Simplify network transformation with Zscaler Cloud Firewall

More powerful than an NGFW,
without the cost and complexity

Network security is becoming irrelevant

> “Eighty-four percent [of organizations] say traditional security solutions either don’t work at all in cloud environments or have only limited functionality.”[1]
>
> *—2018 Cloud Security Report, Cybersecurity INSIDERS*

Applications have moved out of the data center and into the cloud

Users have moved off the corporate network and are connecting from everywhere

So why is your firewall still sitting in your data center?

It’s time to rethink your network and security

OLD WORLD	THE CHALLENGE
On-premises next-generation firewall in the data center	Can’t follow off-network users; easily overwhelmed by the connection demands of cloud and SSL inspection requirements
Hub-and-spoke: backhauling traffic to the centralized firewall	MPLS adds cost and increases latency, which ultimately degrades the user experience
Castle-and-moat security	Security perimeters are too rigid to follow today’s user, and forcing users back onto the network degrades the cloud experience

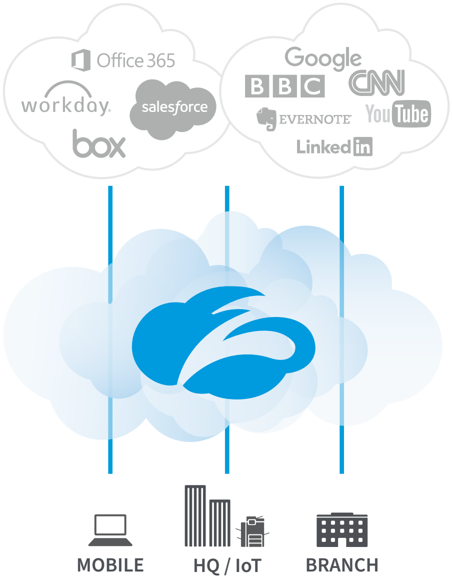
[1] https://www.cybersecurity-insiders.com/portfolio/download-cloud-security-report/

The cloud is exposing firewall limitations

To give users fast and secure access to cloud apps, many organizations are turning to local internet breakouts. But, what is the best way to secure these direct-to-internet connections? Today's firewall options simply can't meet the requirements organizations need.

	Local internet breakouts with firewalls or UTMs at every branch	Local internet breakouts with virtualized firewalls
Performance	• Cloud apps require a high volume of long-lived connections that can overwhelm firewalls	• Not designed for the high throughput rates required to meet today's cloud app demands
Management	• Policy and change control management across distributed appliances increases complexity	• Managing the VNF lifecycle adds complexity to already complex policy management requirements
SSL inspection	• Inspecting SSL traffic significantly erodes performance • Certificate management across distributed appliances is far too complex	• Inspecting SSL erodes performance and is limited by shared and finite CPU, storage, and memory resources
Security policy	• Deploying different firewall sizes and models in branches results in inconsistent security and policies	• Deploying different virtual firewall sizes and models to save costs results in inconsistent security and policies
Cost	• Deploying stacks of security appliances or firewalls at every branch is prohibitively expensive • Traffic growth and increasing demands require hardware refreshes	• Cost increases as bandwidth grows and may also require expensive upgrades of the underlying physical hardware

Secure your users with Zscaler Cloud Firewall



With Zscaler Cloud Firewall, you can say good-bye to expensive, difficult- to-manage appliances. Our comprehensive, fully cloud-delivered firewall enables faster performance and consistent security across all users in your organization.

Zscaler Cloud Firewall advantages

Consistent performance and elastic scale

Provides security and access controls across all ports and protocols and scales services to handle cloud application traffic with long-lived connections

SSL inspection at scale

Natively intercepts and inspects SSL/TLS-encrypted traffic at scale, and seamlessly manages certificates for all applications

Reduced cost and complexity

Reduces MPLS backhauling spend, and minimizes costly and time-consuming management of patches, outage windows, and policies

Increased visibility and simplified management

Delivers real-time visibility and logs every session—all users, locations, applications, ports, and protocols—from a single console

Brings the entire security stack close to the user

Delivers firewall-as-a-service for internet and cloud-bound traffic on all ports, and ensures identical protection wherever users connect

Fast and secure user experience

Allows internet and cloud-bound traffic to be routed locally and securely to deliver a fast user experience—without expensive hardware

What sets Zscaler Cloud Firewall apart?

Proxy-based architecture

- Dynamically inspects traffic for all users, applications, devices, and locations
- Natively inspects SSL/TLS traffic—at scale—to detect malware hidden in encrypted traffic
- Enables granular firewall policies based upon user, location, and application

Cloud IPS

- Delivers always-on IPS threat protection and coverage, regardless of user connection or location
- Inspects all user traffic on and off network, to restore full visibility into user, app, and internet connections

DNS security and controls

- Protects users from reaching malicious domains as the first line of defense
- Optimizes DNS resolution to improve user experience and app performance
- Provides granular controls to detect and prevent DNS tunneling

Increased visibility and simplified management

- Provides real-time visibility and control and delivers immediate policy enforcement across the platform from a single console
- Logs every session in detail
- Uses advanced analytics to correlate events and provide threat insights for all users, apps, and locations

A full-featured firewall

Contextual awareness provides a richer understanding of threats

Zscaler Cloud Firewall provides contextual awareness that goes far beyond applications, users, and locations. Our proxy-based firewall architecture also provides a deeper understanding of ports and protocols, along with security analysis and predictive capabilities.

Zscaler Cloud Firewall:

- Intercepts DNS requests to bad domains to prevent users from accessing malicious content
- Identifies and prevents polymorphic malware attacks with Cloud IPS
- Analyzes native FTP and FTP-over-HTTP traffic for data exfiltration, applies data loss prevention policies, and detonates files in a sandbox to detect malicious code

Unique features:

- **Standard next-gen firewall policies:** Deep packet inspection (DPI) engine for granular allow/block policies by application
- **Deep context awareness:** Access and security policies based on user identity, application awareness, and location
- **Fully qualified domain name policies:** Easy to configure and manage access policies for cloud and SaaS applications
- **Application usage visibility:** Real-time visibility into traffic usage, threats, and applications
- **Fully integrated security services:** Contextual information shared across all services for stronger protection

A cloud firewall for customers of all sizes and needs

AutoNation

AutoNation: The largest U.S. automobile retailer uses Zscaler to provide the internet accessibility needed for retail business, while ensuring that strong, standardized security controls are enforced across 300+ locations.

“ Prior to having a cloud-based security platform like Zscaler, we were stuck with those little stacks of iron everywhere we wanted to protect an internet point of presence. That’s not the case anymore, and, hopefully, it will never be the case again.”

Ken Athanasiou
Chief Information Security Officer
AutoNation

salmat

Salmat: With Zscaler, the Australia-based marketing services firm eliminated web proxies and multiple firewalls in different locations with different configurations and achieved consistent security and increased visibility.

“ With Zscaler, we will still have a consistent proxy and firewall, regardless of what we’re breaking out…Zscaler is a foundational component that will facilitate our cloud initiatives without compromising security. Zscaler is key to our upcoming network transformation as we continue to execute on our cloud-first strategy.”

Dave Glover
Chief Technology Officer
Salmat

Transform to the cloud with Zscaler if you want to:

- Improve security while eliminating the cost and complexity of appliances
- Deliver a fast user experience with secure local internet breakouts
- Secure SD-WAN deployments and minimize MPLS costs
- Migrate to Office 365 and other cloud applications
- Provide identical protection for users everywhere they connect

zscaler.com/firewall