Design Document

Overview

Athena is a specialized firewall that detects and mitigates DDoS attacks. Athena runs on the commodity x64 servers easily found in modern datacenters and server farms. Athena's target market consists of medium-to-large sized enterprises that run at least one business critical service accessible from the Internet (such as a website, a REST API endpoint, etc). For these companies, service downtime due to a DDoS attack directly translates into a loss in revenue.

Athena's primary users are the systems administrators and dev-ops teams that deploy and maintain the system. Athena's main interfaces will be command-line interfaces.

Functional Requirements:

- DDoS detection and prevention with a low rate of false positives
- Runs on commodity x64 servers

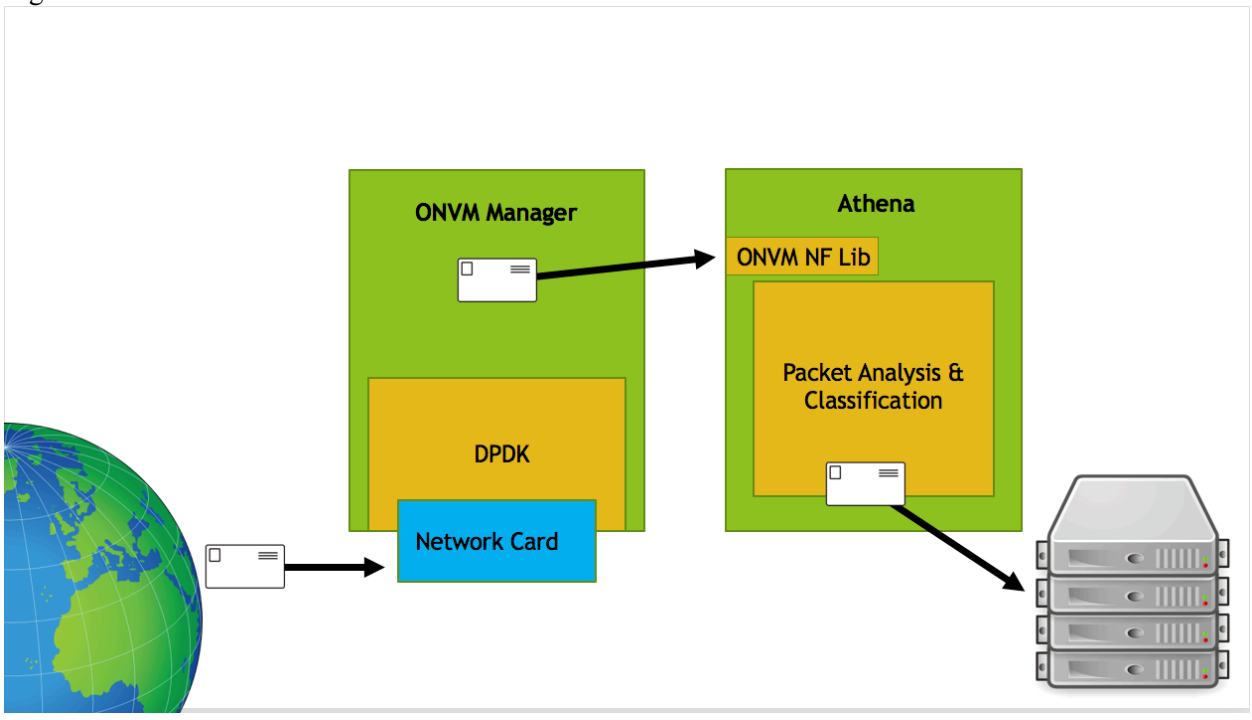
Non-functional Requirements:

- Scalable on modern hardware
- Affordable

Components:

- **OpenNetVM platform**- the high performance networking platform that Athena uses to process packets at line rate
- **Athena anti-DDoS network function**- detects and denies DDoS traffic using OpenNetVM's API

Fig 1. An overview of Athena's architecture



Subcomponent: OpenNetVM Platform

The OpenNetVM (ONVM) platform is the bedrock upon which the rest of the system is built. The platform consists of 2 components: 1) the Network Function library, and 2) the ONVM manager.

Programs that use the OpenNetVM API are called Network Functions. All Network Functions use the Network Function library (NFlib) to communicate with the ONVM manager and perform network I/O.

The ONVM manager acts as the "message bus" for the rest of the system. It is responsible for reading network packets from the network, and distributing those packets to the correct Network Function for processing. It is also responsible for writing network packets to the network. All network I/O is performed with the help of Intel's DPDK library; DPDK allows the ONVM manager to bypass the kernel and talk directly with the network card.

Functional Requirements:

- Must be able to process packets at line rate (10Gbps)

Subcomponents:

- **Intel DPDK library**- Intel's Data Plane Development Kit, or DPDK, is a collection of libraries designed to allow fast packet processing. ONVM uses these libraries to provide high performance network I/O for Network Functions.
- **Network Function library (NFlib)-** the NFlib is a static library implementation of the OpenNetVM API written in C. Client applications (or "Network Functions" in ONVM parlance) link with this library, and use it to communicate with the ONVM manager to process packets.

Subcomponent: Athena Anti-DDoS NF

The Athena Anti-DDoS NF is the second component of the Athena system. This component uses various heuristics to detect packets tied to a DDoS attack and drop them.

Functional Requirements:

- Must be able to process packets at line rate (10Gbps)
- Must be able to analyze a stream of incoming packets and determine which are malicious
    - Must operate in real-time

Subcomponents:

- Connection state tracker- updates a hash map that maps incoming network packets to connection state
- Connection classifier- uses the connection state tracker to classify packets as malicious or non-malicious
- Packet dispatcher- sends packets to the correct machine using ONVM, or drops them (if they are malicious packets)

Fig 2. An overview of the Athena NF's architecture