Defense4All Proposal

Name

Defense4All (previously known as OpenDefenseFlow)

Repo Name

defense4all

Description

In recent years we have seen a dramatic increase in cyber-attacks, in particular Distributed Denial of Service attacks (DDoS) which attempt to bring down the targeted services by exhausting the service compute and/or network capacity. These attacks can impose a real threat to the economy; market studies show that, financial organizations lose an average of 0.5% to 2.5% of annual revenue due to security-related downtime. Hence, there is a growing need for efficient mechanisms to detect and mitigate the effects of those attacks. Protection against DDoS attacks in Out-Off-Path (OOP) systems consists of three steps: 1) collection of traffic statistics and behavior, 2) detection of anomalies (suspicions of attacks), and 3) mitigation (traffic cleansing, selective source blockage, etc.). Traditionally, OOP DDoS attack protection solutions use Netflow for statistics collection and BGP to divert the infected traffic to a “scrubbing center” where the mitigation equipment cleans it up and then returns the valid traffic to the target servers, as shown in the following figure, where red lines represented infested traffic, while green lines represent clean valid traffic:

blocked URL

There are several limitations to the Netflow/BGP approach to DDoS mitigation, in particular long detection times, as well as lack of granularity in selecting traffic to divert (BGP diversion is limited to L3 addresses only). Moreover, to avoid routing loops, these solutions usually require the establishment of tunnels (MPLS, GRE, etc) which impact performance and add complexity. We can overcome these limitations with SDN:

- The capability of easily deploying "programmable probes" (in the form of openflow flow entries) allows setting very short statistics collection intervals, and controlling the granularity of those statistics (i.e., coarse flows at the edge of the network for high volume DDoS detection, finer flows near the protected servers), which lead to attacks being detected in seconds rather than in minutes or hours. Also diversion can be realized very quickly (in seconds or less) since there is no need to correlate Netflow records and/or wait for BGP convergence and change propagation.
- With SDN diversion is not limited to L3 IP addresses only - it can support L4 traffic (TCP and UDP with source and target ports) as well. This allows for very economic attack mitigation since only the suspicious traffic flow(s) is diverted.
- With SDN routing loops can be avoid altogether, i.e., no need for MPLS/GRE tunnels

The Defense4All project will provide to OpenDaylight a system for attack detection and traffic diversion (steps 1 & 2) above, based purely on monitoring and control capabilites exposed by OpenDaylight. As an attack detection tool Defense4All will function standalone, however, for actual attack mitigation (step 3) it needs to rely on specialized devices in a scrubbing center. While these devices are, at least for the time being, outside the scope of the OpenDaylight project, to provide a fully functional solution (detection **and mitigation**), Defense4All will include vendor-independent hooks to configure and control those devices. The entire system is shown in the following figure:

blocked URL

The Defense4All Anti-DoS system is composed of four major functional subsystems:

1. Statistics collection subsystem: responsible for placing traffic counters in different locations in the controlled network, and for collecting the data from these counters.
2. Anomaly detector subsystem: responsible for building peace time traffic baselines and identifying deviations from these baselines.
3. Traffic redirection subsystem: responsible for configuring the network such that the suspicious traffic (and only the suspicious traffic) is diverted to scrubbing center. After the attack, this subsystem is also responsible for restoring the network to original configuration.
4. Mitigation manager subsystem, responsible for selecting and configuring the mitigation device(s), invoking traffic redirection and monitoring the progress attack mitigation process.

The statistics collection and traffic redirection subsystems interact with the controlled network directly, hence they will be developed as extensions to the controller platform, including extensions to the ODP NB API. The anomaly detector and mitigation manager subsystems are independent of the controlled network topology, hence constituting a “network application” (according to the OpenDaylight definitions) and, as such it will be developed on top of the Controller’s NB API. The high level architecture of the Defense4All, as well as how the different subsystems fit in overall OpenDaylight architecture are shown in the following figure:

blocked URL

Additional Information

- Defense4All was presented (as OpenDefenseFlow) in the OpenDaylight technical workstream call on July 8, 2013 (see here for material)
- Presentation showing how use Affinity to implement Traffic Redirection

Scope

The Defense4All will provide the following:

1. An implementation of the Anomaly Detector subsystem, including a vendor independent framework for plugging different detection algorithms and a reference implementation of such a detection plugin. This sample detector will be able to handle common DoS attacks, and it will serve as an example for developers of more sophisticated detectors.
2. An implementation of the Mitigation Manager subsystem, including a vendor independent framework for plugging different mitigation devices and a reference implementation of such mitigator plugin.
3. An OSGI bundle for the Statistics Collection subsystem, including a REST API
4. An OSGI bundle for the Traffic Redirection subsystem, including a REST API
5. The Defense4All NB API.

Resources Committed (developers committed to working)

Who is, or will be working on this effort?

- Ehud Doron ehudd@radware.com
- Gera Goft gerag@radware.com
- Konstantin Pozdeev konstantinp@radware.com
- Benny Rochwerger bennyr@radware.com
- Kobi Samoray kobis@radware.com

Initial Committers

Who would be the initial committers to the project?

- Ehud Doron ehudd@radware.com
- Gera Goft gerag@radware.com
- Konstantin Pozdeev konstantinp@radware.com
- Benny Rochwerger bennyr@radware.com
- Kobi Samoray kobis@radware.com

Vendor Neutral

- No vendor package names in code
- No vendor branding / trademark present in code or output of build with the exception of the mitigation driver. This driver will be provided as an example of how vendors of attack mitigation systems can integrate their devices with Defense4All/OpenDaylight.
- No vendor branding / trademark present in documentation except with the documentation of the mitigation driver.

Meets Board Policy (including IPR)

Inbound Code Review has been completed with no issues found. {Phil Robb: 8/1/2013}