Machine Learning: Identification of attackers and clients during DDOS

Course:
Aprendizagem aplicada à segurança

Group:
Guilherme Amaral Ribeiro Pereira 93134
José Luis Rodrigues Costa 92996

Motivation

Distributed denial-of-service is one of the most popular and important attack of today's cyber world.

During a ddos attack it’s important to detect which users are real clients, and block the malicious.

Data sources

Network Packets

Capture of network traffic using wireshark

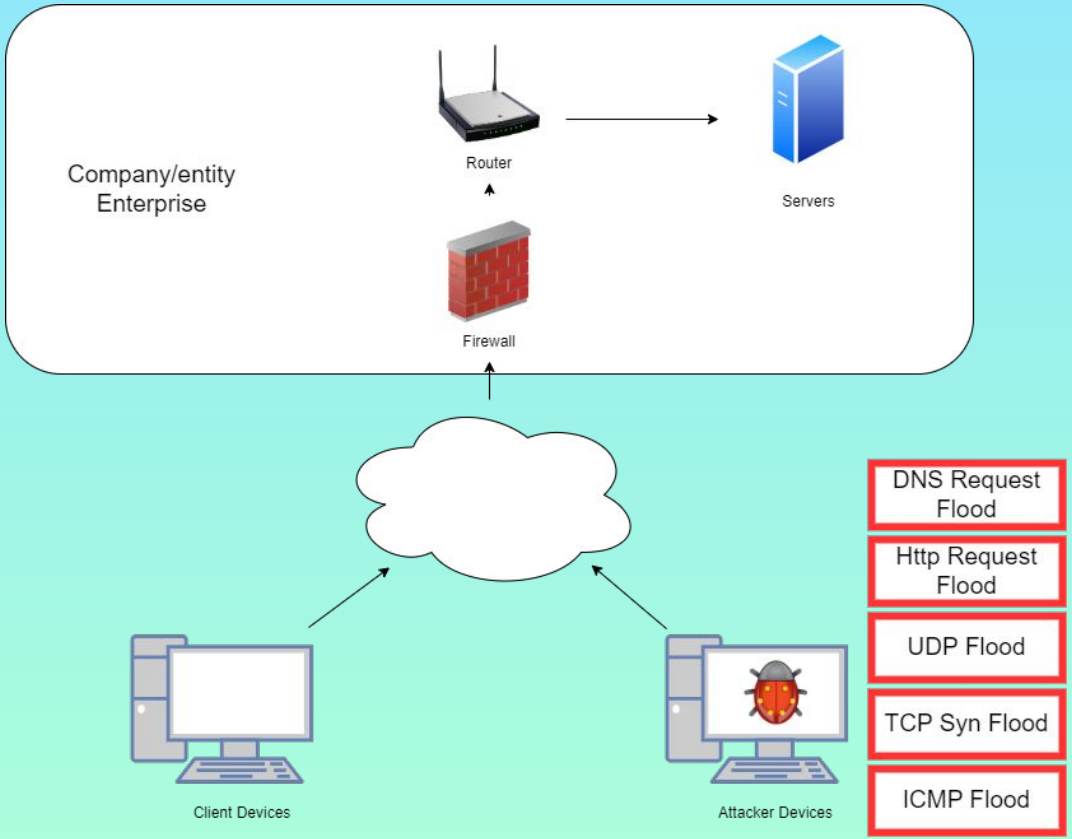
Apache Logs

Retrieve information from apache log files

DNS Logs

Retrieve information from DNS log files

Threat Model



Metrics

Packet Size

Source Ip

Destination Ip

Packet Timestamp

Timestamp when packet was received

Destination Port

Normally identifies the service that is being accessed

Number of packets

Number of packets in a specific timeframe

Metrics (cont.)

Packet Protocol

Tcp,Udp,Icmp

Apache / Dns Events

Multiple event types from logs of both applications

Features

Request Packet Size

Response Packet Size

Destination Ip

Source Ip Distance

Relative distance between the geolocations of the source ip's and the servers location

Packet Protocol

Tcp,Udp,Icmp

Source Ip

Features (cont.)

Time Variance Between Requests

How the time between requests varies by source ip

Number of requests (Apache)

Number of http requests to the apache server by source ip

Number of requests (Dns)

Number of resolutions to the dns server by source ip

Apache Authentication

If the source ip is authenticated in the apache website

Number of errors (Apache)

Number of returned errors from the apache server to the source ip

Number of errors (Dns)

Number of returned errors from the dns server to the source ip

Features (cont.)

Requested dns resolutions variance

Variance between all requested dns resolutions

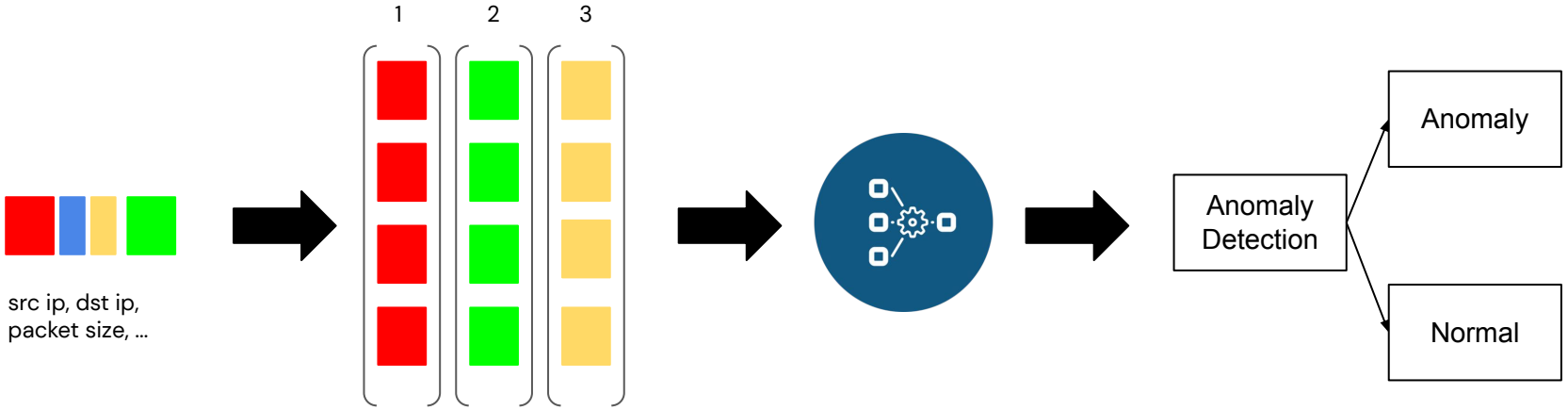
Apache accessed web pages variance

Variance between all http requests

Number of packets

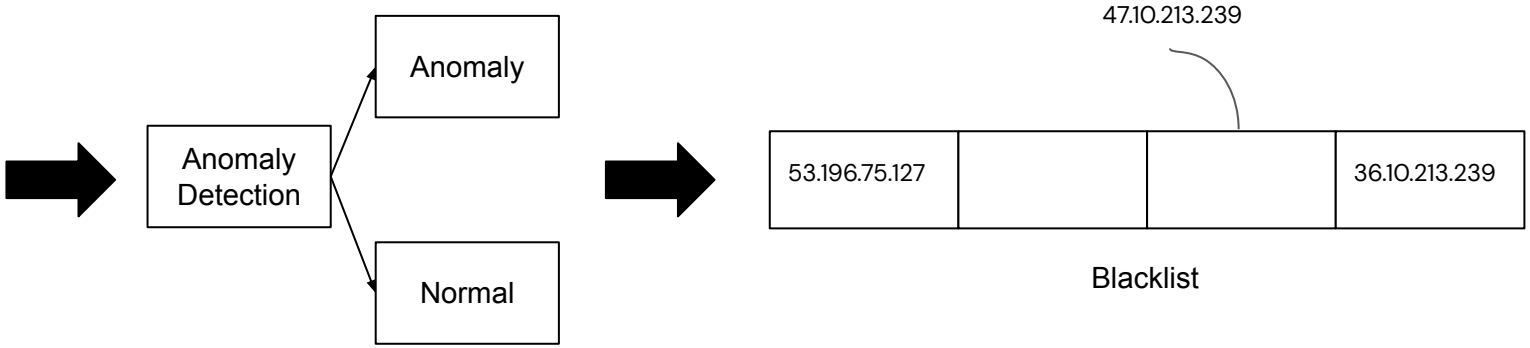
Number of packets in a specific timeframe

Proposed Framework



Data capture → Group Data by Source Ip → Feature Generation → Anomaly detection

Proposed Framework (cont.)



Anomaly detection

Creation of a black list based on the number of times an anomaly was detected for each IP

THANKS!

Do you have any questions?