SMATS' TRAFFIC SIGNAL OPTIMIZATION SOLUTION AND THE FUTURE OF TRAFFIC MANAGEMENT

SMATS' IoT solution specializes in traffic data collection. The solution collects data via mobile MAC addresses so that the data can be analyzed to measure factors like travel-time, origin-Destination data, intersection performance, and traffic signal optimization.

SDN PROJECT OVERVIEW

SOLUTION

SMATS' IoT solution is designed to record time-stamped data in order to help cities better measure and predict travel times on major roadways. This is done by using data analytics software and SMATS' MAC sniffer sensor technology, called TrafficXHub. The solution provides convenient and cost effective time measuring data collection and data analytics for various use cases. For example, traffic signal optimization for roads and queue management in airports.

Here's how it works: The TrafficXHub collects MAC addresses of the devices in its proximity using Bluetooth and WiFi, then transfers collected data to a centralized cloud server for data analytics. The data collected can then be used to analyze travel time, origin-destination data and intersection performance monitoring.

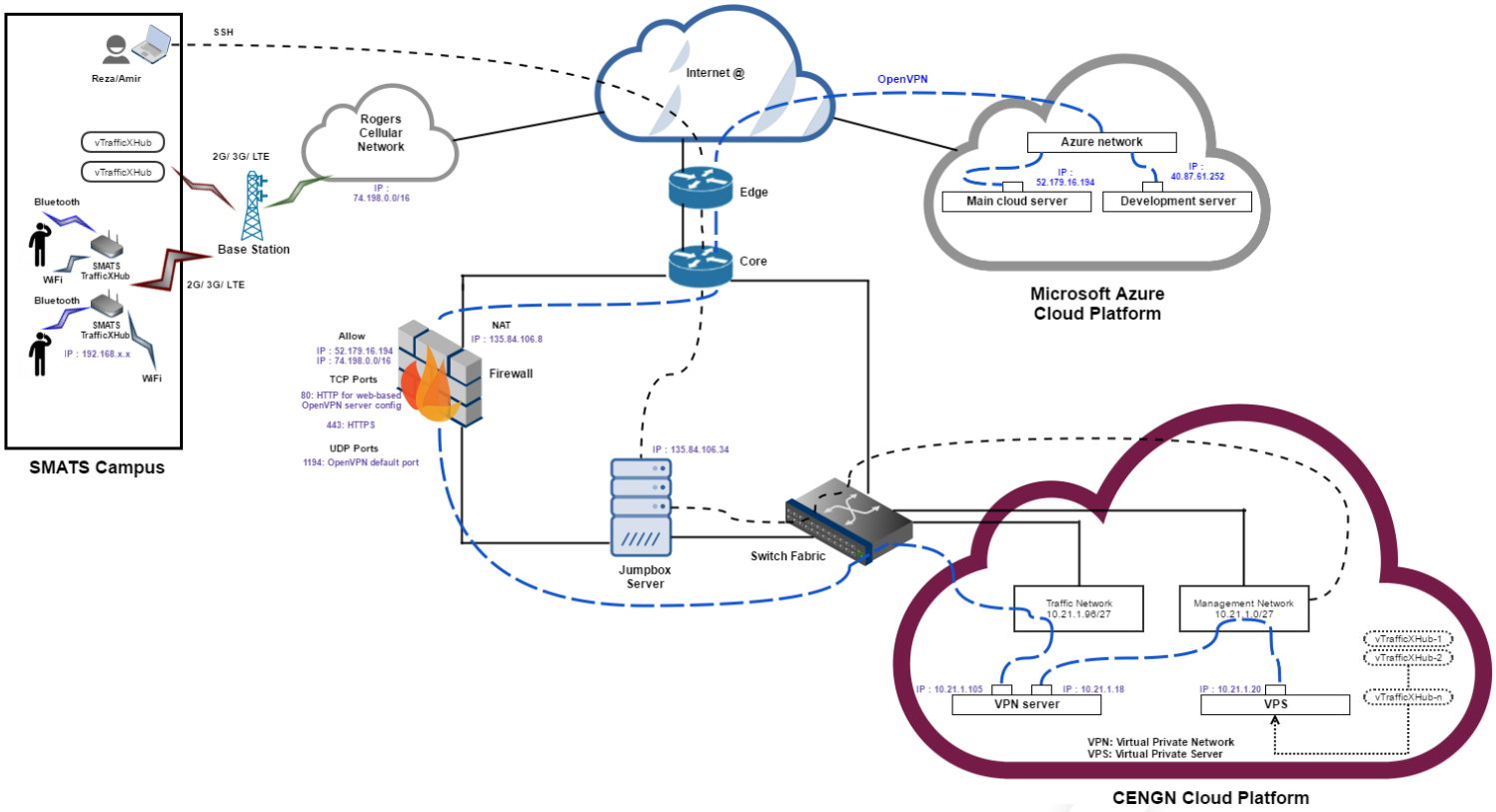
CHALLENGE

One of SMATS' challenges when creating their traffic signal optimization solution was ensuring that the solution was capable of routing traffic efficiently, in terms of both data volume and transfer speed.

CENGN facilitated a lab evaluation of SMATS' traffic signal optimization solution. The project included the deployment and testing of VPN connectivity among the VPN server, TrafficXHub sensors and the application server (located in Microsoft Azure platform). CENGN created success criteria for the test, and determined that a total of 20 real and simulated TrafficXHub sensors would have to be capable of sending data to the application server through a VPN tunnel in order for the solution to be successful.

CENGN also tested the ability of the SMATS solution to quickly transfer data from the TrafficXHub sensors to the application server for analysis. CENGN determined that the success criteria for this test would be the transfer of 100 MAC records per second. In addition, the success criteria required that the data from the sensors was available at the application server for analysis within 1 minute delay of the MAC detection time.

CENGN MEMBERS



THE PROJECT

The Proof-of-Concept project broke up testing the solution into five different steps. The aim of the first test was to verify the VPN network inside the tenant. The second test focused on testing the connectivity between CENGN's tenant nodes (like the VPN and VPS) and the application server in Microsoft Azure. The third test that CENGN conducted was launching the TrafficXHub sensors in Dock containers. The following test verified whether data flow from a TrafficXHub sensor reaches the application server through the VPN tunnel. The final test involved simultaneously sending traffic from multiple TrafficXHub sensors to the application server with a 100 MAC records/sec/sensor rate.

TEST RESULTS

The results of CENGN's testing on the SMATS solution was very successful. It was verified that SMATS' VPN solution for their sensor network was secure and even provided added security. The scalability of the overall solution was also verified. Through the various stages of testing, it was demonstrated that the sensors and the iNode servers were able to establish VPN connectivity to the VPN server using OpenVPN. The connectivity was found to be robust and the data communication was reliable with less than one minute of latency. CENGN was also able to monitor the data communication stream and VM resource utilization over the course of this project using iNode interface and cAdvisor platform installed on iNode as well as CENGN VPN servers. As for the sensors, real-time status and configuration interfaces were remotely accessed through the VPN connection. In terms of scalability, testing showed that iNode CPU usage increase linearly with the number of deployed sensors.

Overall, the testing demonstrated that the solution improves security, scalability, and accessibility of SMATS' IoT sensors. TrafficXHubs and the application server were able to establish a virtual private network with two-way communication between the sensors and the server. With these results SMATS' have advanced the security and scalability of their TrafficXHub sensors.

CENGN
CENTRE OF EXCELLENCE IN NEXT GENERATION NETWORKS

Bhavani Krishnan, VP Program and Product Management
bhavanikrishnan@cengn.ca

Sam Mouallem, SR Sales Manager
Sam.Mouallem@us.fujitsu.com
FUJITSU