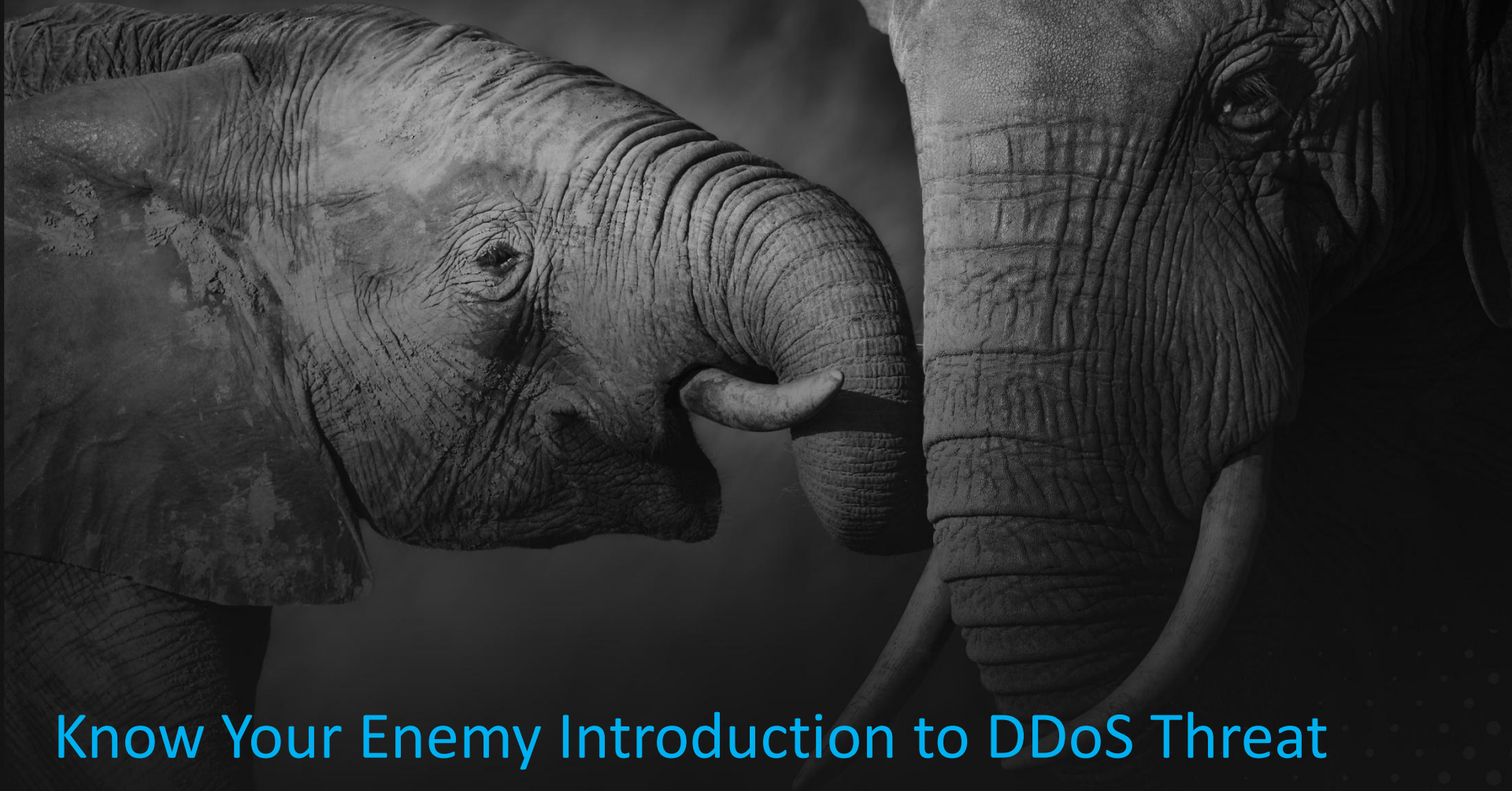


Know Your Enemy Introduction to DDoS Threat

Red Button

RED BUTTON
SEEKING CYBER ACTION

Agenda

- What is DDoS?
- DDoS Attack Types
- Best Practice Mitigation Methods

What is DDoS?

Motivation

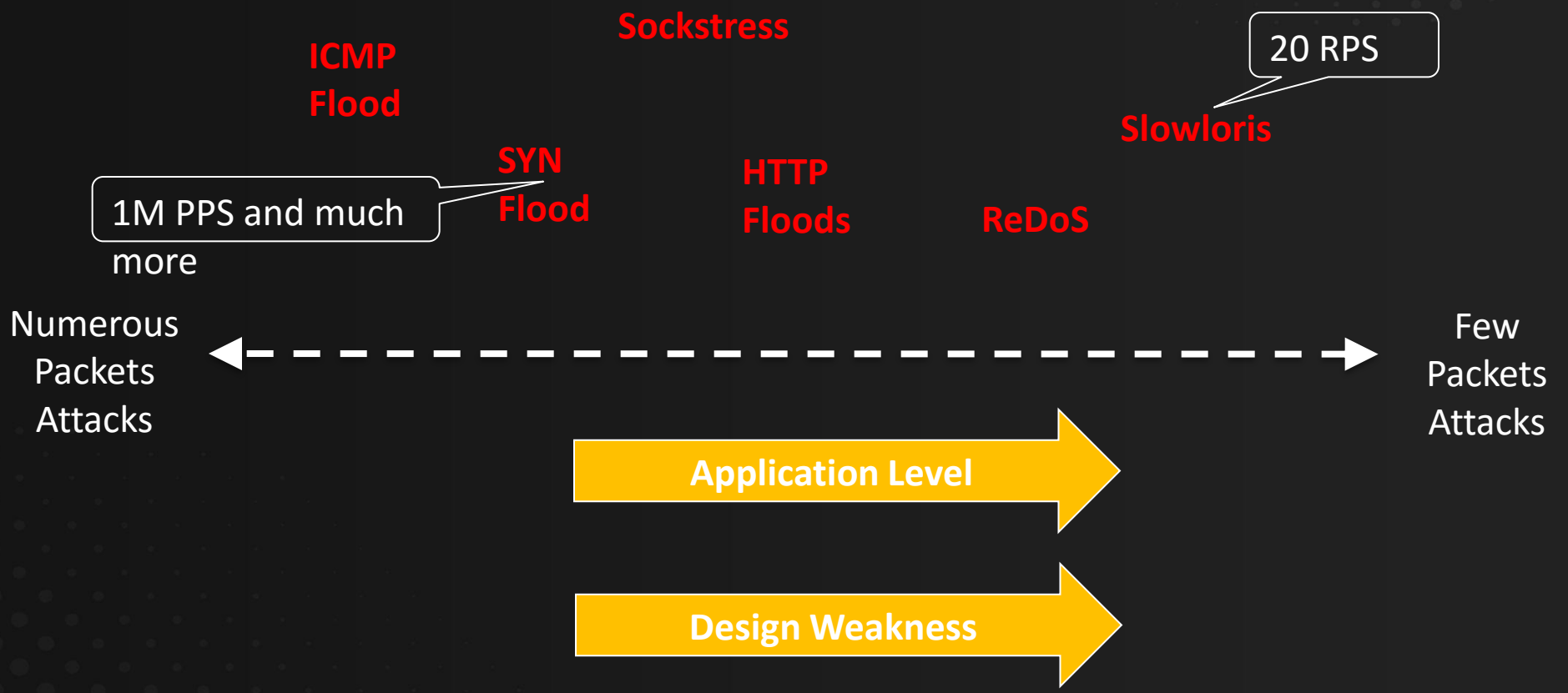
Motivation

- Hacktivism
- Business competitors
- Cyber Warfare
- Ransom
- Angry Users

Technical Motivation

- Denial of service
- Smoke Stream
- Impacting security (FW, IPS)

DDoS Attack Types



DDoS Attack Vector

Type	Example
Volumetric	•SYN Flood •UDP Flood •ICMP flood •DNS Reflection •NTP Flood •CHARGEN Flood
Application	•HTTP Flood •HTTPS flood •DNS query flood •DNS recursive flood
Low-and-slow	•Slowloris •R.U.D.Y •Large file download

Each year more attack vectors are seen in each campaign

DDoS Points-of-Failures

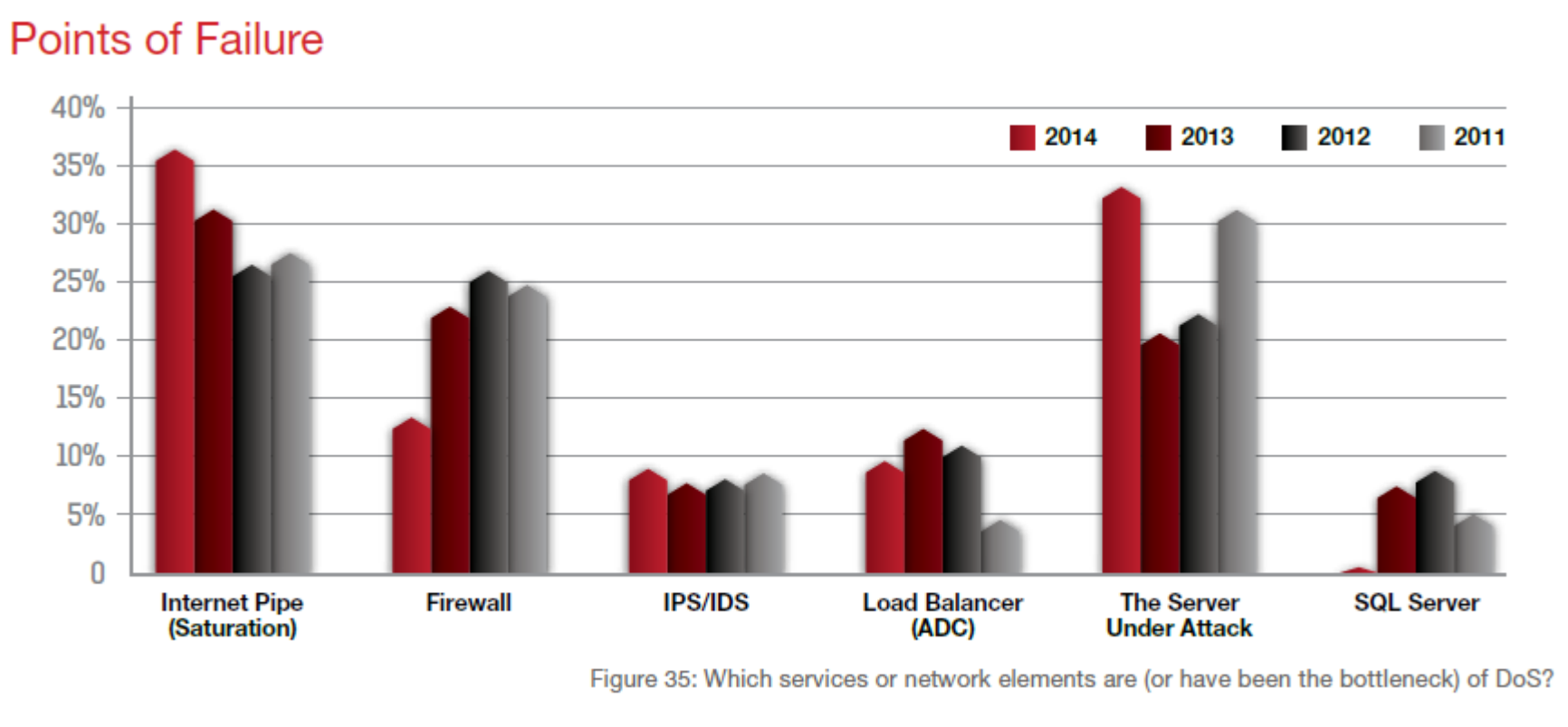


Figure 35: Which services or network elements are (or have been the bottleneck) of DoS?

Radware Global Application & Network Security Report 2014-2015

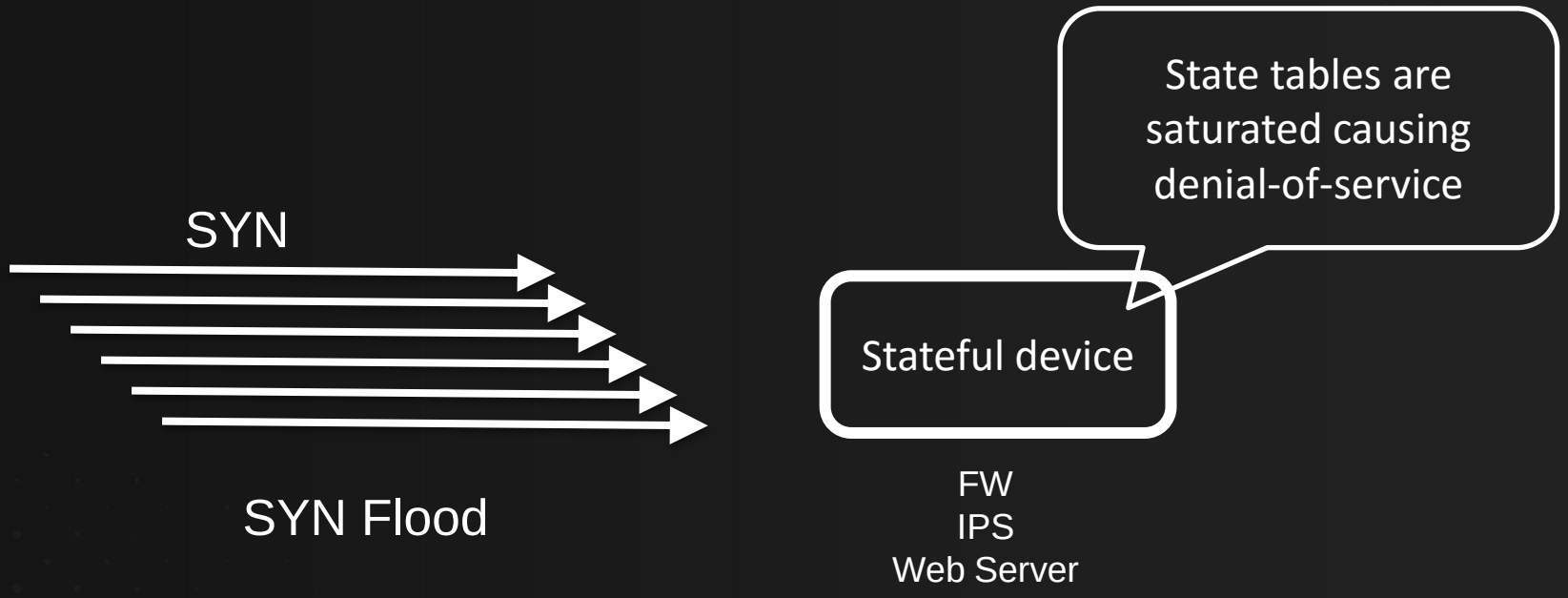
RED BUTTON
SEEKING CYBER ACTION

DDoS Attack Types

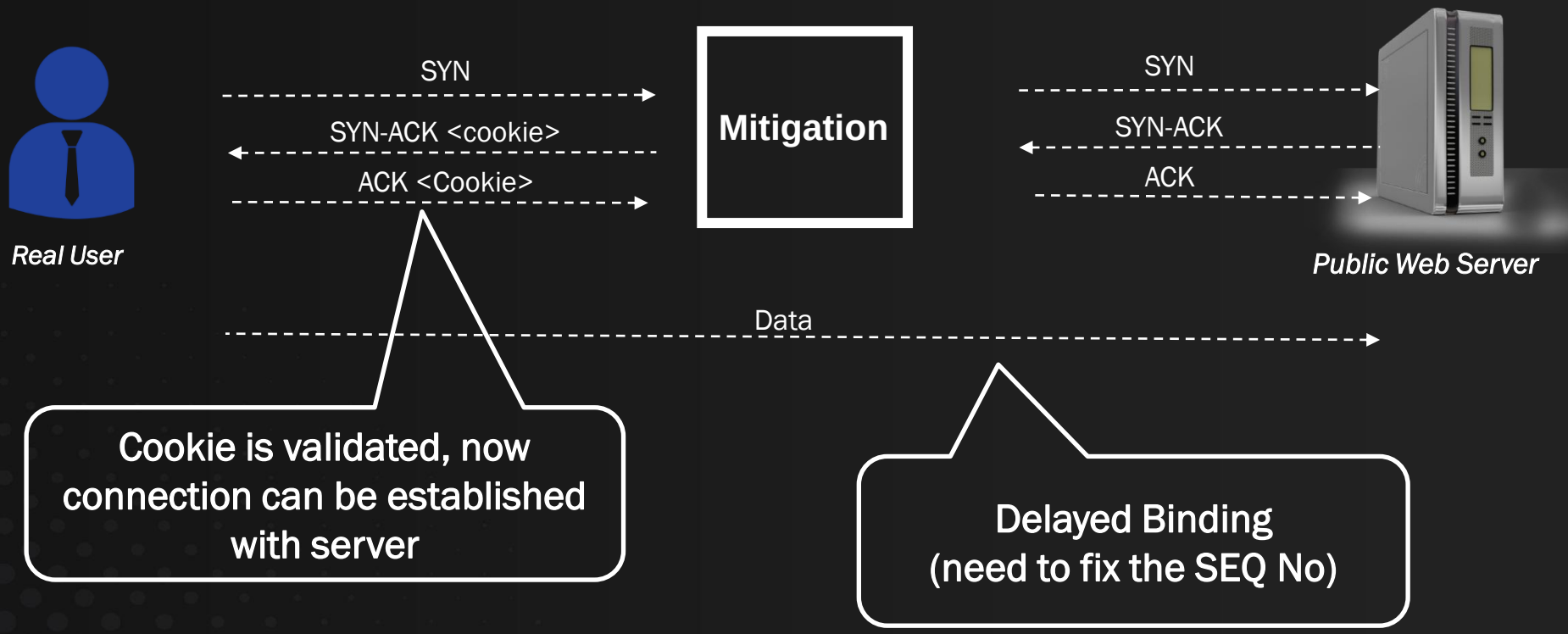
DDoS Attack Types

1) SYN Flood
2) UDP Flood
3) HTTP Flood
4) HTTPS Flood
5) Slowloris
6) R.U.D.Y
7) SSL-Renegotiation
8) DNS Recursive Flood
9) DNS Reflective Flood
10) NTP Reflective Flood

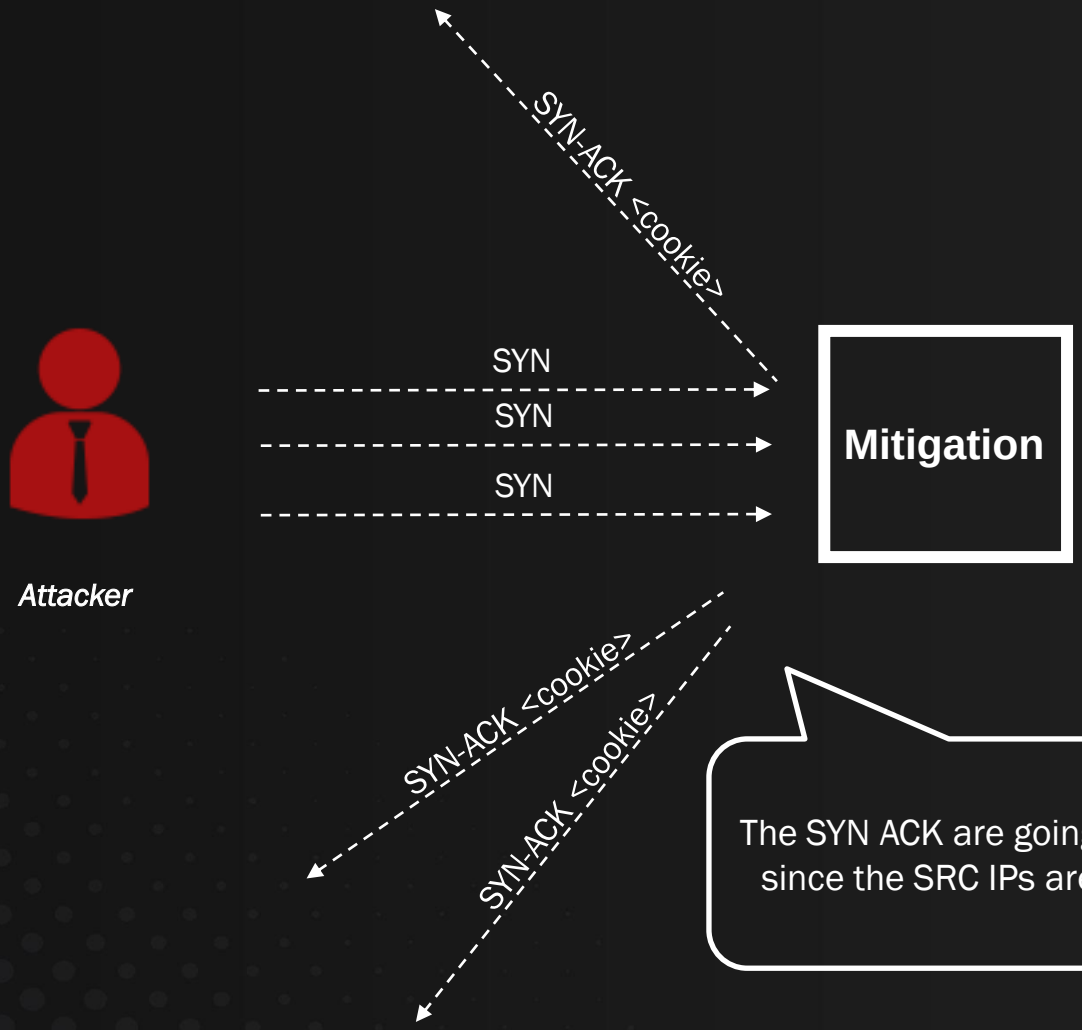
SYN Flood



SYN Cookies (legitimate)



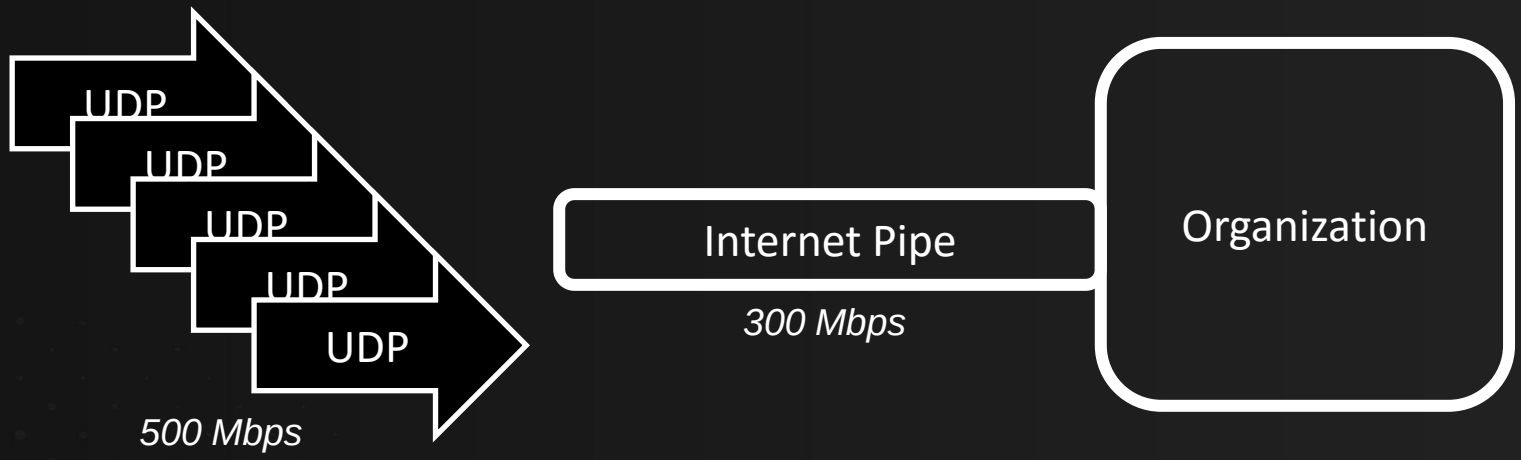
SYN Cookies Attacker



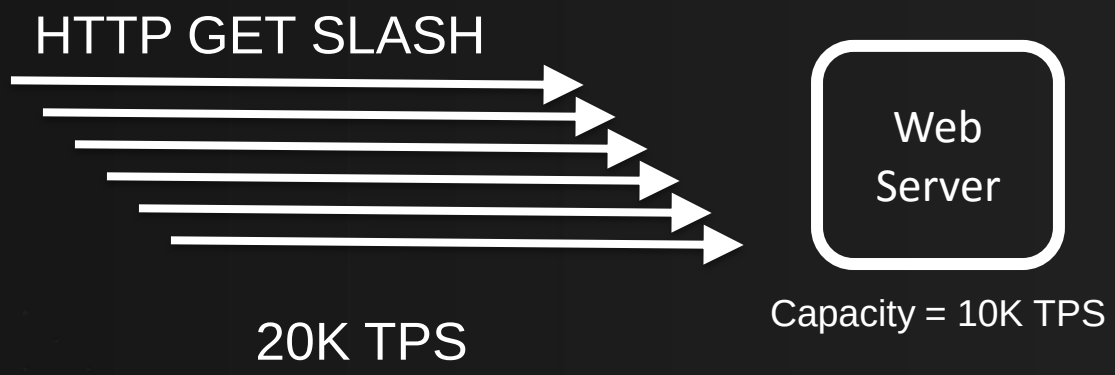
Public Web Server

RED BUTTON
SEEKING CYBER ACTION

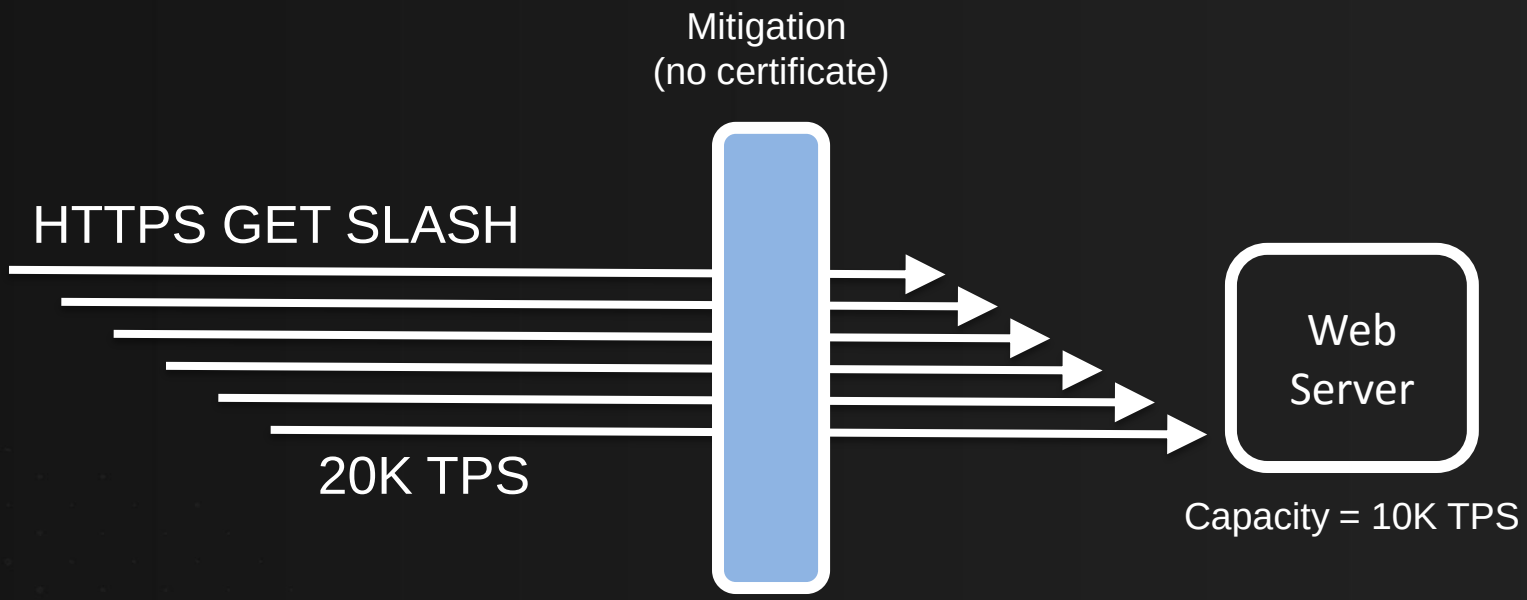
UDP Flood



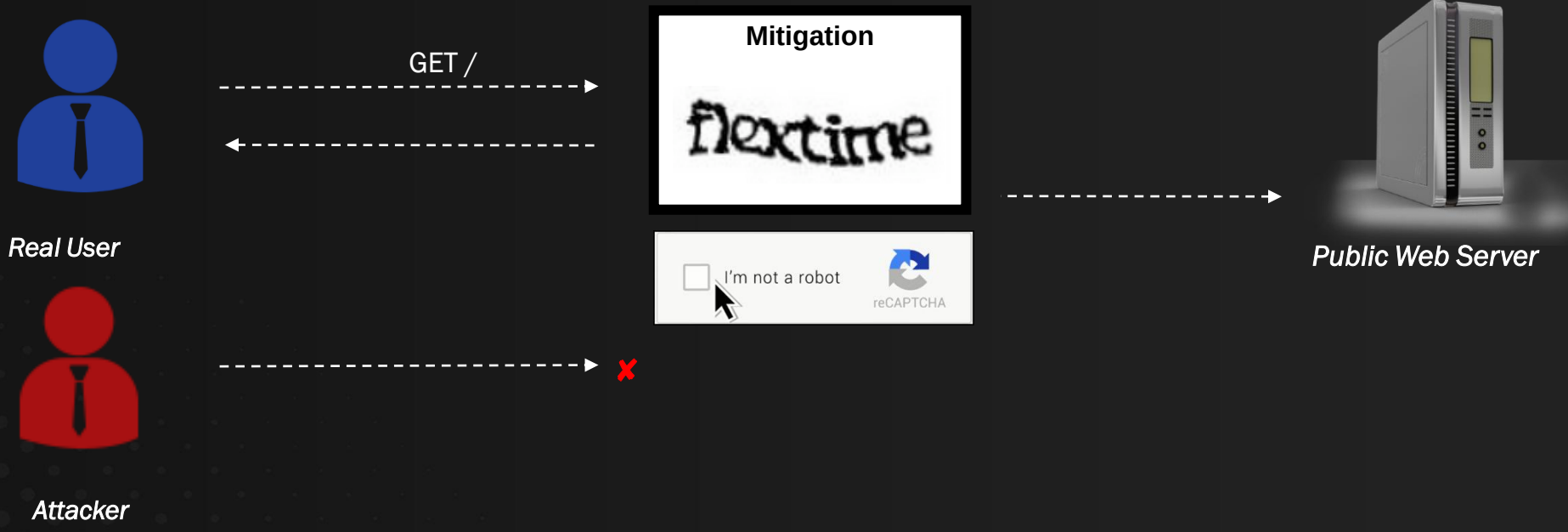
HTTP Flood



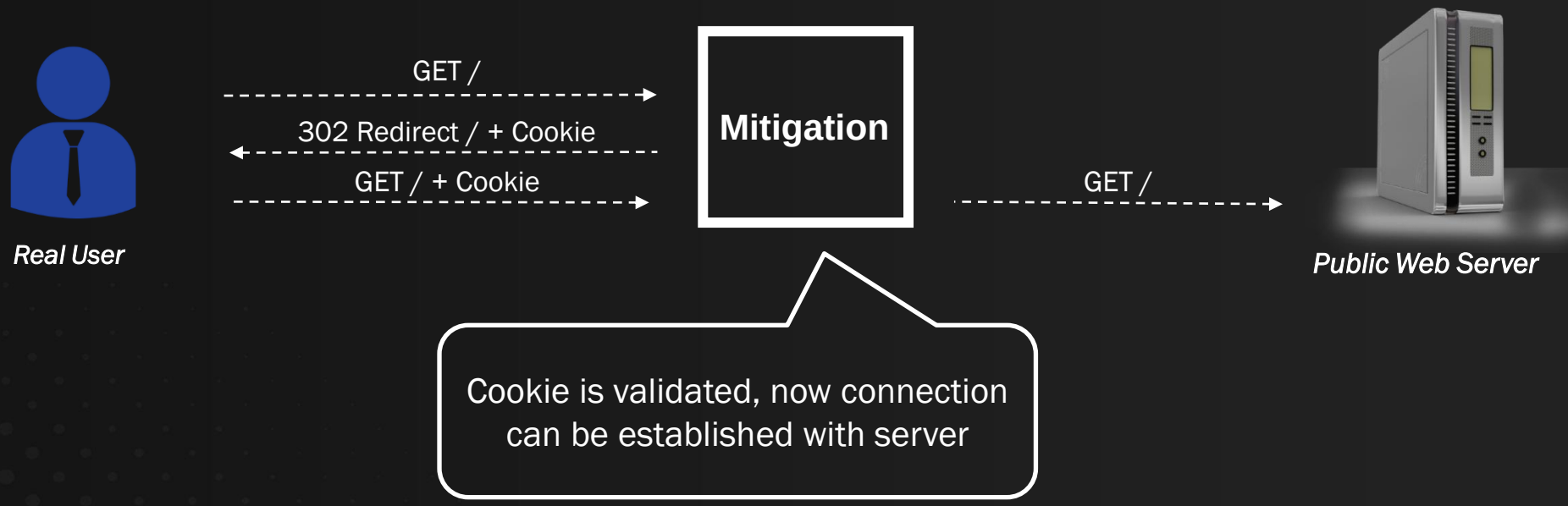
HTTPS Flood


Mitigation
(no certificate)
HTTPS GET SLASH
20K TPS
Web
Server
Capacity = 10K TPS

Web Challenge CAPTCHA

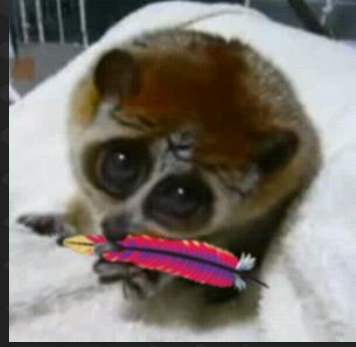


Web Challenge Legitimate (302 Redirect)



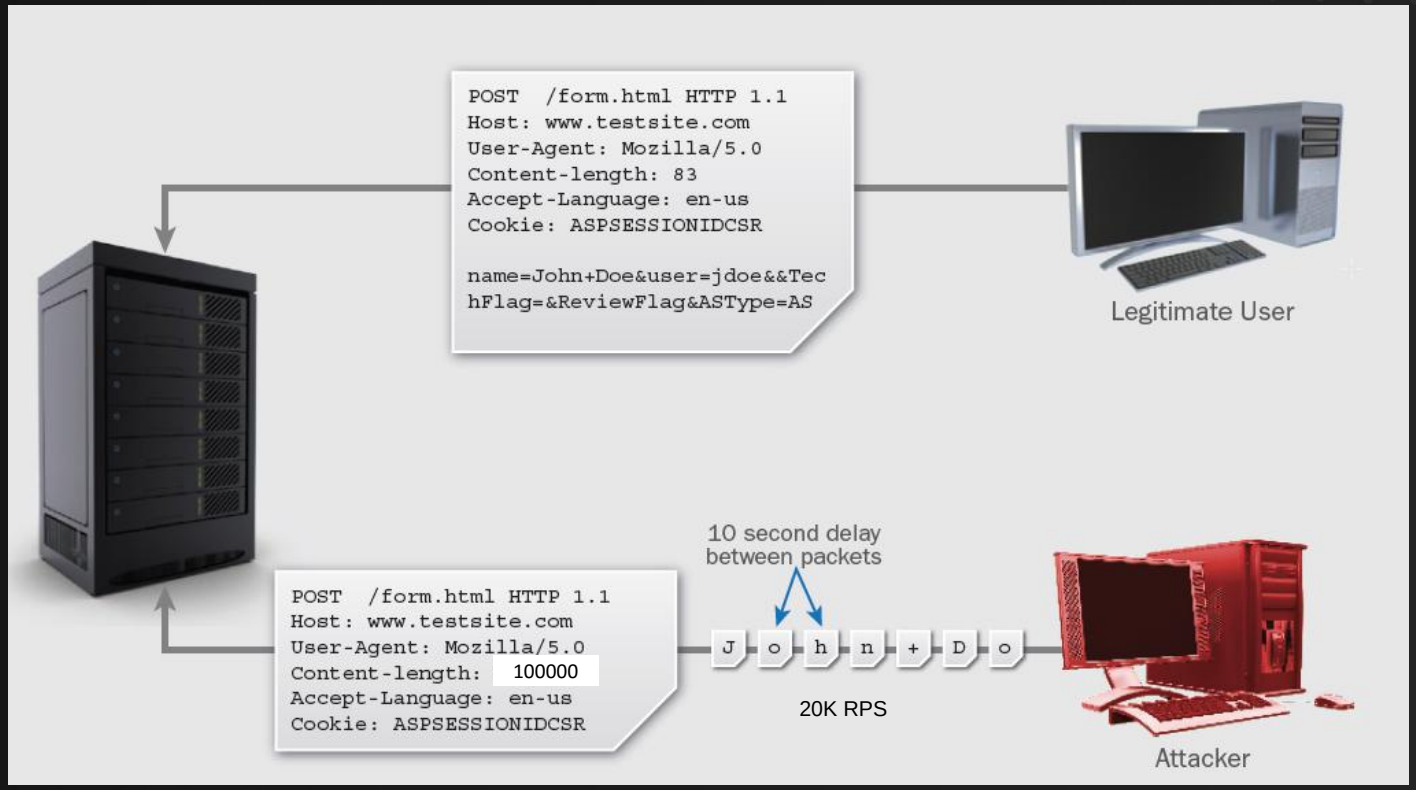
Web Challenge Attacker (302 Redirect)

SLOWLORIS

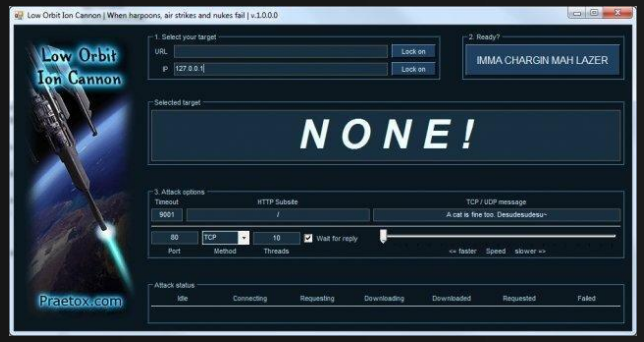


RED BUTTON
SEEKING CYBER ACTION

R.U.D.Y (Are You Dead Yet)



Signature



LOIC
(Low Orbit Ion Canon)

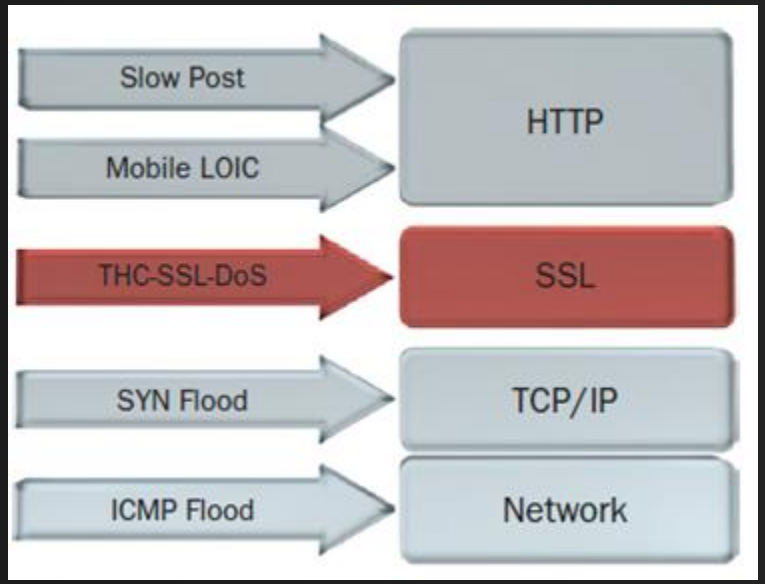
"A CAT IS FINE TOO"

IPS

IPS can block known DDoS patterns with a signature

SSL Renegotiation

- The attacker renegotiations the SSL keys again-and again
- This labor takes x15 more resources from the server

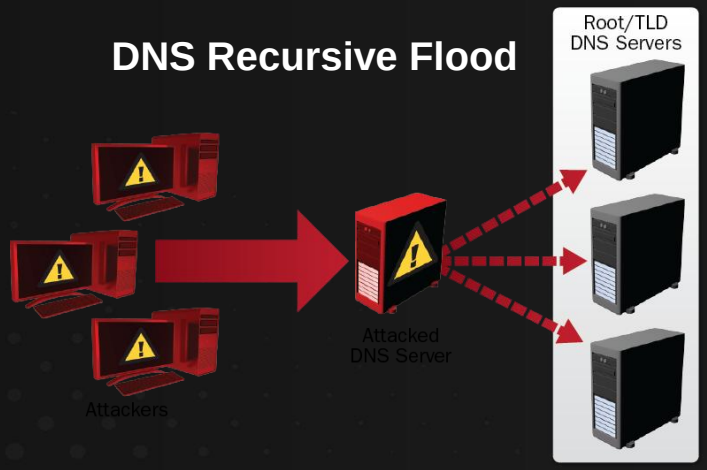


DNS Floods

DNS Query Flood

DNS Reflective Flood

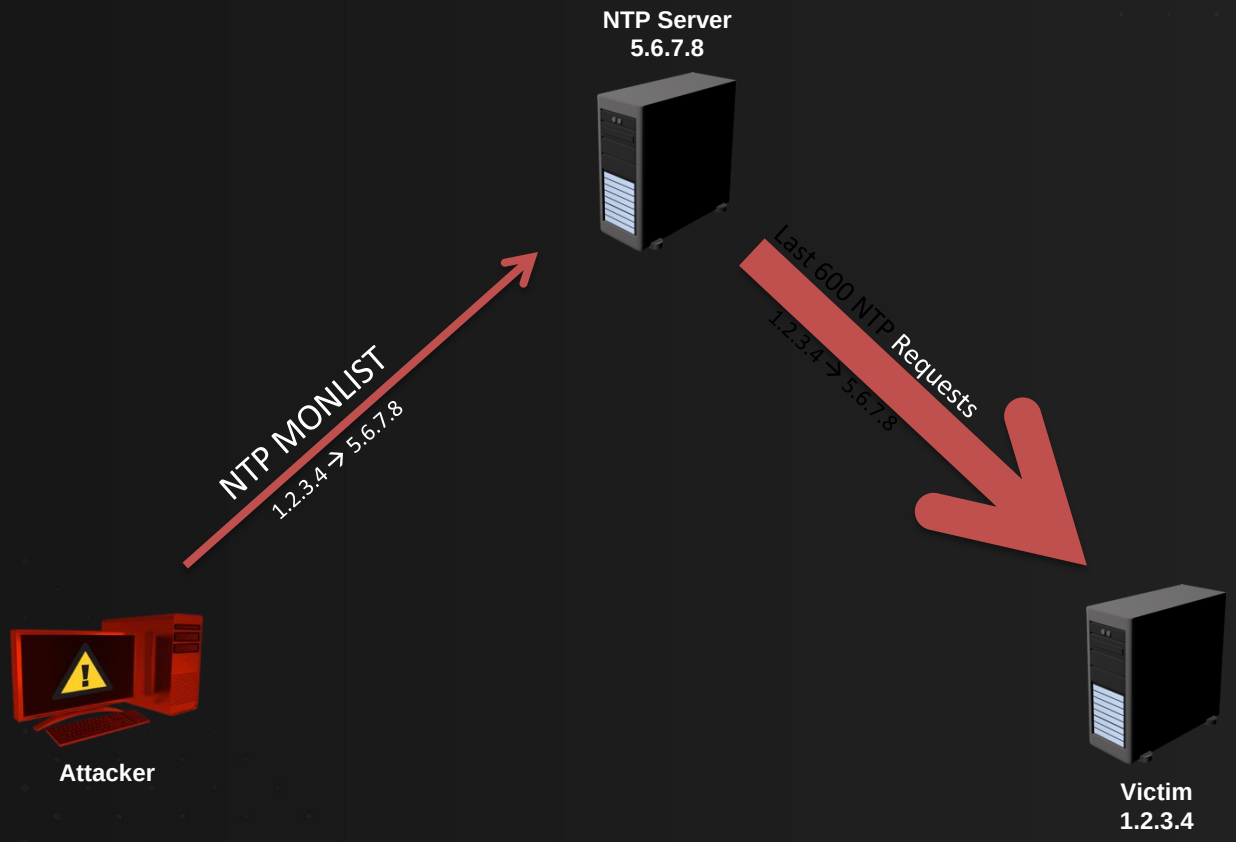
DNS Recursive Flood



DNS Garbage Flood

RED BUTTON
SEEKING CYBER ACTION

NTP Reflective Flood



RED BUTTON
SEEKING CYBER ACTION

Thank You

UNDER ATTACK? +972-77-5001962

Adress: Tagor 29/6 Tel Aviv 6920331 **Site**: red-button.net **Email**: info@red-button.net **Office**: +972-77-5001962 **Fax**: +972-77-320470