Overview

Ayla Cloud: DDoS Mitigation and Protection

Version: 1.0

Date Released: October 5, 2016

Document Number: AY006ODD1-1

Ayla Networks

Copyright Statement

Trademarks Statement

Referenced Documents

Ayla Networks does not supply all documents that are referenced in this document with the equipment. Ayla Networks reserves the right to make the decision on which of the documents it supplies with the equipment.

Contact Information

Ayla Networks TECHNICAL SUPPORT and SALES

Contact Technical Support: https://support.aylanetworks.com
or via email at support@aylanetworks.com

Contact Sales: https://www.aylanetworks.com/company/contact-us

Ayla Networks REGIONAL OFFICES

Chicago
10 N. Martingale Road, Suite 400
Schaumburg, IL 601073

HEADQUARTERS
Silicon Valley
4250 Burton Drive, Suite 100
Santa Clara, CA 95054
Phone: +1 408 830 9844
Fax: +1 408 716 2621

Boston
275 Grove Street, Suite 2-400
Newton, MA 02466

Table of Contents

List of Figures

List of Tables

1. Introduction

This document describes the defenses employed in the Ayla Cloud for DDoS attacks.

1.1 Intended Audience

The target audience for this document is someone who is familiar with Amazon Web Services (hereon referred to as AWS) and common Distributed Denial of Service (hereon referred to as DDoS) attacks and interested in learning about which DDoS defense mechanisms are employed to protect the Ayla Cloud

1.2 Related Documentation

AWS Best Practices for DDoS Resiliency:
https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf

2. Approaches to DDoS Threats

Ayla's DDoS defenses constitute a combination of threat mitigation controls as well as the ability to absorb and disperse high traffic rates.

The defenses include:

- Layered controls for infrastructure level as well application level attacks
- Reduction of the surface area for attacks
- Proactive Monitoring to detect unusual changes in network or access patterns
- Leverage AWS infrastructure to scale network and compute capacity

Layered controls address threats at the network level (e.g., UDP reflection, unauthorized port access), transport level (e.g., SYN floods, non-termination of SSL handshake) and the application level (e.g., flood of unauthenticated HTTP requests).

Having limiting the number of endpoints and instances exposed to the Internet greatly reduces the surface area available to attackers, therefore limiting the damage in the event of an attack.

Operationally, an increased rate of calls, increase in response times, spikes in network activity, CPU or memory utilization trigger alarms that alert operations personnel about unusual activity, thereby facilitating a quicker response.

The Ayla cloud architecture is based on horizontal and linear scaling principles and lends itself to be able to grow and shrink based on traffic patterns.

3. Elements of DDoS Defense

Figure 1 shows the different elements of DDoS Defense

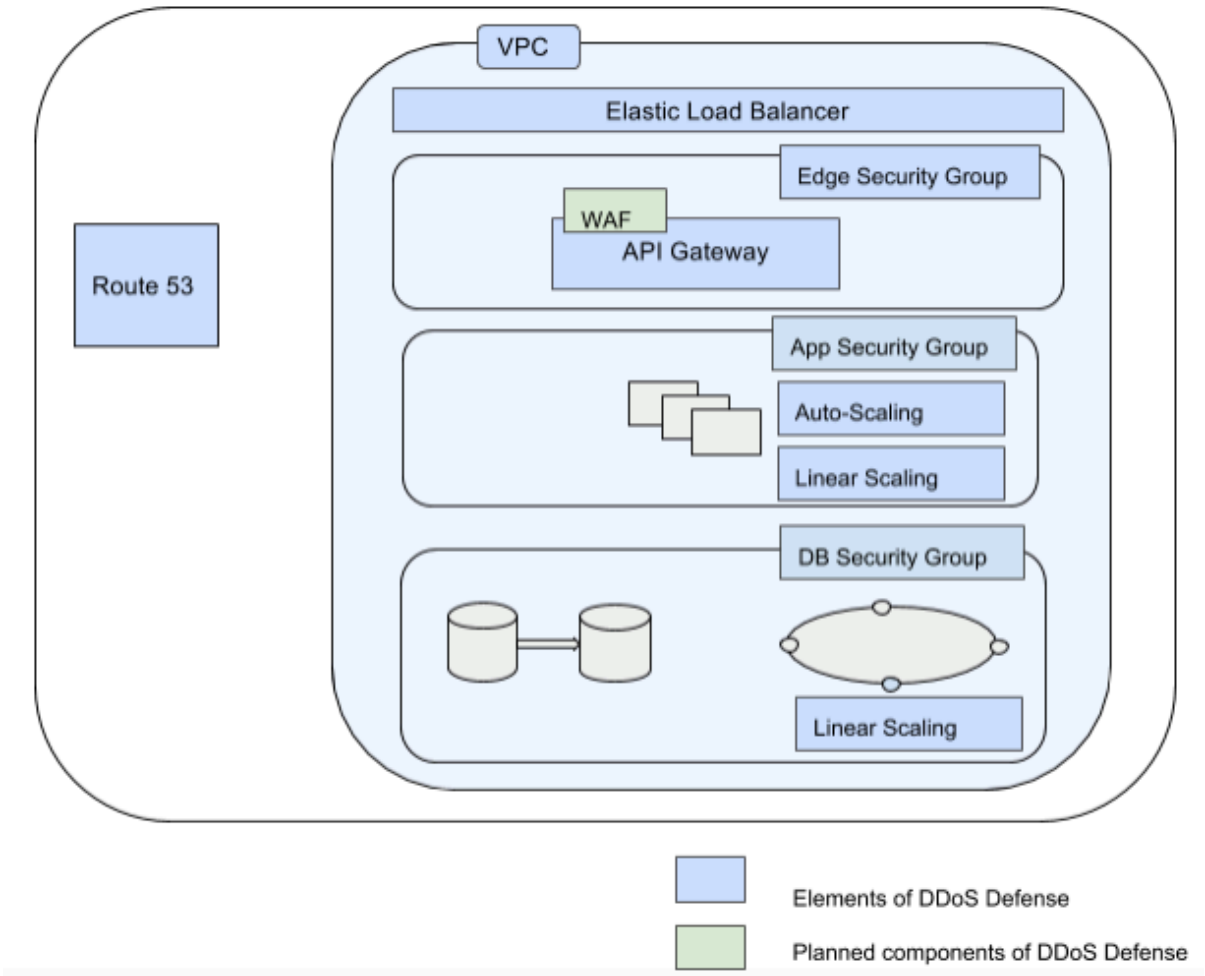

Figure 1: Elements of DDoS Defense

3.1 Route 53

The AWS DNS managed service is a highly available DNS service that uses shuffle sharding and anycast striping. This service offers a 100% SLA.

3.2 VPC

AWS offers a Virtual Private Cloud, which offers a layer of network isolation to instances running within it.

3.3 Elastic Load Balancer

The AWS Managed service that load balances requests across multiple availability zones and auto-scales to handle high traffic rates.

3.4 Security Groups

This is the AWS equivalent of a firewall that blocks access to ports and allows traffic selectively based on the source.

3.5 Auto Scaling

This Feature of AWS allows application instances to scale out and scale down based on traffic patterns.

3.6 Linear Scaling

The principle by which adding more resources results in higher transaction throughput; thereby improving the ability to absorb an increase in traffic. In the Ayla Cloud, the application layer is linearly scalable, i.e., adding more instances proportionally increases the throughput. In addition, since Ayla is an IoT cloud, write operations from always-on devices exceed read operations by an order of magnitude. Write operations are backed by a Cassandra database, which is linearly scalable, i.e. adding more nodes in production increases the throughput of the system.

3.7 API Gateway

This is an Ayla component that is horizontally scalable and acts as a gateway for filtering unclean traffic. It authenticates requests and performs rate limiting based on configurable policies such as user-based, ip-based, device-based, OEM based.

3.8 WAF

Web Application Firewall that is to-be-deployed on the API Gateway to filter out application level requests that have well-known signatures for SQL injection, XSS etc.

4. Threats and Mitigation Matrix

Table 1 shows the Threats and Mitigation support for the different DDoS Elements.

Table 1: Threats and Mitigation Matrix

	Route53	VPC	ELB	Security Group	Auto Scaling	Linear Scaling	API Gateway	WAF (TBD)
Network Level Mitigation (e.g. Volumetric attacks at the IP layer, UDP reflection attacks)	Yes	Yes		Yes				
Transport Layer Mitigation (e.g., SYN flood, SSL attack)	Yes		Yes					
Application Layer Mitigation (Unauthenticated requests, slowloris, malformed requests)							Yes	Yes
Reduction of Surface Area	Yes	Yes	Yes	Yes			Yes	Yes
Ability to handle increased traffic	Yes		Yes		Yes	Yes		

5. Conclusion

The Ayla Cloud runs on AWS infrastructure and adopts the industry's best practices to handle threats from DDoS attacks. In addition to the proactive measures being taken, Ayla also subscribes to Enterprise support from AWS. This gives Ayla access to 24x7 support from Amazon to offer additional operational support in the event of an attack.

4250 Burton Drive, Santa Clara, CA 95054
Phone: +1 408 830 9844
Fax: +1 408 716 2621