Zscaler Firewall

Secure, adaptive zero trust protection for web and non-web traffic. 100% cloud-delivered.

Zscaler Firewall protects internet traffic for all users, applications, and locations with the industry's most comprehensive cloud-native security service edge (SSE) platform.

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.

As a result, users and cloud applications are producing high volumes of traffic that is backhauled to traditional, network-centric security appliances, impacting productivity and creating connectivity bottlenecks while adding risks to the business. Without complete inspection of SSL-encrypted traffic, adversaries are using encryption and non-standard ports to evade detection and deliver stealthy attacks.

Virtualized firewalls attempt to bandage the situation, however they are architectured to extend your network outwards to cloud resources and feature the same capacity limitations.

Benefits of Zscaler Firewall:

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

- **Complete inspection to find hidden attacks.**
  Unlimited inline traffic inspection and native SSL decryption prevents stealthy threats and terminates malicious connections.

- **Catch evasive web traffic on non-standard ports.**
  Quickly identify and intercept evasive and encrypted cyberthreats using 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 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 Firewall provides unmatched security and user experience, fully integrated with Zscaler Internet Access™ and part of the Zscaler Zero Trust Exchange™.

To ensure interconnectivity and secure workloads, you'll still need devoted resources to properly administer or risk misconfigurations.

Zscaler Firewall

Zscaler Firewall delivers cloud-based protection for web and non-web traffic for all users and devices regardless of where they connect. Improve connectivity and availability by securely directing traffic using local internet breakout without backhauling via VPNs and without duplicating the security appliance stack at each location. Routing internet- and SaaS-bound connections to Zscaler ensures inspection of all user traffic, including SSL encrypted traffic, elastically scaling to handle high volumes of long-lived connections.

Easily meet regulatory standards while universally configuring, managing, and enforcing user- and

application-aware threat protection and risk-based policies to ensure network and application visibility with a centralized policy management console. As a firewall-as-a-service solution, the responsibility of updates, upgrades, and patches, including scalability requirements falls on Zscaler. This can provide significant cost savings by replacing appliances and removes complex matrices of policy and network configurations that are tied to physical locations.

Zscaler 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. By transforming your hybrid and branch connections and addressing performance and security needs today, Zscaler supports and scales to meet your cloud transformation needs, including moving to cloud-native applications such as Microsoft 365.

Zero trust with Zscaler Firewall

Legacy Firewall Zone-based Architecture
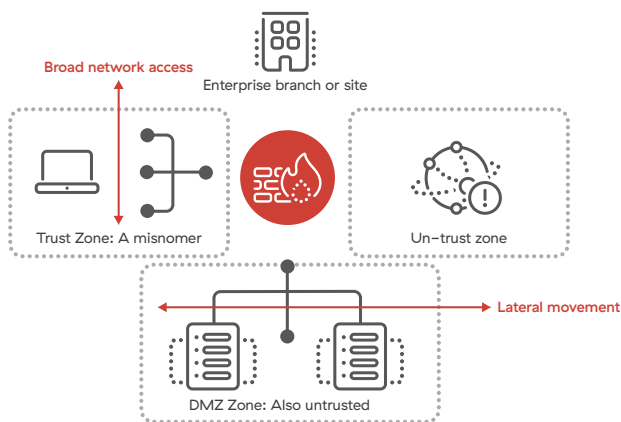
Zscaler Zero Trust Platform

Legacy firewalls and next-generation firewalls are unable to meet the Tenants of Zero Trust from NIST 800-207. Perimeter-based security architecture was not designed to inspect encrypted traffic at scale over unprotected networks and devices. The lack of strict user authentication and continual policy checks at each step could result in a compromised server or device allowing attackers broad network access and unwanted lateral movement. Additionally, using a legacy firewall as a gateway to deploy a virtual private network (VPN) exposes your public and private networks. Only a cloud-delivered firewall on a true zero trust platform can deliver dynamic, least privileged access to drive network and security transformation.

Benefits from a cloud native firewall

Purpose-built for today's digital world, Zscaler 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 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.

Gartner.

Zscaler named a Leader in Gartner's SSE MQ, positioned highest in Ability to Execute.

Learn More →

Ubiquitous security for modern workforces

Leverage real–time security updates informed by 3OO trillion daily signals and shared across the entire cloud each day for identical protection on any device wherever users connect. 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. With SSL inspection at scale, gain back visibility and stop attackers from abusing DNS–over–HTTPS (DoH), better protecting users and employees from reaching malicious domains and bypassing enterprise policies. By delivering DNS–as–a–service, Zscaler minimizes latency and secures local internet breakouts using full proxies for all DNS traffic and leverages machine learning to detect and block data exfiltration tunnel activity.

Easy–to–understand policy management

Universally define, deploy, and immediately enforce policies for all users, across all locations from a single console. In place of complex matrices of policy, network configurations and recreating policies for each location of typical firewalls, cloud–delivered firewall simplifies policy management by centralizing granular firewall rules based upon user, application, location, group, and department. Additionally, administrators can send forensically complete logs enriched with user details, request, responses, services used, and more to SIEM and XDR tools to enhance security investigation and incident response.

Zscaler Firewall Core Features

Centralized policy management	Define and immediately enforce policies across all locations without the need to recreate policies for each location
Fully–integrated security services	Contextual information is shared across DLP, APT, sandbox, and other services to provide better protection and deeper visibility
Real–time granular control, logging, and visibility	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
User–aware threat protection	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

Zscaler Firewall Core Features (cont.)

App-aware threat protection	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 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
Adaptive IPS security and control	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.
Advanced security inspection	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
DNS security and control	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 **Resolution:** DNS-as-a-service provides optimal resolution with localization, tenancy and lowest latency **DNS Filtering:** Create custom DNS filtering rules to block, allow or redirect different types of DNS requests against known and malicious destinations **Security and Data Exfiltration:** Detect malware, phishing, DNS tunneling and data exfiltration using ML **DNS over HTTPS (DoH):** Prevent DoH blindspots and bypassing of organizational controls when encrypting DNS connections in common HTTPs traffic
Fully qualified domain name (FQDN) policies	Easily configure and manage access policies for applications hosted across multiple IPs
File transfer protocol (FTP) control and network address translation (NAT) support	Support for access control of FTP and FTP over HTTP and support for NAT destination proxy and NAT forwarding
Privacy and compliance certifications	Compliant with rigorous global Commercial and Government risk, privacy, and compliance
Industry and data privacy regulations	Compliance adherence to industry-specific and in-country data privacy regulations
Globally shared protection	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

As a fully integrated part of Zscaler Internet Access, Zscaler Firewall is included in ZIA and Zscaler for Users Essentials and Business editions. Advanced features of Zscaler Firewall are included in ZIA and Zscaler for Users Transformation and Unlimited editions, as well as an add-on module to Essentials and Business editions.
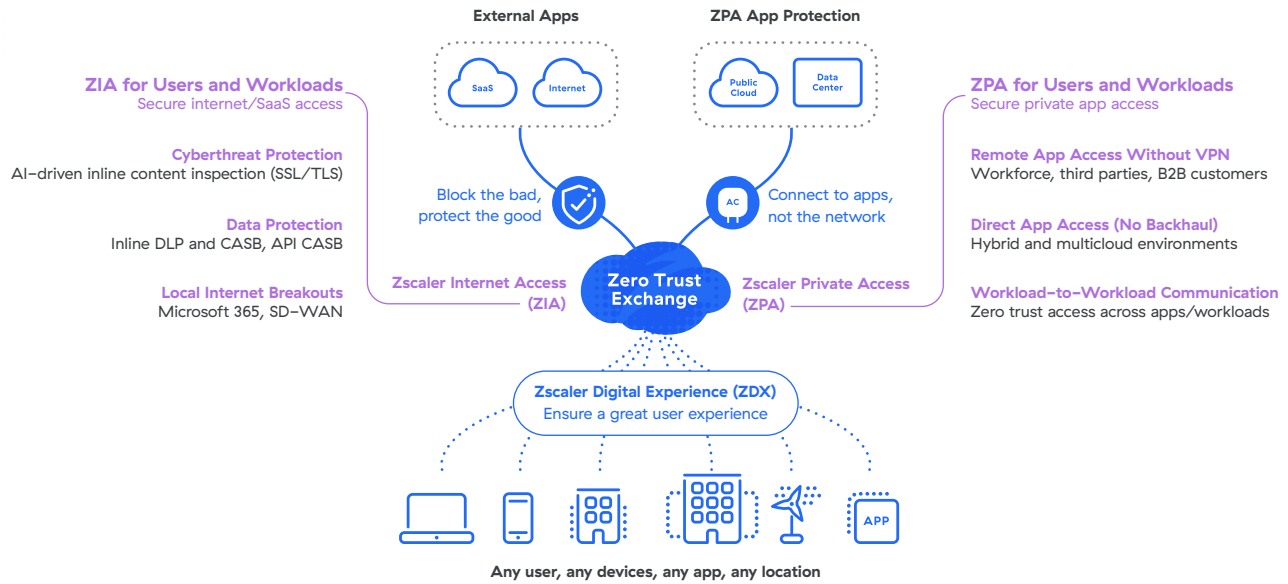
	Standard	Advanced
Firewall Policy Criteria:		
Network and Application Services		✓
FQDN Filtering	✓ Up to 10 rules	✓
Location Awareness		✓
User Awareness	—	✓
Application Awareness	—	✓
Dynamic Risk–Based Policy	—	✓ Available only with ZIA Transformation & Unlimited Zscaler for Users Transformation & Unlimited editions
DNS Control:		
Trusted DNS Resolver	✓	✓
DNS Filtering & Security	✓ Up to 64 rules	✓
DNS Tunnel and App Detection	—	✓
IPS Control	—	✓
FTP Control	✓	✓
NAT Control	✓	✓
Platform Features:		
Full SSL Inspection	✓	✓
Real–time Logging	✓ Aggregate and blocked Firewall logs & full DNS logs	✓ All logs, including client connector bypass logs
	Included with ZIA Essentials, ZIA Business, and Zscaler for Users Business editions	Included with ZIA Transformation, ZIA Unlimited, Zscaler for Users Transformation & Unlimited editions, or as a standalone add-on module

ZPA is 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, workloads, and IIoT/OT

Deploy in weeks to enhance cyber protection and user experience

External Apps
SaaS · Internet

ZPA App Protection
Public Cloud · Data Center

ZIA for Users and Workloads
Secure internet/SaaS access

Cyberthreat Protection
AI-driven inline content inspection (SSL/TLS)

Data Protection
Inline DLP and CASB, API CASB

Local Internet Breakouts
Microsoft 365, SD-WAN

Block the bad, protect the good

Zscaler Internet Access (ZIA)

Zero Trust Exchange

Connect to apps, not the network

Zscaler Private Access (ZPA)

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 multicloud environments

Workload-to-Workload Communication
Zero trust access across apps/workloads

Zscaler Digital Experience (ZDX)
Ensure a great user experience

APP

Any user, any devices, any app, any location