STRATA™
BY PALO ALTO NETWORKS

Kubernetes-Umgebungen schützen mit Firewalls der CN-Series

Neuartige Containerfirewalls für cloudnative Anwendungen

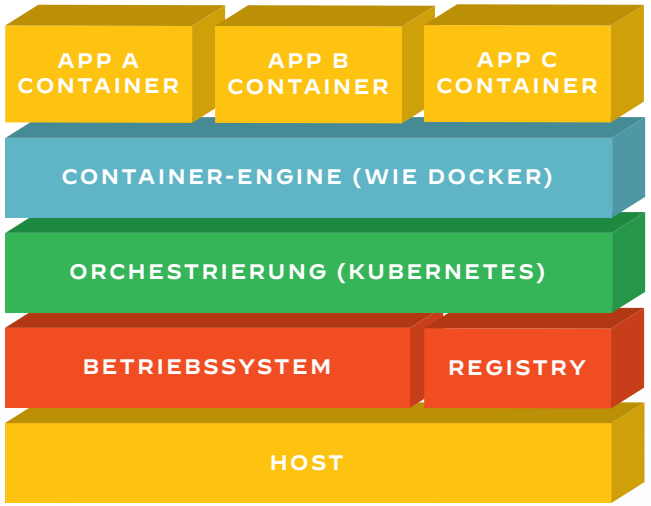
paloalto® NETWORKS

Inhalt

Dynamisches Duo: Container und Kubernetes

In nur wenigen Jahren sind Containertools – besonders Docker – zur wichtigsten Komponente bei der Entwicklung und Bereitstellung von Software-Anwendungen in Cloud-Umgebungen geworden. Prognosen zufolge werden Ende 2023 über 70 Prozent der global agierenden Unternehmen mindestens drei containerisierte Anwendungen in ihren Produktionsumgebungen nutzen. 2019 waren es weniger als 20 Prozent.[1]

Dieser explosionsartige Anstieg spiegelt sich auch in der zunehmenden Nutzung von Kubernetes® wider,[2] das de facto zum Standard für die Containerorchestrierung geworden ist. Damit sind Kubernetes und Container nun ebenso wie DevOps-Prozesse und Microservices Schlüsselelemente der cloudnativen Revolution.



[1] Forschungsergebnisse von Gartner, zitiert von Janakiram MSV in „5 Modern Infrastructure Trends To Watch Out for in 2019“, Forbes, 20. Dez. 2018.

[2] „6 Best Practices for Creating a Container Platform Strategy“, Gartner, letzte Änderung am 23. April 2020. Hinweis: Veröffentlicht am 31. Oktober 2017.

Ursprünglich waren Entwickler die wichtigsten Befürworter von Kubernetes und Containerisierung, aber inzwischen gibt es auch im IT-Betrieb mehr und mehr Fürsprecher. Weiterlesen

Wer treibt die Containernutzung voran?

Kubernetes wurde bei Google von Technikern für Techniker entwickelt. Bei DevOps-Teams und Entwicklern waren Kubernetes und Container schon bald sehr beliebt, doch im Betrieb stand man ihnen zunächst skeptisch gegenüber.

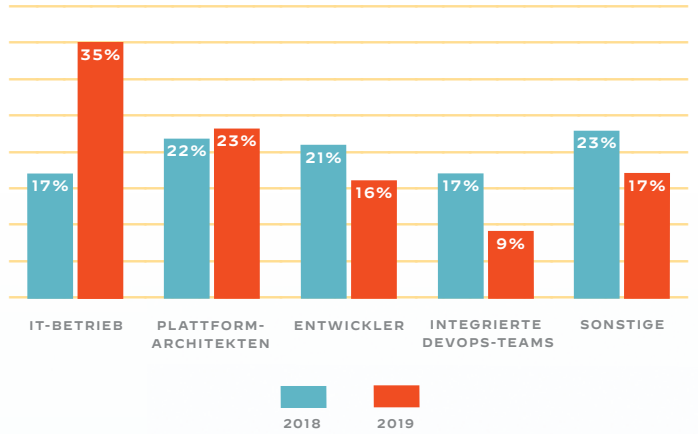
Das hat sich grundlegend geändert. Kubernetes und Container gehören nun zum Mainstream und genießen die volle Unterstützung des IT-Betriebs. 2018 wurde die Containernutzung in nur 17 Prozent der untersuchten Unternehmen vom IT-Betrieb vorangetrieben; ein Jahr später lag dieser Anteil bereits bei 35 Prozent.

In vielen Organisationen fallen Container nicht mehr in den Verantwortungsbereich einzelner Plattformarchitekten, Entwickler, DevOps- und anderer Teams, sondern in den des IT-Betriebs.[3] Nichtsdestotrotz stehen Entwickler weiterhin unter Druck, ihre Anwendungen vor der Übergabe an die Betriebsteams hinreichend zu sichern.

Wussten Sie schon?

„In der cloudnativen Entwicklung gibt es immer neue Prozesse und Threads, die Anwendungen gefährden können … Workloads müssen schon gesichert sein, wenn sie gestartet werden.“[4] – Gartner

Befürworter der Containernutzung in Unternehmen



Quelle: Diamanti, 2019

[3] „2019 Container Adoption Benchmark Survey“, Diamanti, 2019.

[4] „Market Guide for Cloud Workload Protection Platforms“, Gartner, 8. April 2019.

DevOps ist ein extrem dynamischer Bereich und stellt Entwickler beim Schutz von Anwendungen und Services vor erhebliche Herausforderungen.
Mehr dazu im nächsten Abschnitt.

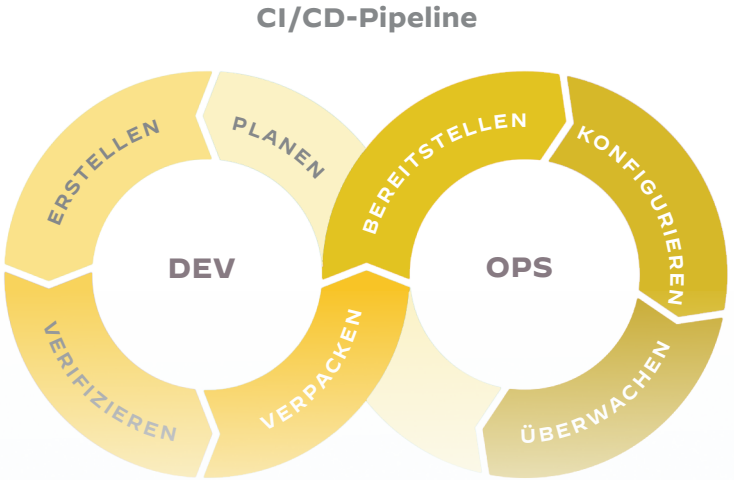
Das DevOps-Sicherheitsdilemma

Einer der Hauptvorteile eines DevOps-Ansatzes ist eine beschleunigte Markteinführung mithilfe von CI/CD-Prozessen (Continuous Integration/Continuous Delivery).

CI/CD-Pipelines verbinden Komponenten wie Code- und Image-Repositorys, Container, Build-Server und Drittanbietertools, um für eine effiziente Integration und Bereitstellung zu sorgen. Die damit einhergehenden komplexen Abhängigkeiten und Konfigurationen können jedoch zu Schwachstellen führen, die von Hackern ausgenutzt werden können, um Daten auszuschleusen, die Produktion zu stören und sogar die ganze Infrastruktur lahmzulegen.

Da sie kurzlebig und voneinander isoliert sind, erscheinen Container als sichere Umgebung zur Ausführung von Anwendungen. Oft werden jedoch mehrere Container im selben IP-Adressbereich bereitgestellt. Hacker müssen sich nur Zugang zu einem einzelnen Container in diesem Bereich verschaffen, um sich im gesamten Cluster auszubreiten.

Unter anderem aus diesem Grund sollte der Schutz der CI/CD-Pipeline zu den Top-Prioritäten jedes DevOps-Teams gehören. Das ist aber oft leichter gesagt als getan. Es ist riskant, die Implementierung von Schutzmaßnahmen ausschließlich den Entwicklern zu überlassen, da dies kritische Ressourcen binden kann, die dann bei der Anwendungsentwicklung fehlen und die Sicherheit insgesamt letztendlich schwächen, statt sie zu stärken. Die CI/CD-Sicherheit kann nicht nachträglich aufgesetzt werden – sie muss von Anfang an in den Anwendungslebenszyklus integriert werden.[5]



Wussten Sie schon?

Volle Kraft voraus: Releasezyklen werden, vom zunehmenden Einsatz von DevOps, CI/CD-Tools und agilen Methologien vorangetrieben, immer kürzer. Die Anzahl der Unternehmen mit täglichen Releasezyklen wurde zwischen 2018 (15 Prozent) und 2019 (27 Prozent) fast verdoppelt und wöchentliche Releasezyklen sind von 20 Prozent auf 28 Prozent gestiegen.[6]

[5] „The Greatest Security Risks Lurking in Your CI/CD Pipeline“, Twistlock, 8. Juli 2020.

[6] „CNCF Survey 2019“, The Cloud Native Computing Foundation, 2019.

Mikrosegmentierung spielt beim Schutz cloudnativer Anwendungen eine wichtige Rolle – doch auch sie hat ihre Grenzen, wie Sie im nächsten Abschnitt erfahren.

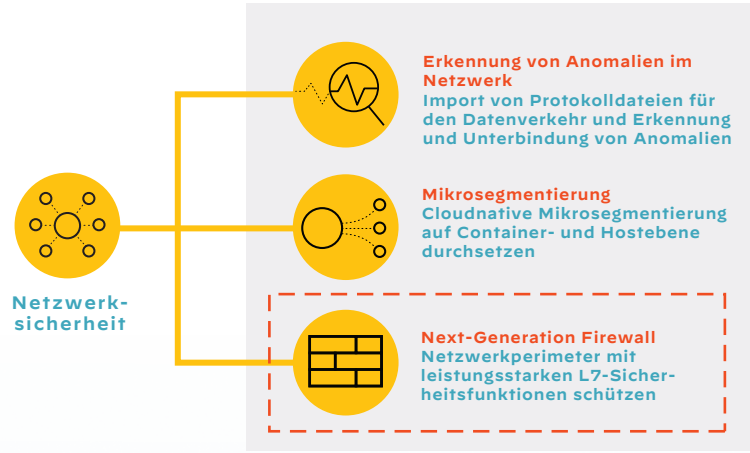
Was mit Mikrosegmentierung möglich ist – und was nicht

Bewährte Techniken wie Richtliniengruppen, Zugriffskontrolllisten und die Sperrung von Ports sind für den Schutz von On-Premises- und Cloud-Bereitstellungen immer noch wichtig. Doch Cloud-Umgebungen bringen ganz eigene Herausforderungen mit sich und erfordern daher zusätzliche Sicherheitsmaßnahmen – insbesondere die Mikrosegmentierung, die bei der Bedrohungsabwehr eine zentrale Rolle spielt. Mikrosegmentierung schafft die Voraussetzungen für das Blockieren von Angriffen auf Container- und Hostebene und verhindert so die Angriffsausbreitung in containerisierten Umgebungen.

Das Blockieren von Datenverkehr allein ist jedoch ein Schwarz-Weiß-Ansatz, der nicht alle Nuancen der internen Interaktionen zwischen cloudnativen Anwendungen berücksichtigen kann. Hier kommen Next-Generation Firewalls (NGFWs) ins Spiel. Mithilfe von Analysen auf Anwendungsebene, Intrusion Prevention, Threat Intelligence und weiteren Schutzfunktionen bieten NGFWs eine zusätzliche Sicherheitsebene. Sie schützen den ausgehenden Datenverkehr (wie Code-Repositorys) zwischen Entwicklern und ihren Websites, den Ost-West-Verkehr zwischen mehreren containerisierten Anwendungen bzw. zwischen containerisierten und älteren Anwendungen und prüfen den eingehenden Datenverkehr auf Bedrohungen.

Wussten Sie schon?

„Der Perimeterschutz ist keine effektive Strategie mehr. Mit Zero Trust erschließen Sie sich Methoden wie Microcore, Mikrosegmentierung und granulare Transparenz, mit denen Sie Bedrohungen identifizieren und isolieren und damit die Auswirkungen einer Sicherheitsverletzung begrenzen können.“ – Forrester



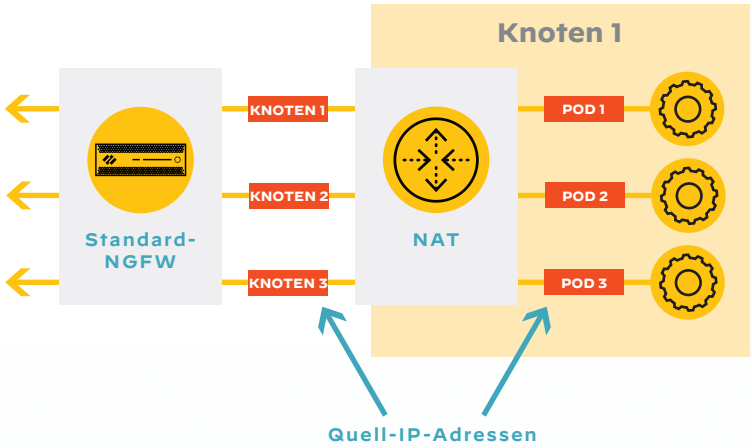
Um in cloudnativen Umgebungen für umfassende Sicherheit zu sorgen, sind Funktionen zur Erkennung von Anomalien im Netzwerk sowie Mikrosegmentierung und Firewalls erforderlich.

NGFWs sind ein kritischer Bestandteil der Netzwerksicherheit in cloudnativen Umgebungen. Es reicht jedoch nicht aus, noch mehr von den NGFWs zu kaufen, die Sie bereits im Rechenzentrum haben – lesen Sie im folgenden Abschnitt, warum nicht.

NGFWs: von außen betrachtet

Konventionelle NGFWs sind beim Schutz von On-Premises-Umgebungen unentbehrlich – die wenigsten Rechenzentren kommen ohne sie aus. Cloudnative Umgebungen bringen jedoch ganz spezielle Herausforderungen mit sich, für die NGFWs nicht konzipiert wurden, insbesondere, wenn es um die interne Analyse einer Kubernetes-Umgebung geht.

In Kubernetes werden Pods (Containergruppen) auf Knoten ausgeführt, wobei die Knoten physische Hosts oder virtuelle Maschinen (VMs) sein können. Für die Entwickler nur selten von Interesse, für die Firewalls hingegen schon. NGFWs können nicht erkennen, von welchem Pod in einem Knoten ein Datenpaket stammt, weil sämtliche Quell-IP-Adressen in die IP-Adresse des Knotens übersetzt werden. Für konventionelle Firewalls sieht der gesamte ausgehende Traffic von einem Knoten gleich aus.



Bei der Network Address Translation (Netzwerkadressenübersetzung, NAT) erhalten alle ausgehenden Datenpakete die Quell-IP-Adresse des Knotens.

Wussten Sie schon?

Grundlagen von Kubernetes:

- Container werden in Kubernetes in Pods zusammengefasst, die dann bestimmten Knoten zugewiesen werden.
- Ein Cluster ist eine Sammlung von Pods, die auf demselben Host ausgeführt werden. Durch Cluster kann für High Availability (hohe Verfügbarkeit, HA) gesorgt werden.
- Ein Kubernetes-Service ist eine zusammengehörende Gruppe von Pods, zum Beispiel eine Schicht einer mehrschichtigen Anwendung.

Optimale Netzwerksicherheit in cloudnativen Umgebungen lässt sich durch den Einsatz nativer Kubernetes-Konstrukte erreichen – insbesondere durch Namespaces. Im nächsten Abschnitt erfahren Sie Näheres.

Namespaces: ein leistungsstarkes Tool für cloudnative Sicherheit

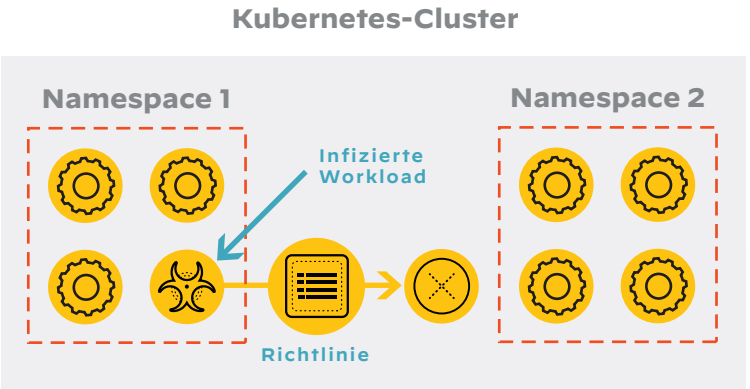
Kubernetes stellt konventionelle Sicherheitstools zwar vor einige Herausforderungen, bietet aber gleichzeitig auch die Möglichkeit, diese Sicherheit durch den Einsatz nativer Konstrukte zu stärken – zum Beispiel durch Namespaces.

Mit Kubernetes-Namespaces ist es leichter, einzelne Richtlinien gezielt auf bestimmte Teile eines Clusters anzuwenden. Das vereinfacht die Clusterverwaltung insgesamt. Security-Teams können Namespaces nutzen, um Workloads in einem Cluster zu isolieren und so das Risiko der Ausbreitung von Angriffen zu reduzieren. Zudem können sie zur Schadensbegrenzung im Fall eines erfolgreichen Angriffs Ressourcenquoten festlegen.[7]

Viele zukunftsorientierte Sicherheitsarchitekten wollen den Datenverkehr, der namespace-übergreifend oder an ältere Workloads wie Bare-Metal-Server übertragen wird, besser schützen können. Doch dazu benötigen sie Einblick in die physischen Cluster und den Status der darin enthaltenen Objekte wie Namespaces, Pods und Container. Da diese Informationen außerhalb der jeweiligen Umgebung nicht verfügbar sind, muss eine Sicherheitslösung innerhalb der Kubernetes-Umgebung installiert werden.

Wussten Sie schon?

Namespaces sind virtuelle Cluster innerhalb eines physischen Kubernetes-Clusters.



Auf Namespaces basierende Sicherheitsrichtlinien verhindern die Ausbreitung von Exploits innerhalb eines physischen Clusters.

[7] „Kubernetes Security Best Practices“, Twistlock, 6. Juni 2019.

Nun haben wir die Schlüsselelemente einer effektiven cloudnativen Firewall vorgestellt.
Im nächsten Abschnitt wenden wir uns einer solchen Firewall zu: der CN-Series von Palo Alto Networks.

Netzwerksicherheit für Kubernetes: die CN-Series von Palo Alto Networks

Die Anforderungen und Herausforderungen cloudnativer Umgebungen rund um eine neue Art der Netzwerksicherheit gaben Palo Alto Networks den Ansporn zur Entwicklung der NGFWs der CN-Series – und damit der branchenweit ersten speziell für Kubernetes konzipierten Lösung.

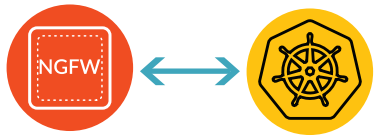
Diese Firewalls werden in Form von zwei verschiedenartigen Pods bereitgestellt: Ein Pod fungiert als Managementebene (CN-MGMT) und ein weiterer Pod als Firewalldatenebene (CN-NGFW). Der Managementpod läuft stets als Kubernetes-Service. Die Pods der Datenebene können auf zwei Arten bereitgestellt werden: verteilt oder im Cluster. Im verteilten Modus läuft die Firewalldatenebene auf jedem Knoten als DaemonSet. Somit können Administratoren Firewalls mit einem einzigen Befehl auf jedem Clusterknoten und Sicherheitskontrollen so nah wie möglich an den einzelnen Workloads bereitstellen. Im Clustermodus läuft die Firewalldatenebene auf einem dedizierten Sicherheitsknoten als Kubernetes-Service. In diesem Modus nutzt die CN-Series native Kubernetes-Funktionen, um die Sicherheitsvorkehrungen automatisch zu skalieren und dadurch selbst die dynamischsten Kubernetes-Umgebungen effektiv zu schützen. Die Bereitstellung in Clustern eignet sich am besten für große Kubernetes-Umgebungen, in denen der verteilte Modus zu ressourcenintensiv und teuer wäre.

Dank der nativen Integration mit Kubernetes können die Firewalls der CN-Series bei der Erstellung von Sicherheitsrichtlinien auf Kontextinformationen zu den Containern in der Umgebung zugreifen. So kann beispielsweise ein Containernamespace als Datenverkehrsquelle in eine Firewallregel aufgenommen werden.

Wussten Sie schon?

Die CN-Series ist die neueste Lösung im Portfolio preisgekrönter NGFWs von Palo Alto Networks.

Bereitstellungsmodelle für NGFWs



Standard-NGFW — Kubernetes

Bereitstellungsmodelle für die CN-Series

Kubernetes-Managementebene

Container: CN-Series-Managementebene

Kubernetes-Datenebene

Container: CN-Series-Datenebene

Die CN-Series wird in Kubernetes-Umgebungen nativ in Form verschiedener Pods für die Management- und die Datenebene bereitgestellt.

Dank ihres einzigartigen Designs und Bereitstellungsmodells bietet die CN-Series wichtige Vorteile zur Stärkung Ihrer cloudnativen Anwendungssicherheit – Näheres dazu finden Sie im folgenden Abschnitt.

Vorteile der CN-Series für Sicherheitsteams und Entwickler

Transparenz und Kontrolle in Kubernetes-Umgebungen

Mit der CN-Series werden Sicherheitsfunktionen direkt in die Containerumgebung integriert, um die Leistungsgrenzen konventioneller Firewalls zu überwinden. Dadurch gewinnen Sicherheitsteams einen umfassenden Überblick über den gesamten Traffic, einschließlich der bislang kaum ermittelbaren Quell-IP-Adressen ausgehender Datenpakete. Dank der nativen Integration mit Kubernetes kann die CN-Series außerdem auf Kontextinformationen über Container zugreifen, um in genehmigtem, namespace-übergreifendem Datenverkehr verborgene Bedrohungen zu erkennen und zu blockieren.

Einheitliche cloudnative Sicherheit in allen Umgebungen

Konventionelle NGFWs ermöglichen nur begrenzten Einblick in Containerumgebungen und bieten cloud-nativen Anwendungen daher nicht genug Schutz. Mithilfe der CN-Series können Netzwerksicherheitsteams in cloudnativen Umgebungen dasselbe Sicherheitsniveau erreichen wie im restlichen Netzwerk. Außerdem können die zu Kubernetes-Umgebungen gesammelten Kontextdaten mit anderen Firewalls von Palo Alto Networks geteilt werden. Dies verbessert den Informationsaustausch und das Sicherheitsniveau des gesamten Netzwerks.

Bessere Integration der Sicherheit in DevOps-Umgebungen

Die CN-Series bindet die Firewallbereitstellung mithilfe nativer Kubernetes-Orchestrierungsfunktionen direkt in den CI/CD-Entwicklungsprozess ein und sorgt damit für einen schnellen, flexiblen und reibungslosen DevOps-Betrieb. Somit können Entwickler die CN-Series mit einem einzigen Befehl in einer YAML-Datei auf sämtlichen Knoten in einem Cluster bereitstellen.

Zentralisierte Sicherheitsverwaltung in hybriden Infrastrukturen

Ein Nachteil vieler hybrider Bereitstellungsmodelle ist, dass die Sicherheitsteams mehrere Management-konsolen nutzen müssen. Das bedeutet, dass sie sich in verschiedene Betriebskonzepte einarbeiten und Sicherheitsrichtlinien auf allen Konsolen manuell miteinander abgleichen müssen. Die Firewalls der CN-Series hingegen werden von den Netzwerksicherheitsfunktionen von Palo Alto Networks Panorama™ verwaltet. Somit können Sicherheitsanalysten alle Komponenten von einer zentralen Konsole aus kontrollieren und sparen viel Zeit und Aufwand.

Die CN-Series ist eine vielseitige Lösung, die sich für die unterschiedlichsten Anwendungsfälle eignet, darunter auch die im nächsten Abschnitt beschriebenen.

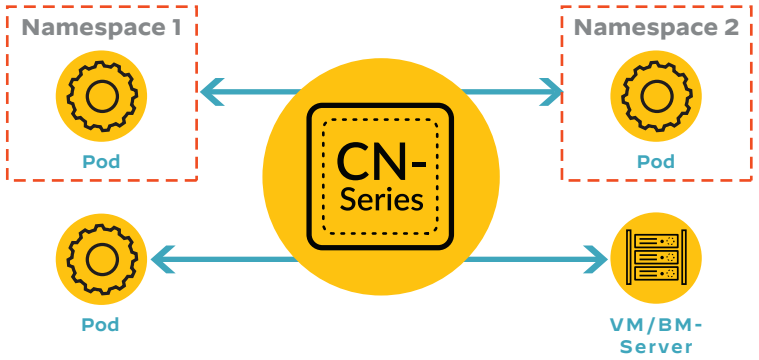
Typische Anwendungsfälle der CN-Series

Schutz des ausgehenden Datenverkehrs

Die CN-Series untersucht den ausgehenden Datenverkehr (auch den verschlüsselten TLS/SSL-Datenverkehr), blockiert verdächtige Aktivitäten und verhindert damit die Ausschleusung kritischer Daten. Im Gegensatz zu konventionellen NGFWs können Firewalls der CN-Series den gesamten von einer containerisierten Anwendung stammenden Datenverkehr analysieren. Die URL Filtering-Funktion der Firewalls der CN-Series ist für Entwickler besonders nützlich, da sie den unbeabsichtigten Zugriff auf Websites mit schädlichem Inhalt (wie Code-Repositorys mit versteckter Malware) verhindert.

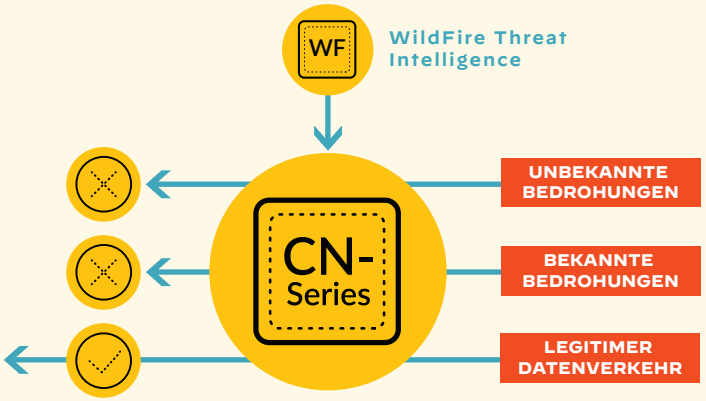
Schutz des Ost-West-Datenverkehrs

Die Firewalls der CN-Series bieten Unternehmen Transparenz und Kontrolle auf Anwendungsebene sowie modernste Sicherheitsservices wie Intrusion-Prevention-Systeme (IPS), um den zwischen Pods in verschiedenen Vertrauenszonen (zum Beispiel zwischen zwei Namespaces) fließenden Ost-West-Datenvekehr zu schützen. Außerdem sichern die Firewalls den Datenverkehr zwischen Pods und anderen Workloadarten, wie VMs und Bare-Metal-Servern, um für konsistente Sicherheit in Ihrer gesamten Umgebung zu sorgen.



Schutz des eingehenden Datenverkehrs

Die Firewalls der CN-Series stoppen mithilfe von speziellen Signaturen, die nicht auf Hashwerten, sondern auf Inhalten basieren, die Einschleusung neuer, bislang unbekannter Varianten bereits bekannter Malware. Unser Malwareschutz WildFire® ist kontinuierlich auf der Suche nach neuartiger Malware und aktualisiert die Firewalls innerhalb von Sekunden, wenn neue Bedrohungen gefunden werden. So ist Ihr Netzwerk selbst vor den jüngsten Bedrohungen geschützt.



Ihre Strategie für cloudnative Netzwerksicherheit

Bei der Entwicklung einer umfangreichen Sicherheitsstrategie für Ihre cloudnativen Anwendungen sollten Sie die CN-Series von Palo Alto Networks unbedingt in Erwägung ziehen. Sie ist anderen Lösungen in den folgenden vier Bereichen überlegen:

1. DevOps-Integration

Die Firewalls der CN-Series unterstützen zwei Bereitstellungsoptionen, DaemonSet und Kubernetes-Service. Letztere nutzt die nativen Funktionen von Kubernetes für die automatische Skalierung. Die Firewallkonfiguration erfolgt in einer YAML-Datei, wodurch sich die Bereitstellung der Firewalls leicht in die Containerorchestrierung integrieren lässt.

2. Detaillierte Containerkontextdaten

Dank der nativen Integration der CN-Series mit Kubernetes können unsere Firewalls bei der Erstellung von Sicherheitsrichtlinien auf Kontextinformationen wie Namespaces zugreifen. Diese Informationen lassen sich mit anderen Firewalls von Palo Alto Networks teilen, um die Sicherheit des gesamten Netzwerks zu stärken.

3. Zentralisierte Richtlinienverwaltung

Die Firewalls der CN-Series werden über dieselbe Oberfläche verwaltet wie andere Next-Generation Firewalls von Palo Alto Networks. Somit können Netzwerksicherheitsteams von einer zentralen Konsole aus alle physischen, virtuellen, containerisierten und Public-Cloud-Workloads sichern.

4. Umfassende, cloudnative Netzwerksicherheit

In Kombination mit Palo Alto Networks Prisma® Cloud bietet Ihnen die CN-Series Mikrosegmentierung und modernste Netzwerksicherheit, um die Angriffsfläche Ihrer cloudnativen Anwendungen zu reduzieren und Bedrohungen zu blockieren.

Vorteile der CN-Series

- DevOps-Integration
- Detaillierte Containerkontextdaten
- Zentralisierte Richtlinienverwaltung
- Umfassende, cloudnative Netzwerksicherheit

Sie möchten mehr über die CN-Series erfahren? Fordern Sie Ihre persönliche Demo an.

Demo anfordern

STRATA
BY PALO ALTO NETWORKS

Sie möchten mehr über die CN-Series erfahren?

Fordern Sie Ihre persönliche Demo an.

paloalto NETWORKS

Oval Tower, De Entrée 99–197
1101 HE Amsterdam,
Niederlande

Telefon: +31 20 888 1883
Vertrieb: +800 723 9771
Support: +31 20 808 4600

www.paloaltonetworks.de