WHITE PAPER

Beyond SD-WAN:

Zero Trust Security and the Internet as Corporate WAN

Why SD-WAN, Secure Access, and Threat Protection Belong Together

The Future of the Enterprise Wide-Area Network

Wide-area networks (WANs) have been around since the 1960s, the earliest days of computer-to-computer communication. They continue to be developed and enhanced as technology evolves and as traffic demands rise. For today's enterprises, WANs are the infrastructure that allow a unified network across locations.

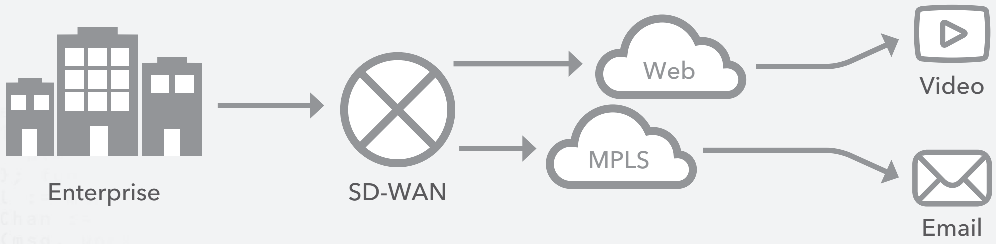
But this critical understructure is not without its constraints. WANs often deliver low or insufficient bandwidth, cause problems with specific applications' performance, have fluctuating reliability, and may pose a security risk to your business. Furthermore, WANs are frequently built on leased lines, or are leased from service providers whose infrastructure uses circuit switching or packet switching methods such as asynchronous transfer mode (ATM) and multiprotocol label switching (MPLS), in addition to the public Internet. While the latter is a somewhat less costly option, it is still a very expensive status quo – and does not lend itself to scalability.

The Corporate Network Is Transforming

In response to these performance, security, and monetary challenges, enterprises are adopting software-defined WANs (SD-WANs), at once reducing costs and enabling agility.

Emerging from the innovation of software-defined networking (SDN) and network function virtualization (NFV) that were originally used in data centers, IT departments quickly adopted the technology for the networks that connected organizations.

Simply put, SD-WAN separates the data and control planes of the wide-area network. SD-WAN monitors the performance of the mix of WAN data connections – MPLS, ATM, and the Internet – and selects the most appropriate connection for each traffic type based on current link performance, the cost of the connection, and the needs of the application or service.



SD-WAN in Action

An SD-WAN might route email over MPLS because latency is not a major issue and the cost-per-bit sent is the lowest. Conversely, the SD-WAN might route video conferencing traffic over the Internet to ensure optimal performance and minimal latency, but at a higher cost-per-bit sent.

Could the Internet Become the New Corporate WAN?

SD-WANs can certainly be flexible, efficient, and cost-effective if they employ multiple transport services, including the public Internet. But since there's no performance guarantee or SLA for such transport options, SD-WANs use the Internet solely for those applications whose performance is not critical.

To increase the use of the Internet to deliver more corporate WAN traffic efficiently, cost-effectively, and securely – and in a manner that can co-exist with current SD-WAN deployments – you must adopt an approach that eliminates the underlying limitations of the Internet. One way to do this is to use an edge platform to deliver secure, fast, and reliable business applications over the Internet – without publicly exposing them on the Internet. This allows you to maximize your current investment in SD-WAN while further reducing costs as you transition more traffic to the Internet.

Routing a larger slice of enterprise traffic to the Internet simply makes sense given the trajectory of modern corporate networks. Increasing cloud workloads, coupled with diversified and mobile users and devices, means that workflows already rely heavily on the Internet. And this trend continues to propagate.

What if you could take this one step further, establishing a secure, scalable, and efficient corporate WAN over the Internet?

In this paper, we'll discuss the processes of transforming your network with SD-WAN and Zero Trust security, and positioning your organization to evolve beyond SD-WAN, adopting a fully Internet-based corporate network.

An edge platform lets you deliver secure, fast, and reliable business applications over the Internet – without publicly exposing them to the Internet.

> *By year-end 2023, more than 90% of WAN edge infrastructure refresh initiatives will be based on virtualized customer premises equipment (vCPE) platforms or software-defined WAN (SD-WAN) software/appliances versus traditional routers (up from less than 40% today)."*
>
> *– Gartner, Magic Quadrant for WAN Edge Infrastructure, October 2018*

The Value of SD-WAN

SD-WAN primarily provides link balancing, automatic device configuration, and third-party security service insertion. The value of these functions – the improved user experience, the reduction of link costs, and the reduction in OpEx – can have a significant impact. Uptake is clear and endorsement is well-illustrated.

Dozens of vendors provide different SD-WAN capabilities, but they can be broadly generalized into three categories:

1. *Flexible link control*
2. *Manageability*
3. *Service insertion*

Flexible Link Control

The first capability, flexible link control, is the primary charter of SD-WAN. As the cloud is a principal destination for many organizations, backhauling traffic over a private network to a data center – serving as a de facto centralized control point – is not practical. SD-WAN solves this challenge by using intelligent traffic control, including dynamic route selection. Additionally, SD-WAN establishes local or branch Internet breakouts, also known as direct Internet access (DIA), that routes traffic to the cloud instead of through a data center. As such, all legacy applications, including voice and video, are designated for MPLS links, while cloud applications and Internet traffic go straight to the Internet.

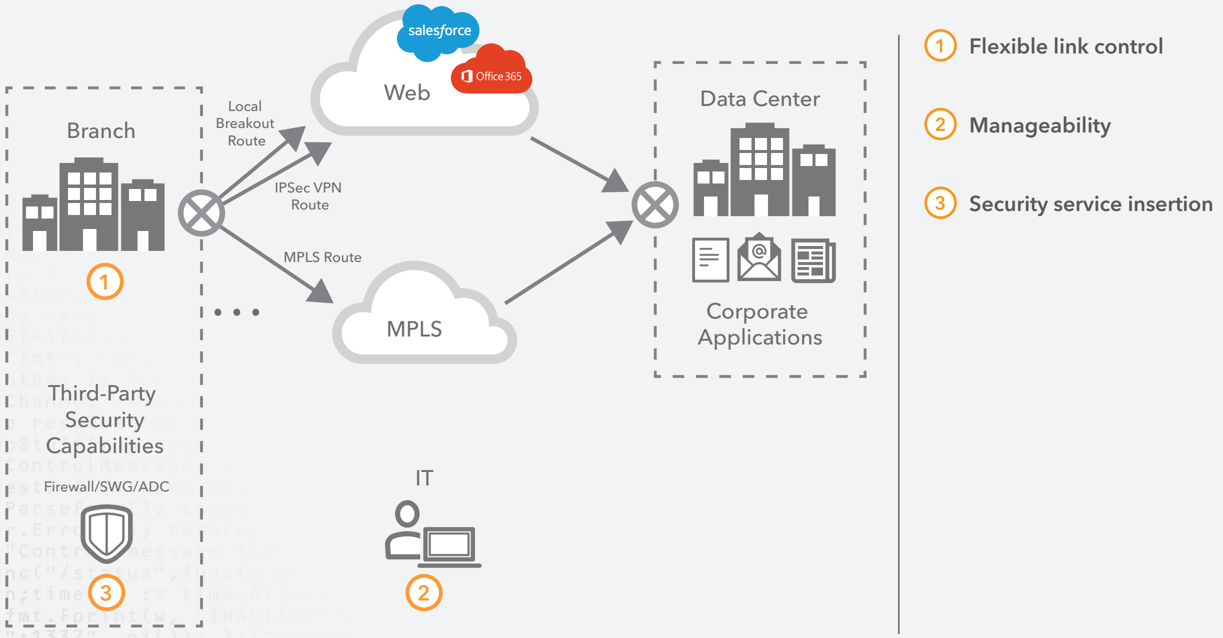
Manageability

SD-WAN vendors can also provide manageability, simplifying the operation and administration of network devices. Since the 1990s, enterprise WANs have been composed of network devices such as multilayer switches and routers. These devices have been largely managed on a per-appliance basis. In other words, administrators have to configure and maintain several hundred to several thousand devices individually, monitoring each device's software stack, across the entire organization. Even if devices dynamically exchange routing information or establish high availability using routing protocols, the effort is enormous. With SD-WAN, all device management can be accomplished in a single, centralized console.

Service Insertion

Finally, some SD-WAN providers specialize in service insertion. The minimum requirement for WAN is IP reachability, namely Layer 3 network connectivity, across the organization. However, as networking has evolved, so too have security functions: firewalls, intrusion protection systems (IPS), and application delivery controllers, to name a few. In the past, you needed a complicated routing design to add these capabilities to the network because the devices that provide such services are typically unable to speak to dynamic routing protocols (open shortest path first [OSPF], border gateway protocol [BGP]), resulting in a complex combination of static routing and redistribution. SD-WAN makes these technologies, often delivered via third parties, easy to configure and simple to manage through a unified portal.

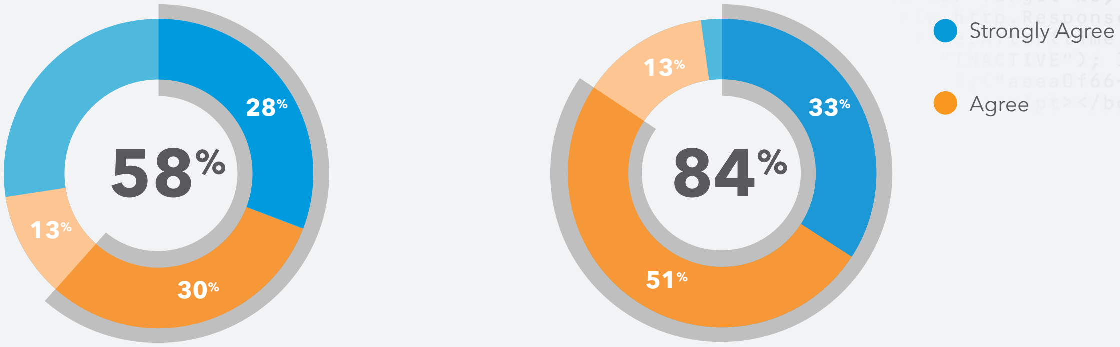
Business Value of SD-WAN



A New Model: Zero Trust Security

New architecture requires new security. As transactions move to the cloud and the Internet, networks have become highly distributed, creating additional attack surfaces. Applications, users, data, and devices have moved outside of the traditional zone of control, dissolving what was once the trusted enterprise perimeter. As such, building and enforcing a security model that relies on a corporate perimeter is no longer viable. A modern defense strategy must solve for today's distributed workloads and workforces.

To What Degree Do You Agree/Disagree?



"The network perimeter is indefensible in today's technology ecosystem of distributed cloud networks and mobile/remote users."

"Digital transformation necessitates adjustments to traditional (perimeter-based) security strategies."

Forrester Research, Build Your Zero Trust Security Strategy With Microsegmentation, September 2018

A Zero Trust security model assumes that there is no inside and that every user and device is equally untrusted. Every access request requires authentication and authorization. Applications and data are only delivered after verification – and even then, on a transient basis and with limited scope. This security framework treats all applications as if they're Internet-facing and considers the network to be compromised and hostile. Additionally, visibility is critical; full logging and behavioral analytics are a must-have.

Core tenets of Zero Trust security include:

- *Ensuring all resources are accessed securely, regardless of location or hosting model*
- *Adopting a "least privilege" and "default deny" strategy when enforcing application access*
- *Inspecting and logging traffic – for both applications you control and those you don't – to identify malicious activity*

There are two major components that support the implementation of Zero Trust security:

- *Identity-Aware Proxy for Secure Application Access*
- *Secure Internet Gateway for Protecting Users*

Identity-Aware Proxy for Secure Application Access

If users, data, and applications are on the cloud, and DIA enabled by SD-WAN provides the connection, why not shift the security and DMZ stack to the cloud as well? That way, you can leverage Zero Trust to ensure secure access to the applications you control, while mitigating the risk associated with users accessing applications that you don't control.

If you currently opt for a simple VPN setup to provide access to corporate applications, you likely allow logged in users to have IP-level access to your entire network. But this is highly risky and goes against the tenets of Zero Trust security. Why do call center employees have the permissions to source code repositories? Why does a contractor using your billing system have the rights to the credit card processing terminals? Access should be granted to just those applications needed in order to perform a role. Traditional VPN doesn't allow for this granular access, instead requiring a continued reliance on a hub-and-spoke network model.

An identity-aware proxy (IAP) architecture provides access to applications through a cloud-based proxy. Identity and authorization occur at the edge and are based on "need to know," least-privilege principles that are similar to access via software-defined perimeters (SDPs), but instead use standard HTTPS protocols at the application layer (Layer 7).

The Two Ways an IAP Can Work

You integrate a CDN into transactions across countries to improve application response

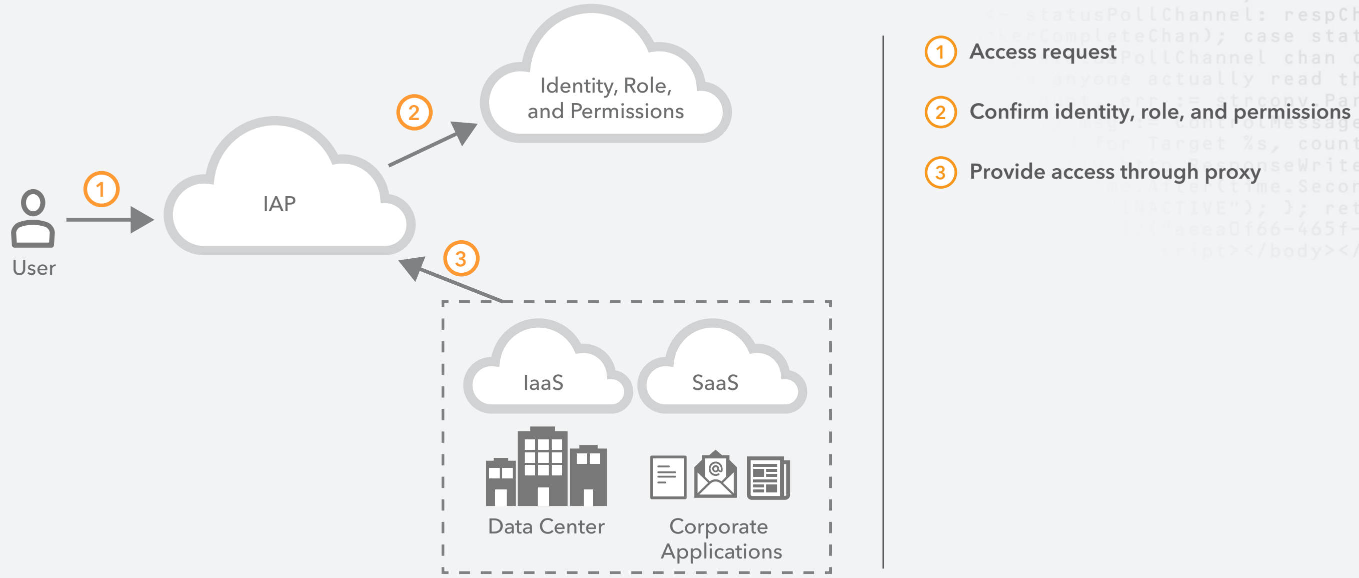
OR

You use a web application firewall (WAF) to safeguard corporate web servers against common vulnerabilities such as SQL injection and cross-site scripting

A key component of an IAP is an identity source that verifies user and device trust (authentication) and what they are allowed to access (authorization). This identity source may be based on corporate directories or cloud-based identity providers. Even before a user's identity is validated, checking a device's posture can ensure that the device attempting to gain access meets certain security criteria, e.g., having a certificate, running the latest OS, being password protected, or having the appropriate endpoint detection and response solution installed and operational.

One remarkable benefit of IAP compared with other access technologies: Not only are users verified, but users' traffic is inspected and individual application requests can be terminated, examined, and authorized. Once a transaction is terminated on the proxy, additional services can be integrated, allowing for improved user experience and application protection.

Identity-Aware Proxy (IAP)



1 Access request

2 Confirm identity, role, and permissions

3 Provide access through proxy

IAP also relies on application-level access controls, not firewall rules; configured policies can reflect user and application intent, not just ports and IPs. Like SDPs, this approach can cloak the applications and other assets in the cloud or behind the firewall, and it is clientless for web applications.

As cloud adoption grows, the challenge of migrating corporate applications has come into focus. Many organizations are struggling to leverage the cloud for cloud-native and traditional applications alike. Not only can IAP be used to authenticate users for native SaaS applications, but it can also be used to essentially "SaaSify" legacy applications in the data center. Furthermore, a proxy facilitates cloud migration and application modernization without resorting to a full rip-and-replace strategy. As a result, enterprises can take a methodical, step-by-step approach toward implementing Zero Trust while reducing the technical debt associated with legacy perimeter-based controls and traditional VPNs.

Secure Internet Gateway for Protecting Users

One critical aspect of transitioning to a Zero Trust security model is ensuring users remain safe while accessing applications you don't control. A vast number of cyberthreats lurk at every click on the Internet. In the past – when users were tied to the corporate network and managed devices – protecting against malware, ransomware, and phishing was as simple as rolling out endpoint antivirus, installing a stack of appliances in a data center, and backhauling traffic for inspection and control.

With users in multiple locations, the Internet becomes the corporate network of choice; a cloud-based SIG gives you a safe on-ramp – proactively protecting users wherever they are.

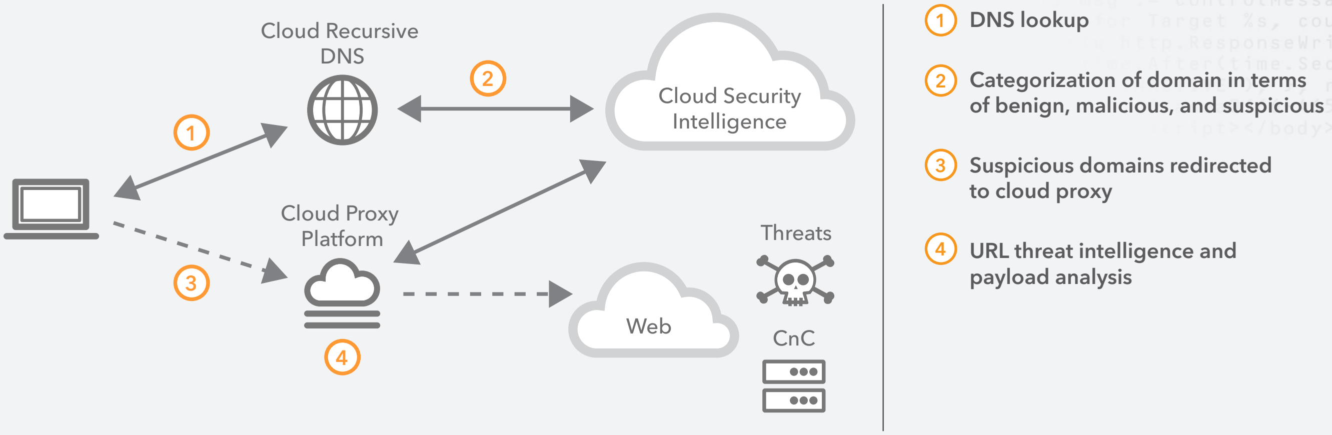
But users have left the building, devices are unmanaged, and the Internet is becoming the corporate network of choice. DIA connectivity renders central control and inspection security solutions obsolete. One alternative is to replicate the security appliance stack at each Internet breakout. However, for most enterprises, this is a nonstarter, both logistically and financially. And, perhaps more important, this approach's inherent complexity introduces security flaws, architected in direct opposition of Zero Trust best practices.

A simpler, faster, and more cost-effective method of securing DIA traffic is to use a cloud-based secure Internet gateway (SIG). A SIG is a safe on-ramp to the Internet, proactively protecting users – regardless of their location – against advanced threats by proxying risky traffic for control and inspection. This is achieved by examining each and every DNS request, blocking requests to malicious domains, allowing requests to safe domains to proceed as normal, and forwarding requests for risky domains to a cloud proxy for further inspection.

At this final stage, when the proxy receives an HTTPS request, it compares the requested URL with a cloud-based threat intelligence knowledge base and blocks malicious URLs. For all other requested URLs categorized as risky, the proxy sends the web content for inline payload analysis via multiple malware analysis engines. These engines use a range of detection techniques – signature, signature-less, and machine learning – to identify and block known threats and previously unknown zero-day threats. By having a range of detection methods, you can direct a payload to the most suitable engine (or engines) depending on the content type, which ensures optimal detection rates and delivers a low rate of false-positives.

It's important to note that this approach is quite different from the approach taken by legacy security appliances such as secure web gateways (SWGs). Specifically, SWGs proxy all Internet traffic – inspecting both good and bad – which can be especially detrimental to complex web pages and heavier HTTPS content. This approach degrades performance, introduces latency, and increases the volume of broken websites and applications, the consequence of proxying all traffic. SWGs often result in more security incidents and false-positives, driving up help desk requests and monopolizing IT resources.

Secure Internet Gateway Architecture



1. DNS lookup
2. Categorization of domain in terms of benign, malicious, and suspicious
3. Suspicious domains redirected to cloud proxy
4. URL threat intelligence and payload analysis

A smart selective proxy can leverage DNS as both the on-ramp to the Internet and as a first layer of security. By enabling safe traffic to go straight to the Internet, blocking bad traffic, and only proxying risky traffic, this approach delivers:

- *Simplified security*
- *Lower latency and better performance*
- *Fewer broken web pages and applications*

Network Transformation with Less Risk: Implementing Zero Trust in an SD-WAN Environment

Many organizations that are migrating to Internet-based architectures consider SD-WAN to be the key enabler due to its link control and ability to potentially drive down the financial onus of MPLS ownership. They may use broadband or wireless networks to augment or complement the MPLS connections, creating a hybrid WAN. But if they already embrace DIA, then surely it makes sense to employ a security model with the same approach.

As SD-WAN is adopted, companies must evolve their security from a perimeter-based framework to a Zero Trust–based framework at the edge. So where do we stand today — and what comes next?

Networks with SD-WAN are typically in one of three situations, depending on the mindset and long-term strategy of the enterprise:

1. *Traditional private WAN with centralized breakout; i.e., considering but not yet implementing SD-WAN*
2. *Hybrid implementation of traditional private WAN to existing sites and SD-WAN to newer branches*
3. *Primarily SD-WAN*

A Zero Trust security approach can fit well in all of these scenarios. But if the enterprise is already considering or implementing SD-WAN, it may have already embraced the Internet as a viable business network tool and is therefore primed to use a Zero Trust security strategy for its corporate network environment.

Let's examine the current-state architectures to identify how each might implement Zero Trust and then move toward the desired future state.

Traditional Private WAN with Centralized Breakout

If the motivations behind SD-WAN migration are cost, agility, and flexibility — benefits that an Internet-based network architecture can provide — it could make sense to skip SD-WAN altogether and move straight to a Zero Trust framework. IAP enables Zero Trust–based access to applications, irrespective of location, while SIG provides users with secure Internet access — all without organizations having to build security stacks at each Internet breakout.

One point to bear in mind: If the business already supports real-time services such as VoIP and video conferencing via an Internet cloud service provider, it is ideally placed to fully embrace an Internet-based network and access architecture. If these services are still primarily housed on-premises, there may be a case for retaining some level of "private" networking between locations — either private (e.g., MPLS-based) or SD-WAN based.

Hybrid with Traditional WAN and SD-WAN

In this scenario, organizations have already taken the first step to a more efficient, Internet-based architecture.

In these environments, it is important to understand how user traffic is handled:

- *Do users have direct Internet access from remote offices or is the Internet link used just for networking back to core sites?*
- *Where are the primary user applications based? On-premises, in a data center, or in the cloud?*
- *If the cloud is used, how do users connect to those applications? Is it facilitated via DIA from a branch or backhauled to a direct connection link?*
- *How extensive is the use of SaaS applications?*
- *For DIA at the branch level, how comprehensive is the security stack at each location?*

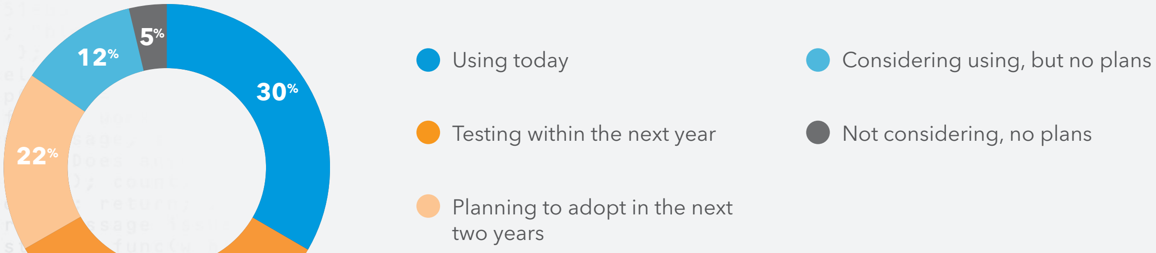
Answers will naturally vary depending on the treatment of user traffic – and, as such, network migration will have varying degrees of complexity. But two constants exist: There will be an increase in Internet use and a need to transition from perimeter-based security to a Zero Trust model.

Take, for example, a situation in which there is some DIA connectivity from a remote office. A SIG can afford additional protection to the centralized security stack, as well as replace some of the stack, reducing complexity and cost.

If users access cloud-based applications, an IAP-based approach could both strengthen the organization's security posture and improve the user experience. It might also boost application performance by enabling direct access to applications over the Internet with a CDN.

You can continue moving from traditional WAN into an SD-WAN environment by enabling DIA for remote offices and embracing the principles of Zero Trust security.

What Are Your Business Plans to Use Software-Defined (SD-WAN) Network Technology Today?



Forrester Research, Digital Transformation Drives Distributed Store Networks to the Breaking Point, April 2018

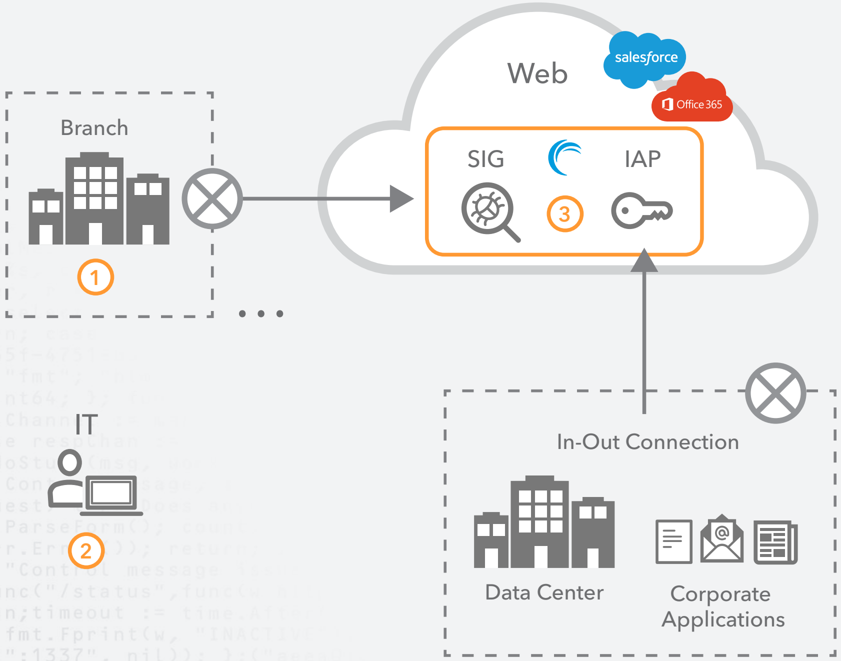
Primarily SD-WAN

In this state, organizations have likely moved away from a traditional private WAN network, using intelligent routing across Internet links among sites for inter-office communication – fully utilizing the advantages of DIA. These businesses already rely on Internet access in most sites, so evolving the network beyond SD-WAN is the logical direction to take.

The next step? Begin to reduce reliance on MPLS links by moving applications onto the Internet to deliver agility and cost efficiency. Corporate applications are accessible via IAP even in a DIA environment. If applications are already in a cloud environment, it doesn't make sense to access them by backhauling traffic to a data center before breaking out at a central location (e.g., using a direct connect type topology).

Finally, this environment is well-suited to a future state of pure Internet-based connectivity and access – all corporate applications could be accessed via IAP, whether they are on-premises or cloud-based. All user traffic could be secured via SIG. And, if Internet-based providers deliver real-time communication, such as voice and video, it may be possible to eventually eliminate the SD-WAN, and even corporate WAN, completely. This could reduce cost and complexity, as well as enhance security via a Zero Trust architectural model.

Value of Internet-Based Architecture with a Zero Trust Security Model



1 **Simplest network access**
- Only Internet access
- No out-in access

2 **Manageability**
- Single point of management
- Device monitoring
- User monitoring

3 **Further security control**
- Zero-day attack prevention
- Centralized AAA (authentication, authorization, and accounting)
- Client posture checking
- Phishing, malware, and CnC prevention

Transform Your Business

The modern realities of business increase exposure in an environment already rife with risk and complexity. A network model governed by hub-and-spoke transactions on a private WAN is as outdated as perimeter-based enterprise defense; both network and security architectures must evolve. While SD-WAN currently enables the corporate network to efficiently handle traffic and move workloads to the cloud, this network model must continue to iterate. The Internet is the corporate WAN of the near future.

Akamai believes that using SD-WAN, combined with the appropriate Zero Trust–compliant security and access services, is the first step to transitioning to the Internet as the corporate network. Couple SD-WAN with the Akamai Intelligent Edge Platform and you can apply access and security policy universally and ensure fast and reliable end-user application experiences over the Internet.

Akamai can help guide your network and security evolution. Contact your account team to learn more about Akamai's Zero Trust assessment – you'll receive tangible recommendations from our security experts on where to start or how to progress your Zero Trust transformation. Or, visit *3 Simple Ways to Start Implementing Zero Trust Security Today* for resources to kick-start your transition.

Akamai

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 06/19.