SOLUTION BRIEF

Zscaler™ Cloud Firewall

Enabling secure local Internet breakouts without appliances

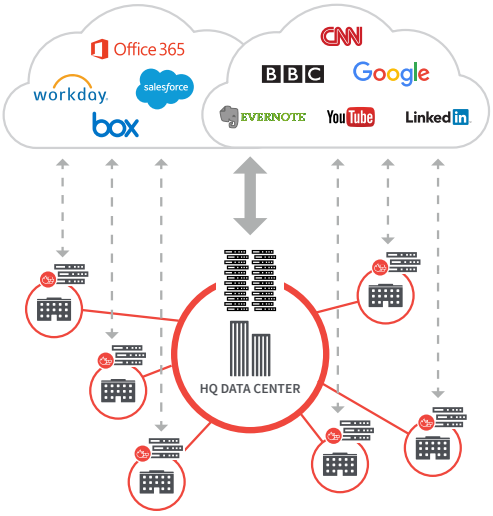
Zscaler Cloud Firewall brings next-gen firewall controls and advanced security to all users in all locations — for all ports and protocols. Zscaler enables fast and secure local Internet breakouts and, because it's 100 percent in the cloud, there's no hardware to buy, deploy, or manage.

CLOUD APPS HAVE BROKEN TRADITIONAL ARCHITECTURES

The workforce is now distributed and mobile, and the number of applications leaving the confines of the data center for the cloud continues to grow. These cloud applications, including Microsoft Office 365, were designed to be accessed directly via the Internet. To securely embrace cloud apps and services and deliver a fast user experience, Internet traffic needs to be routed locally.

One way to route traffic locally and secure this new world is to deploy stacks of security appliances in every branch office. But this option is simply not viable in terms of the cost and complexity of deploying and managing them all. Traditional firewalls are easily overwhelmed by cloud apps, because they cannot scale to support the high volume of long-lived connections the apps create, and 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. But, these local breakouts need to be secured.

UTM/Firewall Appliance Sprawl



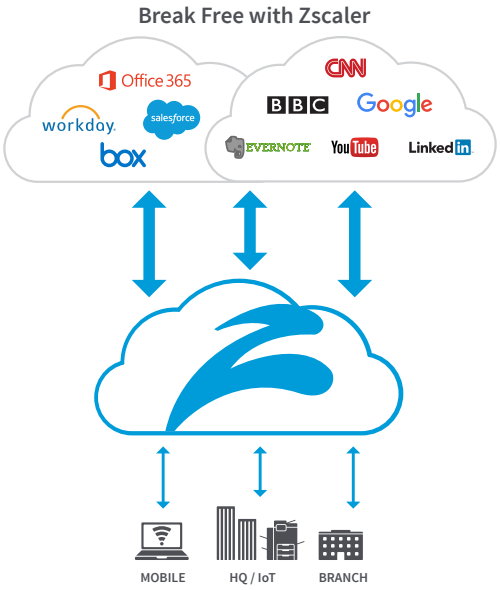
- Creates appliance sprawl
- Cost prohibitive to deploy
- Untenable to manage
- Compromises branch security
- Performance degrades with SSL insection and cloud apps with long-lived connections

ZSCALER: THE CLOUD WAY TO SECURE LOCAL INTERNET BREAKOUTS

Securing local Internet breakouts — without backhauling and without duplicating the security appliance stack at each location — is a critical component of Zscaler Cloud Firewall. Zscaler allows Internet traffic to be routed locally and securely for all ports and protocols. With Zscaler, policies are not tied to a physical location; instead, they follow the users to provide identical protection no matter where they connect. And since Zscaler is a 100 percent cloud-delivered service — part of a global multi-tenant cloud security platform — there is no hardware or software to deploy or manage.

Simply route Internet-bound traffic to Zscaler Cloud Firewall and it immediately begins inspecting all traffic — all ports and protocols — scaling to handle SSL inspection and cloud application traffic with long-lived connections.

Zscaler Cloud Firewall logs every session to provide visibility across all users and all locations in less than a minute, ensuring you have access to the information you need, exactly when you need it. Zscaler addresses your performance and security needs in the branch today, supports your move to cloud applications like Office 365, and scales elastically as your business needs grow.



SSL INSPECTION WITH SLA-BACKED PERFORMANCE

SSL is now the default communication protocol, and many threats like ransomware are delivered over SSL — and sometimes even over 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 inspects all traffic — all ports and protocols, including SSL.

[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/)

AutoNation

Eliminated the need to deploy 540 UTM/NGFW appliances and cut its MPLS backhaul costs by deploying the Zscaler Cloud Security Platform for all users in all locations.

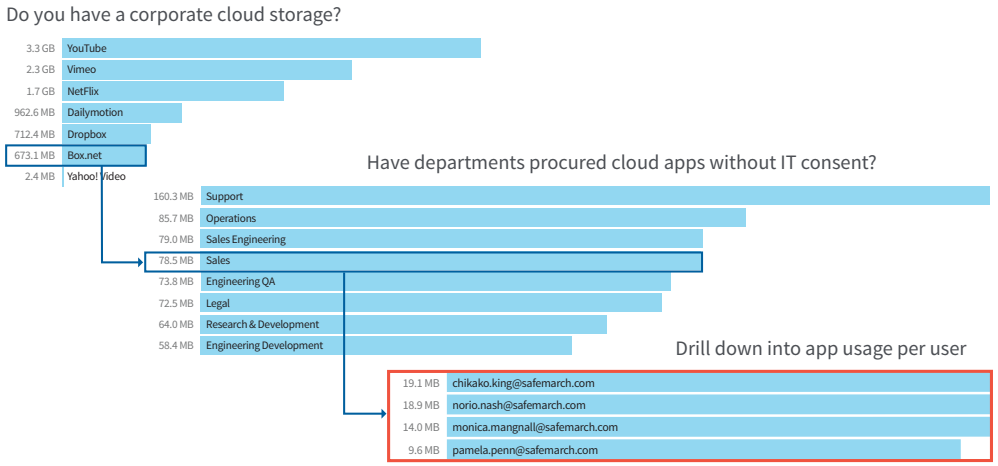
"The next gen firewall capabilities are actually a core requirement. It was one of the primary considerations in selecting Zscaler. We hadn't found any other cloud service that actually had a full protocol next gen capability."

***– Ken Athanasiou**, Chief Information Security Office at AutoNation*

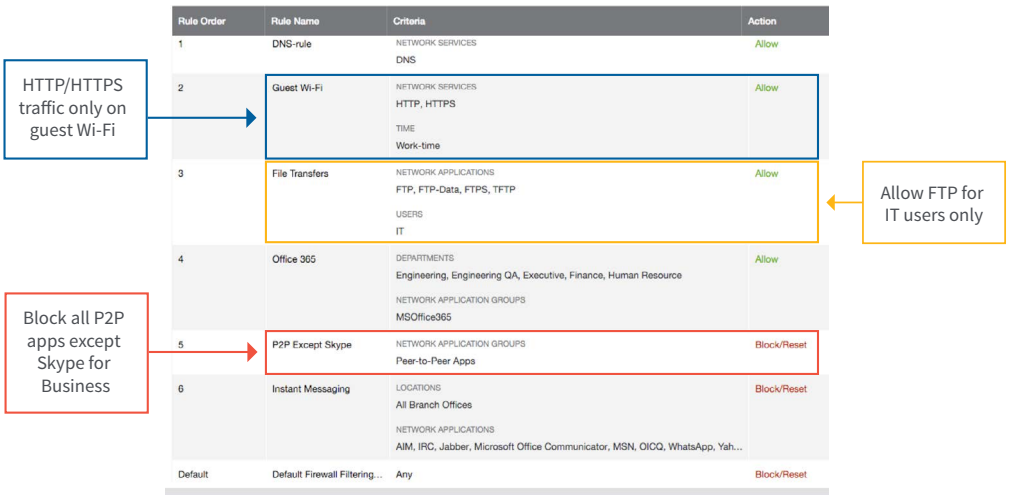
NEXT-GEN FIREWALL CAPABILITIES WITHOUT THE HARDWARE HEADACHES

- **Stateful firewall policies** — Apply allow/block security policy based on source and destination IP address, ports, and protocols
- **Standard NGFW policies** — Apply granular allow/block security policies based on applications using a Deep Packet Inspection (DPI) engine
- **Context-aware policies** — Apply access and security policy based on user identity, group, and location – (truly tied to the user)
- **Fully qualified domain name (FQDN) policies** — Easily configure and manage access policies for applications hosted across multiple IPs
- **Application usage visibility** — Get real-time visibility into traffic usage, threats, and applications by users, groups, and locations within a few clicks
- **Fully integrated security services** — Contextual information is shared across services to provide better protection and deeper visibility
- **Cloud effect** — Every time a new threat is identified in any of the 40 billion requests processed daily by the Zscaler cloud, it gets blocked for all Zscaler users, everywhere

REAL-TIME VISIBILITY INTO APP TRAFFIC FOR ALL USERS AND ALL LOCATIONS



DEFINE GRANULAR POLICIES WHICH FOLLOW THE USER, REGARDLESS OF LOCATION



BREAK FREE FROM HARDWARE LIMITATIONS WITH ZSCALER CLOUD FIREWALL

Reduce costs and complexity

- Enable secure local Internet breakouts for all ports and all protocols without any appliances to deploy or manage
- Reduce MPLS backhauling costs
- Eliminate the need for costly and time-consuming patch management, coordination of outage windows, and policy management

Improve security and performance

- Route Internet traffic locally to enable a fast user experience
- Provide security and access controls for Internet traffic on all ports, not just 80 and 443, to prevent advanced threats
- Deliver full, dynamic inspection of HTTP traffic traversing non-standard ports
- Fully proxy all DNS traffic to protect against vulnerabilities such as DNS cache poisoning

Benefit from the cloud effect

- Bring the entire security stack close to the user, ensuring identical protection for users from wherever they connect
- Scale services elastically to handle SSL inspection and cloud application traffic requiring long-lived connections
- Log every session for complete visibility into all users, locations, applications, ports, and protocols, in near-real time

ZSCALER PURPOSE-BUILT MULTI-TENANT CLOUD SECURITY PLATFORM

Powered by Patented Technologies

SSMA™
All security engines fire with each content scan – only microsecond delay

ByteScan™
Each outbound/inbound byte scanned, native SSL scanning

PageRisk™
Risk of each object computed inline, dynamically

NanoLog™
50:1 compression, real-time global log consolidation

PolicyNow™
Polices follow the user for Same on-premise, off-premise protection

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

facebook.com/zscaler
linkedin.com/groups/zscaler
twitter.com/zscaler
youtube.com/zscaler
blog.zscaler.com