Datenblatt

Zscaler Cloud Firewall

Zuverlässiger adaptiver Zero-Trust-Schutz für den gesamten Internet-Traffic

Die Zscaler Cloud Firewall schützt den Internet-Traffic für alle User, Anwendungen und Standorte.

Der Trend zu zentralen und mobilen Arbeitskonzepten hält ungebrochen an. Anwendungen werden von Rechenzentren in die Cloud verlagert und neue digitale Workloads zunehmend nativ in der Cloud bereitgestellt. User, die an einer Vielzahl unterschiedlicher Standorte arbeiten — im Homeoffice, in Coworking-Büros, Zweigstellen oder unterwegs —, greifen direkt über das Internet auf Unternehmensanwendungen zu.

Mit der Anzahl der Remote-User und Cloud-basierten Anwendungen nimmt auch das Traffic-Volumen stetig zu. Der Versuch, den Internet- bzw. SaaS-Traffic durch Backhauling ins Rechenzentrum abzusichern und die zusätzliche Bandbreite mit herkömmlichen netzwerkzentrierten Sicherheitsrichtlinien zu bewältigen, führt unweigerlich zu Produktivitätsverlusten und verursacht Konnektivitätsengpässe. Virtuelle Firewalls bieten hier nur eine Behelfslösung, da sie an die physischen Standorte des jeweiligen Cloud-Anbieters gebunden sind und in vielen Fällen von eigens zuständigen Fachkräften verwaltet werden müssen. Erschwerend hinzu kommt, dass Bedrohungsakteure die Schutzmechanismen umgehen, indem Malware im verschlüsselten Traffic versteckt und über atypische Ports geleitet wird.

Vorteile der Zscaler Cloud Firewall:

- **Umfassender Schutz für dezentrale User.** Dynamische risikobasierte Sicherheitsrichtlinien schützen die User an jedem beliebigen Standort ohne komplexe Richtlinien- und Netzwerkkonfigurationen.
- **Vollständige Überprüfung zur Erkennung versteckter Bedrohungen.** Durch unbegrenzte Inline-Überprüfung des gesamten Traffics und native SSL-Entschlüsselung werden schädliche Verbindungen unterbrochen und Bedrohungen blockiert.
- **Abfangen von Ausweichmanövern über atypische Ports.** Umgehungsversuche, bei denen Cyberbedrohungen in verschlüsseltem Web-Traffic über atypische Ports versteckt werden, werden erkannt und abgefangen.
- **Cloud-basierte lokale Internet-Breakouts.** Für den gesamten hybriden und Zweigstellen-Traffic werden schnelle und sichere Direktverbindungen zum Internet bereitgestellt, die sich bedarfsgerecht skalieren lassen und eine verbesserte User Experience gewährleisten.
- **Ständig aktives Cloud-basiertes Eindringschutzsystem (IPS).** Adaptive verhaltensbezogene IPS-Signaturen werden von den Bedrohungsexperten von Zscaler ThreatLabz verwaltet und in Echtzeit einsatzfähig zur unkomplizierten Weitergabe bereitgestellt, um SecOps-Workflows zu optimieren.
- **Sicheres Domain Name System ohne Leistungseinbußen.** Die lokale DNS-Auflösung gewährleistet herausragende Performance und schützt User und Endgeräte zuverlässig vor schädlichen Domains und DNS-Tunneln.
- **Cloud-basierter Schutz mit globaler Edge-Präsenz.** Die Zscaler Cloud Firewall besticht durch unübertroffene Sicherheit und User Experience. Sie ist vollständig mit Zscaler Internet Access™ integriert und wird im Rahmen der Zscaler Zero Trust Exchange™ bereitgestellt.

Die vollständige Überprüfung des gesamten Traffics — einschließlich Traffic mit SSL-Verschlüsselung bzw. über atypische Ports und Protokolle — geht in vielen Fällen zu Lasten der Performance und Geschwindigkeit.

Das ist problematisch, zumal physische Firewalls schnell an ihre Kapazitätsgrenzen stoßen und zur Überprüfung des gesamten Traffics zusätzliche Ressourcen erforderlich sind, um Performance-Beeinträchtigungen zu vermeiden. Virtuelle Firewalls wiederum sind an die physischen Standorte des jeweiligen Cloud-Anbieters gebunden und müssen in vielen Fällen von eigens zuständigen Fachkräften verwaltet werden.

Zscaler Cloud Firewall

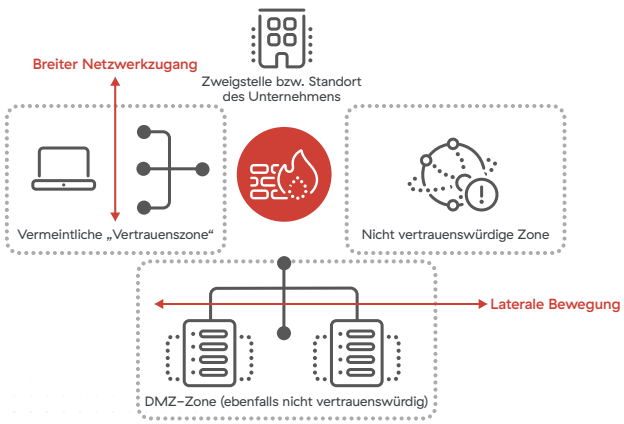
Zur Verbesserung der Konnektivität und Verfügbarkeit muss der User-Traffic sicher über lokale Internet-Breakouts geleitet werden — ohne Backhauling via VPNs und ohne Duplizieren des physischen Security-Stacks an jedem Standort. Die **Zscaler Cloud Firewall** ermöglicht sichere lokale Internet-Breakouts für alle Ports und Protokolle. Durch Routing sämtlicher Verbindungen zum Internet und zu SaaS-Anwendungen über Zscaler kann die Cloud-Generation Firewall den gesamten verschlüsselten und unverschlüsselten User-Traffic nativ überprüfen. Die Kapazitäten lassen sich bedarfsgerecht skalieren, damit permanente Verbindungen mit hohen Traffic-Volumen zuverlässig abgesichert sind.

Es sind weder Hardware-Aktualisierungen noch Software-Updates erforderlich. Zscaler übernimmt die Verantwortung für sämtliche anfallenden Updates, Upgrades und Patches sowie die bedarfsgerechte Skalierung der Cloud-basierten Firewall. Durch das Entfallen komplexer Richtlinien- und Netzwerkkonfigurationen, die an physische Standorte gebunden sind, wird die Verwaltung der Firewall-Richtlinien radikal vereinfacht. Mit adaptiven risikobasierten Richtlinien, die User innerhalb und außerhalb des Unternehmensnetzwerks gleichermaßen schützen, gewährleistet die Zscaler Cloud Firewall unabhängig von Gerät und Standort ein identisches Sicherheitsniveau.

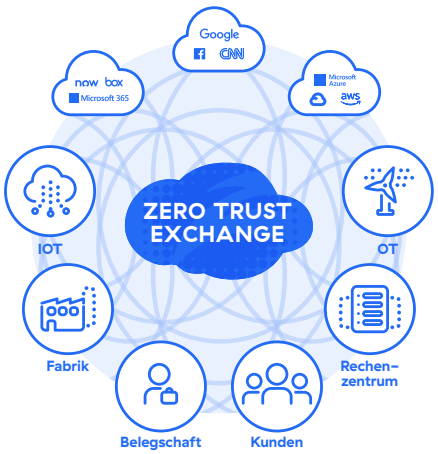
Die Protokollierung sämtlicher Sessions ist im Funktionsumfang der Zscaler Cloud Firewall inbegriffen. Dadurch erhalten Organisationen aussagekräftige Einblicke in die Aktivitäten aller User und Standorte und können bei Bedarf jederzeit auf alle benötigten Daten zugreifen.

Zero-Trust-Sicherheit mit Firewalls der Cloud-Generation

Legacy-Firewall mit zonenbasierter Architektur



Zscaler Zero Trust Platform



Zscaler unterstützt sämtliche Aspekte der Cloud-Transformation durch bedarfsgerechte Skalierung, zukunftsfähige Ansätze zur Gewährleistung sicherer und zuverlässiger Konnektivität für Zweigstellen und hybride Konzepte. So lassen sich Initiativen wie der Umstieg auf Microsoft 365 oder andere Cloud-basierte Anwendungen mühelos bewältigen.

Vorteile von Firewalls der Cloud-Generation

Die Zscaler Cloud Firewall wurde eigens für die Anforderungen einer digitalen Welt entwickelt. Sie gewährleistet standortunabhängig sicheren Zugriff auf das Internet und verarbeitet den gesamten Web- und sonstigen Traffic über alle Ports und Protokolle mit unbegrenzter bedarfsgerechter Skalierbarkeit und unschlagbarer Performance. Geräte- und standortunabhängig wird für sämtliche User — im Homeoffice, in der Unternehmenszentrale bzw. einer Zweigstelle oder auch unterwegs — ein identisches Schutzniveau gewährleistet. Die Kosten, Komplexität und Performance-Einschränkungen herkömmlicher Netzwerksicherheit und sogenannter Next-Generation Firewall-Appliances gehören der Vergangenheit an.

Basiert auf einer adaptiven Zero-Trust-Plattform
Mit der Zscaler Cloud Firewall entfallen statische Überprüfungen ebenso wie die Leistungseinbußen und Kapazitätsbeschränkungen physischer Firewall-Appliances. Sie basiert auf einer vollständig integrierten Cloud-nativen Plattform und lässt sich bedarfsgerecht skalieren, um permanente Verbindungen zu Cloud-Anwendungen zuverlässig abzusichern. Auch bei hohem Volumen wird der gesamte SSL/TLS-Traffic nativ abgefangen und auf darin versteckte Malware überprüft.

Zuverlässige Konnektivität für Zweigstellen und hybride Konzepte
Cloud-basierte lokale Internet-Breakouts statt kostspieliger netzwerkzentrierter Infrastruktur: Durch lokales Routing des Internet-Traffics werden konsistent schnelle Direktverbindungen zu Cloud-Anwendungen bereitgestellt sowie sämtliche Ports und Protokolle durch Zugriffskontrollen abgesichert. Da keine Appliances bereitgestellt und verwaltet werden müssen, werden die Kosten für MPLS-Backhauling reduziert. Auch der Kosten- und Finanzaufwand für Patch-Management, Koordinierung von Ausfallfenstern und Richtlinienverwaltung entfällt.

Standortunabhängige Sicherheit zum Schutz zukunftsfähiger Arbeitskonzepte
Mit der Zscaler Cloud Firewall profitieren Organisationen von Sicherheits-Updates in Echtzeit, die auf der Auswertung von 300 Billionen Signalen pro Tag basieren und täglich in der gesamten Cloud bereitgestellt werden. Dadurch lässt sich geräte- und standortunabhängig ein identisches Schutzniveau für alle User — im Homeoffice, in Coworking-Büros bzw. Zweigstellen oder unterwegs — gewährleisten. Durch Bereitstellung des Security-Stacks in unmittelbarer User-Nähe und dynamische

Richtlinien, die innerhalb und außerhalb des Unternehmensnetzwerks gelten, bietet die Zscaler Cloud Firewall einen unübertroffenen anwendungs- und benutzerbezogenen Bedrohungsschutz.

Blockierung bekannter Bedrohungen in Echtzeit
Das von Zscaler ThreatLabz verwaltete Cloud-basierte, kontextbezogene Eindringschutzsystem (IPS) bietet einen Bedrohungsschutz, der weit über die Möglichkeiten herkömmlicher Lösungen hinausgeht. Im Rahmen der unbegrenzten Inline-Überprüfung des gesamten Traffics — einschließlich IoT/OT- sowie verschlüsselten Traffics innerhalb und außerhalb des Netzwerks — werden verhaltensbezogene IPS-Signaturen in Echtzeit auf Verbindungen mit Tausenden von Web- und anderen Anwendungen angewandt, und zwar unabhängig vom Verbindungstyp und Standort.

DNS-Optimierung zur Verbesserung von Performance und Sicherheit
Durch Pairing von Anwendungen anhand geografischer Standorte und Implementierung von DNS-Sicherheitsrichtlinien (Domain Name System) und -Kontrollen werden User Experience und Performance von Cloud-Anwendungen verbessert und eine schnellere DNS-Auflösung gewährleistet. Dadurch werden DNS-Tunnel und Verbindungen zu schädlichen Domains verhindert. Durch die Bereitstellung von DNS-as-a-Service minimiert die Zscaler-Lösung Latenzen. Lokale Internet-Breakouts werden durch Einsatz von Proxies für den gesamten DNS-Traffic abgesichert. Zur Erkennung und Blockierung von Datenexfiltration/Tunneling werden maschinelle Lernalgorithmen eingesetzt.

Unkomplizierte Richtlinienverwaltung
Richtlinien können für sämtliche User und Standorte über eine zentrale Konsole definiert, implementiert und sofort durchgesetzt werden. Herkömmliche Firewalls machen komplexe Richtlinien und Netzwerkkonfigurationen erforderlich, die für jeden Standort einzeln eingerichtet werden müssen. Firewalls der Cloud-Generation vereinfachen die Richtlinienverwaltung erheblich, indem granulare Firewall-Regeln für einzelne User, Anwendungen, Standorte, Gruppen und Abteilungen zentral definiert werden. Zur Unterstützung von Vorfalluntersuchungen und -reaktionen besteht für Administratoren zudem die Möglichkeit, Protokolle mit vollständigen forensischen Daten zu Usern, Anfragen und Antworten, verwendeten Services usw. an SIEM- und XDR-Tools zu schicken.

Kernfunktionen von Firewalls der Cloud-Generation

Zentrale Richtlinienverwaltung	Richtlinien können für sämtliche Standorte definiert und sofort durchgesetzt werden, statt sie für jeden Standort einzeln einzurichten.
Vollständig integrierte Sicherheitsservices	Austausch kontextbezogener Informationen mit anderen Services wie unter anderem DLP, Sandbox und APT gewährleistet besseren Schutz und mehr Transparenz.
Granulare Kontrolle, Protokollierung und Transparenz in Echtzeit	Die global einheitliche unbegrenzte Protokollierung (für sechs Monate) mit Analytik und Korrelation liefert umfassende forensische Daten und Einblicke zur Unterstützung von Trenderkennung, Produktivitätsanalysen und Fehlerbehebung.
Benutzerbezogener Bedrohungsschutz	User können anhand von Gruppen, Abteilungen oder Standorten definiert werden, wobei auch die Kategorisierung von Homeoffice- bzw. Remote-Usern als Standort möglich ist. Durch Integration mit Anbietern für Identitätsprüfung und lokalen User-Datenbanken wird die konsistente Durchsetzung von Richtlinien unabhängig vom physischen Standort des betreffenden Users gewährleistet.

Kernfunktionen von Firewalls der Cloud-Generation (Forts.)

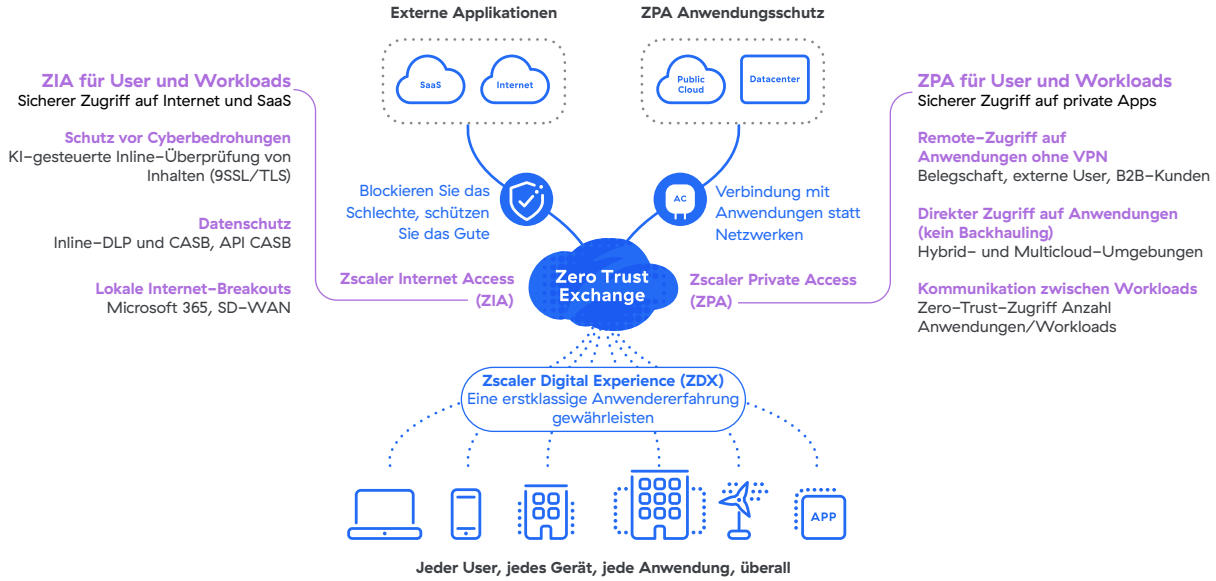
Anwendungsbezogener Bedrohungsschutz	Durch First Packet Identification und Klassifizierung von Anwendungsservices wird die Erstellung von Filter- und Weiterleitungsregeln für die Firewall unterstützt. Kontextbezogene Richtlinien ermöglichen die Priorisierung und sofortige Bearbeitung von Sicherheitsvorfällen. Es werden sämtliche Anwendungstypen und Netzwerkservices unterstützt: Ports und Protokolle, Netzwerk-Anwendungen — SNI (Hostname), DPI-basiert, Anwendungsservices —, UCaaS auf Basis von First Packet Identification, IP, FQDN-Gruppen und weitere heuristische Erkennungsmethoden.
Adaptive IPS-Sicherheit und -Kontrolle	Der gesamte Internet-Traffic aller User wird anhand unternehmensspezifisch definierter IPS-Signaturen sowie Tausender adaptiver und verhaltensbezogener IPS-Signaturen überprüft, um einen jederzeit aktiven Cloud-basierten Bedrohungsschutz für sämtliche Ports und Protokolle unabhängig vom Standort oder Verbindungstyp zu gewährleisten. Eine Liste aller von ThreatLabZ verwalteten IPS-Signaturen kann **hier** eingesehen werden.
Erweiterte Sicherheitsüberprüfung	Durch erweiterte Deep-Packet Inspection für Nicht-Web-Protokolle wie FTP, DNS, RDP und Telnet werden Ausweichversuche durch Routen des Traffics über atypische Ports erkannt und verhindert.
DNS-Sicherheit und -Kontrolle	Der gesamte DNS-Traffic fließt durch die Proxy-Architektur von Zscaler. Dadurch wird ohne jegliche Abstriche an der Sicherheit die Performance der Cloud-Anwendungen optimiert und die Latenz minimiert. Zur Erkennung und Verhinderung von DNS-Tunneln können Organisationen Richtlinien basierend auf User-Identität, Anwendung, Standort und aufgelöster IP-Adresse (nach Land) erstellen, sodass User aus schädlichen Domains automatisch blockiert werden. **Auflösung:** DNS-as-a-Service gewährleistet optimale Auflösung mit Lokalisierung, Instanzfähigkeit und minimaler Latenz **DNS-Filterung:** Basierend auf bekannten schädlichen Zielen können benutzerdefinierte DNS-Filterregeln zum Blockieren, Zulassen oder Umleiten verschiedener Typen von DNS-Anfragen erstellt werden. **Schutz vor Angriffen und Datenexfiltration:** Maschinelle Lernalgorithmen unterstützen die Erkennung von Malware, Phishing, DNS-Tunneln und Datenexfiltration. **DNS over HTTPS (DoH):** Beim Verschlüsseln von DNS-Verbindungen im allgemeinen HTTPS-Verkehr werden DoH-Transparenzlücken und Umgehung unternehmensspezifischer Kontrollmechanismen verhindert.
FQDN-Richtlinien (Fully Qualified Domain Name)	Für Anwendungen, die unter mehreren IPs gehostet werden, können Zugriffsrichtlinien einfach konfiguriert und verwaltet werden.
Unterstützung für FTP-Zugriffskontrollen und NAT	Die Zscaler Cloud Firewall unterstützt Zugriffskontrollen für FTP (File Transfer Protocol) und FTP over HTTP sowie NAT-Umleitung (Network Address Translation) und Portweiterleitung mit Proxy-Server.
Datenschutz- und Compliance-Zertifizierungen	Die Zscaler Cloud Firewall entspricht strengen weltweiten handelsrechtlichen und staatlichen Rahmenvorschriften in Bezug auf Risiko, Datenschutz und Compliance. CSA cloud security alliance · ISO 27001 · AICPA SOC 2 · FedRAMP · StateRAMP
Branchen- und Datenschutzvorschriften	Die Zscaler Cloud Firewall ist konform mit branchenspezifischen und nationalen Datenschutzvorschriften. PCI Security Standards Council · HIPAA · GDPR · NIST
Identischer Echtzeit-Schutz durch globalen Informationsaustausch	Der Cloud-Effekt macht es möglich: Jede neu entdeckte Bedrohung in einer der über zehn Milliarden täglichen Anfragen an die Zscaler-Cloud wird umgehend für alle Zscaler-User weltweit blockiert

Zscaler Cloud Firewall ist vollständig mit Zscaler Internet Access™ integriert und wird im Rahmen der ganzheitlichen Zero Trust Exchange bereitgestellt

Zscaler Zero Trust Exchange ermöglicht es Mitarbeitern, mit schnellen und sicheren Verbindungen von überall auf Anwendungen zuzugreifen, sodass das Internet effektiv als Unternehmensnetzwerk fungiert. Die Plattform beruht auf dem Zero-Trust-Prinzip der minimalen Rechtevergabe und gewährleistet ganzheitliche Sicherheit mithilfe einer kontextbasierten Identitäts- und Policy-Durchsetzung.

Zero Trust für User, Workloads und IIoT/OT — mit Zscaler

Bereitstellung innerhalb weniger Wochen zur Verbesserung der Cybersicherheit und Anwendererfahrung



zscaler™ | Experience your world, secured.™

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Benutzern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Weitere Informationen veröffentlichen wir unter **zscaler.de** oder auf Twitter unter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.de