Zscaler Zero Trust Firewall

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

DATA SHEET

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

Today's workforce is mobile, and applications live in the cloud. Users connect from anywhere—home, branch or remote—and access applications directly via the internet. Meanwhile, cloud workloads are scaling fast, shifting traffic away from traditional data centers.

Legacy and virtual firewalls, however, are not built for this transformation. They lack the ability to fully inspect encrypted traffic, struggle to identify applications using non-standard ports, and fail to secure non-web traffic that is critical to business operations. As a result, attackers exploit these blind spots to bypass detection and launch sophisticated threats. Virtualizing legacy appliances only moves the bottleneck—it doesn't solve the problem. Organizations need a modern, cloud-delivered security approach built for the scale, agility, and full traffic inspection demands of today's cloud-first environments.

Zscaler Zero Trust Firewall

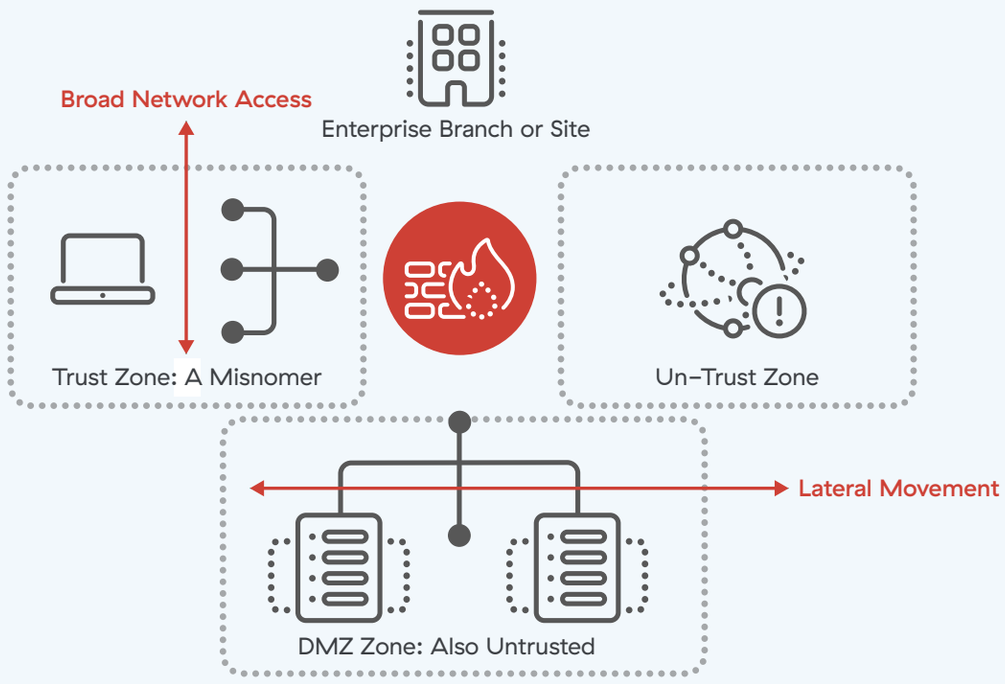
Zscaler Zero Trust Firewall delivers cloud-based protection for non-web traffic (DNS, FTP, RDP, SSH, Telnet and more), while Zscaler Internet Access (ZIA) delivers deep inspection for web traffic (HTTP/HTTPS). Together, they secure all ports and protocols including non-web applications and non-standard web, across all users, devices and locations. Zero Trust Firewall improves connectivity and performance by enabling local internet breakout—eliminating the need for VPN backhauling or redundant on-premises appliance stacks.

Zero Trust Firewall helps organizations 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 true firewall-as-a-service (FWaaS) solution—built from the ground up for the cloud—Zscaler Zero Trust Firewall eliminates the need for hardware provisioning or managed service models, delivering elastic scale and policy control without legacy limitations. 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 Zero Trust Firewall provides forensically complete logs for every session, capturing detailed attributes such as user identity, device info, source and destination IPs, port, country, threat category, and more. This rich visibility across all users, devices, and locations eliminates the need for packet capture tools and ensures organizations have access to the right information at the right time.

Move beyond legacy architecture with Zscaler Zero Trust Firewall

Legacy Firewall Zone–Based Architecture



Zscaler Zero Trust Platform

Legacy firewalls and next–generation firewalls are unable to meet the tenets 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 Zero Trust Firewall 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 Zero Trust 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 Zero Trust Firewall elastically scales to handle cloud application traffic requiring long–lived connections while natively intercepting and inspecting TLS/SSL 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 500+ trillion daily signals and shared across the entire cloud each day for identical protection on any device wherever users connect. Bringing the entire security stack close to the user provides 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 can't with a cloud-delivered intrusion prevention system (IPS) managed by Zscaler ThreatLabz. Through unlimited inline traffic inspection, including IoT/OT and encrypted traffic, behavioral IPS signatures are applied in real time across thousands of web and non-web applications. With Cloud Custom IPS, organizations gain greater control by writing and enforcing their own Snort-based rules tailored to unique threats, applications, or compliance needs.

DNS OPTIMIZATION 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 TLS/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, Zero Trust 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.

ENFORCE PRECISE POLICIES WITH PROCESS-LEVEL AWARENESS

Extend Firewall, DNS, and IPS controls beyond IPs and ports by identifying the actual application process running on the device – such as PowerShell.exe or Chrome.exe. This enables security teams to block or allow activity based on the true source of the connection, reducing false positives, enhancing threat detection, and allowing more targeted risk response.

Unlike traditional firewalls, Zscaler Zero Trust Firewall adds critical context with Endpoint App Control – especially for detecting insider threats, command-and-control activity, and process-specific exploits – aligning enforcement tightly with user behavior and device posture.

Zscaler Zero Trust 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	Share contextual information across DLP, APT, sandbox, and other services to provide better protection and deeper visibility
Real-time granular control, logging, and visibility	Maintain 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 locations
Endpoint App Control	Define and enforce policies based on the actual application process running on the device, such as PowerShell or Chrome, enabling more precise control, reducing false positives, and providing stronger protection against targeted threats and insider activity
App-aware threat protection	Supports a wide range of application types: • All network services – ports and protocols • Network applications identified by SNI (hostname) and Deep Packet Inspection (DPI) • Application Services such as UCaaS, using First Packet Identification, IP address, FQDN groups, and other heuristic-based detection methods
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

Adaptive IPS security with custom rules	Deliver always-on threat prevention with a cloud-delivered IPS engine powered by thousands of adaptive, behavioral, and context-aware signatures managed by Zscaler ThreatLabz. Gain additional control with Cloud Custom IPS, allowing you to define and enforce Snort-based rules tailored to specific applications, threats or compliance needs. View the list of all IPS signatures managed by ThreatLabz.
End user notifications (EUN)	Communicate security policy actions to end users through desktop pop-ups via Client Connector for Firewall, DNS, and IPS, or browser-based messages for DNS blocks with web EUN, helping users understand why access was denied and reducing IT support queries
Granular role-based access control (RBAC)	Create and assign custom admin roles—such as SecOps or NetOps—with controls over who can view, edit, or manage security policies, logs, and alerts to enhance operational clarity and enforce least-privileged access across teams

BENEFITS OF ZSCALER ZERO TRUST 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 TLS/SSL inspection prevent stealthy threats and terminate malicious connections.
- **Catch evasive web traffic on non-standard ports.** Quickly identify and intercept evasive and encrypted cyberthreats using non-standard ports.
- **Always-on cloud intrusion prevention system (IPS).** Adaptive behavioral IPS signatures, managed by Zscaler ThreatLabz, work in real time to enrich SecOps workflows. With Cloud Custom IPS, organizations can write and deploy their own Snort-based signatures tailored to their unique applications, threat models, or compliance needs.
- **Secure DNS with optional resolution.** Zscaler inspects all DNS traffic—standard or encrypted—regardless of the user, device, or type of DNS service. Optional DNS resolution enhances security and performance while simplifying vendor consolidation.
- **Cloud-delivered protection with global edge presence.** Zscaler Zero Trust Firewall provides unmatched security and user experience, fully integrated with Zscaler Internet Access™ and part of the Zscaler Zero Trust Exchange™.
- **Process-level precision with Endpoint App control.** Enforce Firewall, DNS, and IPS policies not only on traditional network attributes (e.g., IP, port, protocol), but also on the actual application process running on the endpoint, such as PowerShell.exe or Chrome.exe.

Zscaler Zero Trust Firewall Core Features (cont.)

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 AI • **DNS over HTTPS (DoH):** Prevent DoH blind spots 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 access control of FTP and FTP over HTTP and support for NAT destination proxy and NAT forwarding
Privacy and compliance certifications	Comply with rigorous global commercial and government risk, privacy, and compliance
Industry and data privacy regulations	Adhere to industry-specific and in-country data privacy regulations
Globally shared protection	**Leverage 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, Zero Trust Firewall (Standard) is included with both Essentials Platform (ZS-ESS-PLATFORM) and Zscaler Platform (ZS-PLATFORM) licenses.

To enable Advanced features, customers must add the ZIA-FIREWALL license (ZS-CTP-1). This provides capabilities like 1,000+ Firewall/DNS rules, Endpoint App control, user-identity policy controls, IPS security with custom rules, DNS tunnel protection, and more.

To begin using Advanced features, organizations need at least the Essentials Platform + ZIA-FIREWALL (ZS-CTP-1) license.

Existing customers (with older non-platform SKUs) can upgrade to Advanced Firewall by simply adding the ZIA-FIREWALL license.

	Standard	Advanced
ZERO TRUST FIREWALL POLICY CRITERIA		
Network and Application Services	✓ Up to 10 rules	✓
Source/Dest L3/4 and FQDN-based policies		✓
Location Awareness		✓
User Awareness	–	✓
Network Application (DPI)	–	✓
Dynamic Risk-Based Policy	–	✓
Firewall Rules	✓ Up to 10 rules	✓ Up to 1,000+ rules
Granular Role-Based Access Control (RBAC)	✓	✓
End User Notifications (EUN)	✓ Web notifications for any DNS action	✓ ZCC notifications for any Firewall, DNS and IPS action
Endpoint App Control for process precision	–	✓
DNS CONTROL		
Trusted DNS Resolver	✓	✓
DNS Filtering and Security	✓ Up to 64 rules	✓
DNS Tunnel and App Detection	–	✓

IPS CONTROL WITH CUSTOM RULES	–	✓
FTP CONTROL	✓	✓
NAT CONTROL	✓	✓
PLATFORM FEATURES		
Full SSL Inspection	✓	✓
Real-time Logging	✓ Aggregated logging details for allow firewall actions and detailed logging details for block actions with full DNS logs	✓ All logs for all actions and all functions including user ID, App ID, IPS, and more
	Included with Essentials Platform (ZS-ESS-PLATFORM) or Zscaler Platform (ZS-PLATFORM) license	Requires ZIA-FIREWALL add-on license (ZS-CTP-1)

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 160 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Zero Trust Everywhere