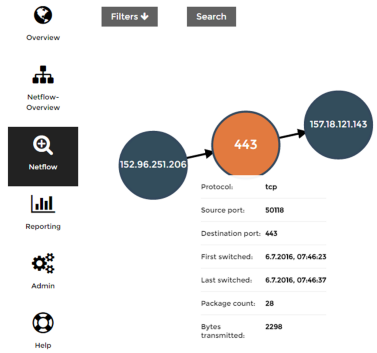
Matthias Gabriel

Philip Schmid

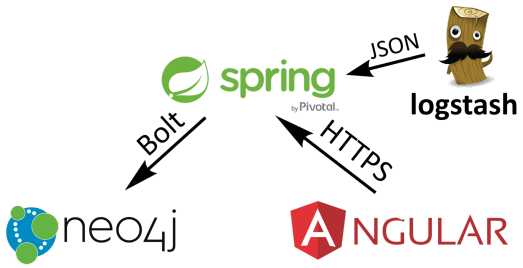
Studenten/-innen	Matthias Gabriel, Philip Schmid
Dozenten/-innen	Prof. Stefan F. Keller
Co-Betreuer/-innen	- -
Themengebiet	Software

ToffiAnalyser

Visualisierung und Analyse von NetFlow-Daten



Ein einzelner Netzwerkverkehrsfluss («NetFlow») zwischen zwei beteiligten Geräten, der über 28 Pakete anhält.

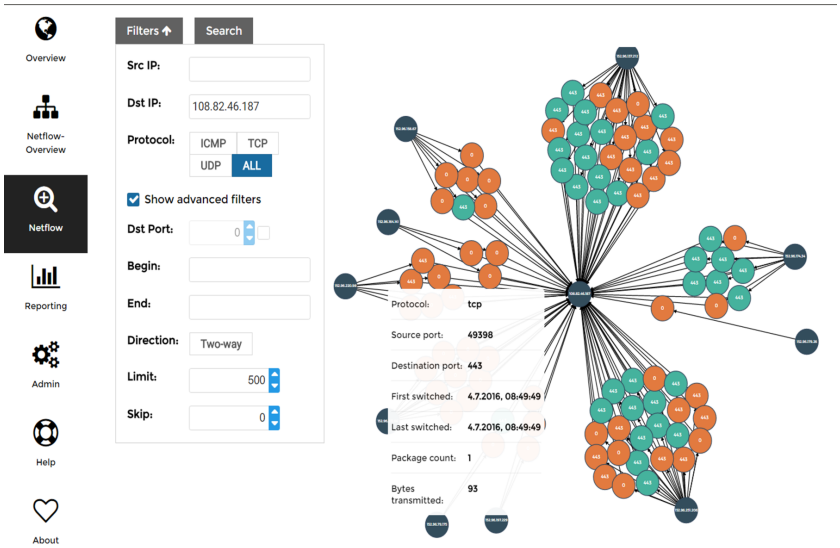


Die abstrahierte Architektur der entwickelten Softwarelösung.

Ausgangslage: Heute gibt es in der IT oft das Problem, dass nicht genau bekannt ist, was für Netzwerkverkehr im firmeninternen Netzwerk existiert. Durch diese Arbeit soll diese Situation verbessert werden, die aktuell in vielen IT-Abteilungen vorhanden ist, indem dem Benutzer eine neue Darstellung des Netzwerkverkehrs geboten wird. Um diese verbindungsspezifischen Daten zu sammeln, existiert bei den Geräten der Firma Cisco die Funktionalität «NetFlow», welche die benötigten Daten direkt auf den Netzwerkkomponenten sammelt.

Vorgehen/Technologien: Im Gegensatz zu bereits existierenden Lösungen zur Analyse von NetFlow-Daten, sollen diese in vorliegender Webapplikation mittels Graphen dargestellt werden. Damit kann erreicht werden, dass der Benutzer eine völlig neue Ansicht auf die Daten bekommt und dadurch neue Zusammenhänge erkennen kann. Als separater Teil des Projektes wurde zudem ein Datenbank-Benchmark durchgeführt, welcher die drei Datenbank-Management-Systeme PostgreSQL, Neo4j und OrientDB unter der Verwendung von anwendungsspezifischen (Graph-)Daten und Abfragen vergleicht. Das Spezielle an diesem Benchmark ist der Vergleich von zwei Graphdatenbanken mit einer relationalen Datenbank.

Ergebnis: Als Resultat des Projektes wurde eine funktionsfähige Webapplikation mit dem clientseitigen Framework Angular sowie dem serverseitigen Framework Spring Boot erstellt. Die Anwendung bietet eine gute Balance zwischen Übersichtlichkeit über die zu analysierenden Daten und dem Detaillierungsgrad. Der Graph-Daten-Benchmark hat hauptsächlich zwei Erkenntnisse gebracht: Bei Änderungsoperationen und «normalen» Abfragen waren alle drei Systeme vergleichbar mit leichtem Vorteil für PostgreSQL. Bei den Abfragen auf Graphen (Traversierung), die hier oft gebraucht werden, war die Performance bei den Graphdatenbanken bis zu 50% besser.



Die Detaillierteste der drei verfügbaren Ansichten mit geöffnetem Tooltip und Filtermöglichkeiten.