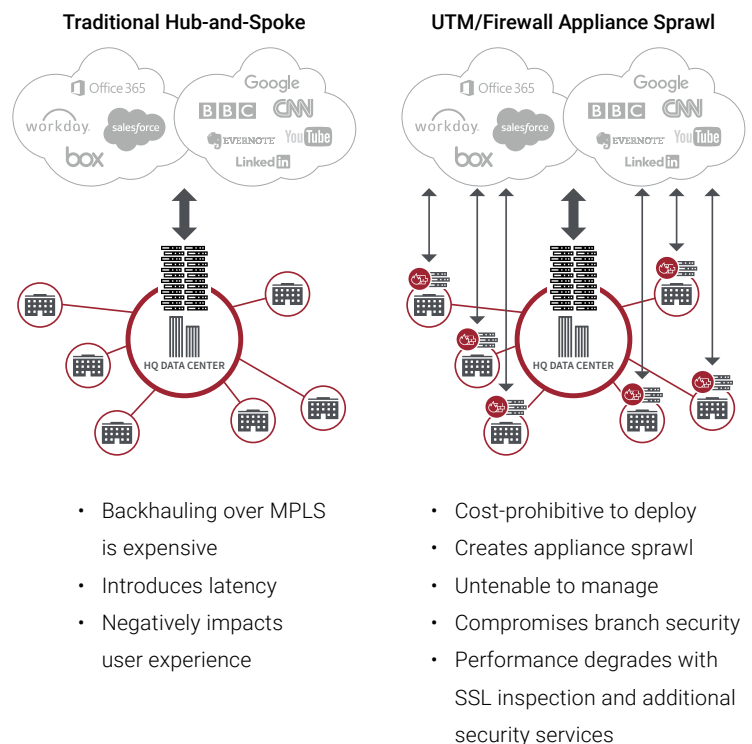# Zscaler™ and SD-WAN

Securing the internet-only branch

Zscaler and SD-WAN make it easy to migrate from a hub-and-spoke network to an internet-only branch architecture by enabling secure local internet breakouts.

Cloud apps have broken traditional architectures

For organizations deploying cloud applications like Office 365, the old approach to routing traffic — backhauling over MPLS to a centralized internet gateway via a hub-and-spoke architecture — is inadequate. To deliver a fast user experience and support cloud applications and services, internet traffic must be routed locally.

But to deliver the same level of security as the centralized internet gateway, organizations must replicate the stack of security appliances at every branch, which is expensive to buy, deploy, and manage. Traditional firewalls and UTMs are a poor alternative, as they cannot handle SSL-encrypted traffic or non-standard ports and protocols. Because of these challenges, organizations are increasingly turning to SD-WAN to establish local internet breakouts and deliver a fast user experience.

Traditional Hub-and-Spoke

- Backhauling over MPLS is expensive
- Introduces latency
- Negatively impacts user experience

UTM/Firewall Appliance Sprawl

- Cost-prohibitive to deploy
- Creates appliance sprawl
- Untenable to manage
- Compromises branch security
- Performance degrades with SSL inspection and additional security services

## SD-WAN and local internet breakouts

Software-defined wide area networking (SD-WAN) simplifies how traffic is routed in the branch, and makes it easy to establish local internet breakouts. Software-defined policies are used to select the best path to route traffic connecting the branch to the internet, cloud applications, and the data center. By defining policies for all branches — in the cloud through a single interface — organizations can easily deploy new applications and services, and manage policies across many locations. But, these local breakouts need to be secured.

Zscaler: The cloud way to secure SD-WAN

Zscaler secures outbound internet traffic and delivers a fast user experience — without backhauling and without duplicating the security appliance stack at each location.

Because the Zscaler Cloud Security Platform delivers the entire security stack as a cloud service, there is no compromising on security. And with Zscaler, policies are not tied to a physical location; instead, they follow users to provide identical protection no matter where they connect.

Simply route internet-bound traffic to Zscaler and immediately begin inspecting all traffic — all ports and protocols, including SSL. You can define and immediately enforce access and security policies across all locations from a single console. And with Zscaler, cloud services scale elastically, allowing you to deploy new services, like bandwidth control, in just a few clicks — without impacting performance and without costly appliance upgrades.
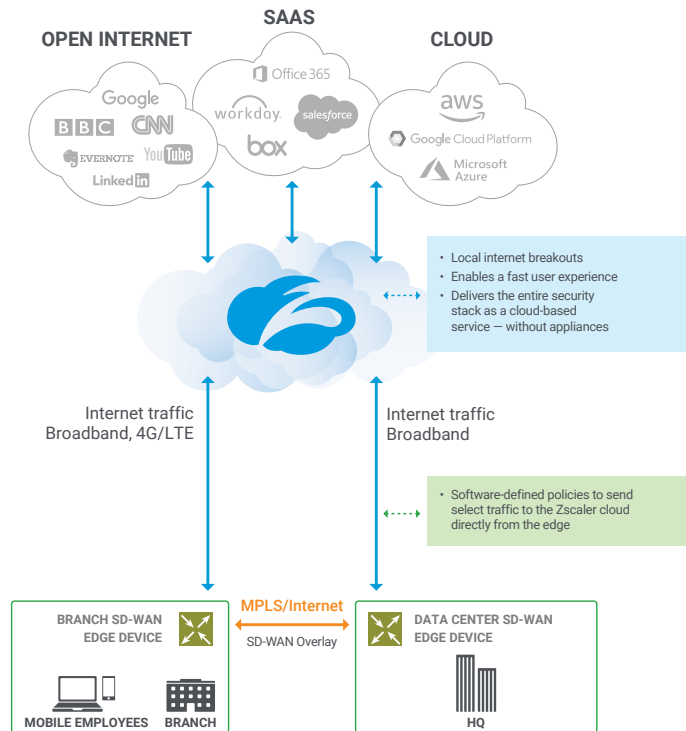
SSL inspection with SLA-backed performance

SSL is now the default communication protocol, and many threats like ransomware try to hide inside SSL — and sometimes even use other ports — so it's imperative to inspect all traffic. But SSL inspection remains a significant challenge for security appliances; decrypting, inspecting, and re-encrypting that traffic is known to decimate a firewall's performance.[2] Zscaler Cloud Firewall, a part of the Zscaler platform of services, inspects all traffic — all ports and protocols, including SSL, with near-zero latency.

>86%

More than 86% of traffic to Google is encrypted[1]

81%

SSL inspection with an appliance creates an 81% average loss in performance[2]

[1] Transparency Report – Google, https://www.google.com/transparencyreport/https/?hl=en
[2] Pirc, John W., "SSL Performance Problems: Significant SSL Performance Loss Leaves Much Room for Improvement. NSS Labs (https://www.nsslabs.com/linkservid/13C7BD87-5056-9046-93FB736663C0B07A/)

Zscaler and SD-WAN

REDUCE COST AND COMPLEXITY

Zscaler and SD-WAN enable the internet-only branch without the cost and complexity of traditional network and security appliances

SD-WAN

- Simplifies connecting branches to the internet by using software-defined policies and eliminating complex access control lists associated with traditional appliances

- Leverages multiple branch connection types (broadband, VPN over broadband, LTE, and MPLS) to allow a seamless migration from a hub-and-spoke architecture

ZSCALER

- Secures local internet breakouts by delivering the entire security stack as a cloud service, eliminating the need for branch firewalls and UTMs

- Enables secure local internet breakouts without any appliances to deploy or manage

- Reduces MPLS backhauling costs

SIMPLIFY OPERATIONS

Zscaler and SD-WAN simplify branch operations by delivering security as a cloud service and using software-defined policies to route traffic

SD-WAN

- Uses software policies that are defined in a single cloud management console to determine how traffic is routed

ZSCALER

- Eliminates the need to buy, deploy, and manage stacks of security appliances in all your branch locations

- Allows central definition of security and access policies in a single console

- Immediately enforces policy changes across all locations

- Enables deployment of new security services across all locations in minutes, with just a few clicks

- Routes internet traffic locally to enable a fast user experience

- Provides security and access controls for outbound internet traffic on all ports, not just 80 and 443, to prevent advanced threats

SECURE AND SCALE

Zscaler delivers the entire security stack as a cloud service, providing identical protection for users wherever they connect — coffee shop, headquarters, or the branch

ZSCALER

- Delivers a full set of security and access controls as a purpose-built, cloud-based service — no compromising on security

- Performs full inline content inspection and access controls for all ports and protocols with full logging capabilities

- Natively inspects SSL traffic

- Scales elastically to enable rapid deployment of new features (like bandwidth control or data loss prevention) without impacting performance or requiring appliance refreshes

- Brings the entire security stack close to the user, ensuring identical protection for users wherever they connect