devices. Once deployed, the Z-APP will create encrypted micro-tunnels over Zscaler's cloud platform directly between the user and the application they are accessing. These tunnels are created dynamically as the user attempts to access the application.

For internal applications hosted in public cloud infrastructure, this removes the step of backhauling traffic to the corporate network and allows users to access the application directly with reduced latency. For internal applications hosted on-premise or in private datacentres, users can access these directly as they would a SaaS application without actively logging in to a VPN client. This is possible because the Z-APP is always active and only creates tunnelled connections to applications as the user requests them.

Additionally, the Z-APP is available for Windows, MacOS, iOS and Android meaning users have a consistent user experience across devices and locations.

Increased and simplified security

When a user attempts to access an internal application remotely, the Z-APP will only be able to connect that user if a policy is in place to allow that access. If no policy has been created, then no micro-tunnel will be created, and the application will not be visible to the user. The reason for this is that when using ZPA, internal applications will only respond to access requests from Zscaler and will never listen for other inbound connections. This removes the risk of denial of service attacks and other unsolicited inbound access attempts as ZPA's Software-Defined Perimeter becomes the only route to accessing that application remotely.

When a policy is in place and access is granted to the user, the IP addresses of both the user and application will be Zscaler IP addresses associated with the linking tunnel rather than network addresses. In this way, the application the user is connected to is isolated from the rest of the network and the other internal applications on that network. This removes the possibility of lateral movement to other applications and reduces the chance of malware propagating across the network from user devices as each application the user is granted access to is provided via a dedicated and isolated tunnel.

The ZPA access policies mentioned above allow for granular access controls to be put in place via the ZPA web interface. These policies allow for application access to be managed based on Security Assertion Mark-up Language (SAML) attributes such as username, email address, Active Directory (AD) group membership or AD department membership. In addition, ZPA allows for device policies to be created that can allow or deny access to specific user devices. This enables rules to be created that can, for example, prevent access from mobile devices to specific applications, if required.

Removal of appliance costs and maintenance

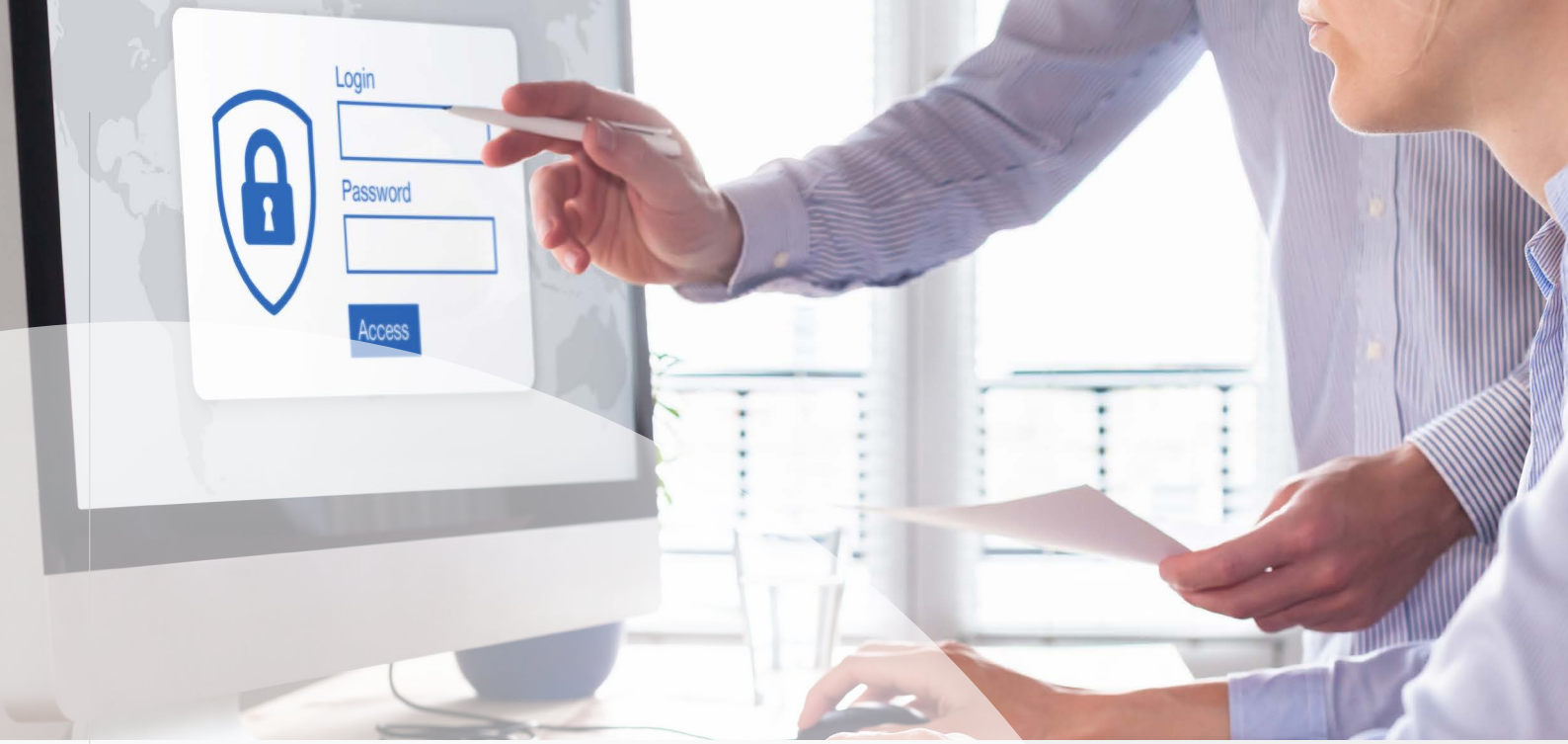
When using ZPA, internal applications will only respond to access requests from Zscaler and will never listen for other inbound connections. This removes the risk of denial of service and other unsolicited inbound access attempts and also removes the need for the security appliances deployed to address those risks. By removing the requirement for DDoS protection, reducing reliance on IDS/IPS and reducing the complexity of firewall rules needed, organizations can recover the costs of procuring and upgrading those appliances and recover time from the administrator effort used in maintaining and monitoring those appliances.

Use case 2

Integration projects following mergers and acquisitions

Mergers and acquisitions present issues to organizations as IP conflicts and network convergence projects can delay internal applications and resources being made available to the acquired company's users. Using ZPA, organizations can provide access to those applications and resources immediately by deploying the Z-APP to all new users' devices and creating access policies to allow the appropriate level of access.

When a user attempts to access an internal application remotely, the Z-APP will only be able to connect that user if a policy is in place to allow that access.



Similarly, as ZPA users can access applications directly over the internet and no longer backhaul traffic to the corporate network, organizations can also remove the VPN gateway appliances, Remote Access Servers and load balancers previously required by VPN solutions. Remote access becomes a cloud service provided by Zscaler in the same way that public cloud infrastructure such as Azure and AWS is provided by Microsoft and Amazon. The availability, scalability and maintenance of the service becomes the responsibility of the cloud service provider.

By taking remote access to the internet and off the corporate network, there is also an opportunity to save costs in bandwidth use. Users accessing applications without backhauling will reduce bandwidth consumption and potentially allow for improved network performance and lower MPLS costs depending on the volume of traffic previously associated with remote user and branch office access.

Greater visibility of applications and user activity

With all remote access being governed and facilitated by ZPA, user access logs can be centralized and provided to administrators in real-time. This greatly assists with the troubleshooting of user access issues, incident management and performance management as the metrics collected from these logs can help organizations to better understand their users' application utilization.

Internal application connectivity to Zscaler is made possible by deploying a Z-Connector virtual machine in front of applications. Once a Z-Connector is provisioned on a network, ZPA has the ability to carry out a wildcard search for any available applications. This allows ZPA to provide the application discovery functionality of a Cloud Access Security Broker (CASB) for internal applications by providing organizations with a list of all applications reachable from the point the Z-Connector was deployed.

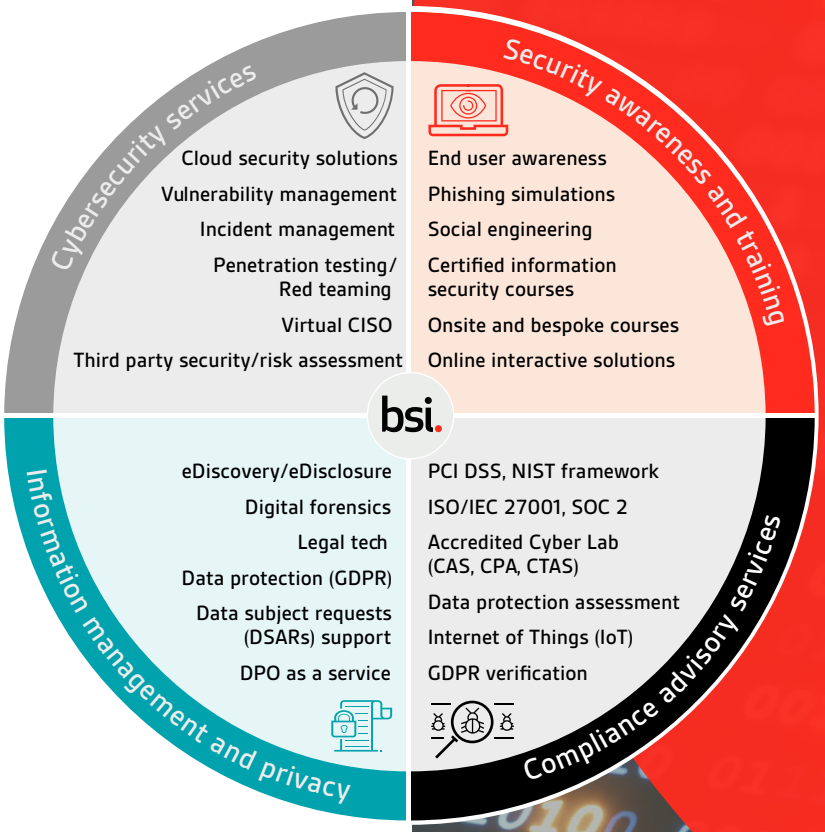
05 Conclusion

A software-defined perimeter approach to remote access using ZPA can allow organizations to take full advantage of the cloud technologies and mobility practices that modern businesses are embracing. By providing users with direct access to internal applications, both on-premise and in the cloud, organizations can give users an improved user experience, remove hardware appliances, realize significant savings in cost and administration associated with VPN technology and greatly reduce their attack surface area by no longer having VPN gateways or applications listening for inbound connections.

Protect your information, people and reputation with BSI

Expertise lies at the heart of what we do. As trusted advisors of best practice, we empower you to keep your business safe through a diverse portfolio of information security solutions. Whether it's certification, product testing, or consultancy services or training and qualifying your people, we'll help you achieve your security goals.

Our Cybersecurity and Information Resilience Services include:



Our expertise is accredited by:

Find out more

EMEA	UK	US
Call: +353 1 210 1711	+44 345 222 1711	+1 800 862 4977
Email: cyber.ie@bsigroup.com	cyber@bsigroup.com	cyber.us@bsigroup.com
Visit: bsigroup.com/cyber-ie	bsigroup.com/cyber-uk	bsigroup.com/cyber-us

bsi.

Subscribe to our newsletter

Follow us on