Zscaler Cloud Firewall
Secure, adaptive zero trust protection for all internet traffic

Zscaler Cloud Firewall protects internet traffic for all users, applications, and locations.

The world of work is now distributed and mobile. Applications are migrating from data centers to the cloud, while new digital workloads are increasingly being deployed natively in the cloud. Moreover, users working from various locations, including home offices, shared workspaces, branch offices, and remotely, access business applications directly from the internet.

This has resulted in users and cloud applications producing high volumes of traffic. Unable to handle the additional bandwidth from backhauling users’ internet- and SaaS-bound traffic, traditional network-centric security rules impact productivity and create connectivity bottlenecks. While virtual firewalls try to bandage the situation, they are limited to cloud providers’ physical locations and often require devoted company resources to properly administer. To add fuel to the fire, bad actors are using encryption and non-standard ports to evade detection and elicit an attack on victims’ networks.

Benefits of Zscaler Cloud Firewall:

- **Full protection for work-from-anywhere users.** Dynamic risk-based security policies follow your users everywhere without a complex matrix of policy and network configurations.

- **Complete inspection to find hidden attacks.** Unlimited inline traffic inspection and native SSL decryption terminate malicious connections and prevent threats.

- **Catch evasive web traffic on non-standard ports.** Quickly identify and intercept evasive and encrypted cyberthreats hiding in traffic on non-standard ports.

- **Cloud-delivered local internet breakouts.** Fast and secure direct-to-internet connections for all hybrid and branch traffic scale elastically and improve user experience.

- **Always-on cloud intrusion prevention system (IPS).** Adaptive behavioral IPS signatures, managed by Zscaler ThreatLabz, work in real time and are easy to share to enrich SecOps workflows.

- **Secure DNS without compromised performance.** Localized resolutions sustain superior performance while your users and endpoints stay safe from malicious sites and DNS tunneling.

- **Cloud-delivered protection with global edge presence.** Zscaler Cloud Firewall provides unmatched security and user experience, fully integrated with Zscaler Internet Access™ and part of the Zscaler Zero Trust Exchange™.
To fully inspect SSL-encrypted traffic and traffic traversing non-standard ports and protocols, network and security teams often sacrifice performance and speed.

This becomes an issue as physical firewalls can quickly hit capacity limits, unable to fully inspect SSL-encrypted traffic or non-standard ports and protocols without additional resources affecting performance. While virtual firewalls are limited to cloud providers’ physical locations and often require devoted company resources to properly administer.

**Zscaler Cloud Firewall**

To improve connectivity and availability, organizations must securely direct user traffic using local internet breakout without backhauling via VPNs and without duplicating the security appliance stack at each location. **Zscaler Cloud Firewall** allows internet traffic to break out locally and securely for all ports and protocols.

By routing internet- and SaaS-bound connections to Zscaler, cloud-gen firewall natively inspects all user traffic, including SSL encrypted traffic, elastically scaling to handle high volumes of long-lived connections.

Without hardware refreshes and software updates, the responsibility of updates, upgrades, and patches, including scalability requirements, for the cloud-based firewall falls on Zscaler. By removing complex matrices of policy and network configurations that are tied to physical locations, firewall policy management is radically simplified.

With adaptive, risk-based policies that follow your users everywhere on and off the corporate network, Zscaler Cloud Firewall provides consistent protection regardless of device or where they connect.

As part of a firewall functionality, Zscaler Cloud Firewall logs every session to provide visibility across all users and locations, ensuring you have access to information you need, exactly when you need it.

---

**Zero trust with cloud-gen firewall**

**Legacy Firewall Zone-based Architecture**

- Broad network access
- Enterprise branch or site
- Trust Zone: A misnomer
- Un-trust zone
- DMZ Zone: Also untrusted
- Lateral movement

**Zscaler Zero Trust Platform**

- Google
- Exchange
- Factory
- Data center
- Customers
- Workforce
- IoT
- Factory
- OT
- Zero Trust
By transforming your hybrid and branch connections and addressing performance security needs today, Zscaler supports and scales to meet your cloud transformation needs, including moving to cloud-based applications such as Office 365.

**Cloud-gen firewall benefits**

Purpose-built for today’s digital world, Zscaler Cloud Firewall ensures you can securely access the internet and handle all web and non-web traffic, across all ports and protocols, with infinite elastic scalability and unbeatable performance. Your users get consistent protection no matter what device they’re using or where they are—at home, HQ or branch offices, or on the road—without the cost, complexity, and performance limitations of traditional network security and next-generation firewall appliances.

**Powered by an adaptive zero trust platform**

Stop compromising for static inspections, performance degradation, and capacity limits from physical firewall appliances. Built on a fully integrated, cloud-native platform, Zscaler Cloud Firewall elastically scales to handle cloud application traffic requiring long-lived connections while natively intercepting and inspecting SSL/TLS traffic—at scale—to detect malware hidden in encrypted traffic.

**Transformative hybrid and branch connections**

Evolve from costly and network-centric infrastructure to true cloud-delivered local internet breakouts. Route internet traffic locally to provide direct-to-cloud connections for consistently fast connections while delivering security and access controls for all ports and protocols. Without the need for any appliances to deploy or manage, this reduces MPLS backhauling costs and eliminates expensive and time-consuming patch management, coordination of outage windows, and policy management.

**Ubiquitous security for modern workforces**

Leverage real-time security updates informed by 300 trillion daily signals and shared across the entire cloud each day for identical protection on any device wherever users connect—from home offices, shared workspaces, branch offices, or on the road. By bringing the entire security stack close to the user, they experience unparalleled user- and app-aware threat protection with dynamic, follow-me policies on and off the corporate network.
Always-on, blocking of known malicious attacks
Go where traditional solutions could not be applied with a cloud-delivered, context-aware intrusion prevention system (IPS) threat protection managed by Zscaler ThreatLabz. Through unlimited, inline traffic inspection, including IOT/OT and encrypted traffic on and off the network, behavioral IPS signatures are applied in real-time when accessing thousands of web and non-web applications regardless of connection type or location.

Optimize DNS for performance and security
Achieve faster resolution by pairing geographically local apps, driving better user experience and cloud app performance while implementing domain name system (DNS) security and control policies. This protects users from reaching malicious domains and prevents DNS tunneling. By delivering DNS-as-a-service, Zscaler minimizes latency and secures local internet breakouts using full proxies for all DNS traffic and leverage machine learning to detect and block data exfiltration tunnel activity.

Cloud-gen Firewall Core Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized policy management</td>
<td>Define and immediately enforce policies across all locations without the need to recreate policies for each location</td>
</tr>
<tr>
<td>Fully-integrated security services</td>
<td>Contextual information is shared across DLP, APT, sandbox, and other services to provide better protection and deeper visibility</td>
</tr>
<tr>
<td>Real-time granular control, logging,</td>
<td>Forensically rich logging for detailed visibility with globally unified and unlimited logging for six months, enabling analysis and correlation for trend discovery, productivity analysis, and troubleshooting</td>
</tr>
<tr>
<td>and visibility</td>
<td></td>
</tr>
<tr>
<td>User-aware threat protection</td>
<td>Define users by Groups, Departments, or Locations, including setting work-from-home or remote users as a location, and integrate with identity providers and local user databases, allowing consistent policies regardless of users’ physical location</td>
</tr>
</tbody>
</table>
## Cloud-gen Firewall Core Features (cont.)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>App-aware threat protection</strong></td>
<td>Identify and classify application services at first packet to enable firewall filtering policy and forwarding policies, taking immediate and higher priority action with adaptive, context-aware policies</td>
</tr>
<tr>
<td></td>
<td>Supporting application types across all network services – ports and protocols, network applications – SNI (hostname), DPI-based, Application Services – UCaaS based on First Packet Identification, IP, FQDN groups and other heuristic-based detections</td>
</tr>
<tr>
<td><strong>Adaptive IPS security and control</strong></td>
<td>Deliver always-on, cloud-delivered threat protection with custom IPS signatures and thousands of adaptive and behavioral IPS signatures on any port and protocol regardless of connection type or location by inspecting all user internet traffic. View the list of all IPS signatures managed by ThreatLabZ.</td>
</tr>
<tr>
<td><strong>Advanced security inspection</strong></td>
<td>Apply advanced deep-packet inspection on non-web protocols, including FTP, DNS, RDP, Telnet, and more to identify and prevent evasive traffic on non-standard ports</td>
</tr>
<tr>
<td><strong>DNS security and control</strong></td>
<td>Optimize cloud application performance and minimize latency while ensuring uncompromised security by proxying all DNS through Zscaler. Enable policies based on user, app, location, and resolved IP country to automatically block users from malicious domains and detect and prevent DNS tunneling</td>
</tr>
<tr>
<td></td>
<td><strong>Resolution:</strong> DNS-as-a-service provides optimal resolution with localization, tenancy and lowest latency</td>
</tr>
<tr>
<td></td>
<td><strong>DNS Filtering:</strong> Create custom DNS filtering rules to block, allow or redirect different types of DNS requests against known and malicious destinations</td>
</tr>
<tr>
<td></td>
<td><strong>Security and Data Exfiltration:</strong> Detect malware, phishing, DNS tunneling and data exfiltration using ML</td>
</tr>
<tr>
<td></td>
<td><strong>DNS over HTTPS (DoH):</strong> Prevent DoH blindspots and bypassing of organizational controls when encrypting DNS connections in common HTTPs traffic</td>
</tr>
<tr>
<td><strong>Fully qualified domain name (FQDN) policies</strong></td>
<td>Easily configure and manage access policies for applications hosted across multiple IPs</td>
</tr>
<tr>
<td><strong>File transfer protocol (FTP) control and network address translation (NAT) support</strong></td>
<td>Support for access control of FTP and FTP over HTTP and support for NAT destination proxy and NAT forwarding</td>
</tr>
<tr>
<td><strong>Privacy and compliance certifications</strong></td>
<td>Compliant with rigorous global Commercial and Government risk, privacy, and compliance</td>
</tr>
<tr>
<td><strong>Industry and data privacy regulations</strong></td>
<td>Compliance adherence to industry-specific and in-country data privacy regulations</td>
</tr>
<tr>
<td><strong>Globally shared protection</strong></td>
<td>Leveraging the cloud effect, every time a new threat is identified in any of the tens of billions of requests processed daily by the Zscaler cloud, it gets blocked for all Zscaler users, everywhere</td>
</tr>
</tbody>
</table>
Zscaler Cloud Firewall is fully integrated with Zscaler Internet Access™ and part of the holistic Zero Trust Exchange

The Zscaler Zero Trust Exchange enables fast, secure connections and allows your employees to work from anywhere using the internet as the corporate network. Based on the zero trust principle of least-privileged access, it provides comprehensive security using context-based identity and policy enforcement.

How Zscaler delivers zero trust for users, workload, and OT
Deploy in weeks to enhance cyber protection and user experience

ZIA for Users and Workloads
Secure Internet/SaaS Access
- Cyber Threat Protection
  - AI driven inline content inspection (95L/TLS)
- Data Protection
  - Inline DLP and CASB, API CASB
- Local Internet Breakouts
  - Microsoft 365, SD-WAN

ZPA for Users and Workloads
Secure Private App Access
- Remote App Access without VPN
  - Workforce, third parties, B2B Customers
- Direct App Access (no backhaul)
  - Hybrid and multi-cloud environments
- Workload to workload Communication
  - Zero Trust access among apps/workloads

Zscaler Internet Access (ZIA)
Secure Internet/SaaS Access
- Fast, Secure
- Block the bad, protect the good
- ZPA App Protection
- Public Cloud
- Connect to apps, not the network
- Data Protection
- Inline DLP and CASB, API CASB
- Zscaler Private Access (ZPA)

Zscaler Digital Experience (ZDX)
Ensure a great user experience
- Any User, Any Device, Any App, Any Location
- External Apps
- ZPA App Protection
- ZPA for Users and Workloads
- Zscaler Internet Access (ZIA)
- Zscaler Private Access (ZPA)
- Zscaler Cloud Firewall
- Zero Trust Exchange
- ZIA for Users and Workloads
  - Secure Internet/SaaS Access
- Cyber Threat Protection
  - AI driven inline content inspection (95L/TLS)
- Data Protection
  - Inline DLP and CASB, API CASB
- Local Internet Breakouts
  - Microsoft 365, SD-WAN

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world’s largest inline cloud security platform.

Learn more at zscaler.com or follow us on Twitter @zscaler.