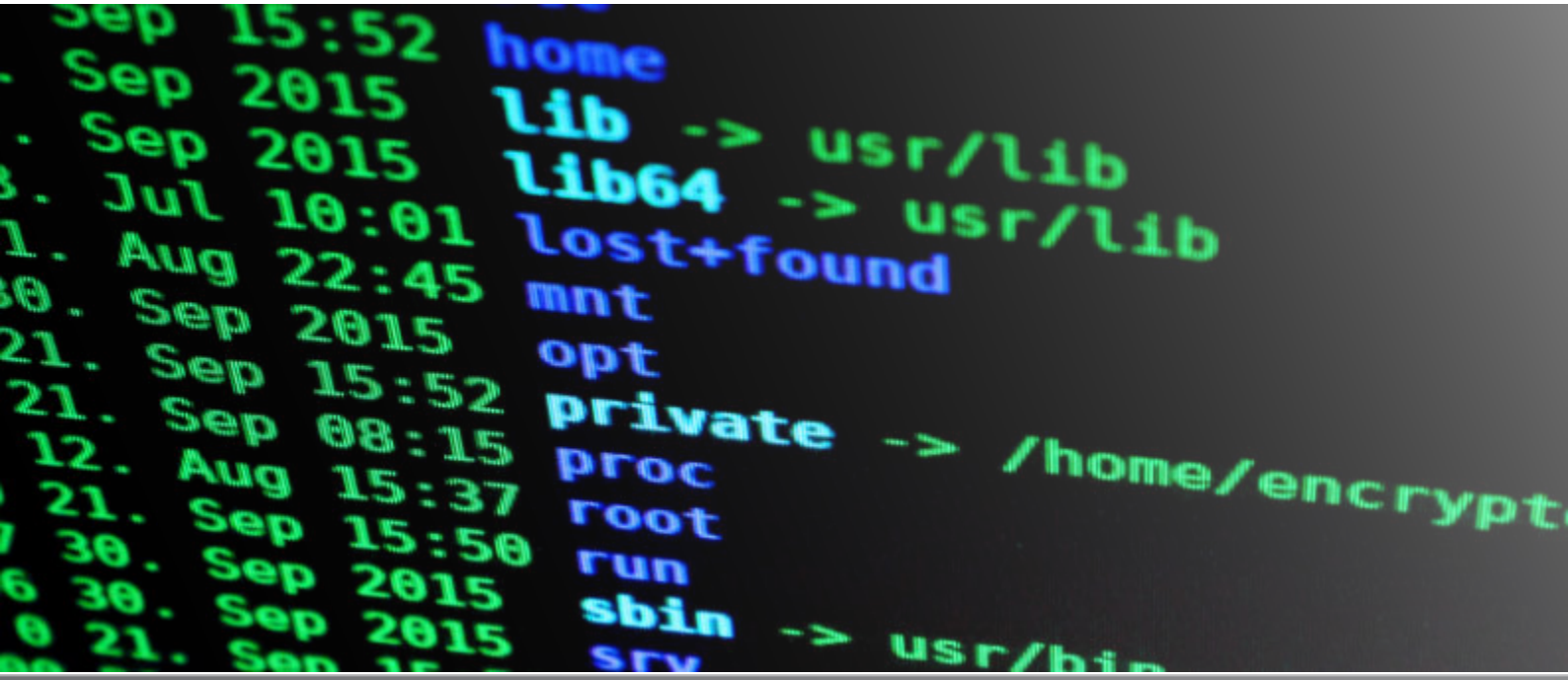
if(is)
internet-sicherheit.



Vergleich von ausgewählten Cloud Firewalls anhand relevanter Kriterien

Eine Empfehlung vom Institut für Internet-Sicherheit

Das Institut für Internet-Sicherheit

Das Institut für Internet-Sicherheit - if(is) ist eine innovative, unabhängige und wissenschaftliche Einrichtung der Westfälischen Hochschule. Neben der Forschung und Entwicklung sind wir ein kreativer Dienstleister auf dem Gebiet der Internet-Sicherheit.

Seit der offiziellen Eröffnung im Mai 2005 hat das junge kreative Forscherteam das Institut schnell zu einer der bedeutendsten Kompetenzen für Internet-Sicherheit entwickelt. Unser Ziel ist es, einen Mehrwert an Vertrauenswürdigkeit und Sicherheit im Internet herzustellen.

Die Herausforderungen

Es gibt keine unwichtigen Daten in der digitalen Welt. Immer mehr IT-Geräte werden verwendet, unterschiedliche IT- Systeme kommen zum Einsatz.

Zahlreiche Angriffsmethoden gilt es zu erkennen und abzuwehren. Vor der Herausforderung, die richtigen Schutz-mechanismen zu ergreifen, steht bereits jetzt jeder Internetnutzer, privat oder beruflich. Komplexe Software, die steigende Anzahl der IT-Geräte, wie auch die Vernetzung untereinander, erschweren die Anforderungen an diese Aufgabe.

Die zuverlässige Filterung von Inhalten aus dem Internet zum Schutze für Kinder und Jugendliche ist eine weitere Heraus-forderung, der sich Eltern stellen müssen. Gegen professionelle Angreifer werden auch professionelle IT- Sicherheitsmaßnahmen für alle Internetnutzer benötigt.

Die Zukunft

Smartwatch, Tablet, Smartphone, IoT-Geräte und Notebooks beherbergen bereits jetzt zahlreiche sensible Daten, die es zu schützen gilt.

In Zukunft steigt die Anzahl der IT-Geräte pro Internetnutzer und mit ihnen auch der Aufwand diese zu schützen. Dabei müssen die IT-Sicherheitslösungen leistungsfähiger, benutzerfreundlicher, günstiger, wartungs-freier, zuverlässiger und innovativer werden.

Setzt sich der Trend fort, werden in Zukunft zahlreiche Haushalte über sehr viele und komplexe Konnektivität zum Internet verfügen. Ohne eine angemessene IT-Sicherheit gelingt keine nachhaltige Digitalisierung!

Kriterien von Cloud-Diensten

Mit den steigenden Bandbreiten und sich verbreitenden Cloud-Services, bieten immer mehr IT-Security Hersteller auch Cloud-fähige Firewalls an.

In diesem Vergleichstest werden die verschiedenen Hersteller von Cloud Firewall-Produkten bewertet. Die Bewertung findet in einem Quadrantensystem statt, welches jeden Hersteller anhand relevanter Kriterien platziert.

Das Lizenzmodell

Gestaffelte Kostenstrukturen erschweren eine einfache Preisstruktur. Angebot und Nachfrage gilt es bei der Nutzung von Cloud Firewalls einfach zusammen zuführen.

Feste Preise pro Nutzer in einem fließenden Kostenmodell sind kunden- und end-benutzerfreundlich.

Die Cloud Ressourcen

Die performante Nutzung vorhandener Cloud Ressourcen ist Voraussetzung einer kosten-effizienten Cloud Firewall.

Die Kompatibilität zu zahlreichen Cloud-Anbietern ist ein Entscheidungskriterium für bereits etablierte Cloud-Umgebungen.

Die Skalierung

Bei zentralen Diensten ist die Skalierung ein ausschlaggebendes Kriterium. Software-systeme, welche von Millionen benutzt werden, erfordern die Möglichkeit der Skalierung von weiteren Ressourcen.

Die Skalierbarkeit soll für das Software-system transparent sein, damit nicht bei jeder Erweiterung Veränderungen an den Programmen notwendig sind.

Eine notwendige Performance-Erweiterung soll möglichst automatisch von statten gehen. Zusätzliche Kosten können so eingespart werden.

Die Elastizität

Bei großen Schwankungen in der Nutzung der Cloud Firewall sollte dem Softwaresystem die Entscheidung überlassen werden, wann nötige Ressourcen allokiert werden sollen - und auch wann es angebracht ist, diese wieder abzuschaffen.

Dadurch lässt sich die Echtzeit-Nachfrage zuverlässig befriedigen. Elastizität hilft, bedarfsgerechte Dienste einfach und benutzerfreundlich umzusetzen.

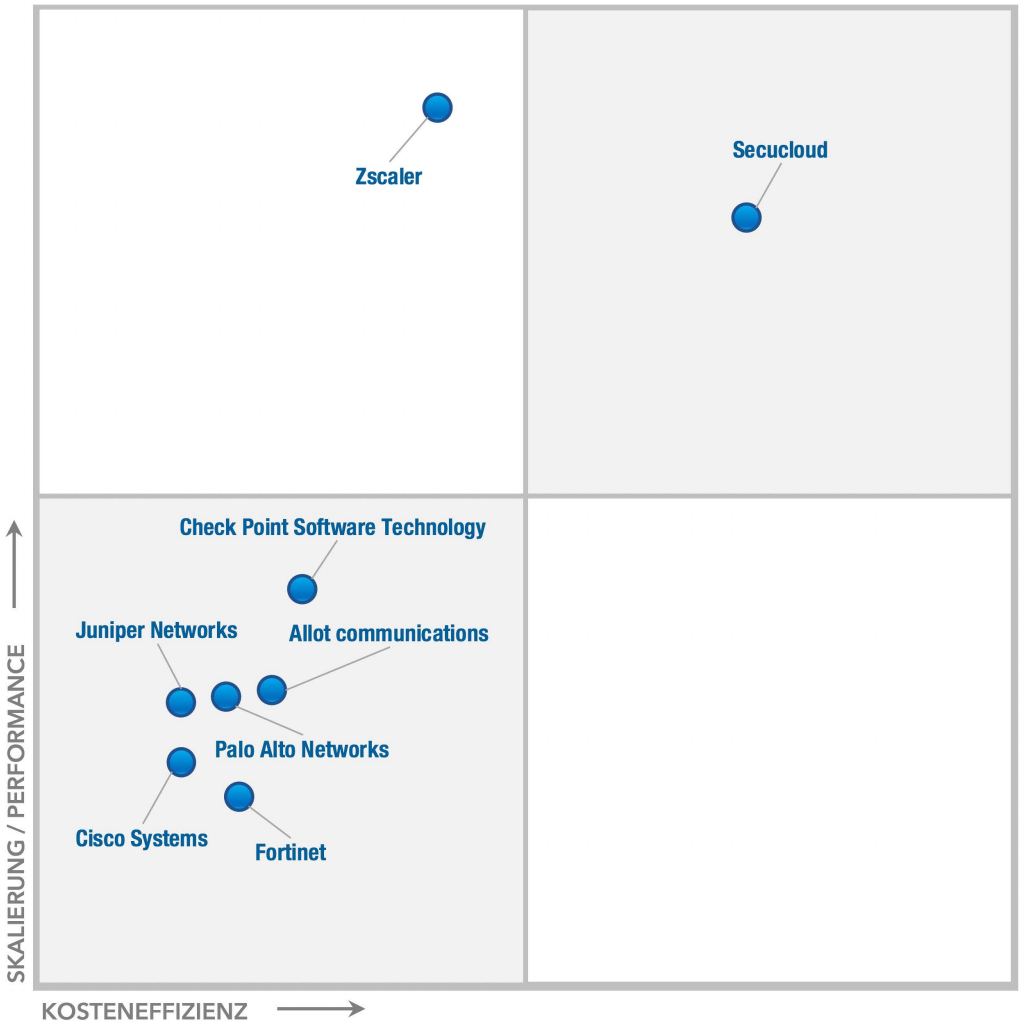
Das Quadrantensystem

In einem kartesischem Koordinatensystem sind die ausgewählten Cloud Firewall-Anbieter anhand der relevanten Kriterien als Koordinate eingetragen.
Über diese Koordinaten wurde im Bereich der erreichten Werte eine zusätzliches Quadrantensystem eingefügt. Diese Quadranten charakterisieren die einzelnen Anbieter in Eignungsstufen für den Massenmarkt im Bereich Cloud Firewall.

Die Achsen

Die Abszissenachse beschreibt die Kosteneffektivität. Hier werden neben den Kosten pro Endbenutzer auch das Lizenzmodell und der kosteneffiziente Umgang mit den Cloud-Ressourcen dargestellt.

Die Ordinatenachse hat die Skalierbarkeit und Performance der einzelnen Cloud Firewall-Lösungen als Kriterien. Dies gibt die als "Elastizität" in der Cloud bekannten Eigenschaften wieder.



Auswahlkriterien der Cloud Firewall-Anbieter

Für die Auswahl zur Einordnung im Quadrantensystem haben sich acht Hersteller qualifiziert. Diese sind weltweit tätig und haben wenigstens eine Cloud Firewall-Produktlinie im Portfolio. Das übergeordnete Kriterium ist hier die Cloud-Nutzbarkeit und nicht die Firewall-Funktionalität, so dass auch Hersteller aus dem Routing-Umfeld mit einbezogen wurden.

Die gesammelten Informationen stammen von den öffentlichen Websites der Hersteller, von Vorträgen, Messen, Konferenzen oder Broschüren.

Mitbewerber im Detail

Check Point

Check Point hat seine Headquarter in Tel Aviv, Israel und San Carlos, Kalifornien. Check Point ist einer der größten Anbieter von IT-Security mit einem breiten Portfolio im Bereich Next-Generation Firewalls, Endpoint- und Mobile Security.

Check Point bietet unter anderem auch virtualisierte Versionen ihrer Appliances über Amazon Web Services und Microsoft Azur an. Außerdem unterstützt die virtualisierte Appliance Firmware VMware NSX und Cisco Application Centric Infrastructure (ACI).

Stärken

- Marktführer im Bereich Enterprise Firewalls
- Sehr gute Management-Lösungen zur Administration umfangreicher Enterprise Firewall Installationen
- Größte R&D Ressourcen im Firewall Markt

Schwächen

- Cloud-Produkte sind virtualisierte Appliances und nicht auf Elastizität optimiert
- Übliche Lizenz-Staffelung wird angeboten
- Sandbox-Lösung ist weit weniger performant als die der direkten Konkurrenz

Zscaler

Zscaler kommt aus San Jose, Kalifornien und ist ein reiner Cloud-Security Anbieter. Gartner bestätigt Zscaler einen Marktanteil von mehr als 50% im cloud-basierten Secure Web Gateway (SWG) Markt weltweit.

Zscaler bietet ein auf der Zscaler-Cloud basierten SWG als Service an und veröffentlicht seinen Verfügbarkeits-Status unter: https://trust.scaler.com

Stärken

- Marktführer mit >50% Marktanteil im cloud-basierten SWG Markt weltweit
- Inspektion von SSL/TLS Web-Traffic
- Globales Zscaler-Cloud Netzwerk mit mehr als 100 Nodes in 30 Ländern

Schwächen

- Keine On-Premise-Lösung ohne die Nutzung der Zscaler-Cloud
- Zscaler App VZEN Virtual Proxy ist seit Dezember 2015 verfügbar und hat noch Schwächen
- An amerikanische Gesetze gebunden

Mitbewerber im Detail

Secucloud

Mit Hauptsitz in Hamburg, Deutschland, bietet die Secucloud GmbH seit Anfang 2013 reine cloud-basierte IT-Security Produkte an, die direkt für die Cloud und ihre Vorteile wie Elastizität und Pay-as-you-go konzipiert wurden.

Secucloud hat nie Hardware Appliances im Portfolio gehabt und ist somit frei von Altlasten, die anderen Herstellern in der Cloud Probleme bereiten.

Stärken

- Einzige echt-virtuelle On-Premise-Lösung auf Cloud-Basis
- Durch Cloud-Lizenzen sehr preisgünstig am Massenmarkt.
- Automatische Skalierbarkeit / Elastizität

Schwächen

- Geringer Marktanteil im weltweiten Cloud Security Markt
- Secucloud ist ein junges Unternehmen
- Produkte für den Enterprise Security Einsatz wenig optimiert

Cisco

Cisco stammt aus San Jose in Kalifornien und hat verschiedene Cloud Produkte im Portfolio. Die Web Security Appliance (WSA) ist auch als virtuelle Appliance erhältlich. Die Firmware der Appliance ist auf einem Hypervisor virtualisiert worden. Sie ist identisch mit der Firmware der Appliances und somit nicht auf eine Cloud-Nutzung ausgerichtet.

Cloud Web Security (CWS) ist ein reiner Cloud-basierter Webservice. Dieser wird seit 2016 angeboten und erlaubt die zentrale Administration verschiedener Hardware (oder virtualisierter) Cisco Appliances.

Stärken

- Extrem weit verbreitet im gesamten Enterprise-Netzwerk-Umfeld
- Einer der Marktführer im IT-Security-Bereich
- Sehr breites Portfolio an Netzwerk und IT-Security-Produkten

Schwächen

- Cloud Service ist erst seit 2016 am Markt und befindet sich noch in einer frühen Phase
- Virtuelle Appliances sind nicht auf Cloud-Eigenschaften ausgelegt
- Keine automatische Skalierung bei Nutzerzahl-Änderung

Mitbewerber im Detail

Juniper

Juniper Network hat seinen Hauptsitz in Sunnyvale, Kalifornien. Die Juniper-Produkte der IT-Security haben einen hohen Schwerpunkt auf Routing, was daran liegt, dass Juniper mit diesem Business begonnen hat und erst später zum IT-Security Markt kam.

Die SRX Firewall-Serie wird in 28 verschiedenen Hardware Varianten geliefert und basiert immer auf dem eigenen Betriebssystem JunOS. Diese Firewall-Lösung ist auch als virtuelle Appliance erhältlich.

Stärken

- Hardware liefert extrem hohe Daten-durchsätze
- Breite Verteilung von Offices weltweit
- Software Defined Network wird seit längerem voll unterstützt

Schwächen

- Firewall Features werden spät veröffentlicht
- Hängt mit neuen Public Cloud Support und dem Support von Virtualisierungen hinterher
- Verliert seit Jahren Anteile im IT-Security Markt

Palo Alto

Der reine IT-Security-Hersteller Palo Alto Networks stammt aus Santa Clara, Kalifornien. Mit seinen Innovationen im Bereich Application-Control und Intrusion Prevention System definierte Palo Alto den Begriff Next Generation Firewall maßgeblich mit.

Die Firewall-Produktlinie umfasst 19 Modelle mit einem maximalen Durchsatz von 200 Gbps des Spitzenmodells. Mit der Unterstützung von VMware NSX liefert Palo Alto seinen Kunden die Möglichkeit seine Alliances zu virtualisieren.

Stärken

- Marktführer im Next Generation Firewall Enterprise-Umfeld
- Liefern innovative Next Generation Firewall Features lange vor der Konkurrenz aus
- Neben Check Point die am weitesten verbreitete Enterprise Firewall-Lösung

Schwächen

- Virtualisierte Firewall Appliance unterstützt weit weniger Hypervisor-Systeme als die Mitbewerber
- Als Enterprise Firewall Hersteller für den Klein- und Mittelstand zu teuer
- Kaum Marktanteile im Endpoint Markt

Mitbewerber im Detail

Fortinet

Aus Sunnyvale, Kalifornien, stammt Fortinet. Der Hersteller von Firewalls hat vor Allem Hardware-Appliances im Portfolio. Die Spezial-Hardware-Komponenten ermöglichen hohe Durchsatzraten in der Enterprise-Klasse ihrer Firewalls. Fortinet ist mit SMB Firewalls im Enterprise-Umfeld weit verbreitet. Als Hersteller von auf Spezial-Hardware-basierten Firewall Appliances liefert Fortinet durchnittlich performante virtualisierte Version seiner Firewall Firmware.

Stärken

- Appliances liefern höhere Durchsatzraten als die der Konkurrenz
- Hardware wird in Testberichten gelobt
- Das Preis/Leistungs-Verhältnis der Appliances dominiert den Markt

Schwächen

- Virtualisierte Appliances liefern nicht den Performance Vorspung der Spezial-Hardware-Appliances
- Keine auf Cloud-Nutzung ausgelegte Lizenzen verfügbar/ Keine Skalierung
- Virtuelle Appliances sind an feste virtuelle Hardware-Stufen gebunden

Allot / Optenet

Mit dem Hauptsitz in Israel hat sich die Allot mit der Akquisition der Firma Optenet auch Hardware-basierte Web-Filter ins Portfolio eingekauft. Ursprünglich aus dem IP-Traffic-Steering Business, sind in den Allot Appliances nur Basis-Funktionen einer Firewall verfügbar.

Mit den Web-Security-Produkten liefert Allot einen Cloud-Service, der nicht auf virtuellen Ressourcen, sondern auf Hardware Appliances basiert.

Stärken

- Die Spezial-Hardware-Appliances liefern hohe Durchsatzraten im Enterpise-Umfeld
- Als US-NASDAQ gelistetes Unternehmen ist Allot im Cloud-Security Markt ein großes Unternehmen
- Durch seine Routing Wurzeln bereits aud SDN und Network Function Virtualisierung vorbereitet

Schwächen

- Für SSL/TLS Traffic keine Filter-möglichkeiten
- Eine Skalierung kann aufgrund der Hardware-Appliances nur auf Hardware-Blöcken stattfinden
- Preis/Leitung befindet sich nicht auf dem Niveau wie die Security-Cloud-Konkurrenz

Unsere Empfehlung

Der innovative Schutz von IT-Endgeräten ist eine Herausforderung, welche bewältigt werden muss, damit das Internet in Zukunft weiterhin sinnvoll genutzt werden kann. Die Angst vor Erpressung, Identitäts- und Datendiebstahl hemmt bereits zum jetzigen Zeitpunkt viele Unternehmen und Mitbürger vor dem Einsatz technischer IT-Geräte mit Internet-Konnektivität.

Den nötigen, innovativen Schutz bietet unserer Meinung nach die Secucloud ECS^2 Cloud-Firewall am Besten an. Die sehr gute Elastizität der Secucloud ECS^2 Cloud-Firewall ist eine zentrale Funktion, um möglichst dynamisch Millionen Benutzer gleichzeitig schützen zu können.

Die Bezahlung nach genutzten Ressourcen ermöglicht es dem Betreiber der ECS^2 Cloud-Firewall, einen kosteneffzienten, flexiblen und zukunftsorientierten Schutzmechanismus anzubieten. Ohne Altlasten und Legacy-Systeme ist es der Cloud Firewall möglich, einen zentralen Beitrag zur Sicherheit des Internets zu leisten.

Da das Thema Vertrauen bei der Wahl von IT-Sicherheitslösungen eine besondere Rolle spielt, hat die Secucloud ECS^2 Cloud-Firewall aus Deutschland auch hier einen besonderen Vorteil zu bieten.

Prof. Dr. (TU NN) Norbert Pohlmann
Direktor des Instituts für Internet-Sicherheit – if(is)
Neidenburger Str. 43
45897 Gelsenkirchen