# Zscaler Intrusionsschutz

zscaler™

IPS-Untersuchung ist zwar eine Schlüsselkomponente einer angemessenen tiefgreifenden Abwehrstrategie, ebenso wichtig ist es jedoch zu wissen, wie und wo sie innerhalb Ihrer Organisation umgesetzt werden sollte. In diesem Papier werden wir untersuchen, wofür IDS/IPS-Geräte konzipiert sind, wie sich ihre Fähigkeiten in Bezug auf ihre Hauptfunktion unterscheiden und wo ihre Funktionalität am besten eingesetzt wird. Wir werden auch das Angebot von Zscaler berücksichtigen, bei dem IPS-Fähigkeiten neben einer Reihe ergänzender Techniken wesentlicher Bestandteil der Advanced Persistent Threat Protection sind.

## IDS- und IPS-Funktionalität

Intrusion Detection-Systeme wurden entwickelt, um Traffic auf unautorisierte Netzwerkaktivitäten hin zu überwachen. Hierfür analysieren sie das Paket in seiner Gesamtheit, einschließlich Header und Nutzdaten, und vergleichen es mit den Signaturen bekannter Malware. Eine IDS-Appliance befindet sich in der Regel außerhalb des direkten Datenstroms und meldet erkannte schädliche Pakete, einschließlich:

- Schadcodes
- Botnetz
- Viren
- Gezielte Angriffe und Exploits
- Spyware
- Angriffe durch Cross=Site Scripting (XSS)
- SQL-Einspeisungen

...und andere

Ein richtig abgestimmtes Intrusion Detection System ist zwar von Vorteil, man sollte jedoch beachten, dass IDS-Technologie ein IT-Team bestenfalls auf ein Problem aufmerksam macht, es aber nicht verhindert. Ein Intrusion Prevention System hingegen kann schädliche Pakete erkennen und Maßnahmen ergreifen. Ein IPS ist dazu in der Lage, weil es inline, mit dem Netzwerk-Traffic selbst eingesetzt wird. IPS-Technologie kann schädlichen Traffic blockieren, indem sie die Verbindung zurücksetzt und sperrt oder Pakete verwirft. Da Pakete während der Verarbeitung durch das IPS weitergeleitet werden, muss die Erkennung in Echtzeit erfolgen, um Angriffe zu blockieren, bevor sie ihre anvisierten Opfer erreichen. Das IPS kann zudem Logs und Warnungen für Administratoren erzeugen.

Sowohl IDS als auch IPS befinden sich in der Regel hinter einer Firewall. Die Firewall analysiert Paket-Header und setzt Richtlinien auf Basis von 5-Tupel-Informationen durch, einschließlich Protokoll, Quell-/Zieladresse und Ausgangs-/Zielport. Wenn Traffic nach einem Firewall-Scan zugelassen wird, durchläuft er das IDS/IPS, welches das gesamte Paket und die Nutzdaten untersucht.

# Methoden der Advanced Threat Detection

## Auf Signatur basierte Erkennung (IPS)

Ein IPS erkennt schädlichen Traffic hauptsächlich anhand von Signaturen. Signaturen sind bestimmte Muster, die das Verursachen von Schwachstellen oder das Ausnutzen von Sicherheitslücken identifizieren. Signaturen repräsentieren Elemente einer Schwachstelle oder Malware, die bei einem Angriff auf das Netzwerk vorhanden sein müssen. Signaturen müssen spezifisch genug sein, um keinen Fehlalarm auszulösen und legitimen Traffic fälschlicherweise als schädlich zu identifizieren. Gleichzeitig müssen Signaturen aber auch breit genug gefasst sein, um Varianten eines bekannten Angriffs stoppen zu können und sicherzustellen, dass ein echter Angriff nicht durchkommt.

Netzwerk-Traffic wird analysiert und vorverarbeitet, um Signatur-basierte Erkennung effizienter und genauer zu machen. Bei HTTP beispielsweise können Signaturen auf bestimmte Header, auf entschlüsselten Inhalt oder auf Server-Anfragen und -Antworten angewendet werden. Der IPS-Anbieter muss Schwachstellen und Exploits überwachen und erforschen, um neue Signaturen zu schreiben. IPS-Anbieter aktualisieren ihre Signaturdatenbank normalerweise täglich.

## Erkennung von Anomalien (IPS)

Mit der zunehmenden Verbreitung von Intrusion Prevention-Systemen haben Angreifer Wege gefunden, Signatur-basierter Entdeckung auszuweichen. Wenn der Angreifer die Vorverarbeitung des Traffic unterbrechen kann, indem er Traffic erzeugt, der vom IPS inkorrekt analysiert, aber vom Ziel korrekt gehandhabt wird, werden Signaturen auf den falschen Teil des Netzwerk-Traffic angewendet und lösen möglicherweise keine Aktion des IPS aus. Zu den üblichen Ausweichtechniken gehören die Mehrfachkodierung der URL mittels ungewöhnlicher Leerzeichen zur Trennung von HTTP-Headern oder die Verwendung ungewohnter Kodierungstechniken (7-bitASCII). IPS-Technologie entdeckt Anomalien, um solche Ausweichtechniken zu verhindern. Anormaler Traffic kann dann markiert und inline blockiert werden.

## Verhaltensanalyse (Sandboxen)

Obwohl ein IPS eine starkes Verteidigungsmittel gegen eingehende Bedrohungen sein kann, haben Angreifer Wege gefunden, um nicht entdeckt zu werden. Indem er eine Datei zur Waffe macht und die Datei ständig leicht ändert, kann ein Hacker sowohl die Signatur als auch die auf Anomalie basierte IPS-Erkennung umgehen. Wenn die Datei mit den schädlichen Nutzdaten leicht verändert wird, ändert sich auch der daraus resultierende Filehash-Wert. Der Filehash-Wert beruht auf einer mathematischen Berechnung, die ein IPS verwendet, um zu bestätigen, dass die Datei bekannt ist und zuvor gesehen wurde. Die in der Sandbox-Technologie übliche Verhaltensanalyse kann das Verhalten einer Datei eingehend untersuchen, um festzustellen, ob das aus der Ausführung dieser Datei resultierende Verhalten für das Zielsystem schädlich sein wird. Wenngleich das Thema den Rahmen dieses Papiers überschreitet, sollten Sie Sandbox-Technologie unbedingt in Ihre Abwehrstrategie einbeziehen, um bestehende Sicherheitslücken zu schließen.

## Form folgt Funktion

Die Grundfunktionen von IDS/IPS werden zwar weitgehend genutzt, Art und Weise der Bereitstellung, Einsatzorte und Informationsauswertung können jedoch sehr unterschiedlich sein. Es gibt noch stets Anbieter „reiner" IDS/IPS-Einzellösungen, die in der Regel in Rechenzentren eingesetzt werden, um Server oder aggregierten Benutzer-Traffic zum Internet zu schützen. In vielen Fällen ist IDS/IPS-Technologie allerdings in anderen Produkten enthalten.

### Unified Threat Management Appliances

Eine der ersten Produktkategorien mit integrierter IDS/IPS-Funktionalität war Unified Threat Management (UTM), das Firewall, IDS/IPS-Funktionalität und Gateway-Antivirus in einer einzigen Appliance vereint. Gartner bezeichnet den UTM-Markt als multifunktionale Netzwerksicherheitsprodukte, die von kleinen oder mittleren Unternehmen verwendet werden[1].

Wenn Unternehmen Fernbüros oder Niederlassungen schützen wollen, denken sie oft zuerst an UTMs, da eine einzelne Appliance einigermaßen erschwinglich zu sein scheint. Leider kann der Schein trügen, und die Anschaffungskosten von UTM-Geräten für mehrere Niederlassungen können erschreckend hoch sein. Wenn Sie die Installation und Bereitstellung der Appliances, das Sicherstellen der Richtlinieninteraktion mit vor- und nachgeschalteten Geräten, die konsistente Richtliniendurchsetzung in den Niederlassungen, die Aktualisierung und Wartung sowie das anschließende Korrelieren von Logs für ein vollständiges, unternehmensweites Bild in die Kosten einbeziehen, wird selbst das preiswerteste Einzel-UTM extrem teuer.

### „Next-Generation" Appliances

IDS/IPS-Funktionalität wird häufig als Komponente einer Next Generation Firewall (NGFW) betrachtet. Obwohl der Begriff etwas nebulös bleibt, sind sich die meisten einig, dass eine NGFW ein Gerät ist, das Richtlinien unilateral durchsetzt und die Überprüfung mehr als nur die Informationen „traditioneller" Firewalls über die Header von Netzwerkdatenpaketen umfasst. NGFWs können vor den Servern des Unternehmens platziert werden, um vor unberechtigtem Zugriff auf Firmenwerte zu schützen. Sie sind besonders für das Rechenzentrum geeignet, wo eingehende oder interne Angriffe möglich sind. NGFW-Appliances können auch innerhalb des LAN eingerichtet werden, um Client und Server vor internen Angriffen zu schützen, und sie können an Ausgangspunkten platziert werden, um Benutzer zu schützen, die auf das Internet zugreifen. Da NGFW-Appliances jedoch alle Ports und Protokolle abdecken müssen, ist ihr Einsatz in Niederlassungen im Allgemeinen unnötig und definitiv zu kostspielig, weil der überwiegende Teil des Traffic in der Niederlassung aus HTTP/HTTPS besteht.

[1] Gartner Magic Quadrant for Unified Threat Management Devices

## Cloud-basierte Advanced Threat Protection von Zscaler

Wenngleich das Rechenzentrum ein zentraler Standort bleibt, der geschützt werden muss, können auch andere Standorte wie Fernbüros oder Niederlassungen eine Herausforderung darstellen. In den meisten Fällen besteht Traffic in Fernbüros/Niederlassungen überwiegend aus Web-Traffic, und die einzige scheinbar kostengünstige Verteidigung ist in der Regel ein UTM-System. Ein einzelnes Gerät mag zwar erschwinglich sein, aber die Duplizierung dieser Geräte in allen Niederlassungen ist es nicht. Infolgedessen verfügen viele Niederlassungen nur über unzureichende oder inkonsistente Intrusion Detection und Prevention. Außerdem wird der Traffic von Remote-Benutzern generell überhaupt nicht untersucht, es sei denn, er wird über Latenz verursachende VPN-Tunnel oder kostspielige MPLS-Verbindungen durch das IPS des Rechenzentrums geleitet. Hacker sind sich dieser Tatsache durchaus bewusst.

Es wird immer Gruppen geben, die auf die größten Organisationen abzielen, und sie wissen, dass sie dort auf die robusteste Abwehr treffen. Aber die größten Organisationen haben Niederlassungen und Fernbüros, und sobald ein Benutzer an einem dieser Standorte eine Phishing-E-Mail angeklickt oder unwissentlich Malware über einen Zero-Frame-Exploit auf sein Gerät heruntergeladen hat, findet der Hacker auf diesem Weg Zugang auch zum größten Unternehmen.

Zscaler ist die Antwort. Der Cloud-basierte Advanced Threat Protection-Engine von Zscaler kombiniert den besten IPS-Schutz mit einer Reihe anderer Funktionen wie Antivirus/Antimalware, Blacklisting und Sandboxen. Niederlassungsbüros und Remote-Benutzer senden ihren ausgehenden HTTP- und HTTPS-Traffic einfach direkt an einen ZIA Public Service Edge (ehemals Zscaler Enforcement Node, ZEN) und Zscaler leitet jede Verbindung zum geografisch nächstgelegen ZIA Public Service Edge (ehemals Zscaler Enforcement Node, ZEN) in einem der Hunderte von Rechenzentren weiter, in denen Zscaler operiert. Anschließend untersucht Zscaler jeden Byte des Traffic sowie jede Antwort. Sie brauchen keine Hardware zu kaufen, Software zu aktualisieren oder Versionen zu warten und zu koordinieren. Zscaler wurde von Grund auf entwickelt, um Probleme mit Verarbeitung, Leistung und Skalierung zu eliminieren, die bei Perimeter-basierten Appliances regelmäßig auftreten.

## Herausforderungen von IPS-Appliances

Die Bereitstellung von IPS-Funktionalität in einer Perimeter-basierten Appliance führt zu einer Reihe von Problemen, die weit über den Einsatz und die Wartung von Hardware- und Software-Geräten hinausgehen. Diese Herausforderungen sind bei Perimeter-basierten Sicherheitsgeräten üblich, insbesondere bei denen, die sich außerhalb des Rechenzentrumsperimeter befinden. Zu den Problemen zählen:

### Begrenzte Technologie

Die Leistung eines IPS hängt vom Umfang der Protokolldekodierung und der Menge der Musterkennung ab, die eine Appliance bewältigen muss. IPS-Technologie ist nicht für den Umgang mit großen Blacklists von URLs oder IP-Adressen ausgelegt. Es fehlt auch der Support für Antivirus und fortschrittlichere Analysetechnologien wie das zuvor erwähnte Sandboxen von Dateien. Heute ist IPS in umfassendere UTM-Systeme integriert, um eine breitere Sicherheit zu bieten. Aber wie bereits

erwähnt, sind UTM-Systeme keine logische Option für Remote-Benutzer oder Niederlassungen.

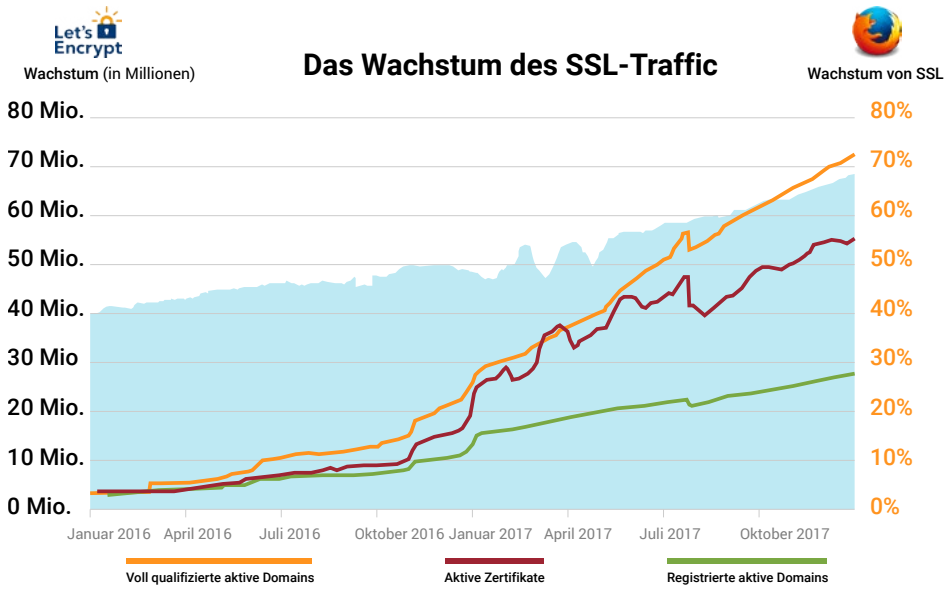
## Leistung

Die Leistung von IPS-Appliances hängt von der Anzahl der aktivierten Signaturen und dem Durchsatz der zu überprüfenden Inhalte ab. Im Fall von HTTP, wo die Antwort in der Regel viel größer als die Anfrage ist, verlangsamt die Aktivierung von Server-zu-Client HTTP-Signaturen die Leistung von IPS-Appliances erheblich; tatsächlich schalten die meisten IPS-Appliances das Scannen von Antworten bei Erreichen des höchstmöglichen Datendurchsatzes standardmäßig ab.

Leider hat dies zur Folge, dass die Sicherheit dramatisch abnimmt. Eine vollständige Untersuchung der HTTP-Antworten ist jedoch erforderlich, um viele Arten von Angriffen zu erkennen, einschließlich Browser-Exploits, Exploit-Kits und mehr. Darüber hinaus ist die Mehrzahl des Botnet-Traffic dynamisch, und die beteiligten Domains ändern sich ständig. In diesem Fall kann der schädliche Traffic effizienter durch Untersuchung der Antwort statt der Anfrage blockiert werden, da dies eine Visualisierung von Elementen ermöglicht, einschließlich Konfigurationsdownload, Liste der ISP oder Domains, zu denen eine Verbindung hergestellt werden soll.

## Fehlende SSL-Entschlüsselung

Als transparente Geräte haben viele IPS-Appliances Probleme mit der Man-in-the-Middle (MiTM) SSL-Entschlüsselung. HTTPS-Entschlüsselung ist Prozessor-intensiv und schränkt die Verarbeitungsleistung von IPS-Harware-Appliances erheblich ein. Dieses Problem wird mit steigendem SSL-Traffic noch gravierender. Laut Google Transparency Report sind mehr als 90% des über Google abgewickelten Traffic inzwischen verschlüsselt[2]. Zudem können Hacker jetzt auf Websites wie LetsEncrypt kostenlose SSL-Zertifikate erhalten, die ihnen




[2] Google Transparency Report: https://transparencyreport.google.com/https/overview?hl=en

SSL-Übertragung selbst von schädlichen Websites aus ermöglichen. Da immer mehr Bedrohungen und Hacker auf SSL umsteigen, müssen Unternehmen eine leistungsstarke SSL-Überprüfung unbedingt in ihre Abwehrstrategie integrieren.

### Asynchroner Traffic

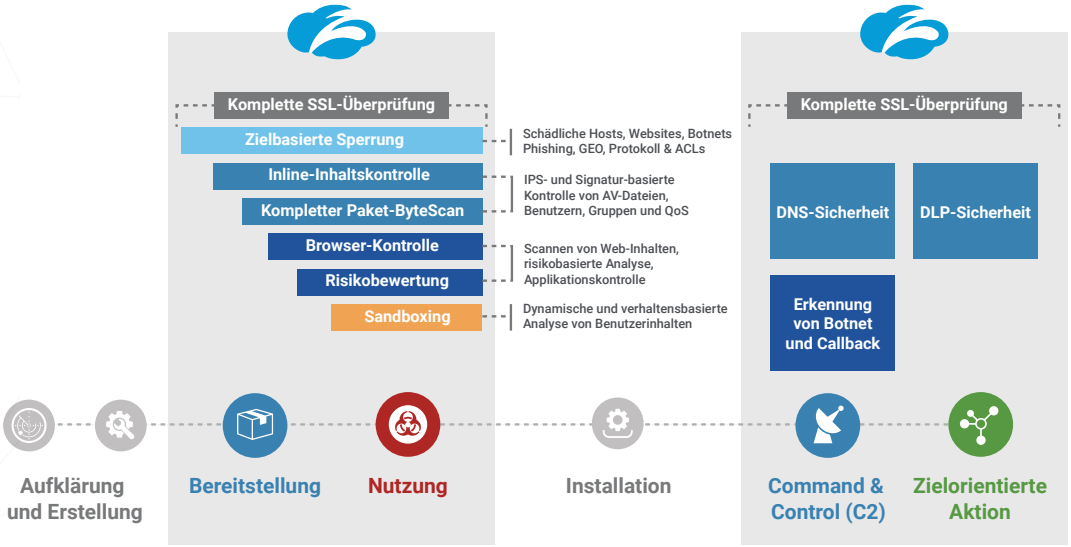
Bei vielen Netzwerken kann der Traffic eines Benutzers von verschiedenen Gateway-Standorten innerhalb des Netzwerks aus- und eintreten. Diese als asynchroner Traffic bezeichnete Routing-Situation führt häufig dazu, dass IPS- und andere Überprüfungsgeräte relevante Bedrohungen übersehen. Für eine adäquate Bedrohungserkennung muss ein IPS oder eine andere Überprüfungs-Appliance die Client- und die Serverseite des Kommunikationsmusters des Benutzers miteinander korrelieren können, um eine korrekte Signaturerkennung durchzuführen. Da die Platzierung einer einzelnen IPS-Appliance über mehrere Gateway-Standorte hinweg oft unmöglich ist, kann dieser getrennte ein- und ausgehende Benutzer-Traffic von der Appliance nicht korrekt verfolgt werden, wodurch Angriffe übersehen werden.

### Unerwünschte Paketverluste

IPS blockiert Traffic auf Layer 4, Anwendungen wie Web-Browser hingegen arbeiten auf Layer 5 und höher. Einige IPS-Plattformen bieten kein vernünftiges TCP-Reset, wenn Pakete verworfen werden. Viele Anwendungen werden daher immer wieder versuchen, auf zurückgesetzte Verbindungen zuzugreifen, was zu einem Anstieg des Traffic im Netzwerk führt.

## Zscaler Cloud IPS

Zscaler integriert IPS-Technologie in die Advanced Threat Detection. IPS ist eine von vielen Arten der Untersuchung, die zusammen mit Blacklisting, Heuristik (Page Risk), Antivirus, Datei-Sandboxen und anderen durchgeführt werden. Da Zscaler nicht die Server sondern die Benutzer schützt, sucht das IPS nicht nach Server-Angriffen wie SQL-Einspeisung, Denial-of-Service oder Remote-Codeausführung, also nach Bedrohungstypen, die man im Rechenzentrum erwarten würde. Stattdessen konzentriert sich das IPS von Zscaler auf die Erkennung von Bedrohungen für




*Die Cloud-Plattform von Zscaler integriert IPS-Schutz in einen kompletten Security-Stack. Sie erhalten vollständigen Schutz vor allen Bedrohungen, selbst bei SSL, ohne die Leistungseinschränkungen von Hardware oder komplexen Integrationsaufwand.*

## Signatur-basierte Kategorien abgedeckt von Zscaler Cloud IPS

**Schutz vor Botnets**

- Command and Control Server
- Command and Control-Datenverkehr

**Schutz vor bösartigen aktiven Inhalten**

- Webseiten & Inhalte mit Schadcode
- ActiveX Controls mit Schwachstellen
- Browser-Exploits
- Dateiformat mit Schwachstellen
- Blockierte Webseiten mit Schadcode

**Schutz vor Mißbrauch**

- Bekannte Phishing-Seiten
- Potenzielle Phishing-Seiten
- Spyware oder Adware
- Web Spam

**Schutz vor nicht autorisierter Kommunikation**

- IRC Tunneling
- SSH-Tunneling
- Anonymizers

**Schutz vor Cross Site Scripting (XSS)**

- Cookie-Diebstahl
- Potenziell bösartige Anfrage

**Schutz vor verdächtigen Zielen**

**Schutz vor P2P File Sharing**

**P2P Anonymizer-Schutz**

**Schutz vor P2P VOiP**

**Cryptomining**

Benutzer, die über HTTP und HTTPS übertragen werden. Dies macht es zur idealen Lösung für Niederlassungen, Fernbüros und mobile Benutzer. Denn Dank der Leistung, Skalierbarkeit und integrierten Sicherheitsdienste kann Zscaler problemlos jedem Deployment an jedem Ort eine zusätzliche Sicherheitsebene hinzufügen.

Zscaler verwendet seine urheberrechtlich geschützte Technologie zum Scannen des gesamten Traffic, sowohl von Client-zu-Server als auch von Server-zu-Client. Anfrage und Antwort werden beide analysiert, um Schwachstellen abzugleichen und Signaturen auf den gesamten Web-Traffic anzuwenden. Zscaler ist in der Lage, sowohl die Anfrage als auch die wesentlich umfangreichere Antwort zu berücksichtigen, wodurch Sie ein vollständiges Bedrohungsbild erhalten. Alle Signaturen werden in Echtzeit auf die Anfrage und Antwort jeder Transaktion angewendet. Der gesamte Web-Traffic durchläuft das IPS von Zscaler, unabhängig davon, ob er von einem Web-Browser oder von einer auf dem Client-Gerät ausgeführten Anwendung stammt.

### Signatur-basierte Erkennung

Der gesamte ein- und ausgehende HTTP- und HTTPS-Traffic wird analysiert, um URL, Header, POST-Daten, Antwortkörper und mehr zu extrahieren. Das Sicherheitsteam von Zscaler veröffentlicht jedes Jahr mehr als 2.000 neue Signaturen, die Schwachstellen von Browsern und Anwendungen abdecken, einschließlich die des Microsoft Active Protections Program (MAPP) sowie Offenlegungsprogramme anderer Anbieter. Andere Signaturen stammen unter anderem von Exploit-Kits, Command & Control Traffic und Cross-Site-Scripting.

Vielleicht noch wichtiger ist, dass Signaturen bei Zscaler über die gesamte Zscaler-Cloud hinweg mehrmals täglich transparent aktualisiert und ergänzt werden. Dies steht in krassem Gegensatz zu Appliance-basierter IPS-Funktionalität, bei der Signaturen höchstens einmal täglich aktualisiert werden. Ein weiterer Vorteil ist, dass Zscaler alle erkannten Bedrohungen sofort für alle Benutzer blockiert. Das bedeutet, dass jeder Benutzer geschützt ist, sobald eine Bedrohung erstmals erkannt wird.

### Erkennung von Anomalien – Proxy-IPS

ZIA Public Service Edge (ehemals Zscaler Enforcement Node, ZEN) sind Proxys, keine transparenten Geräte. ZIA Public Service Edge erhalten eine Anfrage vom Client und erstellen eine neue Anfrage an den Ziel-Server. Um diese Funktion auszuführen, müssen ZIA Public Service Edge die gesamte Anfrage korrekt analysieren können. Umgehungstechniken, die Sicherheitsgeräte dazu verleiten, Anfragen falsch zu verstehen, funktionieren nicht bei einer Proxy-Architektur wie der von Zscaler. Wenn ein ZIA Public Service Edge eine Anfrage nicht analysieren kann, wird diese nicht an das Ziel weitergeleitet. Bei Versuchen, die Protokoll-Decoder von Zscaler zu umgehen, wird verhindert, dass schädliche Anfragen weitergeleitet werden.

### Prävention

ZIA Public Service Edge senden benutzerfreundliche HTML-Benachrichtigungsseiten an Benutzer und Anwendungen, wenn Traffic blockiert wird. So erfahren Benutzer, dass eine Anfrage blockiert wurde sowie den Grund dafür, und können entsprechende Maßnahmen ergreifen. Alle Angriffe werden in Echtzeit blockiert, protokolliert und gemeldet. Administratoren können Angriffe leicht korrelieren oder die Benutzeraktivität vor den Angriffen überprüfen, wodurch die Forensik wesentlich vereinfacht wird.

### SSL-Inspektion

Als Proxy kann Zscaler SSL entschlüsseln und den gesamten HTTPS-Traffic scannen, um Signaturen abzugleichen. Der gesamte Web-Traffic, ob verschlüsselt oder nicht, erhält dasselbe Maß an Sicherheitsschutz. Dadurch wird das große Problem der „toten Winkel" bei SSL eliminiert, und Zscaler ermöglicht dies ohne die Leistungseinbußen, die bei Appliances spürbar sind. SSL-Überprüfung kann je nach URL-Kategorie oder Cloud-Anwendung und Standort ein- und ausgeschaltet werden.

### Hochleistung und niedrige Latenz für den gesamten Traffic

Zscaler hat seinen eigenen skalierbaren IPS-Engine entwickelt. Die Signatur-basierte Erkennung von Anfrage und Antwort ist immer eingeschaltet und es entstehen keine zusätzlichen Latenzen, wenn die Advanced-Threat-Richtlinie auf das Blockieren von Bedrohungen eingestellt ist. Darüber hinaus verursacht die Überprüfung von asynchronem Traffic keine Probleme mehr, da die Zscaler-Cloud mühelos alle Verbindungswege abdeckt, über die ein Benutzer auf das Internet zugreifen kann. Infolgedessen brauchen sich Kunden von Zscaler nicht zwischen Geschwindigkeit und Abdeckung entscheiden; sie erhalten jederzeit hohe Geschwindigkeit und hervorragende Abdeckung.

## Fazit

IPS spielt beim Schutz der Benutzer vor bestimmten Arten von Bedrohungen eine große Rolle. Zscaler verwendet ByteScan und Signatur-basierte Erkennung sowie einen voll integrierten Security-Stack, der Sandboxen und SSL-Überprüfung einschließt, um die meisten Exploits und den größten Teil des schädlichen Traffic, der auf Benutzer abzielt, zu blockieren. Durch die Aktivierung von SSL-Entschlüsselung erhält der gesamte Traffic dasselbe Maß an Sicherheitsüberprüfung. Ohne die Beschränkungen von Hardware und mit elastischer Skalierbarkeit entsprechend des Traffic-Bedarfs einer Organisation kann die Zscaler-Suite der Advanced Threat Protection-Techniken das Schutzniveau anderer IPS-Angebote auf dem Markt bei weitem übertreffen.

Weitere Informationen über **Zscaler Cloud IPS, Zscaler Cloud Sandboxing,** oder die komplette Suite des **Zscaler Advanced Threat Protection** finden Sie auf unserer Website, oder wenden Sie sich an uns **für eine Demo.**



**Zscaler, Inc.**
110 Rose Orchard Way
San Jose, CA
+1 408 533 0288
**www.zscaler.com**