illumio

Entkopplung der Security von der Netzwerk-Architektur: Die Evolution der Segmentierung

WP201911

Überblick

Segmentierung gibt es schon so lange wie Netzwerke, beginnend mit den ersten TCP/IP-Protokollen, die die zuverlässige Übertragung von Paketen gewährleisten sollen. Doch die Aufgabe von Netzwerken ist, Dinge zuverlässig zu *verbinden* – während es bei Segmentierung darum geht, Dinge zuverlässig zu *isolieren.*

Dieses Whitepaper hat folgende Ziele:

- Erklärung der Evolution von Netzwerken, SDN und Host-basierter „Sicherheitssegmentierung“
- Erklärung der Kernkompetenzen und Kompromisse der verschiedenen Segmentierungsansätze
- Argumente für die Entkopplung der Sicherheit vom Netzwerk basierend auf Designlogik und Effizienz

Segmentierung berücksichtigt, was womit verbunden werden kann, und schränkt mit Policy-Regeln alles andere ein. Das funktioniert in etwa wie bei einem Türsteher vor einem Club: Wenn Sie nicht auf der Gästeliste stehen, werden Sie nicht hereingelassen. Diese beiden Ziele sind jedoch komplett gegensätzlich. Und dennoch versuchen wir, mit den gleichen Geräten beides zu erreichen.

Dies gilt auch für Software-Defined Networks (SDN). Ebenso wie bei herkömmlichen Netzwerken ist die Hauptaufgabe des SDN die zuverlässige *Paketübermittlung* – und nicht die Durchsetzung von Sicherheitsregeln, die darüber entscheiden, welche Daten zwischen zwei Punkten im Netzwerk ausgetauscht werden dürfen (d. h. Segmentierung).

Und selbst wenn Sie Segmentierung in Ihrem Netzwerk implementieren können: Die IT-Umgebung ist mittlerweile über das Rechenzentrum hinausgewachsen und umfasst Public Clouds, Drittanbieter-Services und APIs. Unsere Umgebungen befinden sich also nicht mehr im Netzwerk. Die flexible und agile Infrastruktur, die DevOps benötigt, erfordert dynamischere Workloads und bedeutet, dass sich Anwendungskomponenten nicht im Rechenzentrum befinden.

Auch Endgeräte sind dynamisch. Sie müssen also die wertvollsten Assets dort schützen, wo sie sich befinden. Das lässt sich jedoch nur erreichen, wenn die Sicherheitssegmentierung vom Netzwerk entkoppelt wird. Unternehmen wechseln verstärkt zu Host-basierter Segmentierung, um die Probleme herkömmlicher Ansätze hinter sich zu lassen. Um die Motive für diesen Schritt zu verstehen, werden wir diese Probleme und die Gründe für die Entkopplung der Sicherheitssegmentierung vom Netzwerk erläutern.

illumio

Segmentierung mit der Netzwerkinfrastruktur

Manuelle Abläufe an erster Stelle

Herkömmliche Segmentierung begann im Netzwerk und wird dort auch weiterhin mithilfe virtueller LANs (VLANs) implementiert werden. Wenn der Datenverkehr zwischen VLANs gefiltert werden soll, kommen Zugriffssteuerungslisten (Access Control Lists, ACLs) ins Spiel.

Die Erstellung von ACLs erfolgt manuell und erfordert genaue Kenntnisse des Datenverkehrs: Wenn eine ACL hinzugefügt wird und dabei etwas übersehen wurde, kann es unbeabsichtigt zu Unterbrechungen kommen, sodass die zuverlässige Paketübermittlung gestört wird und Anwendungen nicht mehr ordnungsgemäß funktionieren. Daher kann die Erstellung, Überprüfung und Bereitstellung von ACLs sehr viel Zeit in Anspruch nehmen. Wenn es zudem *dennoch* zu Fehlern kommt, ist die Problembehebung bei ACL-Konfigurationsfehlern sehr aufwändig.

Netzwerksegmentierung passt sich nicht an Veränderungen an, weil sich die Architektur klassischer Netzwerke nicht ohne Weiteres verändern lässt. In einem herkömmlichen Netzwerk können die Neukonfiguration eines Servers oder die Bereitstellung eines neuen Subnetzes sowie die daraus resultierende Veränderung der Netzwerkarchitektur aufgrund der Komplexität von IP-Adressen mehrere Wochen in Anspruch nehmen. Und nun halten Sie sich vor Augen, dass Unternehmen ständig verlangen, dass IT *schneller und agiler* bereitgestellt und betrieben werden soll.

illumio

Segmentierung mit Software-Defined Networks

Geschwindigkeit ist Trumpf

Durch die zunehmende Virtualisierung wurde Geschwindigkeit für die IT und den Erfolg des Unternehmens noch wichtiger. Das führte auch dazu, dass Entwickler eine Möglichkeit benötigten, Anwendungen schnell bereitzustellen – ohne dass das Netzwerk im Weg steht. Dennoch müssen Sie weiterhin Dinge miteinander verbinden, zudem benötigen Sie weiterhin IP-Adressen.

Der Zeitaufwand für die Zuweisung von IP-Adressen wurde zu einem Hindernis. Zum Beispiel war die Zahl der verfügbaren IP-Adressen der Klasse C (von denen meist eine oder zwei einem physischen System zugewiesen wurden) durch das große Aufkommen virtueller Maschinen schnell erschöpft. Wenn keine weiteren IP-Adressen mehr zur Verfügung stehen und dennoch mehr Adressraum benötigt wird, ist die Neukonfiguration des Netzwerks mit herkömmlichen Methoden zur Nutzung nicht verwendeter Adressen nicht mehr möglich.

Hier kommen **Software-Defined Netzworks (SDN)** ins Spiel.

SDN ist quasi „Uber für IP-Adressen“: Während Uber die Nutzung gerade nicht genutzter Pkw ermöglicht, steigert SDN die Effizienz nicht genutzter IP-Adressen, damit Workloads und Anwendungen schneller bereitgestellt werden können. Mit Tools wie VMware NSX und Cisco ACI wird das Netzwerk agiler, da Erweiterungen und Änderungen programmgesteuert durchgeführt werden, während gleichzeitig die Kernkompetenz des Netzwerks – die zuverlässige Paketübermittlung – gewährleistet bleibt. Dennoch unterliegt SDN bei der Segmentierung ebenfalls starken Beschränkungen durch das Netzwerk.

SDN-Segmentierung: Volle Komplexität, keine Transparenz

Anbieter für Software-Defined Networks versuchen ebenfalls, ihre Produkte für Sicherheitssegmentierung einzusetzen. Dazu erstellen sie ein Overlay

aus Netzwerken, die Pakete durch verteilte Firewalls schleusen, oder sie verwenden das Netzwerk selbst für stateless Filterung. Das Problem liegt bei SDN darin, dass es durch die Abhängigkeit von Underlays, Overlays und Tunneln die Komplexität zusätzlich erhöht.

Doch ebenso wie herkömmliche Netzwerke ist das SDN letztlich an die Infrastruktur gebunden, in die es eingebettet ist, d. h. an den Hypervisor oder Router und Switches.

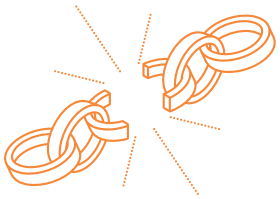
Durch die zunehmende Nutzung der Cloud sind Workloads außerhalb des herkömmlichen Netzwerks häufig ebenso wichtig. Doch da sie sich in einem Netzwerk befinden, das Ihnen nicht gehört, ist es schwer, einen vollen Überblick über diese Workloads zu erhalten und konsistente Segmentierungsrichtlinien durchzusetzen.

Hinzu kommt, dass Unternehmen häufig auf Multi-Cloud-Bereitstellungen setzen, um Resilienz und Effizienz zu steigern sowie die Bindung an einen Anbieter zu vermeiden. Wenn es dann keine Möglichkeit zur zentralen Verwaltung der verschiedenen Umgebungen im gesamten Unternehmen gibt, werden oft mehrere separate Segmentierungslösungen verwendet, die sich nicht überschneiden und keinen umfassenden Überblick ermöglichen.

Sicherheitsbeschränkungen von SDN

Netzwerkbasierten Lösungen fällt es bereits schwer, einen Überblick und einheitliche Kontrolle für das eigene Netzwerk zu liefern – ganz zu schweigen von der Public-Cloud-Infrastruktur, in der bei den meisten Unternehmen zumindest ein Teil der IT ausgeführt wird. Und auch hier gilt: Wenn die Kernfunktion statt in der Paketübermittlung bei Sicherheit liegt, sind Netzwerke nicht in ihrem Element.

Netzwerke sollten auf Zuverlässigkeit ausgelegt sein. Die Isolierung von Anwendungen durch Netzwerksegmentierung kann dazu führen, dass die Datenübertragung über das Netzwerk gestört wird. Das gilt ganz besonders bei einem fehlenden vollständigen Überblick und führt zu einem sogenannten Kobayashi-Maru-Szenario, d. h. zu einer ausweglosen Situation für die Netzwerkteams.



Segmentierung: Entkopplung der Sicherheit von der Netzwerk-Infrastruktur

Wenn wir in der Vergangenheit Reisen planten, gingen wir davon aus, auf dem Land oder zu Wasser unterwegs zu sein. Beide Wege schaffen Reibungspunkte, die uns letztendlich ausbremsen. Manchmal erfordert die beste Antwort auf ein Problem einen komplett anderen Ansatz. Indem wir uns vom Landweg lösen und durch die Luft reisen, können wir uns viel schneller bewegen und vom Widerstand der Erde entkoppeln. Aus diesem Grund wechseln wir beim Überqueren des Ozeans vom Auto ins Flugzeug – und entkoppeln die Reise vom Land. So kommen wir schneller von A nach B und erreichen entlegene Orte, die mit dem Auto unzugänglich wären. Gleichzeitig sind wir mit weniger eigenem Aufwand unterwegs, da uns ein Pilot transportiert. Zudem ist die Reise auch sicherer, schließlich gibt es deutlich weniger Flugzeugkatastrophen als Autounfälle. Ein netter Bonus ist der Blick aus der Luft auf die Landschaft – eine Perspektive, die man nur aus 10.000 Metern Höhe hat.

Mit den Einschränkungen durch die Kopplung der Sicherheitssegmentierung an die Netzwerksegmentierung verhält es sich ähnlich: Eine Lösung besteht darin, das eine vom anderen zu entkoppeln. Das ist sicherer, weil die Durchsetzung der Sicherheitssegmentierung keine Auswirkungen auf das Netzwerk hat und die Netzwerkabläufe daher nicht stören kann. Und es ist schneller, weil jede noch so kleine Änderung an einem „gekoppelten“ Netzwerk mit intensiver Planung (oder gleich einen Umbau) verbunden ist. Durch die Entkopplung ist die Anfälligkeit für „Unfälle“ geringer. Zudem erhalten wir die notwendige Agilität, um in Netzwerken oder Clouds ausgetretene Pfade verlassen zu können.

Host-basierte Segmentierung: Nähe zur Anwendung erzwingen

Wie kann die Sicherheitssegmentierung vom Netzwerk entkoppelt werden? Rufen Sie sich als erstes in Erinnerung, dass das Netzwerk die Aufgabe hat, Anwendungen zu dienen – und nicht umgekehrt.

Das Lösen der Sicherheitssegmentierung vom Netzwerk befreit nicht nur die Sicherheit von den Beschränkungen der darunter liegenden Infrastruktur. Es ermöglicht auch die Durchsetzung von Sicherheitsrichtlinien genau dort, wo der Schutz benötigt wird: bei der Anwendung. Anwendungen bestehen aus Workloads, die auf einem Host verarbeitet werden. Wenn Sie also die Workloads absichern können, beseitigen Sie damit jegliche Abhängigkeit vom Netzwerk (bis auf die zuverlässige Paketübermittlung).

Host-basierte Segmentierung ist angetreten, diese Lücke zu schließen – unterstützt von einer Reihe von Anbietern wie Illumio, Cisco, VMware und anderen. Bei Host-basierter Segmentierung setzt ein Agent Sicherheitsrichtlinien durch, indem er in gängige Betriebssysteme integrierte Firewalls koordiniert. Auf Linux-Systemen ist das iptables, auf Windows-Servern die Windows-Filterplattform (WFP). Diese Tools überwachen den Netzwerkverkehr, setzen Sicherheitsregeln für bestimmte Anwendungen sowie Workloads auf dem Host durch und ermöglichen dadurch detaillierte Segmentierung.

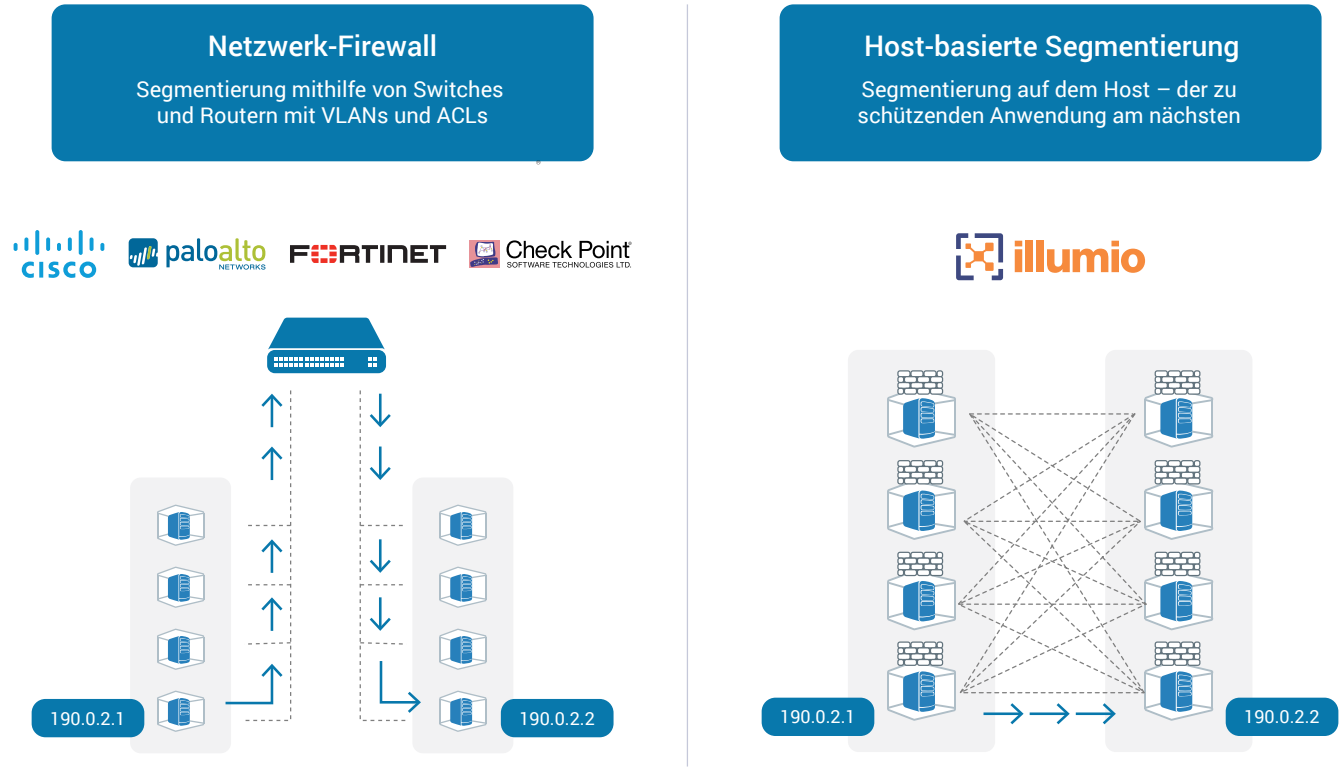


Abbildung 1: Segmentierungsansätze

Da iptables und WFP zu den Standard-Betriebssystemen gehören, sind sie auf jedem Host mit diesen Betriebssystemen verfügbar: physischen Servern, virtuellen Maschinen, Public Cloud und sogar Container-Plattformen. Einer der größten Vorteile der Segmentierung auf dem Host ist die Nutzbarkeit in jeder Umgebung. Der Gedanke ist dabei, durch die Koordinierung von Richtlinien mithilfe zentraler Kontrollen viele unterschiedliche Umgebungen zu unterstützen. Dies erlaubt die einheitliche und detaillierte Segmentierung in weit verteilten und heterogenen Umgebungen – ein wichtiger Vorteil, da Unternehmen ihre Aktivitäten weg vom Netzwerk in die Cloud und dabei meist in Multi-Cloud-Umgebungen verlagern, um die Bindung an einen Anbieter zu vermeiden.

Zusammenfassung: Wichtige Prinzipien der Segmentierung

Anhand welcher wichtigen Attribute sollten Anwendungen bewertet werden?

- **Skalierung:** Ist die Lösung skalierbar, um die Anzahl der Workloads in Ihrem Rechenzentrum und der Public Cloud zu bedienen? Unserer Erfahrung nach bauen bereits 800 Workloads zwischen 180.000 und 360.000 individuelle Verbindungen auf. Bei 10.000 Workloads explodiert diese Zahl auf 17–43 Millionen Verbindungen (siehe Abbildung 3: Kirners Formel) und damit ebenso viele Regeln, da für jede Ihrer Anwendungen pro Verbindung eine Regel notwendig ist.

$$R = \rho W^{\sigma}$$

Faktor der Konnektivitätsgröße $\sigma = 1{,}8 - 1{,}9$

Faktor der Regeln pro Verbindung $\rho = 1{,}1$

$R_{max} = 1{,}1W^{1{,}9}$

$R_{min} = 1{,}1W^{1{,}8}$

Workloads	Regeln insgesamt
800	180.000–360.000
2.500	1,4 Mio–3,1 Mio
10.000	17 Mio–43 Mio

Abbildung 2: Kirners Formel

- **Workflows:** Ein weiterer Aspekt ist das Schreiben der Regeln für all diese Verbindungen. Bietet die Lösung Workflows, die Ihnen helfen, Segmentierung mit minimalem wirtschaftlichem Ressourceneinsatz und ohne Unterbrechung der Geschäftsabläufe zu implementieren?
- **Unabhängigkeit von der Infrastruktur:** Besteht die Lösung auf bestimmten Voraussetzungen? Oder unterstützt sie jede Ihrer Umgebungen (auch außerhalb des Netzwerks in der Public Cloud) mit hoher Detailauflösung und Konsistenz unabhängig von der Infrastruktur, auf der sie ausgeführt wird?
- **Transparenz fördert die Sicherheit:** Echtzeitüberblick bildet die Grundlage für das Verständnis des Anwendungsverhaltens sowie gemeinsamer Serviceabhängigkeiten. Damit lässt sich die ideale Segmentierungsstrategie entwickeln, die keine Anwendungen (z. B. Geschäftsanwendungen, Active Directory, Exchange, DNS) beeinträchtigt – denn Sie können nur das schützen, was Sie sehen.

- **Erst testen, dann durchsetzen:** Stellt die Lösung Rückmeldungen und Workflows bereit, damit gewährleistet ist, dass Sie Ihre Richtlinien vor der Durchsetzung testen können? Im Idealfall erlaubt Ihre Lösung die Nutzung von Regeln zum Einschränken des Datenverkehrs. Diese sollten jedoch zuvor in einem Testmodus überprüft werden, der die Anzahl der Warnungen offenbart und notwendige Anpassungen ermöglicht. Sie können Sicherheitsrichtlinien erstellen und erhalten visuelle Echtzeit-Rückmeldungen, bevor Sie in den Produktivbetrieb gehen, um die Beeinträchtigung von Anwendungen durch das Durchsetzen neuer Richtlinien zu verhindern.

	Netzwerk (Cisco, PAN, Fortinet, Checkpoint)	SDN (Cisco, VMware)	Host-basiert (Illumio)
Segmentierung der Umgebung			
Anwendungssegmentierung	●	●	●
Stufensegmentierung	●	●	●
Benutzersegmentierung	●	●	●
Prozesssegmentierung	◑	◑	●
Bereitstellung: Cloud, Container	○	○	●
Einfache und schnelle Bereitstellung	◔	○	●
Inkrementell, kleiner Einstieg	◔	○	●
Datenverkehrübersicht	○	○	●
Test der Richtlinie vor der Durchsetzung	○ ○	○ ○	● ●
Unabhängigkeit von Netzwerk/ Infrastruktur	○	○	●
Kosten	$$$$	$$$	$
Risiko durch Segmentierung	Hohes Risiko	Hohes Risiko	Geringes Risiko
Anzahl der Richtlinienregeln	Hoch	Hoch	Gering

Abbildung 3: Dreifache Segmentierung

● Unterstützt ○ Nicht unterstützt ◑ ◔ Teilweise unterstützt

Fazit: Segmentierung, die funktioniert – überall

Wir nutzen das Netzwerk zur Bereitstellung von Anwendungen. Doch da die IT wächst, die Zahl der Verbindungen steigt und die Umgebungen zunehmen, die nicht mehr auf das Netzwerk beschränkt sind sondern die Public Cloud umfassen, benötigen wir einen neuen Ansatz für die Absicherung von Anwendungen. Das Netzwerk ist nicht die beste Option für das Konzipieren, Entwickeln und Bereitstellen von Sicherheitssegmentierung.

Es bietet den Sicherheitsverantwortlichen keine Benutzeroberfläche, mit denen sie Anwendungsverbindungen darstellen und verstehen können, um anschließend detaillierte und zuverlässige Segmentierung aufzubauen und zu verwalten. Dem Netzwerk fehlt die Agilität für die Anpassung an Veränderungen und selbst mit SDN ist es an Infrastruktur gebunden, die nicht ausreichend skalieren kann, um die Geschwindigkeitsanforderungen des Unternehmens zu erfüllen.

Die Lösung: Die Entkoppelung der Sicherheitssegmentierung vom Netzwerk. Dadurch können wir Anwendungen überall dort schützen, wo sie ausgeführt werden, da sie sich nicht mehr ausschließlich in unseren Netzwerken befinden und die Richtliniendurchsetzung ihnen folgen muss.

Folgen Sie uns

Informationen zu Illumio

Illumio, ein führender Anbieter für Mikrosegmentierung, verhindert die Ausbreitung von Sicherheitsverletzungen in Rechenzentrum- und Cloud-Umgebungen. Unternehmen wie Morgan Stanley, BNP Paribas, Salesforce und Oracle NetSuite nutzen Illumio zur Reduzierung des Cyberrisikos sowie zur Einhaltung von Vorschriften-Compliance. Nur die Illumio Adaptive Security Platform® schützt wichtige Informationen durch die Echtzeit-Zuordnung von Anwendungsabhängigkeiten und Schwachstellen in Kombination mit Mikrosegmentierung, die alle Rechenzentren und Public- oder Hybrid-Cloud-Bereitstellungen auf Bare-Metal-Systemen, virtuellen Maschinen und Containern angewendet werden kann. Für weitere Informationen zu Illumio besuchen Sie uns unter http://www.illumio.com/what-we-do oder folgen Sie @Illumio.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA, USA 94085 Tel. +1 (669) 800-5000 www.illumio.com