Research Topic: Application Identification

Christian Tsirlis, Brad Wilson
Advisor: Jorge Crichigno

1. Introduction

In the context of Next-generation Firewalls (NGFWs), an application is a specific program or feature whose communication can be labeled, monitored, and controlled. The applications can be delivered through a web browser, a client-server model, or a decentralized peer-to-peer design. Applications include business tools and services that must be allowed, and entertainment or personal services that might need to be blocked.

2. Research Project

In this research project, you will explore how modern NGFWs implement application identification. The goal is to test and measure the effectiveness of application identification. For example, the project must test at least five applications (e.g., Google, Facebook, Skype, etc.) and sub-applications (e.g., for Google, sub-applications are Google Drive, Google Maps, etc.), and measure the success rate of policies using App-ID. Figure 1 shows the network topology used for this project.
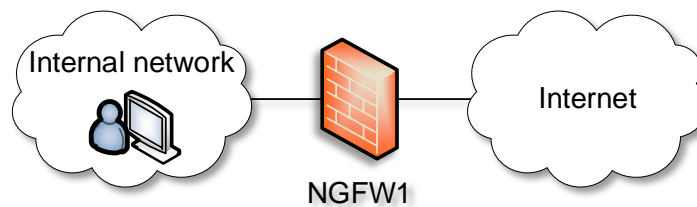

Figure 1. Network topology.