Five

PITFALLS TO AVOID
as you plan to route branch traffic direct-to-internet

Relying on regional gateways

Instead of deploying security at every branch, many organizations backhaul traffic to regional hubs or a few data center gateways. It saves a bundle, but the downside is a poor user experience, and it complicates privacy and other compliance issues.

Instead: Use fast, local connections, secured by the Zscaler cloud.

1

Believing that virtual appliances equal cloud security

A virtual firewall has the same capacity limits as a physical one, and it will still buckle under the strain of SSL inspection or added security features. No firewall appliance, physical or virtual, can scale to meet growing demands. Only a true cloud firewall can do that.

Instead: Look to a 100% cloud firewall for security that scales.

2

Putting up with security gaps

Your users in the branch and regional offices deserve identical security to users at headquarters, with inspection for all ports and protocols, including SSL, and a full stack of security and access services, including sandbox, firewall, and advanced threat prevention.

Instead: Protect branch users with comprehensive, cloud-delivered security.

3

Bolting on a proxy

Now that 91 percent of traffic across Google services is encrypted,[1] SSL inspection is a must. But most devices can't natively inspect SSL-encrypted traffic. That means a bolt-on proxy...which means an end to performance.

Instead: Inspect all traffic using security built on a global cloud.

4

Leaving bandwidth to chance

Bandwidth-hungry applications, traffic increases, and the addition of new features can crush performance and send costs skyrocketing. You must prioritize applications or define traffic limits if you want to keep productivity up.

Instead: Deploy a bandwidth control solution that lets you prioritize business-critical apps.

5

Zscaler can help you avoid these pitfalls and route your branch traffic securely to the internet. Learn how at **zscaler.com/transform**

≋zscaler™