COMTACT
ALWAYS ON. ALWAYS SECURE.

zscaler

THE DEFINITIVE GUIDE TO BRANCH TRANSFORMATION

"GUIDANCE FOR ROUTING TRAFFIC TO ENABLE DIRECT ACCESS TO THE INTERNET & CLOUD APPLICATIONS.

NOC
ALWAYS ON.

24/7

SOC
ALWAYS SECURE.

www.comtact.co.uk enquiries@comtact.co.uk 03452 75 75 75

The purpose of this document is to provide security guidance for routing traffic locally from your branch office locations to enable direct access to the internet and cloud applications. We will outline the five requirements for architecting the ideal solution. But first, let's discuss why secure local internet breakouts have become necessary.

The situation

Applications continue to accelerate their move to the cloud. At the same time, increasing numbers of employees are working outside the corporate headquarters in branch or remote offices. Organizations are discovering that legacy network and security strategies that worked in the past no longer make sense.

Hub-and-spoke architectures centered around backhauling traffic to applications that sit in the data center are becoming increasingly irrelevant. Yet, many organizations still find themselves forcing branch traffic back through legacy architectures to access cloud applications and the internet, which largely defeats the purpose of moving applications to cloud in the first place.

Cloud applications were designed to provide an excellent user experience, enabling users to be more productive, while making businesses more flexible and agile. And realizing these benefits requires direct-to-internet connections. But getting there requires a fundamental change in the way you approach your network and security.

Challenges with traditional architectures

Poor user experience

As users move to branch offices and work remotely, they need fast access to the internet and cloud applications. Backhauling traffic from these locations across a hub-and-spoke network to the HQ data center creates traffic bottlenecks and latency that leave users waiting and sap their productivity—and they are probably not happy about it.

High costs

Legacy hub-and-spoke architectures leave organizations struggling to keep their MPLS spending in check. Backhauling traffic to the data center from your branch locations introduces the hairpin effect, essentially forcing you to pay twice for your internet-bound traffic—once to carry your traffic from the branch to the data center, and again to return that traffic to the user. These costs grow exponentially in widely distributed and multinational enterprises, and IT teams are constantly looking for ways to reduce MPLS spend.

> "Before the emergence of cloud services, network infrastructure was generally designed to connect an organization's user locations to their data. This is a simple planning methodology to implement. With cloud services such as Office 365, that methodology no longer makes sense…"
>
> **–March 2017,**
> Microsoft TechNet

Reduced visibility

Many organizations believe that routing traffic back through a centralized gateway provides them with greater visibility and control. But the reality is that as applications move to the cloud, you no longer have visibility into those applications or the networks upon which they reside.

Complexity

According to RightScale, 79 percent of workloads now run in the cloud[1]. Your branch employees may not even need access to the corporate network as most of your applications migrate to the cloud. By keeping those users on the network, you are only adding unnecessary cost and complexity to pay for and manage MPLS and appliances. Your branch users simply need fast and secure access to the internet and cloud applications—something that can't be accomplished by backhauling.

Scalability

Applications like Office 365 were designed to be accessed directly over the internet. Hub-and-spoke architectures were not designed for long-lived connections, and the considerable increases in per-user SaaS connections can quickly overwhelm traditional architectures and firewalls, because they cannot scale to support the required connections.

The path to the cloud

Resolving these challenges requires a new way of thinking. To move to the cloud, you need to establish local internet breakouts in branches and securely route traffic direct to internet. Organizations are increasingly turning to software-defined wide area networking (SD-WAN) as a logical and cost-effective way to establish local breakouts and simplify traffic routing in the branch. The advantages of SD-WAN include lower costs, centralized cloud-based policy management, simplified IT, and faster, more reliable internet access. But those local breakouts still need to be secured, because SD-WAN solutions don't provide native security.

To secure SD-WAN deployments in branch offices you must address the challenge of providing consistently secure internet connections across all your locations without adding complexity. You have two primary options: deploy security appliances at every branch or move security to the cloud. As we explore the five key requirements for a successful branch transformation, your best path to the cloud should become clear.

[1] RightScale, " State of the Cloud Report," 2017

Five key requirements to secure direct-to-internet connections

1. Comprehensive security platform
2. Proxy-based architecture
3. Global cloud
4. Visibility and management
5. Elastic scalability

Securing direct-to-internet connections

Now that we've discussed the challenges facing distributed organizations in a cloud world, let's look at how to successfully address them. It should now be clear that you need to establish secure, local internet breakouts, and we believe that the right solution for enabling these connections should meet five key requirements to deliver comprehensive protection, reduce costs, simplify IT, and provide a fast user experience for all branch users.

Comprehensive security platform

Comprehensive security means you need identical protection across all locations, and that is possible only with a true cloud solution. Your solution must inspect all ports and protocols, and include a full stack of integrated security and access services, including cloud sandboxing, cloud firewall, and advanced threat prevention. And, your security needs to follow users, wherever they connect. Think about it. Your local branch is your new egress point to the internet and cloud apps. You need to provide the same level of security at each branch that you have at your data centers, regardless of the number of employees at the branch.

A comprehensive security solution also requires breaking out traffic for all ports and protocols, including DNS and video traffic, because apps like WebEx, Box, and Dropbox use ports beyond the usual 80 and 443.

Why legacy technology falls short

Traditional firewalls cannot proxy HTTP or FTP traffic, which means they do not have the full context of the type of security that is required. They can only inspect traffic based upon known signatures, which catch only three to eight percent of all vulnerabilities, leaving organizations exposed to attacks like DNS tunneling. In addition, not breaking out DNS traffic typically results in users not being connected to the nearest instance, which negatively impacts application performance and user experience.

Cutting corners is not an option

To secure local breakouts, some organizations deploy security appliances at each location, but few organizations are likely to replicate the HQ internet gateway security stack at every location due to the cost of purchasing, configuring, managing, and maintaining such a complex branch deployment.

To cut corners, organizations compromise on security by deploying smaller firewall and UTM appliances, with less than optimal security controls, at branch locations. This approach leaves you to manage different capacities and capabilities across your organization, complicating policy control, and often resulting in inconsistent policies and fragmented audit trails. These security compromises leave your branches, and therefore your entire network, vulnerable.

"41%
of network attacks use encryption to evade detection."

–Ponemon Institute, "Hidden Threats in Encrypted Traffic: A Study of North America and EMEA." 2016

Alternatively, appliance vendors will recommend establishing hubs and backhauling traffic to these regional data centers. This approach may alleviate the cost and complexity of deploying appliances at each of your branch locations, but you are simply creating a modified hub-and-spoke network, which does not resolve the challenges you set out to address, and does not establish the direct-to-internet connections you need. To effectively and securely route traffic direct to internet demands a cloud security platform.

Not all clouds are created equal

It wouldn't make sense to build a power plant using home generators—it's inefficient and lacks scale. And neither does it makes sense to build a security cloud with single-tenant appliances. Legacy technology, like next-generation firewalls and UTMs, lack the architecture needed in a cloud solution and cannot be repurposed for cloud.

Using virtualized firewalls is not the same as a multi-tenant cloud security platform designed for the cloud from the ground up. Virtualized firewalls still have capacity issues, and performance becomes affected when inspecting SSL traffic or adding new security features. It is still a box, just not a physical one. It cannot scale to meet your evolving demands.

A multi-tenant platform can provide all your security services in a single pass, without requiring additional hops that increase latency—unlike service chaining that happens with appliances and virtualized appliances. And because the platform is cloud-based, your security stack goes with you whether you are in the branch or at headquarters. Securely enabling cloud applications requires a multi-tenant platform that scales elastically to meet your needs.

Proxy-based architecture

SSL encrypted traffic is increasing, and so are threats hiding within that traffic. Google reports that more than 90 percent of the traffic crossing its properties is encrypted[2], so SSL inspection is no longer optional. But, SSL inspection requires a proxy. For the best security, you need a proxy that natively inspects SSL-encrypted traffic, at scale, without degrading performance.

Why legacy technology falls short

Traditional appliance-based firewalls and UTMs cannot natively inspect SSL encrypted traffic, so they require software-based bolt-on solutions. But, once SSL inspection is turned on, appliance performance takes a significant hit—check the specifications for yourself. Appliance lifecycles make the situation worse. Because organizations typically plan for a three-to-five-year appliance refresh cycle, you must speculate what your SSL inspection and performance needs will be five years out.

[2] Google Transparency Report

Microsoft suggested standard connectivity principles for Office 365

- Optimized connectivity to Microsoft's global network
- Localized network egress as close to the user as possible
- Unhindered access to the endpoints required
- Local DNS resolution

–March 2017,
Microsoft TechNet

Forecasting future SSL inspection requirements is difficult at best, and typically results in one of three potential outcomes. When performance becomes an issue, you may need to make costly, unplanned security appliance upgrades. Alternatively, you may be forced to bypass SSL inspection. With 41 percent of network attacks using encryption to evade detection[3], bypassing SSL is ill-advised. It's more likely that you will over-spend and over-provision the appliances you purchase today in anticipation of future increases in SSL traffic and associated threat volume.

And don't forget about certificate management. With appliance or VNF solutions, certificates must be installed manually on every device. It is unrealistic to expect that you can manage this process and keep certificates up to date if you have many branches or remote locations. To effectively handle SSL-encrypted traffic, your solution should enable native SSL inspection at scale and provide centralized certificate management—all without performance degradation.

Global cloud

The notion of the network perimeter has dramatically changed. You need to provide security and access controls for users that work and connect everywhere. And, they need a consistent level of security—that of the entire security stack— wherever they go. A global cloud with a multi-tenant architecture delivers that consistent security, regardless of where users travel. It provides the reliability and availability required by organizations with multiple branches and locations.

Why legacy technology falls short

Limiting egress points by backhauling traffic to regional hubs over MPLS, or routing traffic to a small number of data centers, creates geographic gaps, latency and a poor user experience. It also complicates data privacy compliance, because regulations vary by region. For a better user experience and simpler compliance, select a vendor that truly provides a global footprint. Data centers and egress points must be in carrier-neutral exchanges close to your branch users in all geographies. Close proximity, combined with peering with your critical applications[4], provides the fastest connections, better application performance, and enables easier compliance with data privacy requirements. Don't take our word for it. In 2017, Microsoft emphasized the importance of local egress and direct-to-internet connections as more applications, like Office 365, move to the cloud[5].

[3] Ponemon Institute, "Hidden Threats in Encrypted Traffic: A Study of North America and EMEA," 2016
[4] Validate peering at peeringdb.com and check how much peering bandwidth is available for both your cloud security and application vendors.
[5] Microsoft TechNet, March 2017

Enterprise-grade visibility and management

Real-time visibility by user, application, and location is essential to any security deployment, particularly for a widely distributed organization. You should not have to worry about dropped logs, piece together fragmented logs, or use multiple management platforms to view internet logs.

Why legacy technology falls short

Correlating activity across different appliances and providing visibility and reporting in a timely manner are nearly impossible with appliances scattered across every branch. At millions of transactions per day, carrying out such tasks is simply unrealistic. Implementing network and policy changes across the entire network using traditional security appliances typically requires the use of individual management interfaces or requires specialized IT staff to deploy configurations manually at each site, making it difficult to maintain consistent policies everywhere. Whether you have 20 locations or 200 or more, you probably don't have the time or resources to write location-specific configurations and push them. You need to simplify policy management.

Making matters worse, NGFW and UTM solutions require you to estimate your log sizes and volume when sizing appliances. Once log space is filled, your appliances will overwrite logs. Some appliances record only seven days of logs, and their manufacturers suggest that you purchase a central manager (at extra cost and size) to build your own log repository—a solution that doesn't scale well with business growth.

Your solution should simplify IT operations, not complicate it. The ideal solution would enable policy to be created centrally and pushed to multiple branches immediately, without adding licenses or without writing additional scripts. It should be as easy as creating a policy, selecting locations, and pushing a button to apply and enforce the policy.

Elastic scalability

Optimizing cloud application capabilities relies on the consistent delivery of performance and security functions, regardless of traffic volume. It also means that users are not impacted when features, functions, or users are added. To put it simply, you need a multi-tenant security platform that scales elastically to support resource-intensive applications, enables new security capabilities, and handles increases in network traffic—without increasing costs or complexity.

Why legacy technology falls short

Cloud applications, like Office 365, are resource intensive, and generate more long-lived connections per user. Such connectivity changes can overwhelm appliances and significantly erode performance, even when the appliances are deployed locally, because they cannot support the required connections. To compensate, organizations must often replace security hardware and implement expensive appliance upgrades.

Benefits of branch transformation with Zscaler

- Happier, more productive users
- Uncompromised security
- Operational simplicity
- Lower costs

To effectively manage traffic, you need the ability to prioritize business-critical applications and limit the bandwidth an application consumes. Appliances are not designed to prioritize business applications over other traffic. Bandwidth policing used by NGFW and UTM appliances introduces packet drops and additional latency. You end up with complex and expensive appliance sprawl, a poor user experience, and an enterprise vulnerable to bottlenecks and bandwidth contention. To address these challenges, your solution should include bandwidth controls that enable you to prioritize traffic for your most critical applications over YouTube, streamed sporting events, or even over non-critical business traffic.

Let's shift focus towards bandwidth allocation and enabling additional services. Imagine you are a global company, sending traffic from dozens of locations. If you choose a single-tenant technology, the resources required to perform security scanning for your organization will be limited. When your traffic spikes, you may not have been allocated adequate bandwidth to accommodate that spike, and that can be costly. At the end of the day, you want a solution that will scale in real-time to handle traffic spikes seamlessly. One benefit of a multi-tenant security platform is scalability—any tenant can consume any percentage of the cloud. As your needs grow, you can scale accordingly.

Turning on additional services in your security platform should also occur in real time, without impacting performance. With appliances, enabling new services often requires dedicated units or appliance refreshes at each site deploying the new capability. Implementation is costly and time consuming, and leads to appliance sprawl and inconsistent protection across the organization. Virtualized firewalls are no different. They are limited in capacity, and performance is impacted when inspecting SSL traffic or adding new security features. Though it is not a physical box in your data center, a virtual machine is still a box that needs to be upgraded every few years. It cannot scale to meet your rising demands.

Realizing branch transformation

Zscaler developed the Zscaler™ Cloud Security Platform—including its flagship security suite Zscaler Internet Access (ZIA)—to address these five key requirements. Zscaler enables you to shift from a hub-and-spoke network to an agile, cloud-enabled architecture by delivering the entire gateway security stack as an easy-to-manage service. A true alternative to complex and costly appliances, Zscaler simplifies IT operations and optimizes MPLS spend.

By routing traffic directly to the internet, ZIA places security closer to the user for a fast and secure user experience. Delivery as a cloud service allows security to follow the user to provide identical protections across all locations, whether the user is at corporate headquarters, or traveling to a branch location. All users, on or off network, get the same consistent, constant protection.

ZIA is a secure internet and web gateway delivered from the cloud. As is part of the global Zscaler Cloud Security Platform, ZIA enables networking teams to provide comprehensive access controls as a service. And, by routing traffic to Zscaler, security teams can deliver in-depth protection and instantly begin stopping malware, advanced threats, malicious web content and more. The Zscaler Cloud Security Platform, built on a 100% cloud-enabled architecture, embodies the five key requirements, which uniquely position it in relation to other security solutions on the market.

1. Full security platform – Zscaler Internet Access (ZIA) delivers the entire security stack as a cloud service, including cloud firewall, cloud sandbox, bandwidth controls, threat prevention, and data loss prevention, without backhauling or deploying security appliances at every branch. The service inspects all ports and protocols, including HTTP, HTTPS, DNS, and SSL-encrypted traffic, ensuring consistent and persistent security. No more security compromises.

2. Proxy-based architecture – Native SSL inspection at scale means that Zscaler can handle your SSL-encrypted traffic, without appliances or bolt-on solutions and without impacting performance. And, centralized certificate management makes inspecting SSL traffic from your branches easy. With Zscaler, there is no need to bypass SSL inspection for your branch traffic.

3. Global cloud – Zscaler Internet Access is built on a multi-tenant security architecture designed for the cloud from the ground up. Zscaler provides identical protection for users no matter where they choose to connect—at headquarters, branch offices, or on the go. More than 100 data centers on five continents, and direct peering with critical applications, means that Zscaler brings the internet closer to the user for fast connections, better application performance, delivering the productive user experience your business needs.

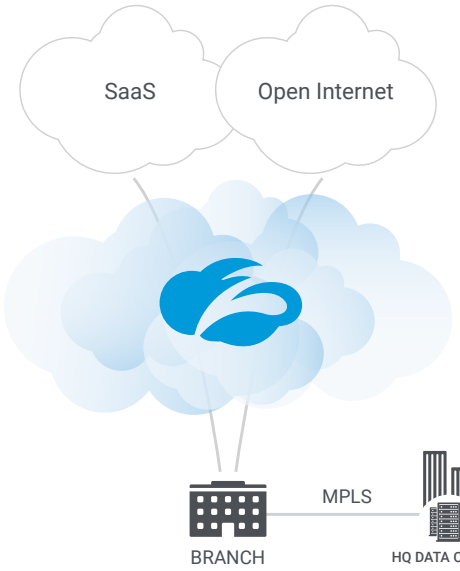
4. Visibility and management – Zscaler provides real-time visibility into applications, users, and threats across all locations. Customized transaction logs can be streamed from Zscaler to your SIEM with the Nanolog™ Streaming Service (NSS), to provide insights that help you detect and respond to threats and gain additional visibility into your network. Your IT team can activate new services, define and immediately enforce policies, and manage all branch locations from a single, centralized cloud-based console.

5. Elastic scalability – With the Zscaler multi-tenant security platform, you can route traffic locally to the internet and deliver consistent security and performance, regardless of traffic volume, and enforce bandwidth management policies to prioritize critical business applications over other traffic. Zscaler scales elastically to support cloud applications, increases in network traffic, and unexpected traffic spikes.

> " Before we had Zscaler, we had internet breakouts without any protection. Zscaler is directly in line and does packet inspection at a very high speed… Zscaler has reinvented how to do security because it's been built from scratch with the right vision. "
>
> **–Tony Ferguson**
> IT Infrastructure Architect
> **MAN Diesel & Turbo**

Direct to Internet

Block the bad, protect the good



Real-time policy engine

Policies follow the user.

Changes are immediate enforced, worldwide.

Business reporting and analytics

Global visibility and real-time reporting for every user in any location.

Your security stack as a service

Access Control	Threat Prevention	Data Protection
Cloud Firewall	Advanced Protection	Data Loss Prevention
URL Filtering	Cloud Sandbox	Cloud Apps (CASB)
Bandwidth Control	Anti-Virus	File Type Controls
DNS Filtering	DNS Security	

Are you ready to transform your branches and establish secure local breakouts?

Forcing branch traffic over a traditional hub-and-spoke network is not effective when your applications are in the cloud and your users are in branches all over the world. It's time to transform your network and security by routing your traffic direct to internet. As you consider your next steps, keep in mind the five key requirements. Begin your branch transformation journey with a solution that was designed and built to support a cloud-first enterprise—a solution that will reduce costs, enable a better user experience, and provide the same enterprise protections across all your locations, at the HQ or branch office.

For more information on Zscaler and how we can help fuel your branch and network transformation, email sales@zscaler.com. Be sure to ask how you can get started today.

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com

ABOUT COMTACT

Established in 2005, Comtact Ltd. is an award-winning, Government-approved service provider, supporting clients 24x7x365 from high security Network (NOC) & Security Operations Centre (SOC) in Northampton, UK.

24x7x365 SUPPORT

Comtact has a multi-skilled, three-tiered professional support, providing 1st line and 2nd line support operated from our 24x7x365 high security Tier 3 data centre.

ISO27001

Comtact and its operations are entirely ISO27001 accredited, providing customers with the assurance that their service solution is being supported by true professionals.

“

Based in Northampton, Comtact’s Security (SOC), Network (NOC) and Service Delivery Centre (SDC) are located within our state-of-the-art Tier 3 data centre.

Comtact Ltd. (Head Office)
Clive House, 12 - 18 Queen’s Road
Weybridge, Surrey KT13 9XB

Tel: 03452 75 75 75
Email: enquiries@comtact.co.uk

Comtact-Ltd

@comtact_ltd

Government Procurement Service *Supplier*

www.comtact.co.uk