CISCO
SECURE

Whitepaper
Cisco Public

Die Zukunft der Firewall

Von der Stärkung des Sicherheitsstatus heute und dem Spannen von Brücken, die die Business- und Security-Anforderungen von morgen erfüllen

cisco The bridge to possible

Inhalt

Übersicht

Dieses Whitepaper beleuchtet die Entwicklungsstadien der Netzwerksicherheit und untersucht, was benötigt wird, um Unternehmen auch in Zukunft schützen zu können.

Netzwerke werden immer heterogener, und so wird es für Unternehmen zunehmend schwieriger, Richtlinien konsistent zu verwalten und durchzusetzen und eine umfassende Sicht auf ihre Umgebung zu erhalten. Das komplexe Gefüge verschiedenster zusammengeschalteter Netzwerke erhöht die Wahrscheinlichkeit von Fehlern oder falschen Konfigurationen, was wiederum zu einer erhöhten Anfälligkeit gegenüber den zunehmend komplexen Bedrohungen von heute führt.

Wie also können Unternehmen vor diesem Hintergrund die Kontrolle zurückgewinnen und Konsistenz erreichen? Der erste Schritt hierfür liegt in einem integrierten Sicherheitsansatz mit der Firewall im Zentrum.

Firewalls bilden auch heute noch das Rückgrat des Netzwerkschutzes, müssen sich jedoch genauso weiterentwickeln, wie es Netzwerke getan haben. In der Vergangenheit wurde die Firewall über eine einzelne Appliance am Eingangs-/Ausgangsperimeter umgesetzt, die als Kontrollpunkt basierend auf Richtlinien Netzwerkverkehr entweder zuließ oder verweigerte. In der digitalisierten Welt von heute aber gilt es, das Konzept der Firewall weiterzudenken und auf sogenanntes „Firewalling“ zu erweitern, bei dem fortschrittliche Sicherheitsmaßnahmen mittels Richtlinien auf allen logischen Kontrollpunkten innerhalb heterogener Netzwerke koordiniert werden.

Firewalling ist der entscheidende Schritt hin zu einer besseren Abstimmung der Sicherheit auf die Anforderungen von Business und Netzwerk. Die Umsetzung dieses Konzepts erleichtert Cisco durch seine forcierten Anstrengungen rund um die Entwicklung einer integrierten Security-Plattform mit seiner Firewall als Grundbaustein.

„Firewalls bilden auch heute noch das Rückgrat des Netzwerkschutzes, müssen sich jedoch genauso weiterentwickeln, wie es Netzwerke getan haben.“

Firewalling ist der Schlüssel, mit dem Unternehmen im Zuge ihrer digitalen Transformation ihren Sicherheitsstatus heute stärken und gleichzeitig die Brücke zur Erfüllung ihrer Business- und Security-Anforderungen von morgen spannen können.

1. Ein Blick auf die Geschichte der Firewall

Netzwerksicherheit im Wandel der Zeit

Ursprünglich hatte die Firewall ihren Platz am Netzwerk-Edge, an dem sie quasi als „Pförtner“ einen zentralen Kontrollpunkt bildete, der den gesamten durch diesen Perimeter geleiteten Netzwerkverkehr überwachte. Am Eingangs-/Ausgangspunkt des Netzwerks war die Firewall für die Validierung der Kommunikation verantwortlich: Interner Netzwerkverkehr galt grundsätzlich als vertrauenswürdig und externer Datenverkehr grundsätzlich als nicht vertrauenswürdig. Regelsätze und Richtlinien wurden erstellt und an diesem zentralen Kontrollpunkt durchgesetzt, sodass erwünschter Datenverkehr in das und aus dem Netzwerk zugelassen und unerwünschter Datenverkehr blockiert wurde.

Vergleicht man den Netzwerkperimeter mit einem Burggraben, fungierte die Firewall als Zugbrücke, die den gesamten Datenverkehr innerhalb und außerhalb der Burganlage kontrolliert.

Der klassische Netzwerksicherheitsansatz

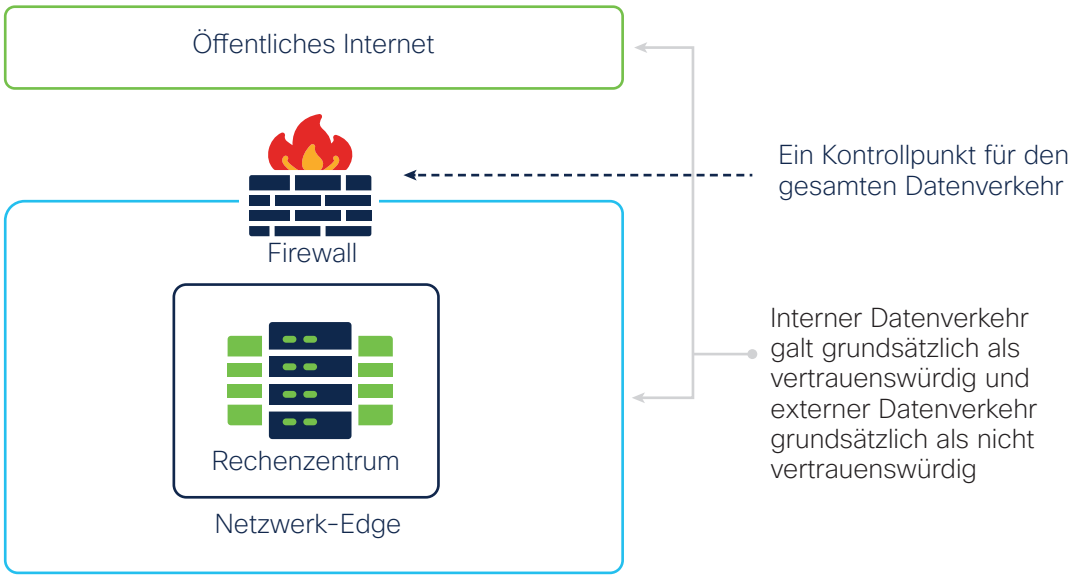


Abbildung 1: Klassischer Ansatz für die Firewall

Nächste Station: Cloud ... und Apps

Es ist noch gar nicht allzu lange her, dass der Ansatz eines einzigen Kontrollpunkts zur Durchsetzung der Sicherheit in Frage gestellt wurde. Ins Wanken brachte diesen Ansatz zunächst der Aufstieg von Remote-Zugriff und Enterprise Mobility, den Umbruch perfekt machte dann aber erst das Cloud-Computing. Mit dem Weg in die Cloud wurden Geräte und Benutzer massenhaft außerhalb des kontrollierten internen Netzwerks migriert, was das Modell eines einzigen Kontrollpunktes ad absurdum führte. Denn so wurden aus einem Perimeter schon bald viele verschiedene, die es allesamt zu schützen galt. Eine effektive Möglichkeit, den besagten Burggraben um dieses Netzwerk zu legen, gab es jedoch nicht.

Heute verlaufen Datenflüsse im Zuge von Zweigstellen, Remote-Arbeit und der steigenden Nutzung von Cloud-Services zunehmend außerhalb des klassischen Perimeters. Sie umgehen dabei den traditionellen Sicherheitskontrollpunkt vollständig. Dazu kommt, dass immer mehr Unternehmen ihren Mitarbeitern im Rahmen von BYOD-Modellen (Bring-Your-Own-Device) inzwischen den Zugriff auf vertrauliche Geschäftsanwendungen über ihre privaten Computer oder Mobilgeräte gestatten: Nicht weniger als 67 % der Mitarbeiter nutzen ihre privaten Geräte am Arbeitsplatz, und ein Ende dieses Trends ist nicht in Sicht. Auch die Anbindung von Geräten und Laptops über öffentliche Wi-Fi-Netzwerke ist heute weit verbreitet, für den täglichen Geschäftsbetrieb vielfach sogar unabdingbar.

Auch benötigt die überwältigende Mehrheit der Geschäftsstandorte und Benutzer einen Direktzugang zum Internet, um auf die zunehmende Zahl an Cloud-basierten, kritischen Anwendungen und Daten zugreifen zu können. Über immer mehr unterschiedliche Cloud-Services, Betriebssysteme, Hardware-Appliances und Datenbanken usw. werden Workloads bereitgestellt, und so werden Anwendungen und Daten zunehmend dezentralisiert und in der Folge Netzwerke stärker diversifiziert.

Die neue Realität

In der IT-Landschaft von heute greift der ursprüngliche Ansatz nicht mehr.

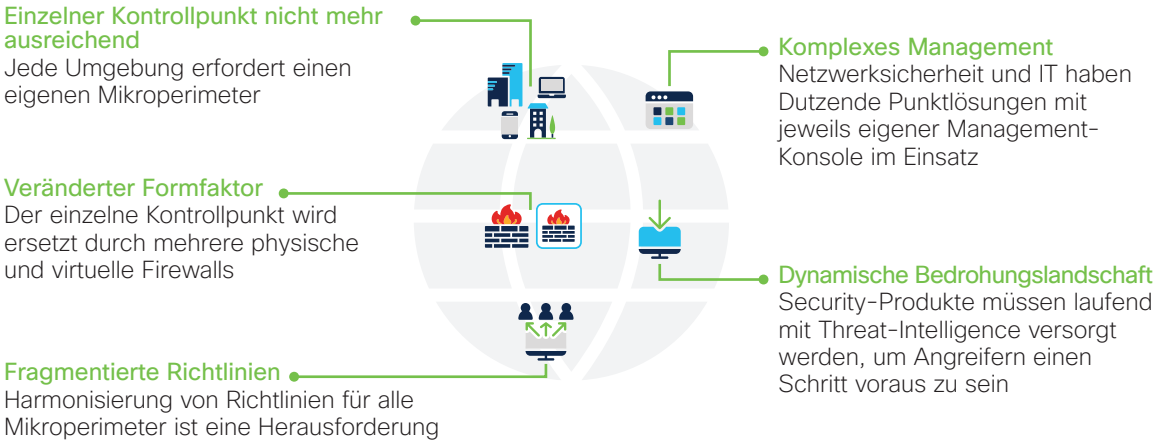
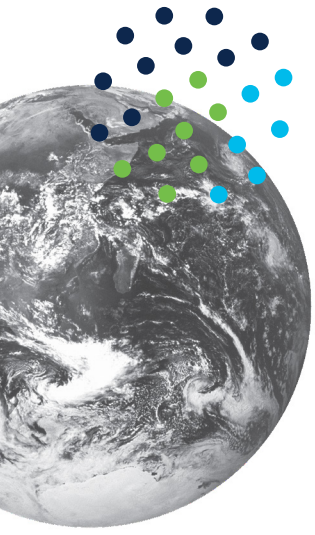


Abbildung 2: Komplexität des Netzwerks und neue Bedrohungen stellen das klassische Modell der Firewall in Frage

Komplexität bestimmt die heutige Realität

Die genannten Innovationen rund um die Arbeitsumgebung haben zwar mehr Vernetzung und Produktivität ermöglicht, dabei aber auch Geschäftsprozesse insgesamt grundlegend verändert. Denn wo Anwendungen früher noch kontrolliert und Benutzer vor Ort autorisiert wurden, haben wir nun dynamische Multicloud-Ecosysteme, über die Services und Anwendungen unternehmensweit bereitgestellt werden. Dazu kommen geschäftskritische Beziehungen zu Dritten, die es zu managen gilt. Umfangreiche Expansion und Outsourcing sorgen für Skaleneffekte und Effizienz, haben jedoch auch eine Kehrseite. Denn im Zuge dieser Entwicklung der Netzwerkarchitekturen vergrößert sich die Angriffsfläche erheblich, und der Schutz von Unternehmensnetzwerken, Daten und Benutzern gestaltet sich deutlich schwieriger.

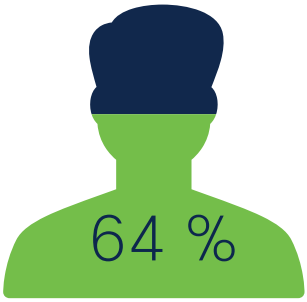


Punktlösungen als Antwort

In der Regel begegneten Unternehmen diesen Herausforderungen mit der Strategie, ihre Security-Infrastruktur für jedes neu aufkommende Problem direkt um die vermeintlich „beste“ Punktlösung zu ergänzen. Das aber hat zu einer regelrechten „Geräte-Schwemme“ geführt: Im Schnitt haben Unternehmen bis zu 75 unterschiedliche Security-Tools im Einsatz.[1] Eine solche Menge an Security-Produkten unterschiedlicher Anbieter stellt die Teams aus der Netzwerksicherheit vor erhebliche Probleme im Hinblick auf das Management. Das Risiko von Angriffen kann tatsächlich sogar zunehmen. So gaben 94 % der Verantwortlichen aus IT und Informationssicherheit an, dass ihre Netzwerke im Zuge ihrer zunehmenden Komplexität anfälliger würden, während 88 % nach Wegen suchten, wie sie ihre Richtlinien für die Netzwerksicherheit flexibler anpassen können.[2]

In der Zeit von Januar bis Juli 2019 wurden 3.800 Datensicherheitsverletzungen gemeldet, was gegenüber dem ersten Halbjahr 2018 einer Zunahme von nicht weniger als 54 % entspricht.[3] Ein derart steiler Anstieg zeigt zweierlei: Angreifer entwickeln immer ausgefeiltere Methoden, um sich Zugang zu Netzwerken zu verschaffen, und herkömmliche Methoden sind nicht mehr in der Lage, den modernen Bedrohungen Paroli zu bieten.

1 „Defense in depth: Stop spending, start consolidating“, CSO, 4. März 2016.
2 „Navigating Network Security Complexity“, ESG Research Insights Report, Juni 2019.
3 „Navigating Network Security Complexity“, ESG Research Insights Report, Juni 2019.



Menschliche Fehler waren die Hauptursache für eine Fehlkonfiguration

Mehr Bedrohungen, mehr Rauschen, noch mehr Risiken

Mit dem Aufkommen neuer Angriffsvektoren, die von E-Mails über nicht geprüfte Endpunkte im Rahmen von BYOD-Richtlinien bis hin zu Webportalen und IoT-Geräten reichen, versuchten sich Unternehmen an immer neuen Strategien, um sich zu schützen.

Wie bereits erwähnt, trägt das fortlaufende Ergänzen von Einzelprodukten insgesamt jedoch nicht zur Verbesserung des Sicherheitsstatus eines Unternehmens bei. Tatsächlich bewirkt es sogar das Gegenteil. Denn für Security-Teams bedeutet es mehr „Rauschen“: Ohnehin schon schwer damit gefordert, nach neuen, auf bekannte oder unbekannte Schwachstellen abzielenden Angriffen und Malware-Varianten Ausschau zu halten, wird ihnen durch diese zusätzliche Komplexität die Erstellung, Verwaltung und Durchsetzung von Sicherheitsrichtlinien immer weiter erschwert.

Als Reaktion darauf müssen Security-Teams verschiedenste Cloud-Ressourcen einzeln konfigurieren, was die Wahrscheinlichkeit einer Fehlkonfiguration, die zu einer Sicherheitsverletzung führen kann, weiter erhöht. Fehlende oder fehlerhaft implementierte Sicherheitskontrollen entpuppen sich tatsächlich oft als der größte Übeltäter: 64 % der Unternehmen geben an, dass eine Fehlkonfiguration bei ihnen auf menschliche Fehler zurückzuführen war.[4] Ganz gleich, ob ein solcher Fehler zu einem Verstoß gegen Compliance-Bestimmungen, einem Ausfall oder einer angreifbaren Sicherheitslücke führt, ist klar: Ein solches Risiko ist nicht tolerierbar.

Zeit, das Thema Firewall neu zu denken

Der Schutz von Netzwerken ist zu einer Herkulesaufgabe geworden, die das IT-Personal heute nicht mehr bewältigen kann, indem es eine Vielzahl punktueller Security-Lösungen, Cloud-Ressourcen und Appliances zu verwalten versucht. Gefragt ist ein gänzlich anderer Ansatz.

Es ist an der Zeit, dass die Firewall ihren Platz als Grundlage für eine flexible und integrierte Netzwerksicherheitsplattform einnimmt, die Unternehmen heute und in Zukunft voranbringen kann.

2. Aus Firewall wird Firewalling

Warum Firewalling?

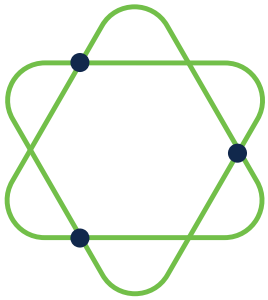
Genauso, wie sich Netzwerke an neue Geschäftsmodelle anpassen, muss dies auch ihre Sicherheit tun. In der Welt von heute, in der IT-Ressourcen immer weiter verteilt sind, bleibt die Firewall noch immer zentral für einen starken Sicherheitsstatus.

Allerdings muss die Firewall erheblich höhere Anforderungen erfüllen, um die zahlreichen Netzwerkinfrastrukturen, vernetzten Geräte und Betriebssysteme vor den komplexen Bedrohungen von heute zu schützen. Dazu werden „herkömmliche“ Firewall-Geräte durch eine Mischung aus physischen und virtuellen Appliances ergänzt – einige von ihnen eingebettet in das Netzwerk, andere bereitgestellt als Service, wieder andere Host-basiert oder in Public-Cloud-Umgebungen integriert. Einige kommen sogar in neuen Formfaktoren, darunter etwa geclusterte Appliances, die entsprechend der hohen Anforderungen an den Datenverkehr skalierbar sind, auf privaten Geräten ausgeführte Software, SD-WAN-Router und Secure Internet Gateways. Unabhängig davon, an welcher Stelle diese Firewall-Geräte implementiert sind, ist dabei entscheidend, dass sie alle untereinander Threat-Intelligence austauschen, um eine vollständige Sicht auf Bedrohungen und damit einen starken Sicherheitsstatus zu gewährleisten.

Um diesen Wandel vollziehen und die Netzwerke von heute besser schützen zu können, müssen Unternehmen vom klassischen Perimeter-Ansatz Abstand nehmen. Stattdessen gilt es, in der gesamten Netzwerk-Fabric strategische Durchsetzungspunkte einzurichten, die näher an den zu schützenden Informationen oder Anwendungen liegen. Insbesondere vonnöten ist dabei die Erstellung von Mikroperimetern an physischen und logischen Kontrollpunkten.

Die Firewall muss weniger als eigenständiges physisches Netzwerkgerät betrachtet werden, und mehr in Bezug auf ihre *Firwalling*-Funktionalität.

4 „Cloud Security Breaches and Human Errors“, Fugue, 7. Februar 2019.



Was ist Firewalling?

Um jegliche Missverständnisse auszuräumen: Die Firewall ist relevanter denn je. Tatsächlich erfordert der Schutz der Netzwerke von heute sogar **mehr** Firewalls. Und das **überall**. Firewalling verschiebt lediglich den Fokus – nämlich darauf, **wie** sich in der gesamten Umgebung richtlinienbasierte Kontrollen einrichten lassen.

Mit Firewalling wird ein flexibler, integrierten Ansatz für die Zentralisierung von Richtlinien, erweiterter Security-Funktionalität und der konsistenten Durchsetzung in zunehmend komplexen, heterogenen Netzwerken implementiert. Dies ermöglicht umfassenden Schutz, Transparenz, Richtlinienharmonisierung und eine stärkere Benutzer- und Geräteauthentifizierung. Außerdem lässt sich mittels Firewalling der Austausch von Threat-Intelligence über alle Kontrollpunkte hinweg umsetzen. Dies sorgt für eine vollständige Sicht auf und Kontrolle über Bedrohungen, was wiederum den Zeit- und Arbeitsaufwand für ihre Erkennung, Untersuchung und Beseitigung erheblich reduziert.

All dies macht Firewalling zu einem strategischen Kernelement für den Schutz der komplexen Netzwerke von heute und zugleich zu einer Brücke, über die sich im Zuge der Weiterentwicklung sowohl von Unternehmen als auch der Bedrohungslandschaft auch zukünftige Anforderungen erfüllen lassen.

Wie gestaltet sich die Umsetzung?

Ganz gleich, ob es um den Schutz von Ressourcen und Daten in der Cloud, On-Premises oder an einem Remote-Standort geht: Firewalling muss einen fortschrittlichen Schutz vor Bedrohungen, Richtliniendurchsetzung sowie den Austausch von Threat-Intelligence konsistent gewährleisten. Die Herausforderung besteht darin, diese Konsistenz in den unterschiedlichen Umgebungen aufrechtzuerhalten, in denen Geräte bereitgestellt und genutzt werden.

Sicherheitsverletzungen können von jedem Gerät ausgehen, das Zugriff auf das Internet hat, unabhängig davon, ob es sich in der Unternehmenszentrale, im Rechenzentrum, an Remote-Standorten in Public Clouds oder anderswo befindet. Umso wichtiger ist es daher, an mehr Standorten Sicherheitskontrollpunkte einzurichten, um die Angriffsfläche und damit Risiken zu minimieren. Diese Sicherheitskontrollen werden dem Bedarf entsprechend auf eigene Umgebungen (physische oder virtuelle Appliances sowie Netzwerkgeräte wie etwa Router) sowie auf nicht-eigene Umgebungen (Security-as-a-Service, SECaaS), native Kontrollen und Workloads angewendet.

Was ist Firewalling?

In den heterogenen Netzwerken von heute befinden sich die Durchsetzungspunkte überall.

Firewalling sorgt für Konsistenz sowohl in Bezug auf Richtlinien als auch auf die Sicht auf Bedrohungen und ermöglicht so in der gesamten Umgebung eine schnellere und präzisere Prävention, Erkennung und Abwehr von Angriffen.

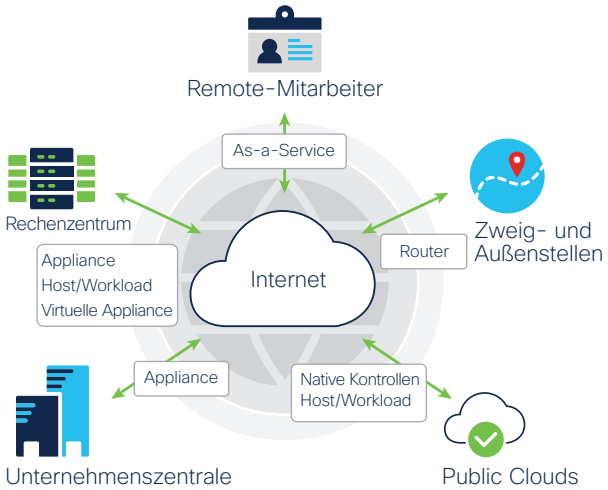


Abbildung 3: Die Kernelemente, mit denen Firewalling die Security-Herausforderungen moderner Netzwerke adressiert

Erweiterung der Sicherheitskontrollen

Beim klassischen Firewall-Ansatz, bei der der gesamte interne Datenverkehr sowie autorisierte Benutzer grundsätzlich als vertrauenswürdig galten (und externer Datenverkehr nicht), wurde der Schutz des Unternehmens vollständig am Netzwerkperimeter erreicht. Dieser Netzwerkperimeter wurde zum logischen Sicherheitskontrollpunkt, um das gesamte Unternehmen zu schützen. Unabhängig davon, ob er von der Zentrale, einem Rechenzentrum oder einem Remote-Mitarbeiter kam, wurde aller Netzwerk-Traffic über diesen zentralen Kontrollpunkt geleitet.

In den komplexen Umgebungen von heute, in denen die IT-Infrastruktur eines Unternehmens eine Vielzahl von Formfaktoren und Bereitstellungsmodellen wie etwa physische und virtuelle Appliances, in das Netzwerk integrierte, als Service bereitgestellte, Host-basierte oder im Rahmen einer Public Cloud umgesetzte Router oder Switches umfasst, funktioniert dieses Modell logischerweise nicht mehr.

Firewalling verfolgt einen Ansatz basierend auf konsistenten Sicherheitskontrollen für umfassende Transparenz, einheitliche Richtlinien und eine vollständige Sicht auf Bedrohungen. Diese Sicherheitskontrollen ermöglichen eine stärkere Benutzer- und Geräteauthentifizierung in zunehmend heterogenen Umgebungen. Sie erfassen Kontext zu Benutzern, Standorten, Geräten und mehr, tauschen diesen untereinander aus und reagieren darauf, um sicherzustellen, dass Geräte die festgelegten Sicherheitsanforderungen erfüllen. Gestützt auf an allen Mikroperimetern konsistenten Sicherheitskontrollen wird es Security-Teams möglich, Aufgaben wie etwa die Isolierung von Benutzern und Geräten, die die Compliance-Vorgaben nicht einhalten, die kontrollpunktübergreifende Blockierung fragwürdiger Domains oder auch die Einrichtung effektiver Mikrosegmente zu automatisieren. Beim Firewalling wird durch umfassende Transparenz ein vollständiger Überblick über alle Sicherheitswarnungen und -indikatoren ermöglicht und durch den Austausch von Threat-Intelligence sichergestellt, dass die Bedrohungserkennung auf jedem verbundenen Gerät auf dem neuesten Stand bleibt.

Cloud-basiertes Management

Doch nicht nur durch Punktlösungen ist das Risiko von Sicherheitsverletzungen gestiegen, sondern auch durch die explosionsartige Zunahme von Netzwerkperimetern und Cloud-Ressourcen. Kritische Unternehmensressourcen in komplexen Cloud-Umgebungen zu schützen und dabei auch noch verschiedene Security-Produkte verwalten zu müssen, das ist alles andere als einfach. Was Security-Teams benötigen, ist sofortige Übersicht und unkompliziertes Management, um Fehlkonfigurationen zu vermeiden.

Indem Firewalling das Management in der Cloud zentralisiert, reduziert es die Komplexität für Security-Teams und ermöglicht es ihnen, Richtlinien unternehmensweit anzugleichen. Dabei können Vorlagen die Ausgestaltung und Konsistenz von Richtlinien verbessern, da diese nur einmal geschrieben und dann über Zehntausende Sicherheitskontrollen im gesamten Netzwerk skaliert durchgesetzt werden können. Unter Einsatz von Standardvorlagen für Richtlinien lassen sich neue Geräte schneller bereitstellen und zudem Konfigurationsfehler reduzieren. Bei neuen Bereitstellungen im Zuge des Wachstums eines Unternehmens werden die Änderungen dann automatisch übernommen. Ein auf diese Weise skalierbares System für das Richtlinienmanagement integriert mehrere Sicherheitsfunktionen in einer einzigen Zugriffsrichtlinie und optimiert Richtlinien auf allen Security-Geräten, um Inkonsistenzen zu erkennen und schnell zu beheben.

Eine zentralisierte, Cloud-basierte Management-Lösung hebt zudem die Möglichkeiten der Teams auf ein neues Niveau, denn damit sind sie in der Lage, Risiken auf allen Geräten rasch zu identifizieren und deren Status so konsistent sicherer zu gestalten. So lassen sich mit einer zentralen Management-Konsole etwa Objekte auf allen Geräten vergleichen, um Inkonsistenzen aufzudecken und den aktuellen Sicherheitsstatus zu optimieren. Insgesamt kann das Team so das Richtlinienmanagement optimieren, die Effizienz steigern, Sicherheit konsistent gewährleisten und gleichzeitig die Komplexität reduzieren.

Starke Abwehr durch Threat-Intelligence

Mit der Erweiterung des Netzwerkperimeters und der zunehmenden Anzahl direkt mit dem Internet verbundener Geräte vergrößert sich die Angriffsfläche. Cyberbedrohungen rund um Malware, Kryptowährungen, Phishing und Botnet-Aktivitäten nehmen massiv zu, wobei sich die Kriminellen inzwischen auch Machine Learning und KI bedienen, um bestehende Sicherheitslücken in Software auszunutzen und Angriffe zu beschleunigen. Nur sehr wenige

Unternehmen verfügen über ausreichende Ressourcen, um alle Schwachstellen-Patches von Softwareanbietern vollständig zu testen und zu qualifizieren. Für die meisten ist die Abwehr neuer und sich entwickelnder Bedrohungen tatsächlich eine enorme Herausforderung.

Abhilfe schaffen kann hier ein weiterer Aspekt des Firewallings: Durch branchenführende Threat-Intelligence gestützt auf die neueste, teilweise nahezu minutenaktuelle Bedrohungsforschung sowie Zugang zu Updates zu Schutzmaßnahmen kann es den ständigen Strom an Bedrohungen bändigen. Dahinter stehen Bedrohungsforscher, die schnell Indicators of Compromise identifizieren und Bedrohungen rasch bestätigen und die entsprechenden Informationen verteilen. Skaleneffekte ermöglichen es ihnen dabei, Unternehmen vor neuen Bedrohungen zu schützen, bevor diese ihnen gefährlich werden können. Durch den Austausch von Threat-Intelligence in miteinander verbundenen Netzwerken, Endpunkten, Workloads und Cloud-Umgebungen können Security-Teams augenscheinlich voneinander unabhängige Ereignisse in Beziehung setzen, Rauschen beseitigen und Bedrohungen schneller aufhalten.

Auf Firewalling verzichten birgt Risiken

Im Zuge der Entwicklung ihrer Netzwerke haben Unternehmen verschiedenste Punktlösungen implementiert, um ihre Geschäftsanforderungen und Betriebsabläufe zu unterstützen. So haben sie mit dem Aufkommen neuer Angriffsvektoren immer wieder ein weiteres Produkt X ergänzt, um sich vor der neuesten Bedrohung Y zu schützen. Unternehmen, die mit einer klassischen Firewall alle über die verschiedenen Perimeter hinweg verbundenen Geräte abzusichern versuchen, riskieren jedoch, die wertvollsten Daten und Ressourcen für Sicherheitslücken preiszugeben. Dem Cybersecurity Almanac 2019 zufolge werden sich die im Zusammenhang mit Cyberkriminalität stehenden Kosten für Schäden bis 2021 auf 6 Billionen US-Dollar jährlich belaufen[5].

Bedrohungen dieser Art können sich schnell Zugang zu Netzwerken verschaffen. Fehlt es dann an umfassender Netzwerksicherheit und Endpunkt-Übersicht, ist der Geschäftsbetrieb in Gefahr.

Der Schutz von Netzwerk, Cloud-Umgebungen sowie Geräten und Daten der Unternehmen wird vor diesem Hintergrund zu einer immer größeren Belastung.

Firewalling beginnt und endet mit der Firewall als Tragsäule zukunftssicherer Netzwerksicherheit

Cisco hat erhebliche Anstrengungen in diese Vision investiert. Rund um den Globus arbeiten wir mit Unternehmen aller Größen zusammen, die alle bestätigen: Netzwerksicherheit muss flexibler werden und stärker integriert sein – eingebettet in das Netzwerk selbst. Genau das setzen wir in einer bislang unerreicht sicheren Architektur auf einer ebenso leistungsstarken wie umfassenden Plattform um, deren Grundlage die Firewall bildet.

Dieses Konzept – bzw. das dadurch bislang unerreichte Schutzniveau – ist ein zentrales Element unserer Security-Strategie. Mit dem Security-Portfolio und den Firewalls von Cisco bleiben Sie neuen Bedrohungen immer den entscheidenden Schritt voraus – dank erstklassigen Sicherheitskontrollen, konsistenten Richtlinien und Transparenz sowie Innovationen, die Security-Abläufe verbessern.

In einer Zeit beispielloser Dynamik in der Bedrohungslandschaft vereint Cisco führende Netzwerke und modernste Technologie, die Ihnen heute wie morgen zu einem Sicherheitsstatus von maximaler Stärke verhelfen.

5 „2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics“, Cybercrime Magazine, 6. Februar 2019.

Herkömmliche Firewalls bieten jedoch nur einen begrenzt Einblick. Was die IT benötigt, ist netzwerkweite Transparenz unter Austausch von Threat-Intelligence, um Bedrohungen früher und schneller erkennen und blockieren zu können. Firewalling dagegen geht weiter. Es sorgt für starke Sicherheit, basierend auf zentralisiertem Management und umfassenden Security-Funktionen wie Intrusion Prevention, URL-Filterung und Advanced Malware Protection, die Automatisierung und Machine Learning für mehr Effizienz nutzen.

Ohne Firewalling als strategisches Element des Security-Ansatzes kann die Komplexität des Netzwerks in Fehlkonfigurationen resultieren und das Risiko einer Sicherheitsverletzung erhöhen. So stellt etwa Gartner fest, dass bis 2022 „mindestens 95 % der Sicherheitsvorfälle in Clouds durch Kunden selbst verursacht werden".[6] Mit einer Firewalling-Strategie, in deren Rahmen Sicherheitsrichtlinien über mehrere Kontrollpunkte hinweg harmonisiert werden, erhalten Unternehmen einen insgesamt stärkeren Sicherheitsstatus.

3. Zur Firewalling-Strategie in vier Schritten

Schritt 1: Eine erfolgreiche Firewall-Strategie benötigt eine moderne Next-Generation Firewall als Grundlage. Dies zu Ihnen passende Cisco Secure Firewall gewährleistet konsistente Sicherheitsrichtlinien und Transparenz sorgt innerhalb Ihrer integrierten Security-Lösung für eine verbesserte Reaktion auf Bedrohungen.

Schritt 2: Nach der Wahl Ihrer Cisco Secure Firewall geht es im nächsten Schritt um die Standardisierung einer Management-Lösung. Welche Lösung für Ihr Unternehmen die richtige ist, sollten Sie an folgenden Faktoren festmachen:

- Von wo aus Ihre Lösung verwaltet werden soll (On-Premises oder Cloud) und welcher Bereich das Security-Management übernimmt (SecOps oder NetOps).
- Besonders wichtig dabei ist, ob die Management-Lösung sowohl ihre aktuellen als auch zukünftigen IT-Ziele erfüllen kann. Wenn Sie Workloads in die Cloud überführen, ein Anbieterportal einrichten oder Ihre Digitalisierung oder den Einsatz von SaaS-Anwendungen vorantreiben, sollten Sie auf Cloud-basiertes Management setzen. Arbeitet Ihr Unternehmen mit monolithischen Legacy-Anwendungen, sind Sie womöglich mit On-Premise-Lösungen gut beraten. Im Allgemeinen ist bei Legacy-Anwendungen ein gewisses Maß an Refactoring erforderlich, damit sie in der Cloud ausgeführt werden können. Wenn keine unmittelbaren Pläne für ein Upgrade dieser Anwendungen bestehen, ist On-Premise-Management in der Regel die beste Lösung.
- Mit einer Cloud-basierten Management-Lösung können NetOps-Teams Richtlinien unternehmensweit angleichen, die Komplexität reduzieren und alle Sicherheitskontrollpunkte über ein zentrales Dashboard verwalten. Für den Schutz vor den neuesten Bedrohungen lassen sich auf einfache Weise und von einem Ort aus konsistente Richtlinien orchestrieren und verwalten. Mit einer zentralisierten, Cloud-basierten Anwendung optimieren Sie das Security-Management, stellen neue Geräte anhand von Vorlagen schneller und behalten alle Änderungen an Ihren Umgebungen im Zeitverlauf im Blick.

Schritt 3: Nun stärken Sie durch Integration Ihren Sicherheitsstatus. Ihre Firewalling-Strategie sollte sich auf die umfassende Abdeckung aller Mikroperimeter sowie den Schutz und die Kontrolle für alle verbundenen Geräte und Security-Lösungen stützen. Durch die Integration von Security in Ihr gesamtes heterogenes Netzwerk – von Cloud-Anwendungen und -Services über E-Mail-Systeme bis hin zu allen verbundenen Endpunkten – stärken Sie Ihren Schutz gegenüber der wachsenden Bedrohungslandschaft.

Dieser Schritt bringt ihr Security-Team in Position, um mehr Bedrohungen zu blockieren, schneller auf komplexe Bedrohungen zu reagieren und vom Netzwerk über Cloud-Anwendungen bis hin zu Endpunkten Automatisierung umzusetzen.

Schritt 4: Abschließend implementieren Sie im Rahmen Ihrer Firewalling-Strategie durchgängige, fortschrittliche Bedrohungsanalysen, mit deren Hilfe Sie die Ressourcen Ihres Unternehmens schützen und neuen Bedrohungen

6 „Is the Cloud Secure?", Gartner, 27. März 2018.

einen Schritt voraus bleiben. Am einfachsten erreichen Sie dies mit einer Lösung, die über Ihre Firewall automatisch die neuesten Bedrohungsinformationen für Ihr Netzwerk bereitstellt. Aktuelle Intelligence und umfassende Transparenz vermittelt Security-Teams ein Verständnis bestehender Schwachstellen und lässt sie nachvollziehen, wo und wie Bedrohungen gegebenenfalls ihren Weg in die Umgebung gefunden haben. Mithilfe eines integrierten IPS der nächsten Generation können zudem die Klassifizierung von Risiken und die Kennzeichnung nach Auswirkungen automatisiert und so die wichtigsten Ressourcen und Informationen ausgemacht und priorisiert werden. Für Security-Teams bedeutet das: Sie können direkt Gegenmaßnahmen einleiten und sich bei der Beseitigung von Bedrohungen auf die wichtigsten Ressourcen konzentrieren, ohne dabei durch „Rauschen" abgelenkt zu werden, was den SOC-Betrieb insgesamt effektiver macht.

Die passende Firewall als Grundlage

Security-Teams benötige heute:

Effektivere Sicherheit, die es ihnen durch branchenführende Threat-Intelligence ermöglicht, Bedrohungen in komplexen Netzwerke frühzeitig zu erkennen und somit früher gegen sie vorzugehen.

Einen Weg, Sicherheitsrichtlinien unternehmensweit **effizient einzurichten, zu skalieren und zu harmonisieren**.

Übersicht und reduzierte Komplexität durch übergreifendes Management und umfassende Automatisierung, die Sicherheitsvorgänge beschleunigt und ihre Arbeit erleichtert.

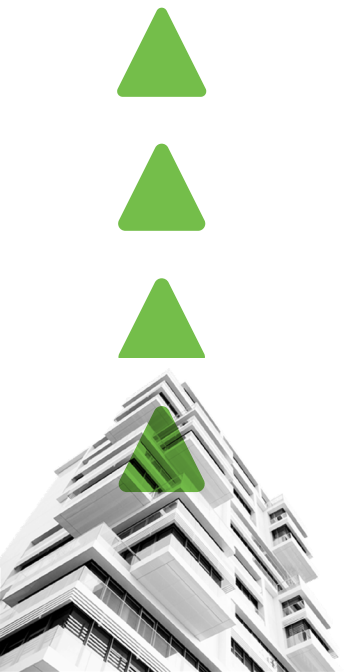
Netzwerk und Sicherheit, die einen Verbund bilden, der die Nutzung bestehender Investitionen maximiert. Die richtige Lösung bietet so umfassende Integrationen, dass Sicherheit jederzeit und überall greift.

Vorteile einer Firewalling-Strategie auf Basis von Cisco Secure Firewall

Ihr gesamtes Netzwerk wird zur Erweiterung Ihrer Sicherheitsarchitektur: Switches und Router können Richtlinien, Intrusion-Prevention-Funktionen und andere Kernfunktionen von Cisco Secure Firewall abrufen, um Sicherheitsvorgaben durchzusetzen. So wird die Netzwerkinfrastruktur zu einem umfassenden Security-Portfolio, mit dem Threat-Intelligence schnell architekturübergreifend ausgetauscht und augenscheinlich voneinander unabhängige Ereignisse korreliert, Rauschen vermieden und Bedrohungen schneller dingfest gemacht werden.

Erstklassige Sicherheitskontrollen: Cisco Secure Firewall schützt komplexe Netzwerke durch hochgradig effektive Mechanismen vor den immer raffinierteren Angriffen von heute. Branchenführende, fortschrittliche Threat-Intelligence hilft Ihrem Unternehmen, neue Malware-Domains und schädliche URLs sowie unbekannte oder nicht veröffentlichte Schwachstellen zu finden und so Bedrohungen früher zu erkennen und schneller zu handeln. Das integrierte IPS der nächsten Generation liefert Security-Teams automatisch Risikoklassifizierungen einschließlich Kennzeichnungen entsprechend Auswirkungen, durch die Rauschen vermieden wird und zielführend priorisiert werden kann. Retrospective Security analysiert durchgängig Bedrohungen nach ihrer ersten Erkennung und vermittelt Ihnen so, wie Sie komplexe Malware, deren Tarnung bislang womöglich noch nicht aufgeflogen ist, besser aufspüren.

Einheitliche Richtlinien und vollständige Sicht auf Bedrohungen: Mittels auf allen Geräten standardisierten Sicherheitskontrollen, die von Netzwerk-Appliances über Hosts bis hin zur Cloud an alle Systeme übertragen werden, erreichen Security-Teams Konsistenz und Harmonisierung von Richtlinien. Dabei lassen sich über das flexible, zentralisierte Management von Cisco auf schnelle und unkomplizierte Weise Kontrollen auf große Zahlen von Geräten anwenden, um durchgehend konsistente Richtlinien zu gewährleisten. Durch die Verwaltung von zentraler Stelle sowie automatische Korrelation von Bedrohungen zwischen eng miteinander integrierten Security-Funktionen wie Anwendungs-Firewalling, NGIPS und AMP reduzieren Sie die Komplexität. Unkomplizierte Prozesse rund um Sicherheitsrichtlinien und das Gerätemanagement beschleunigen zentrale Security-Vorgänge wie die Erkennung, Untersuchung und Beseitigung von Bedrohungen.



4. Eine zukunftsfähige Security-Lösung

Unsere Arbeitsweise hat sich verändert. Neue Entwicklungen rund um Geschäftsprozesse und Netzwerke haben die Karten für ihre Absicherung neu gemischt. Daher gilt es, die Firewall neu zu denken und in ein neues Konzept zu überführen: das Firewalling.

Cisco treibt Innovationen voran, um diesen Trends mit einer Security-Plattform zu begegnen, die erstklassige Sicherheitskontrollen überall dort implementiert, wo sie benötigt werden – mit konsistenten Sicherheitsrichtlinien und Transparenz, unterstützt durch branchenführende Threat-Intelligence. Die neueste Generation von Cisco Secure Firewall bildet die Grundlage für unser Portfolio an eng miteinander integrierten Produkten.

Die Cloud-Management-Lösung von Cisco – **Cisco Defense Orchestrator** – ermöglicht die Harmonisierung der Richtlinien für eine Vielzahl von Cisco Security-Produkten.

In jedem Cisco Security-Produkt ist **Secure Threat Response** enthalten, eine automatisierte Threat Response-Lösung, die auf neue Cyberangriffe reagiert, indem sie automatisch Gegenmaßnahmen in der gesamten Security-Architektur einleitet und implementiert.

Secure Endpoint bietet globale Threat-Intelligence, erweitertes Sandboxing und Malware-Blockierung in Echtzeit. Die Lösung analysiert laufend die Dateiaktivitäten im gesamten erweiterten Netzwerk, sodass Sie komplexe Malware schneller aufspüren, eingrenzen und beseitigen können.

Talos Threat Intelligence ist ein weltweit führendes Team von Sicherheitsforschern, Datenanalysten und Technikern, die sich einzig dem Ziel verschrieben haben, Informationen über bestehende und sich entwickelnde Bedrohungen zusammenzutragen, um diese zum Schutz vor Angriffen und Malware an das gesamte Cisco Security Ecosystem zu übermitteln. Talos liefert Einblicke in die neuesten globalen Bedrohungen sowie konkret für die Abwehr, Eindämmung und konzertierte Reaktion umsetzbare Daten, um alle Cisco Kunden aktiv zu schützen.

SNORT Next-Generation Intrusion Prevention System (SNORT NGIPS) ist ein branchenführendes Open-Source-NGIPS, das Datenverkehrsanalysen, Packet Sniffing/Logging und Protokollanalysen durchführt. SNORT NGIPS trägt zum Schutz der gesamten Security-Community bei, indem es auf Basis der Threat-Intelligence von Talos Richtlinien für die Abwehr neuer Bedrohungen verteilt.

Mit der Identity Services Engine (ISE) ist anpassungsfähiger, vertrauenswürdiger Zugriff überall und kontextbasiert verfügbar. Sie bietet intelligenten, integrierten Schutz durch Intent-Based-Richtlinien und Compliance-Lösungen.

Secure Access by Duo bietet Multi-Faktor-Authentifizierung, Endpunkt-Transparenz, adaptive Authentifizierung und Richtliniendurchsetzung mit Remote-Zugriff und Single Sign-On, um den Zugriff auf Anwendungen proaktiv zu sichern.

Secure Network Analytics, Secure Workload und Application Centric Infrastructure (ACI) bilden einen Verbund, der Ihre Benutzer jederzeit und überall und Ihre Anwendungs-Workloads in jeder beliebigen Umgebung im Blick behält. Gestützt auf Machine Learning, Verhaltensmodelle, Netzwerkinfrastruktur-Telemetrie und Segmentierung werden dabei auch neue Bedrohungen unschädlich gemacht.

Mit der Cisco Security-Plattform einschließlich Cisco Secure Firewall setzen Sie auf eine zukunftsfähige Firewalling-Strategie, die Ihnen bereits heute einen bislang unerreichten Sicherheitsstatus vermittelt und Sie auch für morgen optimal wappnet.

Abschnitt 5: Noch heute die Zukunft der Firewall umsetzen

Cisco vereint führende Netzwerklösungen und modernste Security-Technologie in einer Architektur mit nie dagewesener Sicherheit. Ganz gleich, ob Sie Ihre Netzwerksicherheit durch die Optimierung vorhandener Investitionen verbessern oder Ihre Router in eine Firewall verwandeln möchte – bei Cisco setzen Sie auf kontinuierliche Innovation.

Cisco Secure Firewall sorgt für den Schutz von Unternehmen auf ihrem Weg in die Digitalisierung – mit Netzwerksicherheit von dem Spezialisten, der bereits das Netzwerk konzipiert hat.

Informieren Sie sich noch heute über Cisco Secure Firewall und starten Sie Ihre Firewalling-Reise. Um mehr über die neuesten Trends zu erfahren, die die Netzwerke von morgen prägen, sollten Sie außerdem den Global Networking Trends Report 2020 lesen.