Network functions and isolation for a container-based PaaS environment

Studiengang: BSc in Informatik | Vertiefung: IT-Security
Betreuer: Prof. Hansjürg Wenger
Experte: Dr. Torsten Braun (Uni Bern)

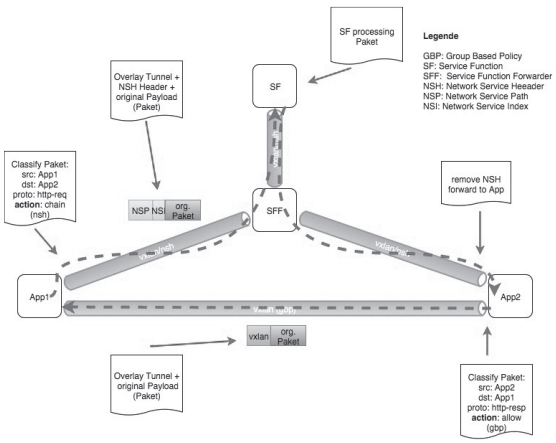
Netzwerkvirtualisierung ist ein wichtiger Bestandteil von modernen Cloud-Plattformen. Mit steigenden Anforderungen, vor allem im Bereich der Netzwerksicherheit, werden neue Lösungsansätze und Technologien benötigt damit diese erfüllt werden können. Die Arbeit umfasst ein Konzept sowie einen Prototypen, wie Netzwerkfunktionen in einer Plattform-as-a-Service Umgebung integriert und genutzt werden können.

Ausgangslage

Aktuelle Container-basierte PaaS-Lösungen verfügen über wenig Funktionalität im Netzwerkbereich. Durch den Einsatz von klassischen NAT-Funktionen wird die Kommunikation sichergestellt. Dies gaukelt einerseits eine Pseudo-Sicherheit vor, andererseits fehlt die Oportunität komplexe Anforderungen umzusetzen. Bei der Transformation traditioneller IT Umgebungen in die Cloud sind diese jedoch gefordert.

Idee

Die Applikationen der PaaS werden als Container abgebildet. Dabei soll jeder Container eindeutig über das IP-Protokoll angesprochen und identifiziert werden können. Neue Konzepte und Technologien im Bereich von **Software Defined Networking** und **Network Functions Virtualization** ermöglichen es Netzwerkverbindungen zwischen unterschiedlichen Applikationen frei zu definieren. So sollen beispielsweise Netzwerkfunktionen wie ein Paketfilter oder ein Intrusion Detection System regelbasiert eingefügt werden können, wobei dies aus Applikationssicht transparent ist.



Beispiel Service Function Chaining mit asymmetrischer Service Chain und einer Service Function

Lösung

Im Rahmen der Arbeit wurde ein Konzept erstellt, wie mithilfe von Group Based Policy und Service Function Chaining die Idee umgesetzt werden kann. Mit dem Ziel nur minimale Anpassungen an der PaaS vornehmen zu müssen, wurde der Fokus auf die netzwerkseitige Integration gelegt. Gleiche oder ähnliche Applikationen können in Gruppen eingeteilt werden, auf Basis derer entsprechende Regeln für den Netzwerkverkehr definiert werden. Verbindungen zwischen Containern werden entweder direkt mittels Regeln in Group Based Policy abgebildet oder es wird auf eine entsprechende Kette (Service Chain) verwiesen. Eine Kette besteht aus einer oder mehreren virtuellen Netzwerkfunktionen. Damit die IP-Pakete den korrekten Weg durch eine Kette wählen, wird ein neues Protokoll «Network Service Header (NSH)» verwendet. Dieses steht erst als Draft zur Verfügung.

Des Weiteren wurde ein Prototyp als Proof-of-Concept entwickelt. Dabei kamen ausschliesslich Opensource Komponenten wie Opendaylight SDN, Openvswitch oder Docker zum Einsatz. Aufgrund der noch in der Entwicklung befindlichen Protokolle, wie NSH, existieren noch keine vollständigen Implementationen. Diese Herausforderungen führten zur Entwicklung einer Proxy-Komponente auf Basis von Openvswitch, mit welcher traditionelle Netzwerkfunktionen zusammen mit Service Function Chaining verwendet werden können. Als virtuelle Netzwerkfunktion wurde ein Paketfilter – ebenfalls als Container – realisiert.

Boban Glisovic