Útoky DDoS a testování bezpečnosti a výkonnosti sítě

Bezpečnost ICT 2

Michael Jurek, Lukáš Malina

Vysoké učení technické v Brně
malina@vut.cz
axe.utko.feec.vutbr.cz

2022

Informační bezpečnost

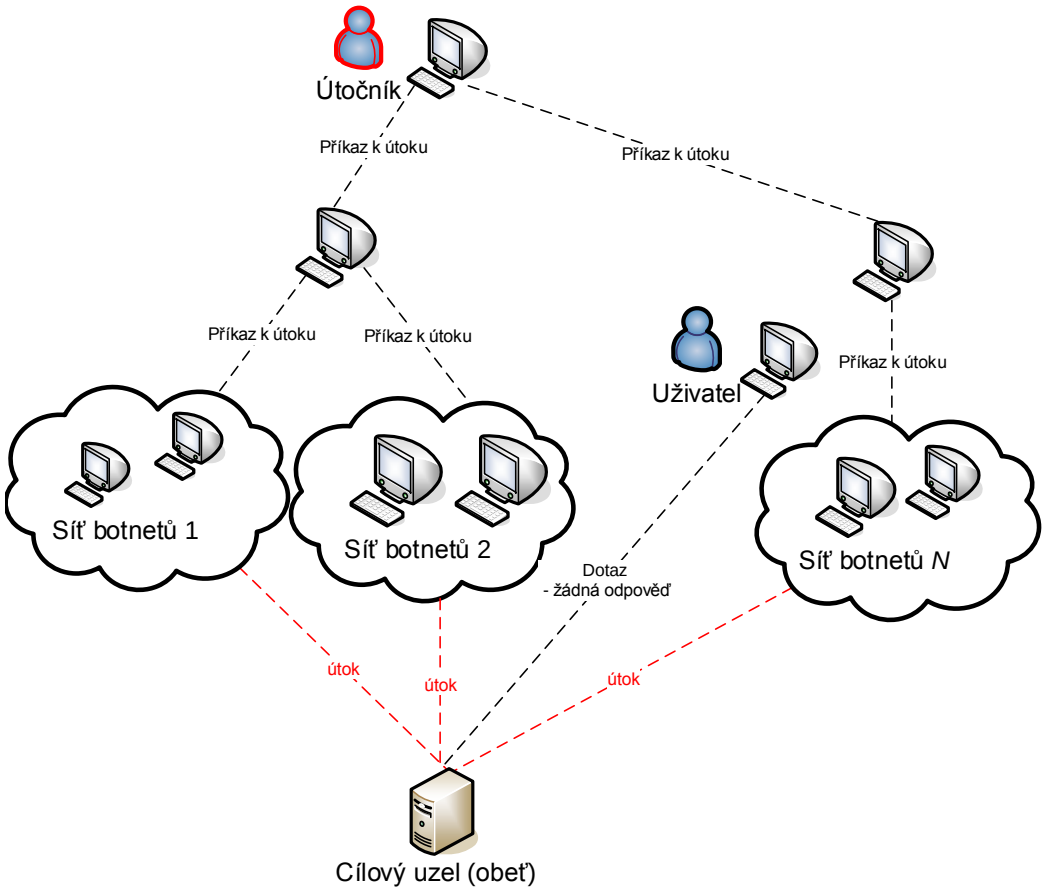
1. Útoky DoS a DDoS
   - Princip a typy útoků (D)DoS
   - Detekce a mitigace DDoS
2. Testování bezpečnosti sítí
   - Proč, co, kdy a jak?
3. Testování výkonnosti a odolnosti proti DDoS
   - Testování výkonnosti
   - Testování odolnosti proti DDoS
   - Testování - příklady, ukázky

Útoky DoS a DDoS

DoS a DDoS?

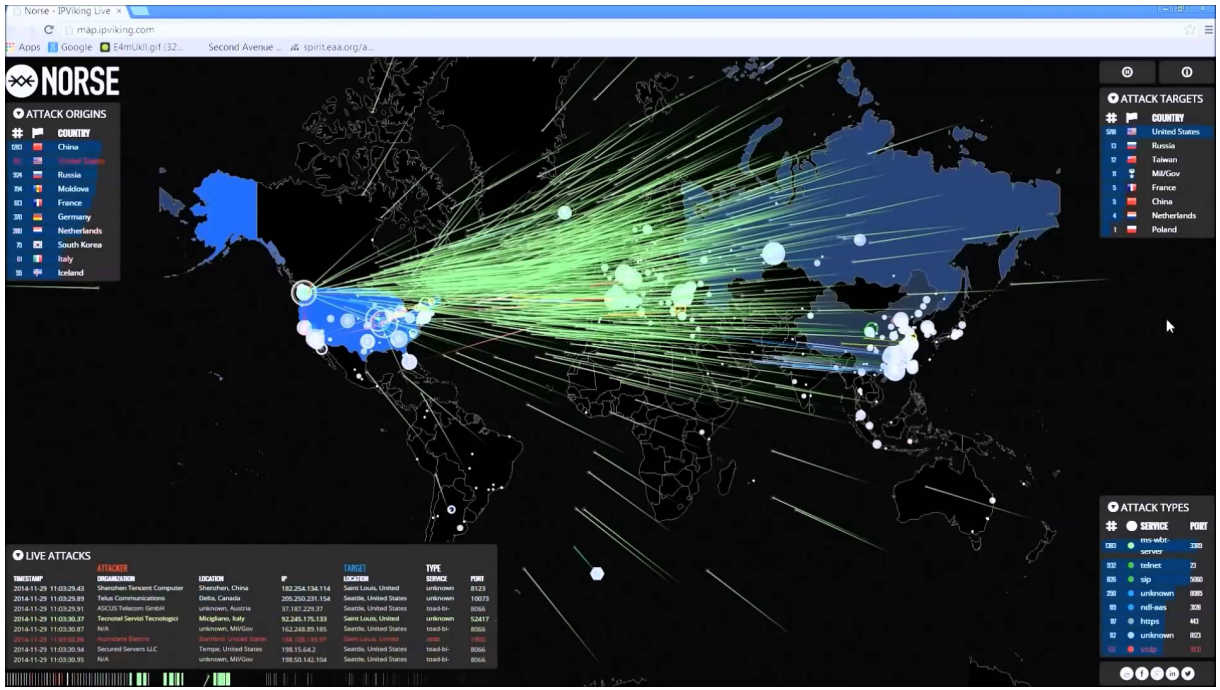
- **DoS (Denial of Service)** - snaha uvrhnout útočníkem vybranou službu do nefunkčního stavu a tím **odepřít** uživatelům této služby její **dostupnost**.
- **DDoS (Distributed Denial of Service) – DoS útok**, který je realizován **od více uzlů**, které s hlavním útočníkem spolupracují a napadají cílový uzel (např. webový server) v určitém čase a s určitou intenzitou útoku.

Útoky DDoS


Útočník
Příkaz k útoku
Příkaz k útoku
Příkaz k útoku
Příkaz k útoku
Příkaz k útoku
Uživatel
Síť botnetů 1
Síť botnetů 2
Síť botnetů N
Dotaz
- žádná odpověď
útok
útok
útok
Cílový uzel (obeť)

Kybernetické útoky online

https://cybermap.kaspersky.com/
https://threatmap.checkpoint.com/
https://livethreatmap.radware.com/



Projevy (D)DoS útoku[1][2]

- Zpomalení služby, dlouhé časy načítání (load time).
- Celková nedostupnost části nebo celé aplikace.
- Nemožnost připojení legitimního klienta ke službě.
- Celková ztráta konektivity zařízení na stejném subnetu.

[1] US-CERT

[2] Náchylné na False Positive události způsobené běžným SW nebo HW výpadkem.

(D)DoS statistiky

- 33 % – meziroční nárůst DDoS útoků mezi roky 2021 a 2022.
- 4 hodiny – průměrná doba DDoS útoku (*Securelist*).
- 509 hodin – nejdéle trvající DDoS útok (*Kaspersky*).
- 853.7 `Gbps` – největší zaznamenaný Evropský DDoS útok na Prolexic (*Akamai* 21. 7. 2022).
- 3.47 `Tbps` – největší zaznamenaný DDoS útok na Microsoft (listopad 2021).
- 46 `Mrps` – největší L7 DDoS (*Google* 1. 6. 2022).
- 4.31 `Gbps` – průměrná velikost útoku (Qrator Labs Q3 2021).[3]
- 14 vektorů – u více než 20 % DDoS útoků.
- 300,000-1,000,000 $ – průměrná hodinová ztráta společnosti

[3] Oproti Q1 2020 je průměrná velikost poloviční.

(D)DoS business

Počet požadavků/spojení	Propustnost	Doba trvání	Cena
10-50 k	-	1 h	15 $
10-50 k	-	24 h	50 $
20-50 k	-	24 h	200 $
10-50 k	-	1 týden	500 $
1 session	125 Gbps	600 s	22 $
1 session	125 Gbps	3600 s	90 $

Table: Ceny DDoS utoků na Darknetu

DDoS botnet

- **Kompromitované uzly** které se podílí na útoku jsou označeny jako zombies a tvoří síť **botnet**.
- Velká geografická rozprostřenost botnetu.
- Od několika desítek až do jednotek milionů uzlů v botnetu.
- Mohutnost `Mpps` s propustností `Tbps`.
- Nenápadnost tzv. Slow DoS útoky v kombinací s více vektory
- DDoSy na objednávku (**DDoSaaS** – Distributed Denial of Service-as-a-Service, **booter** – služba, která obsahuje útok, support, tutorialy, placená na měsíční bázi).

DDoS botnet - principy a vlastnosti

- **Vytvoření botu** - **infikace** cílového PC (Zombie) pomocí exploitu či trojanu (crack, falešné kodeky, rogueware) - škodlivá aplikace - bot.
- Aplikace **bot** se pak **připojí** ke **kontrolnímu serveru** (**botmaster** - útočník pak má přehled kolik má botů online).
- **Komunikace** pomocí **klient** (zombie - bot) - **C&C server** (centrální řídící bot nebo několik řídících botů), např. pomocí DNS (např. botnet Ebury), IRC kánalu, IM jako ICQ/XMPP nebo HTTP/**HTTPS** (nejvíce používán, nefiltruje se tolik), Telnet.
- Novější boty - P2P komunikace, decentralizace.
- Botmaster pak může zjišťovat i přístupové hesla z daných PC (spyware) a ty dále prodávat.
- Bot může dále provádět Bitcoin mining, sbírat adresy a přeposílat spam.

DDoS botnet - příklady

Botnety jsou pojmenovány podle malware použitého k jeho vytvoření.

- 2004 Bagle – červ, který přeposílal spam od bootmastera.
- 2008 Akbot – první botnet, který vykonával DDoS.
- 2009 Zeus – *trojský kůň*, cryptolocker ransomware, rozšíření přes download a phishing (https://github.com/Visgean/Zeus/).
- 2014 MrBlack – *trojský kůň*, cílí na SOHO (*Ubiquiti*) směrovače skrz chybu ve firmware.
- 2016 Mirai – *IoT malware*, IP kamery, routery (https://github.com/jgamblin/Mirai-Source-Code).

DDoS - fáze útoku (Kill Chain)

- Průzkum (Reconaissance) – zjištění IP adresy oběti, technologie, topologie, verze a potenciální zranitelnosti ....
- Definice a doručení (Weapponization & Delivery) – definice vlastností útoku, protokol, port, IP spoofing ....
- Zneužití zranitelností (Exploitation) – provedení útoku.
- Command and Control (C2) – komunikace mezi boty a C&C serverem, úprava payload, reakce na chování serveru. (keylogger, screenshoty, ransom, zachytávaní provozu, krádež dat, eskalace oprávnění, kontrola procesů ...)

(D)DoS rozdělení

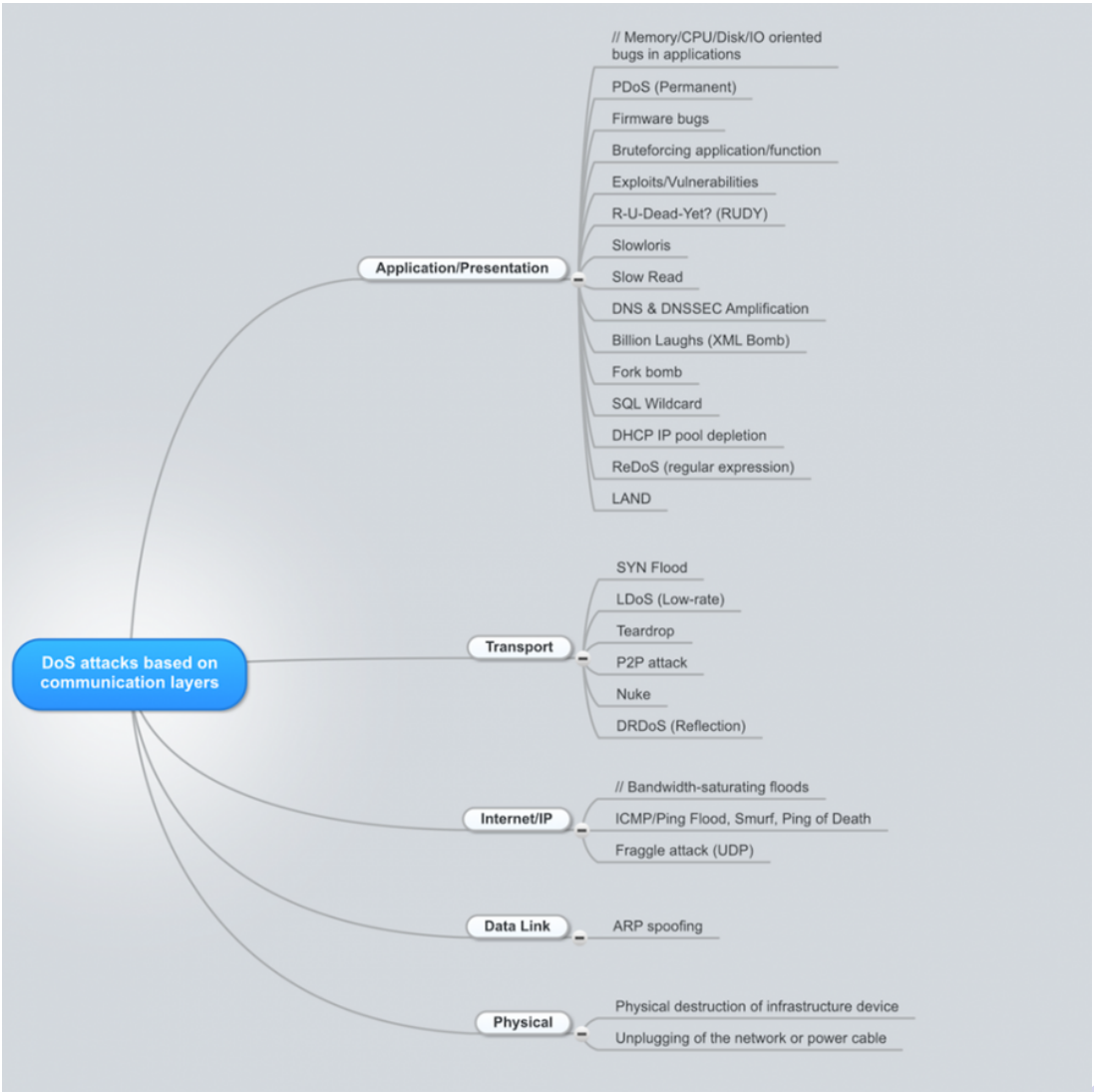
Záplavové útoky/volumentrické (flooding attacks) [bps]

- **Vytížení** komunikační /paměťové/ výpočetní kapacity cíle útoku.
  - Př.: TCP flood, UDP flood, HTTP flood, ICMP flood.
- **Amplifikující** útoky – faktor zesílení.
  - Př.: NTP Amplification, DNS Amplification, SSDP Amplification, Memcached Amplification.

Logické útoky (logical/application attacks)

- Útok na logickou **slabinu** v programu / protokolu / OS.
- dělíme na:
  - **Protokolové** útoky – zneužívá se vlastností protokolu (L3, L4). [pps]
    - Př.: Ping of Death, Land Attack, SYN Flood, TCP State Exhaustion
  - **Aplikační** útoky – zneužívají chybnou implementaci aplikace (L7).
    - Př.: SlowLoris, Slow Read, Slow Drop, Slow Next, Slow Post.

DDoS přehled útoků



DDoS příklady záplavových útoků

- Útok **ICMP Flood** - zaplavení oběti velkým množstvím `ICMP ECHO REQUEST` zpráv. Útočník nečeká na odpověď a neustále odesílá požadavky.
- Útok **ARP Flood** - Address Resolution Protocol (převod IP adresy na adresu MAC). Oběť je zahlcena **velkým počtem falešných dotazů ARP**, které vyčerpají výpočetní nebo paměťové zdroje cílového uzlu.
- Útok **HTTP Flood** - Volumentrický útok vedený z několika zombie klientů, které na cílový webový server (aplikaci) posílají **legitimní**, ale procesně náročnější žádosti **HTTP GET** nebo **POST**. Hůře detekovatelné.

DDoS příklady záplavových útoků

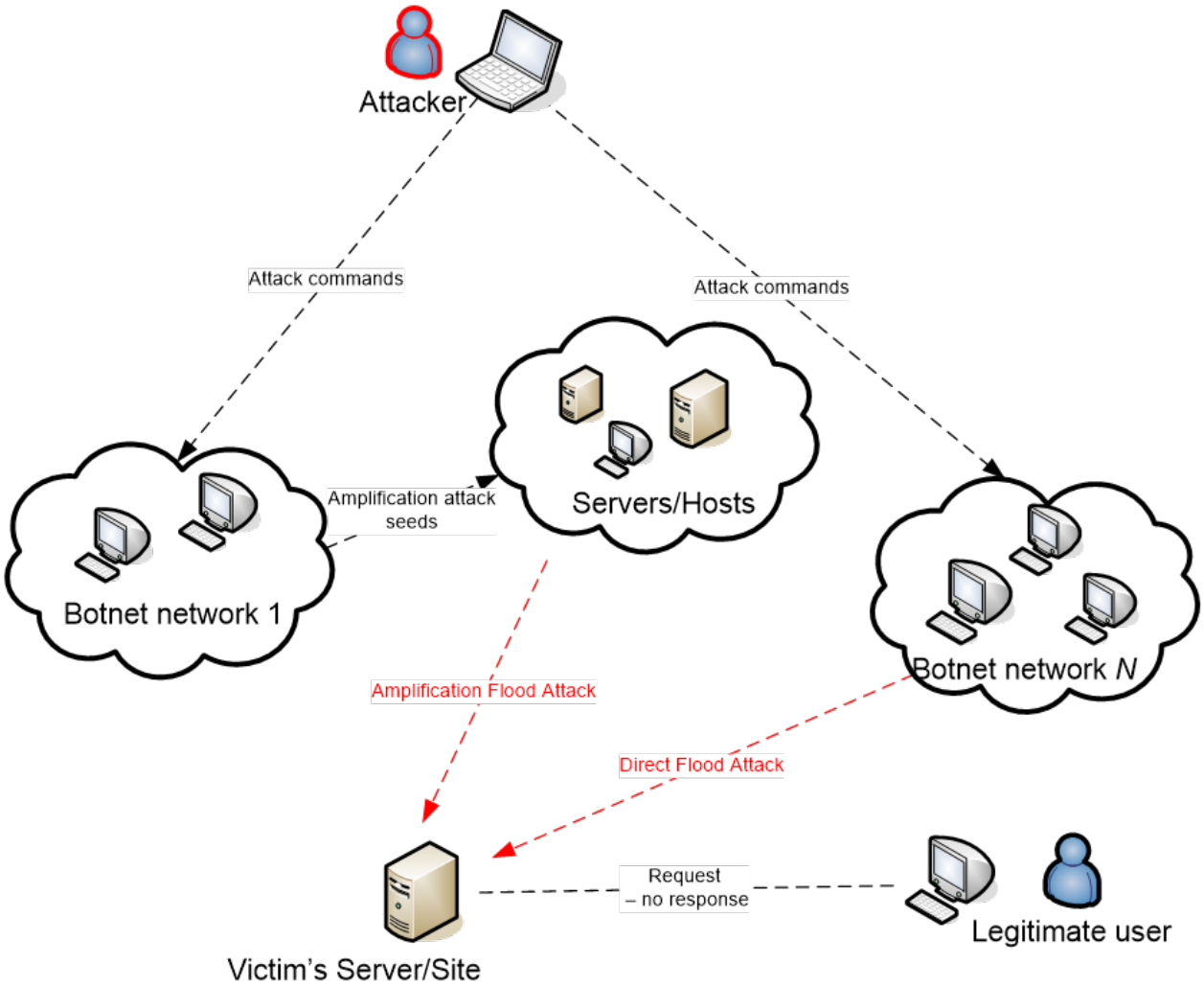
- Útok **UDPFlood** - **Velký počet** IP paketů obsahující datagramy **UDP**, které jsou směřovány na daný cíl. Cíl je po určité době zahlcen a nezvládne obsloužit ani validní spojení.
- Útok **PingSweep** - ICMP echo žádosti s podvrženou src adresou jsou posílány na uzly v síti. Zprávy-žádosti požadují odpovědi, které jdou pak na cílový systém/oběť - zahltí se cílový systém.
- Útok **Smurf** - ICMP žádosti jsou posílány na broadcast adresu se **spoofovanou zdrojovou IP oběti**.

DDoS příklady amplifikujících útoků

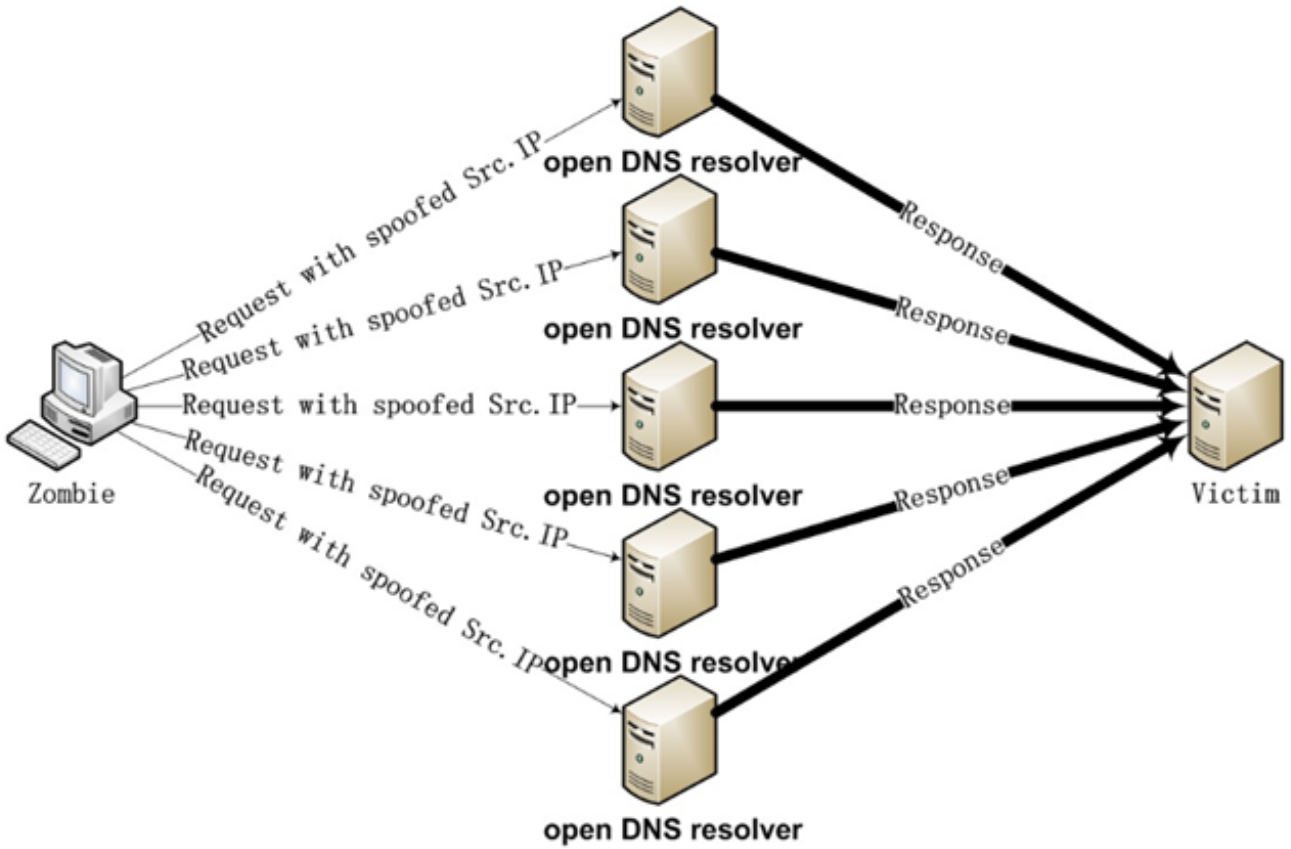
Útoky typu **Traffic Amplification by Reflecting** -

- útočník využívá další strany/legitimní servery v síti (např. DNS servery), kterým zašle dotaz se **zdrojovou adresou cíle/oběti** a požaduje nějakou **odpověď (reflekce)**.
- Podvržené dotazy mají obvykle malou velikost (několik B), ale odpovědi mají **velkou velikost - několik KB**.
- **Faktor amplifikace** (zesílení) AF je pak 28 až 10000.
- Populární od 2013 a velice účinné.
- Např. DNS reflection (AF cca 30 až 54), NTP reflection (AF cca 557), memcached servery (AF od 9000) a další UDP protokoly.

DDoS Amplification by Reflecting



DDoS - DNS reflection ukázka



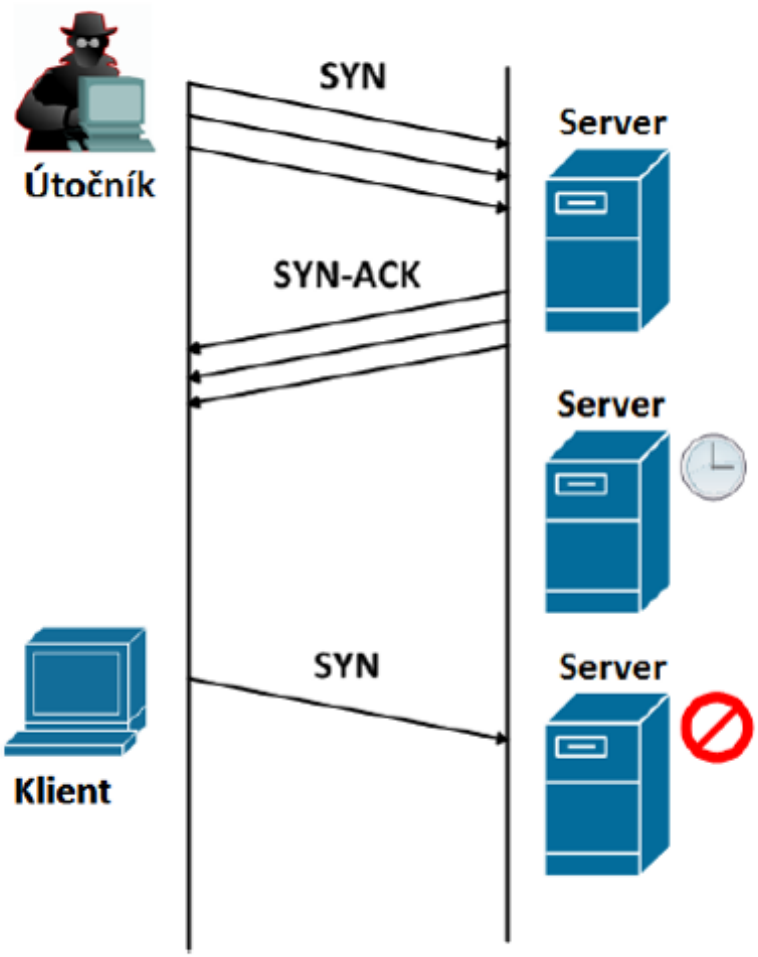
DDoS příklady amplifikovaných útoků

- **DNS Amplification** – spoofing zdrojové IP adresy + velké odpovědi posílané na server oběti
- **NTP Amplification** – spoofing + velké odpovědi
- **Memcached Amplification** – spoofing + záplavová odpověď na server oběti (cache pro zrychlení načítání stránek).
- **Carpet Bombing** – útočník zaměřuje reflekci na více obětí (CIDR /22). Např. útočník pošle spoofovaný TCP SYN několika reflektorům, kteří 1:1 odesílají TCP SYN + ACK na celý subnet.

DDoS příklady protokolových útoků

- Útok **Reset Flood** - Záplava paketů mající falešné zdrojové IP adresy, porty a aktivní příznak RST, který **resetuje spojení**. Skutečná komunikace je neoprávněně ukončena.
- Útok **Syn Flood** - Cíl útoku otvírá několik **polootevřených spojení** a čeká na potvrzovací zprávu, která však od podvržených adres nepřichází a tím dochází postupem času ke snížení dostupnosti až po úplné zahlcení služby u cílové oběti.
-

DDoS - TCP SYN Flood útok



DDoS příklady aplikačních útoků

- **Buffer overflow** – přetečení příchozích/odchozích bufferů (na zařízení oběti x uvnitř sítě).
- **0-Day** – zneužití nových (neobjevených) zranitelností.
- **Slow DoS** – zneužívají nedokonalou nebo chybnou implementaci aplikačního protokolu.

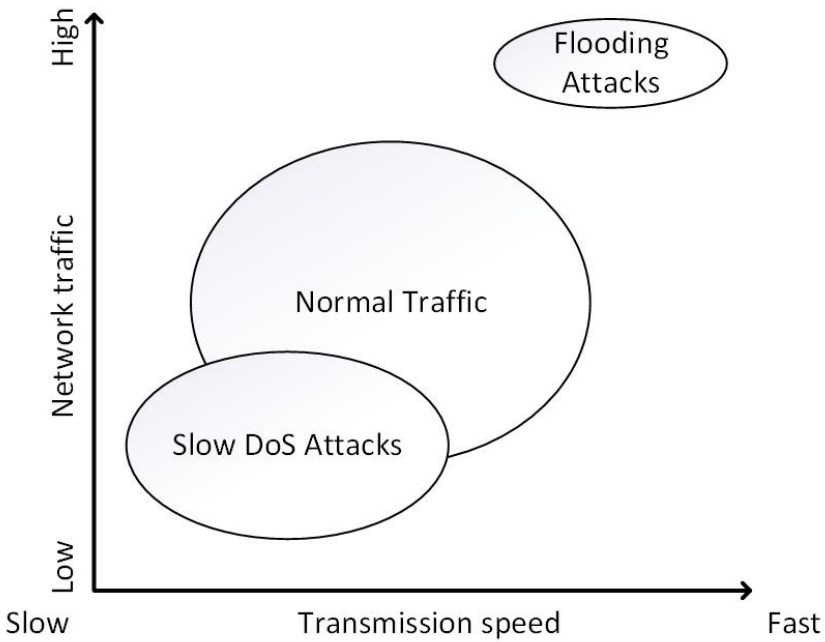
(D)DoS příklady logických útoků

- Útok **Teardrop** - Rozdělené části (**fragmenty**) paketů přesahující **falešně nastavený offset** jsou zaslány k cíli. Cíl není schopen znovu správně sestavit celý paket z informací daného offsetu a celkové velikosti paketu. OS u cílového uzlu na základě chyby při sestavování fragmentů poté spadne.
- Útok **Land** - Pakety TCP-SYN jsou podvrženy tak, že mají cílovou IP adresu a port identickou jako zdrojovou. **Nekonečná smyčka** při jejich zasílání zpět.
- Útok **Ping Of Death** - Škodlivý ping dotaz. Např. ping o velikosti **vyšší než 65 535 bajtů** (maximální přípustná velikost) může způsobit pád cílového systému.
- Útok **Regular expression DoS** - **ReDoS** - nestandardní a extrémní výrazy zatíží procesy zpracování regulárních výrazů. Např. username: $\hat{}(([a-z])+.)+[A-Z]([a-z])+\$$ a heslo: aaaaaaaaaaaaaaaaaaaaaaaaaaaaa!.

DDoS další příklady

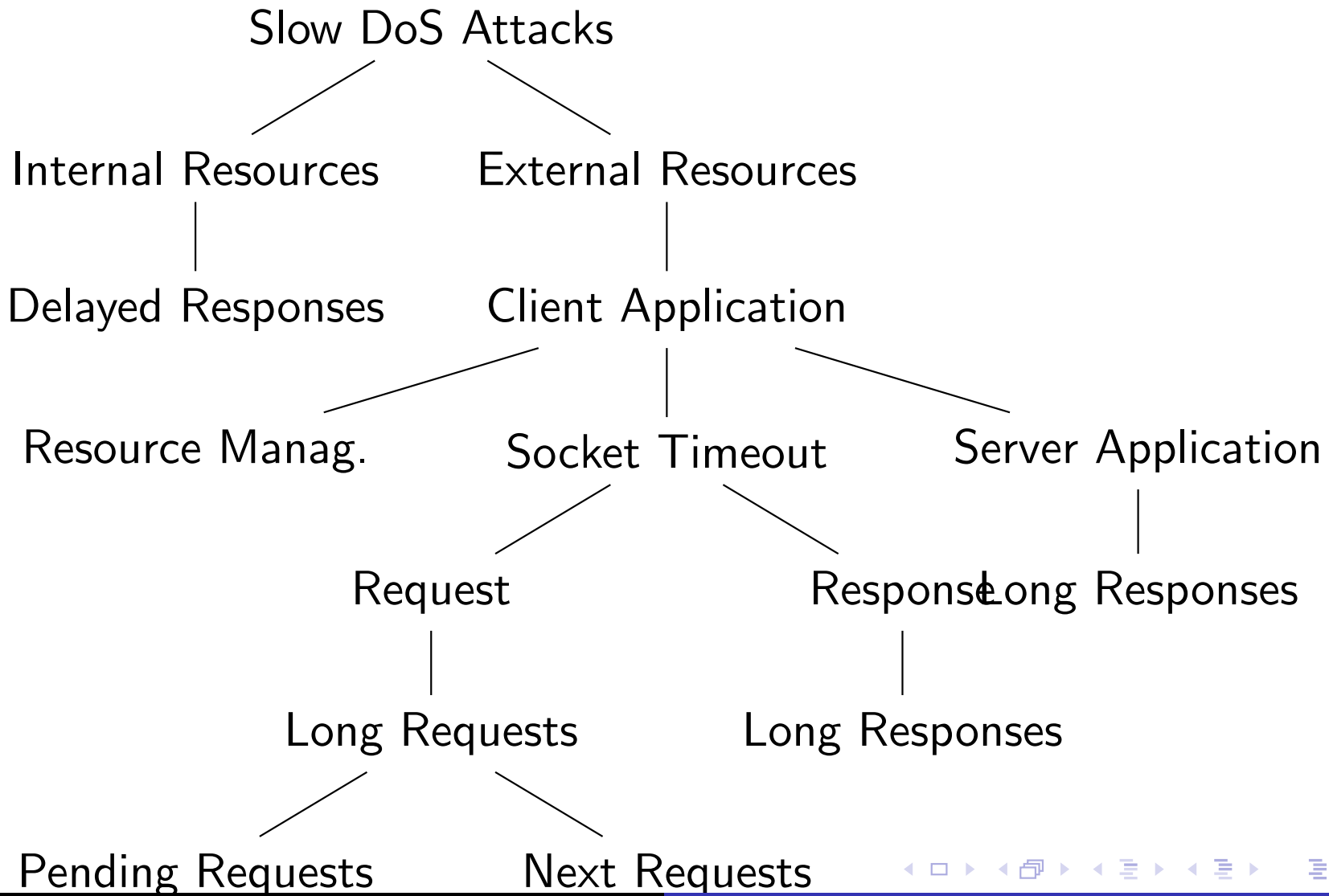
- Útok **RandomUnreachableHost** - Zprávy o nedostupnosti uzlu tj. ICMP host unreachable. Náhodné podvržené (spoof) IP adresy mající být nedostupné, jsou poslány z náhodných IP adres k uživatelům. **Některá spojení** budou v dané síti skutečně **přerušena**.
- Útok **UnreachableHost** - Zprávy jsou poslány útočníkem k danému cíli či k uživatelům, kde mezi nimi již existuje **vzájemné spojení** a spojení bude **přerušeno**.
- Útok **XMasTree** - Generování tzv. paketů Christmas tree, kde jsou **nastaveny příznaky** FIN, URG, PSH v hlavičce TCP, a jsou náročnější na zpracování. Množství těchto paketů zahltí cílový uzel.

Slow DoS útoky



- Využívají zranitelnosti aplikační vrstvy (FTP, HTTP, SMTP, NTP . . .).
- Z 1 zařízení útočníka + využití max. počtu spojení (Apache 150 spojení).
- Často opakující se zprávy v kombinaci s použitím časovače.

Slow DoS útoky - kategorie

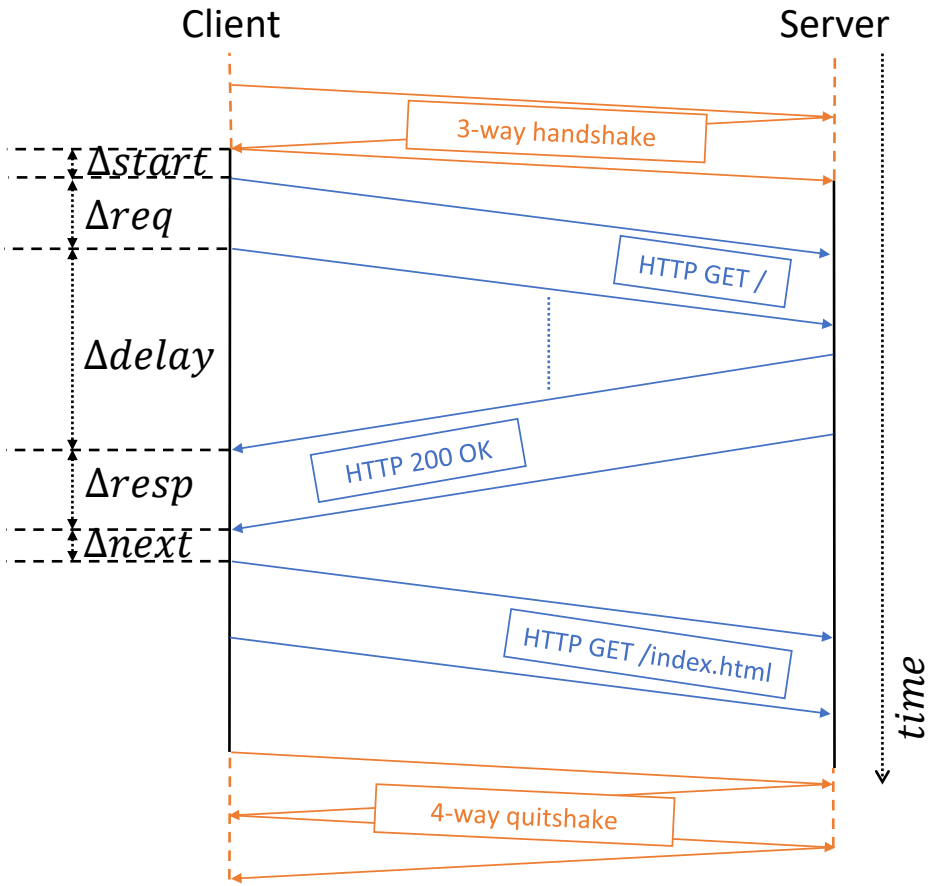


Slow DoS útoky - kategorie

Attack category	Attack Examples	HTTP
Delayed Responses	*Apache Range Headers*	`HEAD`
	#DoS	`POST`
	ReDoS	`POST`
Resource Management	*LoRDAS*	-
	Slow Drop	`GET`
Next Requests	*Slow Next*	`HEAD`
Pending Requests	*Slowloris*	`GET`
	Slow HTTP Post	`POST`
	Slowcomm	`HEAD`
Long Responses	*Slow Read*	-

Slow DoS útoky

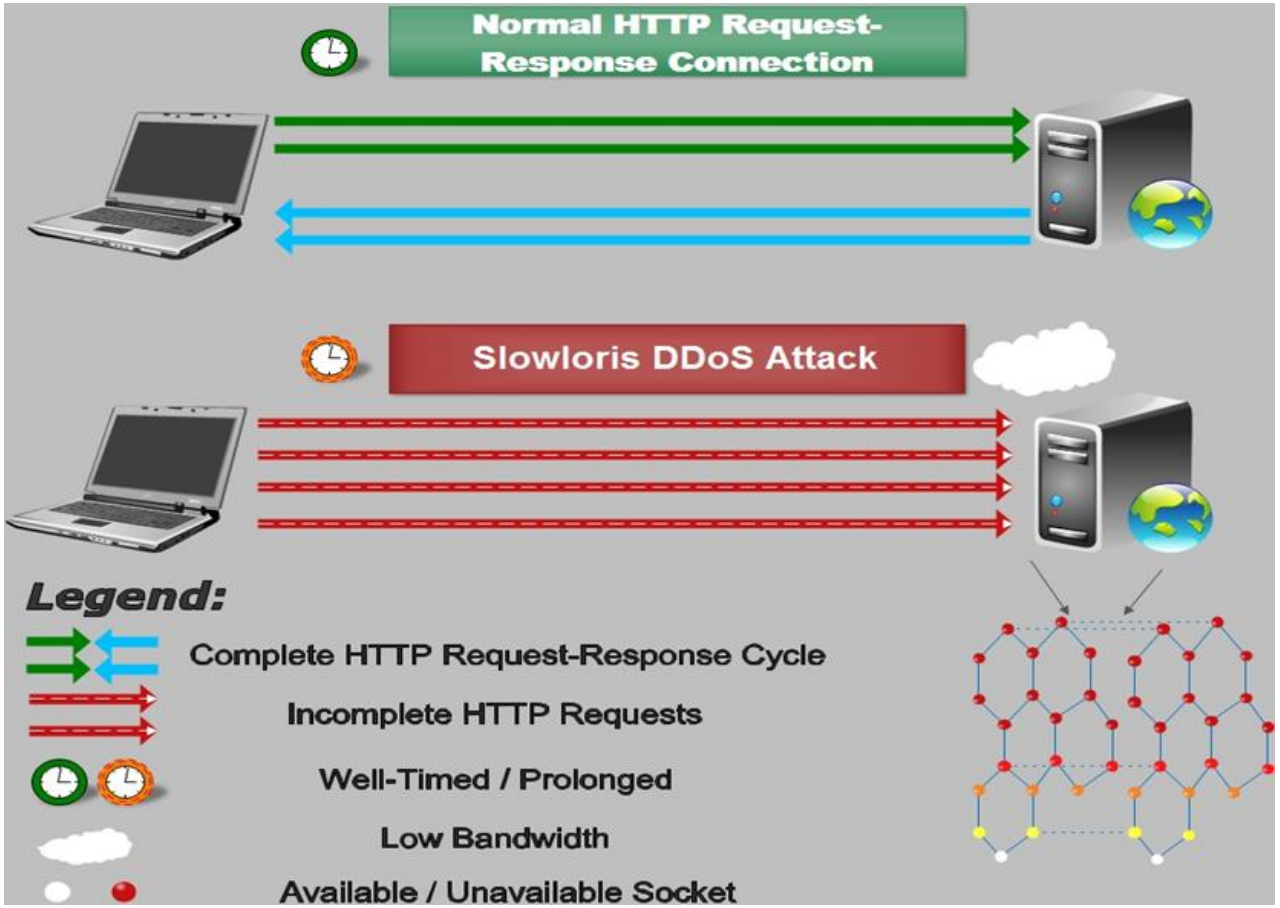
Timeout	Attack types
Δ_{start}	**Lazy Requests**
Δ_{req}	Pending Requests
Δ_{delay}	Delayed Responses
Δ_{resp}	Long requests
Δ_{next}	**Next Requests**



Slow DoS útoky – HTTP/1.1

- **Slowloris (Slow HTTP Headers)** – nástroj generuje a opakovaně posílá **částečné HTTP požadavky**, ale nikdy nedokončí celý požadavek.
- **Slow Read** – útočník požaduje ze serveru velká data, ale velikost příchozícho bufferu nastavi na co nejmenší hodnotu (*window_size=0*).
- **Slow Drop** – utočník náhodně zahazuje příchozí pakety. Server takto zahozené pakety znovu odesílá útočíkovi.
- **Slow Next** – útočník využívá časovač, kdy před jeho vypršením žádá server o další data.
- **Slow Post (R.U.D.Y)** – útočník chce odeslat velké množství dat (*Content-Length*). Reálně posílá pouze malé chunky a ve velkém časovém odstupu.
- **Slowcomm** – útočník odešle neukončený požadavek a s využitím časovače odesílá nesmyslná data.

DDoS - Slowloris



Zdroj: Infosecinstitute.com

DDoS - HTTP Request Slow Header/Slow Content (pomalý útok)

Slow Header:
POST /index.html HTTP/1.0
Content-Length: 5
Header1: Value1
[sleep for few seconds]
Header1: Value1
...
Slow Content:
POST /index.html HTTP/1.0
Content-Length: 5000
B **[sleep for few seconds]** a **[sleep for few seconds]** r [sleep for few seconds] r **[sleep for few seconds]** a **[sleep for few seconds]** c **[sleep for few seconds]** u **[sleep for few seconds]** d **[sleep for few seconds]** a **[sleep for few seconds]**
.....

Slow DoS útoky – HTTP/2

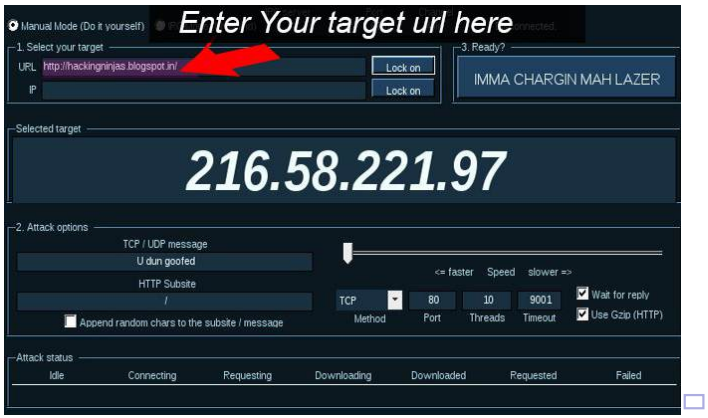
- **Slow Read** – útočník oznamuje serveru, že je zaneprázdněn (*SETTING_INITIAL_WINDOW_SIZE:0*). Server očekává rámec *WINDOW_UPDATE* pro obnovení odesílání dat.
- **Slow Post** – útočník nastaví příznaky tak, že serveru říká, že ukončil stream, ale neukončil odesílání hlaviček. Server čeká na další rámec *DATA*, jehož odesílání útočník pozdrží.
- **Slow Preface** – útočník pošle pouze úvodní rámec pro HTTP/2 spojení. Server čeká na další komunikaci.
- **Slow Headers** – obdoba Slow Post, ale jiná kombinace hlaviček (ukončení hlaviček, ale neukončení streamu).
- **Slow Settings** – útočník nepotvrdí rámec *SETTINGS*, na který server čeká.
- prostor pro další útoky . . .

DDoS botnet - nástroje

- **BYOB** – C&C, generátor útoků a tvorba botů, 12 modulů pro post-exploitaci. (https://github.com/malwaredllc/byob).
- **HULK** – generování unikátního HTTP provozu, vícevláknové (https://github.com/grafov/hulk).
- **hPing3** – ICMP, UDP, TCP floods, protokolové DDoSy, fragmenotvané útoky (https://www.kali.org/tools/hping3/).
- **Torshammer** – Slow HTTP Post, (https://github.com/Karlheinzniebuhr/torshammer).
- **LOIC** – UDP, TCP, HTTP floods, (https://github.com/NewEraCracker/LOIC).
- **DDOSIM** – simulátor botů, DoS na aplikační vrstvě (validní HTTP, nevalidní HTTP, SMTP) (https://github.com/alanackart/DDOSIM).

DDoS botnet - nástroje

- **SlowHTTPTest** – Slow DoS útoky (Slowloris, Slow Read, Apache Range Headers, Slow Post) (https://github.com/shekyan/slowhttptest).
- **PySlowDoS** – Slow Drop, Slow Next, Slow Read + vlastní definice Slow DoS útoků (Detekce moderních Slow DoS útoků).
- **SlowHTTP2Test** – HTTP/2 Slow Read, Slow Post, Slow Preface, Slow Headers, Slow Settings (https://github.com/Michael-Jurek/slowhttp2test).



Historie DDoS útoků

- 1996 `Panix` – provider nedostupný několik dnů (**SYN Flood**).
- 2012 `6 US bank` – několik vektorů, 60 `Gbps` (botnet **Brobot**).
- 2014 `CloudFlare` – 1 zákazník, 400 `Gbps` (**NTP Amplification** 206x).
- 2014 `Occupy Central` – platforma pro demokratické volby, 500 `Gbps`, 5 botnetů.
- 2016 `Mirai Dyn` – DNS provider, 1.5 `Tbps` (více vektorů).
- 2018 `Github` – 20 minut, 1.35 `Tbps`, využití Memcached (**UDP Flood**, port 11211, amplifikace 51000x).
- 2020 `AWS` – 1 zákazník, 2.3 `Tbps` (**CLDAP**, 56-70x).
- 2020 `Google` – 3 čínští ISP, 2.5 `Tbps` (**CLDAP, DNS, SMTP**).
- 2021 `Akamai` – vydírání klienta, 800 `Gbps` (**DCCP protocol**).
- 2021 `Microsoft` – útok na herní platformy na Azure, peak 15 minut, 3.47 `Tbps` (**CLDAP, DNS, NTP**).

Historie DDoS útoků v ČR

- únor 2013: útok na viry.cz (TCP SYN Flood Attack z cca 500 IP adres na Apache Server),
- březen 2013: sada útoků na české servery (portály, banky a mobilní operátoři), TCP SYN Flood, tis. – mil. paketů/s),
- květen 2016: útok DDoS na streamovací servery O2 při hokejovém MS,
- říjen 2017: cílený DDoS útok na O2 infrastrukturu během parlamentních voleb a nedostupnost prezentačních serverů volby.cz a volbyhned.cz.
- duben 2021: *WEDOS*, útok na infrastrukturu a klientskou administraci, špička 300 Gbps.
- říjen 2022: zákazníci v sítí O2, špička 200 Gbps.

Motivace útočníků

- Ideologie – *hacktivists* - rozdílné politické názory.
- Vydírání – *ransom* - získání finančních prostředků pomocí kryptoměn, např. XMR.
- Script-kiddies – adreanlin, pro zábavu.
- Konkurence – získání konkurenční výhody.
- Válka (5. doména) – státem sponzorované útoky (opozice, znepřátelené země).
- Zakrytí hlavního útoku (krádež dat . . .).

Detekce útoků DDoS

Detekce **signatur** (vzorů):

- Dobrá **znalost** samotného **útoku** DDoS - sestavení příznaku/signatury.
- Signatury bývají manuálně sestavovány skupinami expertů.
- Signatury implementovány do bezpečnostních a dohledových síťových prvků.

Detekce **anomálií:**

- Anomálie v síťovém provozu.
- Záplavové útoky zvyšují hustotu síťového provozu / **překročení prahu**.
- Více falešných poplachů.
- Lze zachytit i nové útoky.
- Používají mnohé filtry DDoS.

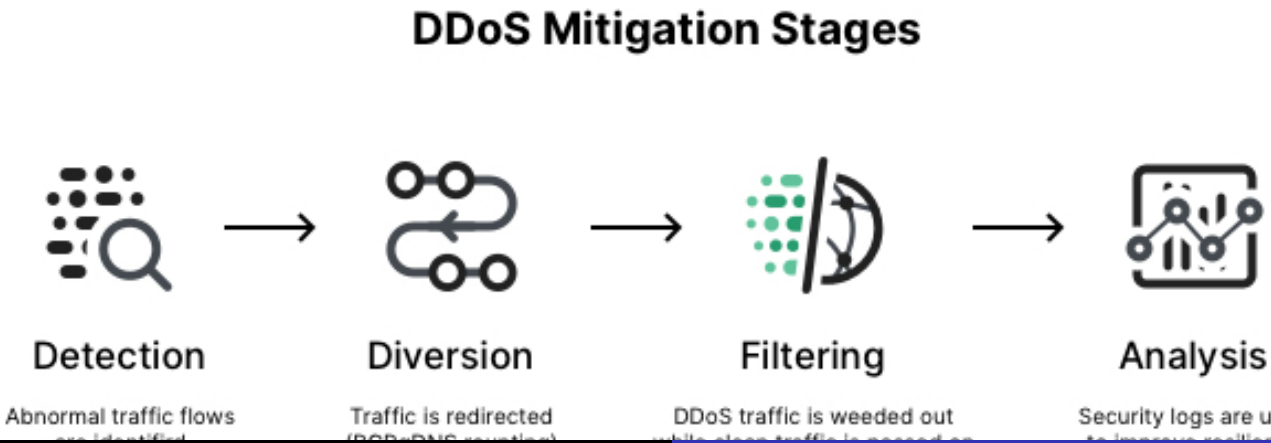
Další rozdělení: heuristická / prahová detekce.

Mitigace DDoS - strategie

- Robustní a bezpečná síťová infrastruktura. Použití **firewallů**, IDS systemů, honeypotů, **redundantních linek** a serverů.
- Použití vysokorychlostních **DDoS filtrů**.
  - Monitoring spojení, rate-limiting (riziko blokování legitimního provozu).
- Ochrana Black and white list. Přesun legitimních uživatelů na záložní linku a na white list. Podezřelé a nevěrohodné IP adresy vložit na black list a jednoduše zahazovat. (Kombinace s reputačními databazemi.)
- Metoda obrany útokem. Zvýšit počet žádostí a paketů od legitimních uživatelů.
- **Tarpit** akce (netfilter, mikrotik) - udržet příchozí podezřelé spojení v open-state, ale snížit TCP window size na 0 a tím neumožnit přenos dat až po eventuální time out.

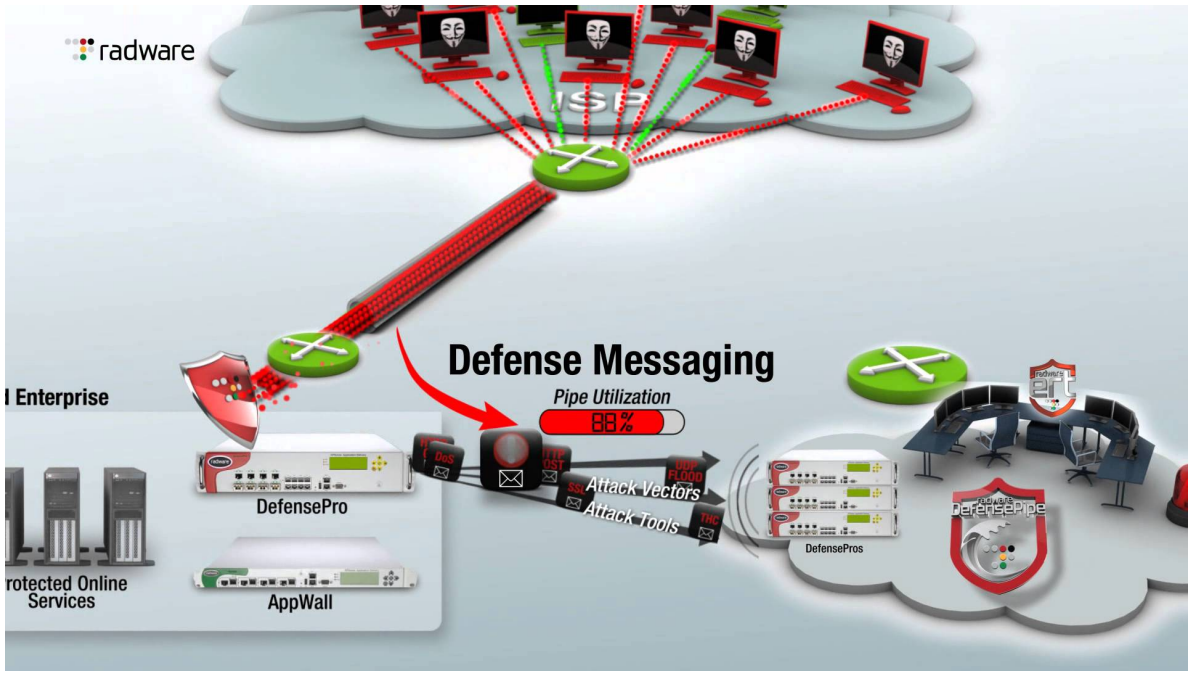
Mitigace DDoS - kroky

- Detekce – označení DDoS útoku (reputace IP adres (geolokace), známé signatury útoků, natrénované ML modely).
- Přesměrování – rozdělení útoků do menších datových toků.
- Filtrace – zahazování označených toků (L7 - WAF, L3, L4 - firewall, IPS).
- Adaptace – trénování a vylepšování současných modelů, signatur.



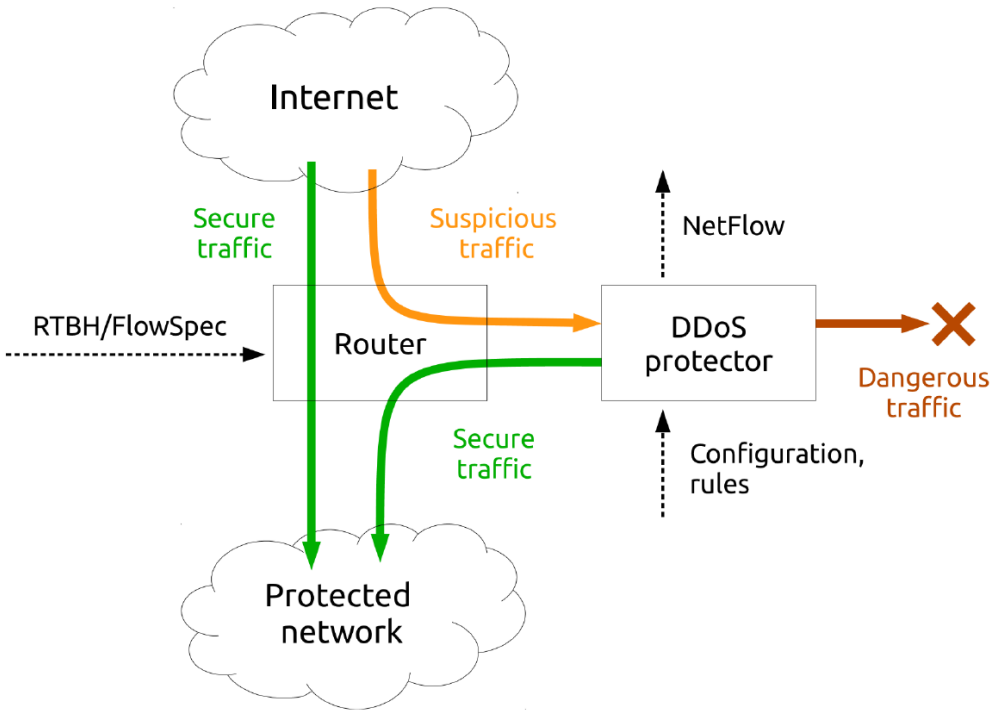
Mitigace DDoS - DDoS pračky

- **DDoS pračky** - čištění provozu, jednoduchá pravidla, hlídají se prahy pro IP adresy/sítě, např. Radware, Cesnet DDoS protector, VUT DDoS protector a některé NGFW firewally. FPGA akcelerace, DDoS mitigace pomocí cloudu atd.



Mitigace DDoS - DDoS Protector

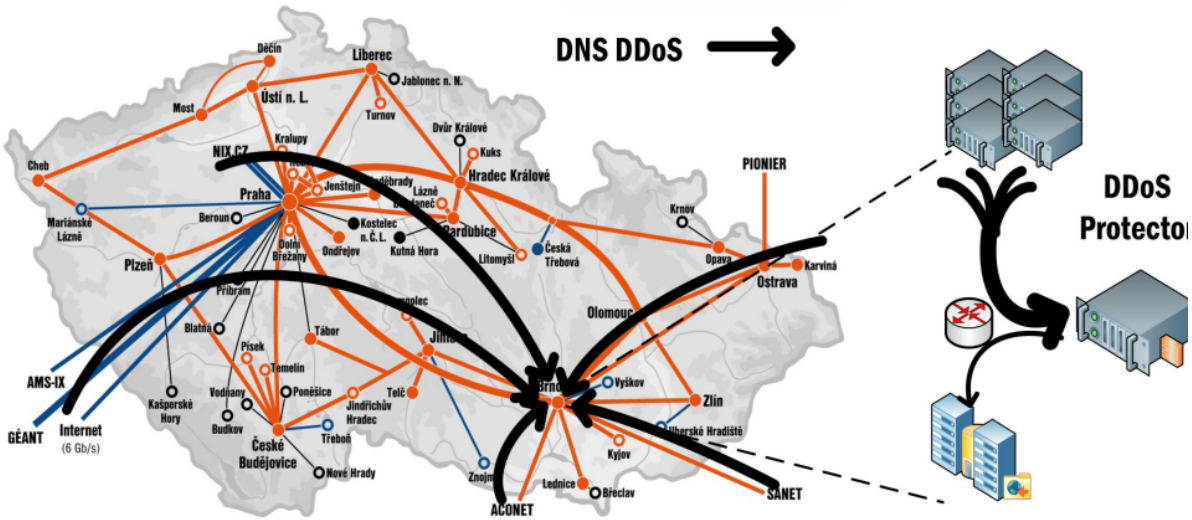
- **Cesnet DDoS Protector** - čištění provozu na bázi pravidel, FPGA akcelerace, 100Gbps full duplex, nízká latence (mikrosekund)/FPGA, IPv4 a IPv6, až 3 tis. pravidel, blokování až 16 tis. zdrojových IP adres.



Mitigace DDoS - DDoS Protector

- Hlídá překročení prahů pro IP/podsítě.
- Volitelné časové rozlišení.
- Jednoduchá pravidla.

```
"VUT UDP" dst net 147.229.0.0/16 protocol 17 src port
53 threshold 1 Gbps limit 100 Mbps
```



Mitigace DDoS - DDoS Protector algoritmus

Příchozí paket:

1. Najdi všechna odpovídající pravidla.
2. U každého pravidla aktualizuj zdrojové IP adresy a statistiky.
3. Je zdrojová IP adresa blokována?
   - Ano – zahoď paket, aktualizuj statistiky.
   - Ne – edituj paket a přepošli.
4. Na konci časového intervalu zkontroluj překročení pravidel.
5. Vytvoř seznam IP adres k blokování.

Testování bezpečnosti sítí

Proč testovat sítě?

- Počítačové sítě a síťové zařízení jsou důležitou součástí firem, institucí a organizací.
- V případě zneužití (exploitací) zranitelností lze napadnou síť, službu či zařízení (poškození či odcizení cenných dat, odepření služeb - DoS,...).
- Preventivní testování odhalí zranitelnosti a umožní jejich odstranění dříve než je zneužije útočník.
- Odstranění zranitelností a ochrana uzlů dále pomáhá proti útokům z naší sítě směrem ven (síť jako součást botnet).
- **Testování výkonnosti sítě** a síťových zařízení **odhalí** také **úzká hrdla sítě, špatnou konfiguraci a limity** sítě.

Co lze testovat?

- Počítačové sítě jako celek.
- Jednotlivé síťové zařízení (servery, routery, firewally).
- Jednotlivé koncové stanice (PC, notebooky, smartphony, tablety, atd.).
- Jednotlivé aplikace, webové služby a OS.
- Další aspekty (nastavení firemní ICT politiky, uživatelský přístup, sociální inženýrství,...).

Kdy testovat?

- Testování zranitelností během provozu (reálnější, ale více nebezpečné).
- Testování zranitelností mimo hlavní provoz.
- **Zátěžové testování** je vhodné realizovat **mimo provoz díky saturování sítě**.
- **Testování emulované sítě** (přenesení konfigurace, virtualizace, emulované prostředí).

Typy a metody testů

- **Zátěžový test (stress test).**
- Test zranitelností (vulnerability test).
- White box test - je známá struktura a parametry sítě.
- Black box test - nemusí být známá struktura sítě. Testování cíle a sledování jeho odezvy bez sledování vnitřních procesů.
- Penetrační testy (podrobné testování odolnosti sítě vůči průnikům).

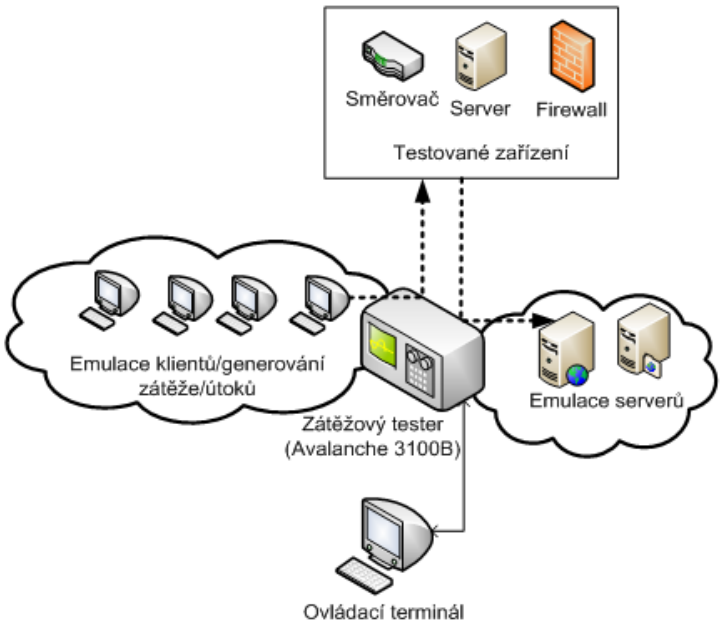
Testování výkonnosti a odolnosti proti DDoS

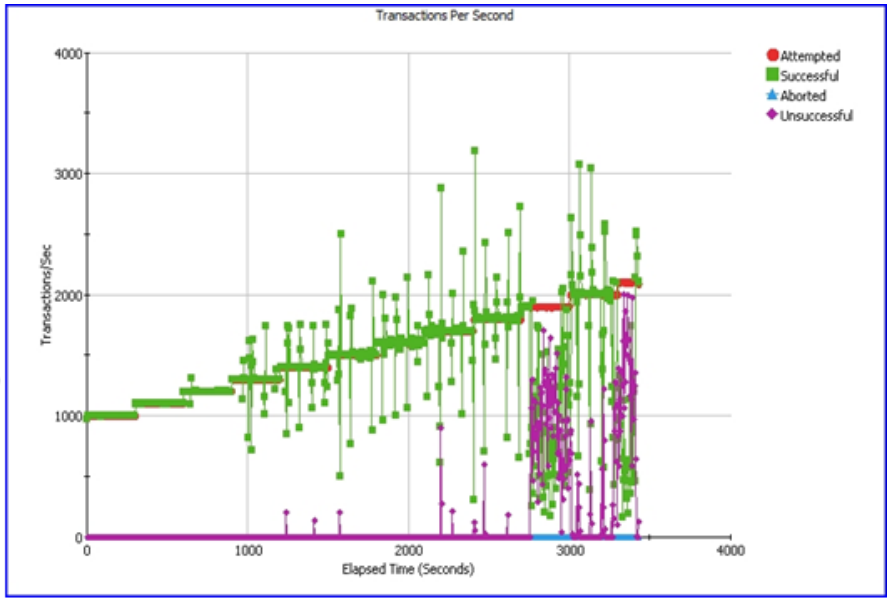
Testování výkonnosti

- Testují se **sítě a síťové prvky**.
- Zjištění **limitů** prvků a úzkých hrdel sítí.
- Testovaní pomocí zátěžových testerů (HW a SW testery), **generování zátěže**.
- Monitoring chování testovaných segmentů (sondy provozu), **analýza provozu**.

Obecné schéma zapojení zátěžového testeru

Testovací scénář se zátěžovým testerem (vlevo), příklad zobrazení výsledků testování při zvyšující zátěži (vpravo).





Zátěžové testování - metodologie

- **Definice testování**, specifikace sítě a požadavků, specifikace běžného provozu.
- **Příprava testování** (zvolení vhodné doby), nastavení sítě na testování (zálohovaní důležitých služeb a aplikací) a nastavení zátěžového testeru. Zajištění monitorovacího SW a HW pro zisk odezvy a pozorování chování sítě/prvků.
- **Realizace testování**, monitoring testování, opakování testování.
- **Vyhodnocení testování**, tvorba dokumentace, vyhodnocení výsledků.

Zátěžové testování - typy testů

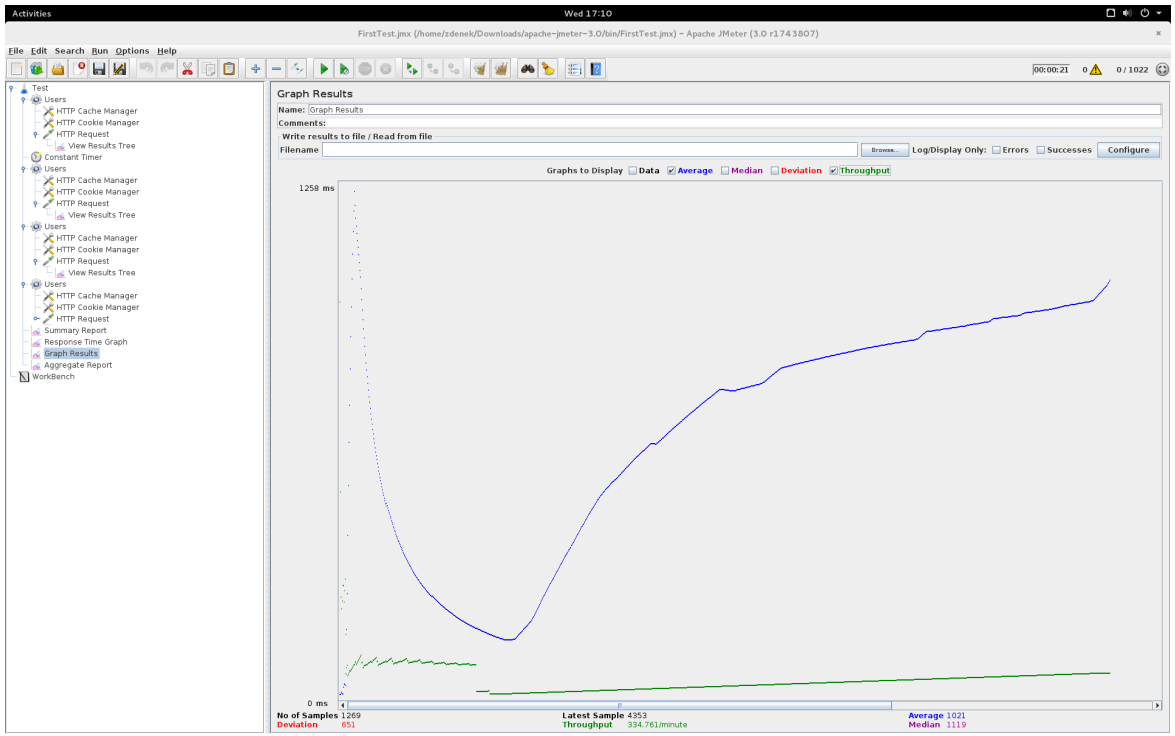
- **Výkonnostní test** (Performance Test): zatížení systému definovanou zátěží pro změření jeho chování. Používá se pro změření reakcí očekávané zátěže, nebo porovnání vlastností systému po provedené změně. Např. testování před a po update.
- **Test hraniční zátěže** (Load/Stress Test): zatěžování systému narůstajícím počtem paralelních procesů. Účelem je najít limit, při kterém aplikace překročí akceptovatelné požadavky (například vzroste doba odezvy serveru nad stanovenou únosnou mez).
- **Test odolnosti** (Soak Test): jedná se o dlouhodobé testy, které odhalují nedostatky v aplikaci při jejím nepřetržitém provozu.
- **Test selhání** (Failover Test): tímto typem testů je možné ověřit chování systému v případě jeho selhání a nahrazení záložním systémem. Také je možné ověřit rychlost jeho zotavení, pokud je pod zátěží proveden restart, nebo přepojen některý ze systémů, se kterým hlavní aplikace komunikuje.
- **Test části infrastruktury** (Targeted Infrastructure Test): test zaměřený na konkrétní úroveň infrastruktury/architektury řešení. Pomocí testu je možné zjistit, ve které části řešení je nejslabší místo. Používá se velice často u složitých systémů.
- **Test objemu dat** (Volume Test): tímto typem testů dochází k ověřování chování aplikace při zvyšujícím se objemu dat (např. dopad rychlosti volání při narůstajícím objemu dat v databázi).

Zátěžové testování - realizace a průběh testů

- Volba a nastavení parametrů testování.
  - Základní parametry jsou: doba testu, počet dotazů, počet úspěšných/neúspěšných dotazů, čas potřebný na jeden dotaz (maximální, minimální, průměrný).
  - Dalšími parametry jsou: počet dotazů za jednotku času (lze vypočítat ze základních parametrů), velikost přenesených dat/přenosová rychlost, distribuční rozdělení časů odpovědí.
- Sledování průběhu testu (např. pomocí IDS sond, netflow,..).
- Sběr a zpracování statistických informací o probíhajícím testu.
- Systematické uložení výsledků.
- Případné opakování testu.

Zátěžové testování - výsledky testů

Výsledky testu - graficky vhodně znázorněny: dosažené limity (úspěšné/neúspěšné transakce, čas odezvy, atp.).
Např. vizualizace testování serveru HTTP dotazy na Apache jmeter-3.0.



Hardwarové zátěžové testery

- **Zařízení s více síťových rozhraní**.
- Generování provozu až do 100 Gb/s.
- **Emulace síťových klientů a serverů**.
- Vrstvy L2 - L7.
- Lze testovat i velké sítě.
- Drahé zařízení (miliony korun).

Hardwarové zátěžové testery - příklad Avalanche

Zátežový tester: Spirent Avalanche 3100B.

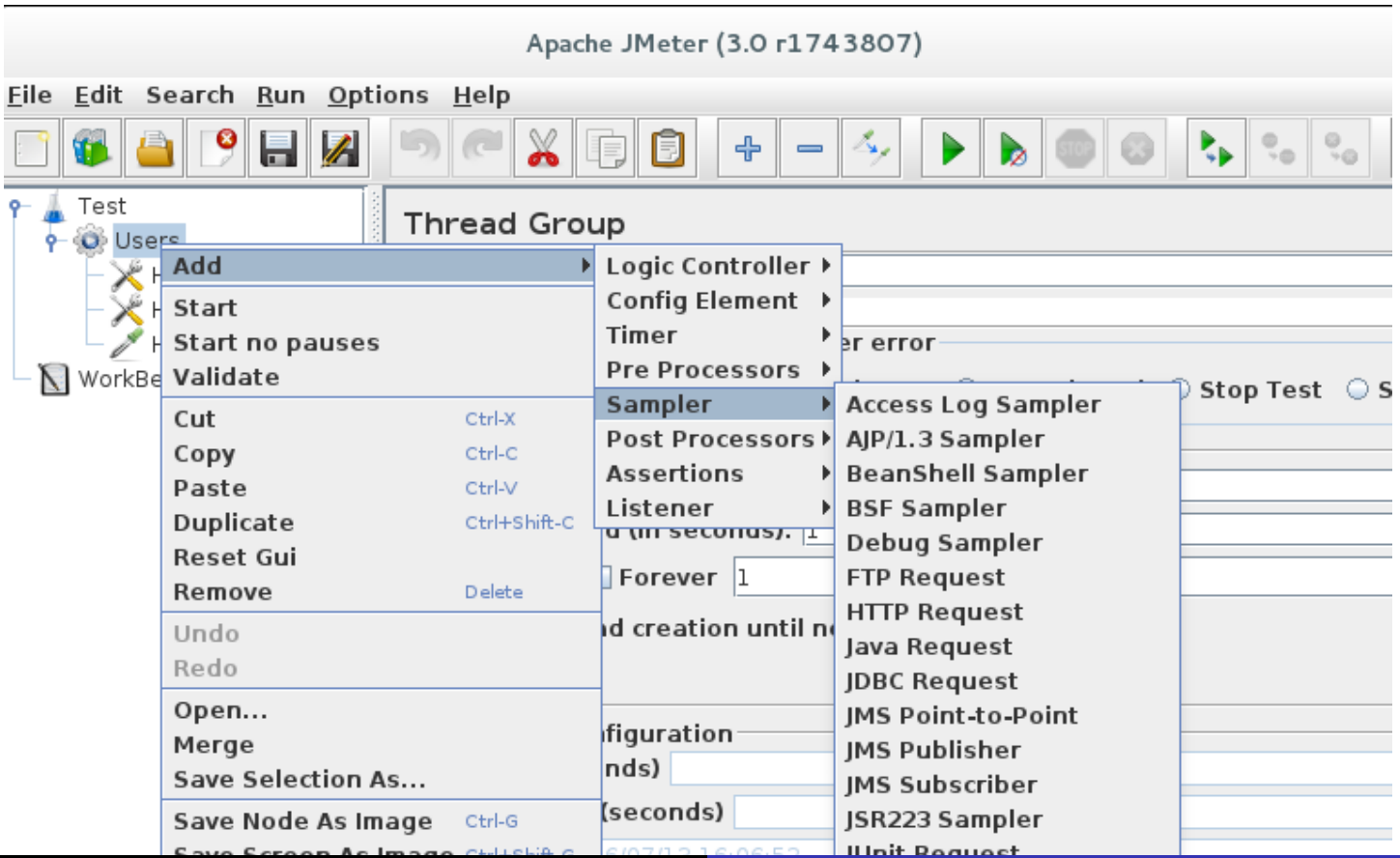
- Generování provozu do 40 Gb/s.
- **Emulace síťových klientů a serverů**.
- Vrstvy L3 - L7.
- 15 útoků DDoS.
- Attack designer – možnost definice vlastního útoku.

Softwarové zátěžové testery

- **SW aplikace** umožňující nastavovat a generovat data (IP pakety, datagramy TCP/UDP, HTTP dotazy atd.).
- Výkon závisí pak na hostujícím HW včetně síťové karty a kabeláže.
- **Levné** a snadné na konfiguraci, vhodné na testování prvků a menších sítí.
- Příklady SW testerů: ApacheBench, Httperf, Weighttp, Httpress, Siege, **JMeter, trafgen**, Tourbus.

Softwarový zátěžový tester - Apache jMeter

Apache JMeter - open source software postavený na Javě k zátěžovému testování serverů (původně jen web. aplikace). GUI (viz dole) i příkazy v shell.



Softwarový zátěžový tester - Apache jMeter

Protokoly a služby pro zátěžové a vykonostní testy:

- Web - HTTP, HTTPS (Java, NodeJS, PHP, ASP.NET, . . .)
- SOAP / REST Webslužby
- FTP
- Databáze JDBC
- LDAP
- Message-oriented middleware (MOM) přes JMS
- Mail - SMTP(S), POP3(S) a IMAP(S)
- Nativní příkazy a shell scripts
- TCP
- Java Objekty

Testování sítí a prvků vůči DDoS

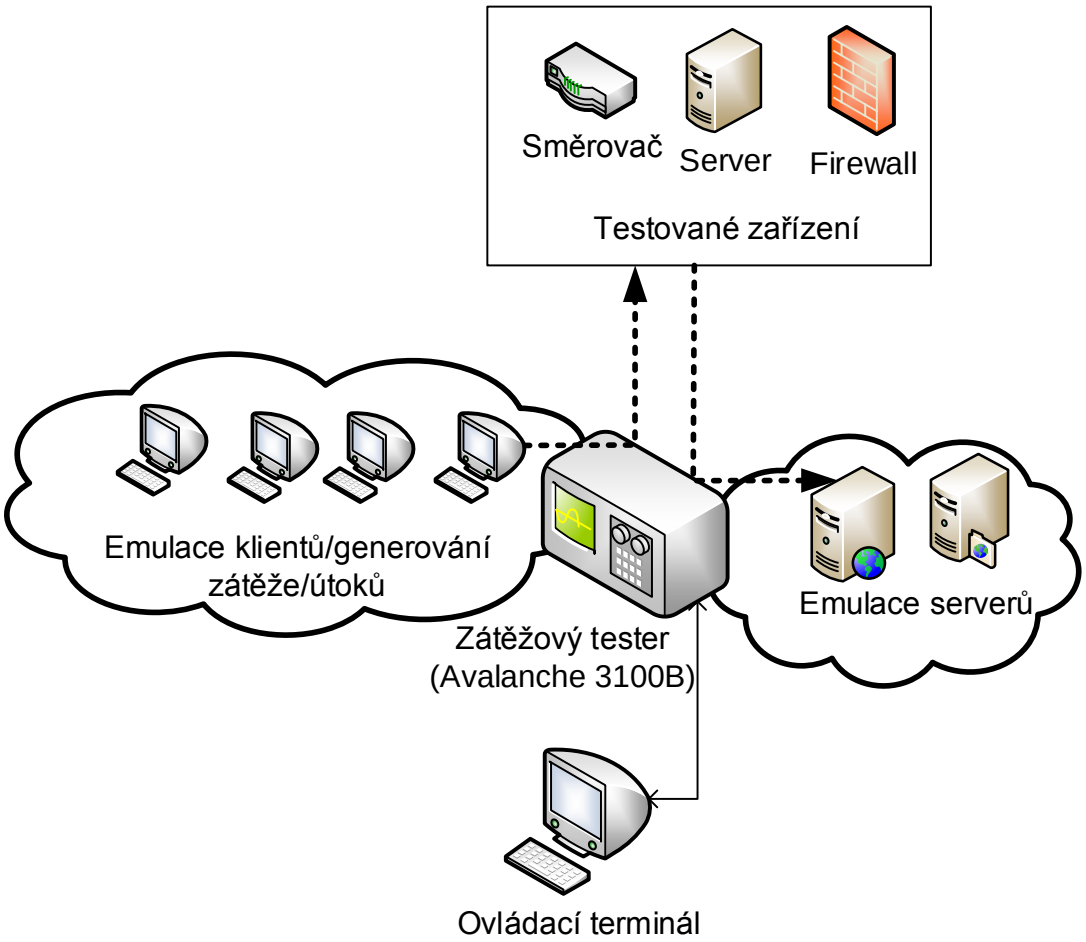
Potřebná výbava:

- Zátěžový tester (HW nebo SW, který umí generovat DDoS).
- Emulátor provozu a **DDoS útoků**.

Benefity:

- Rozpoznání limitů a slabin, detekce úzkých hrdel sítě.
- Zpětná vazba a možnost optimální konfigurace.
- Příprava krizových a záložních scénářů v případě reálného útoku DDoS.

Obecný testovací scénář



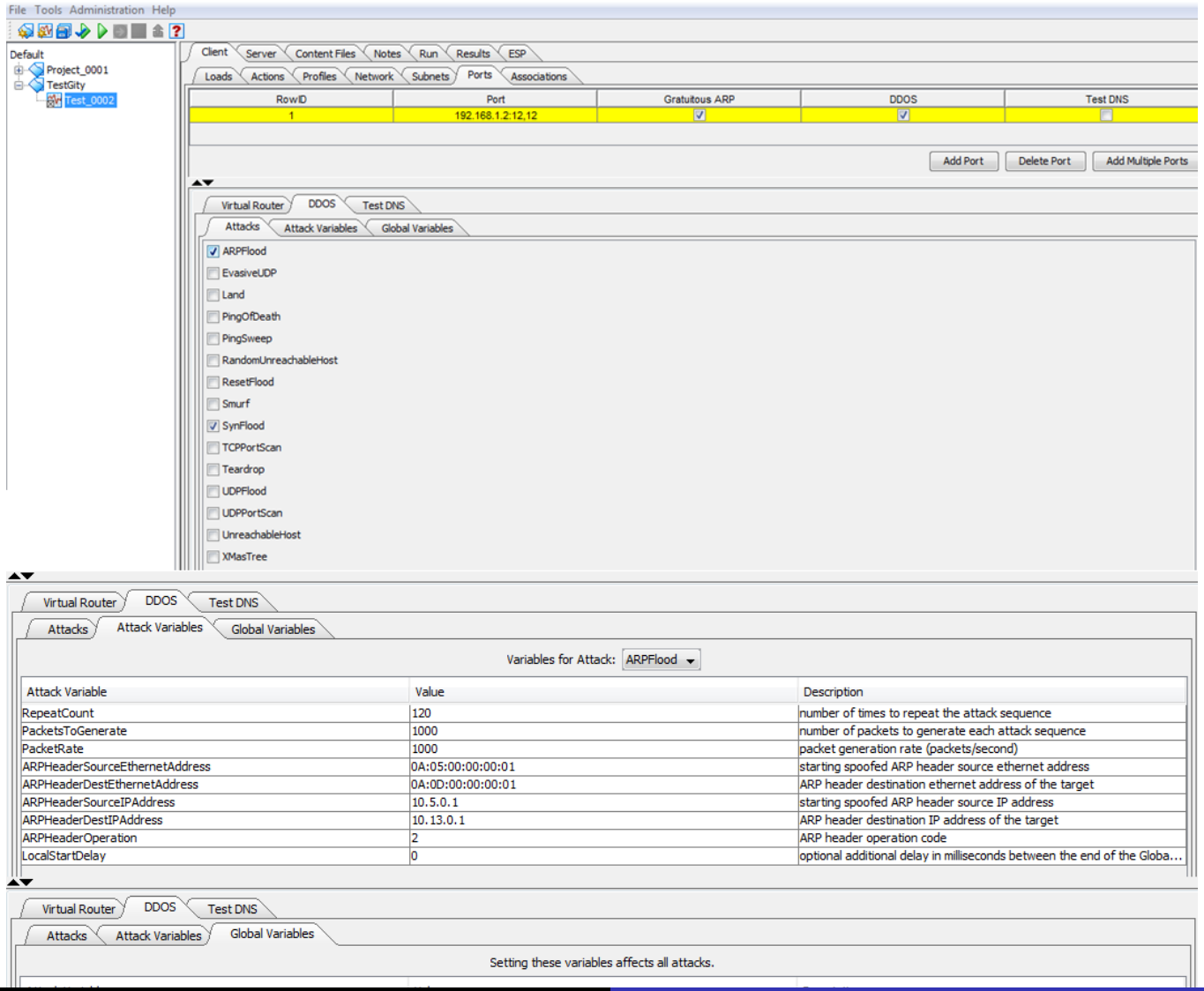
HW testery DDoS

Testery Spirent, Ixia (velké náklady, velká výkonost).
Spirent Avalanche 3100B typy DDoS:

- TCP: SynFlood Attack, TCPPortScan Attack, ResetFlood Attack, Teardrop Attack, XmasTree Attack
- UDP:EvasiveUDP Attack, UDPFlood Attack, UDPPortScan Attack
- ICMP: PingOfDeath Attack, PingSweep Attack, RandomUnreachableHost Attack, Smurf Attack, UnreachableHost Attack
- Další: ARPFlood Attack, HTTPLand Attack, ...

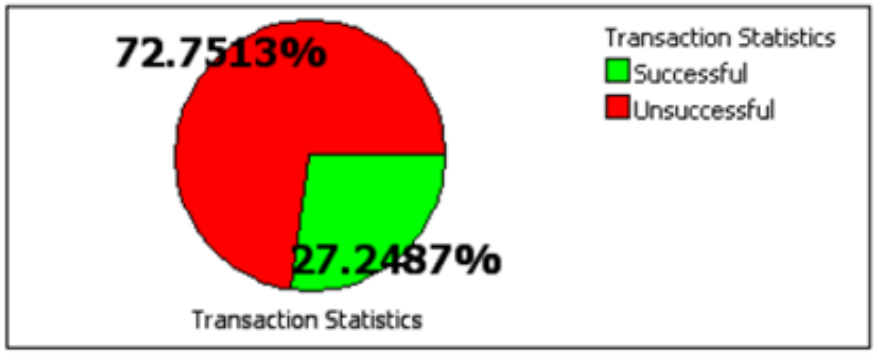
Jednotlivé útoky lze spojovat.
Detailní možnosti nastavení.

Ukázka konfigurace testeru Avalanche

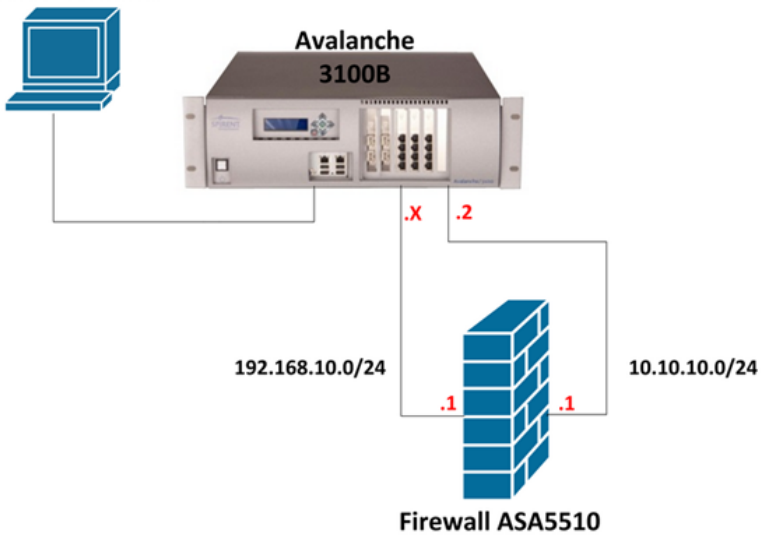


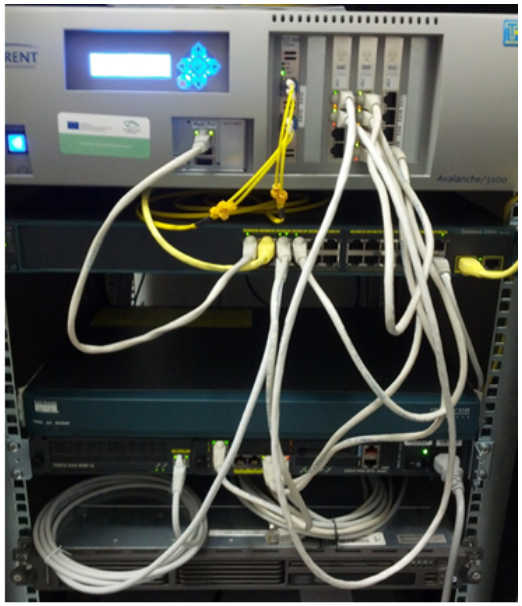
Ukázka výsledků testu na testeru Avalanche

Test Results Summary	Transactions			Time (ms)						TCP Connections	
		Total	Rate Per Second		Page Response	URL Response	To TCP SYN/ACK	To First Data Byte	Est. Server Response		Total
	Attempted	87252	3635	Minimum	1.0	1.0	0.089	0.479	0.0	Attempted	87252
	Successful	23775	990	Maximum	9104.0	9104.0	6004.092	3288.192	3287.359	Established	86528
	Unsuccessful	63477	2644	Average							
	Aborted	0	0								



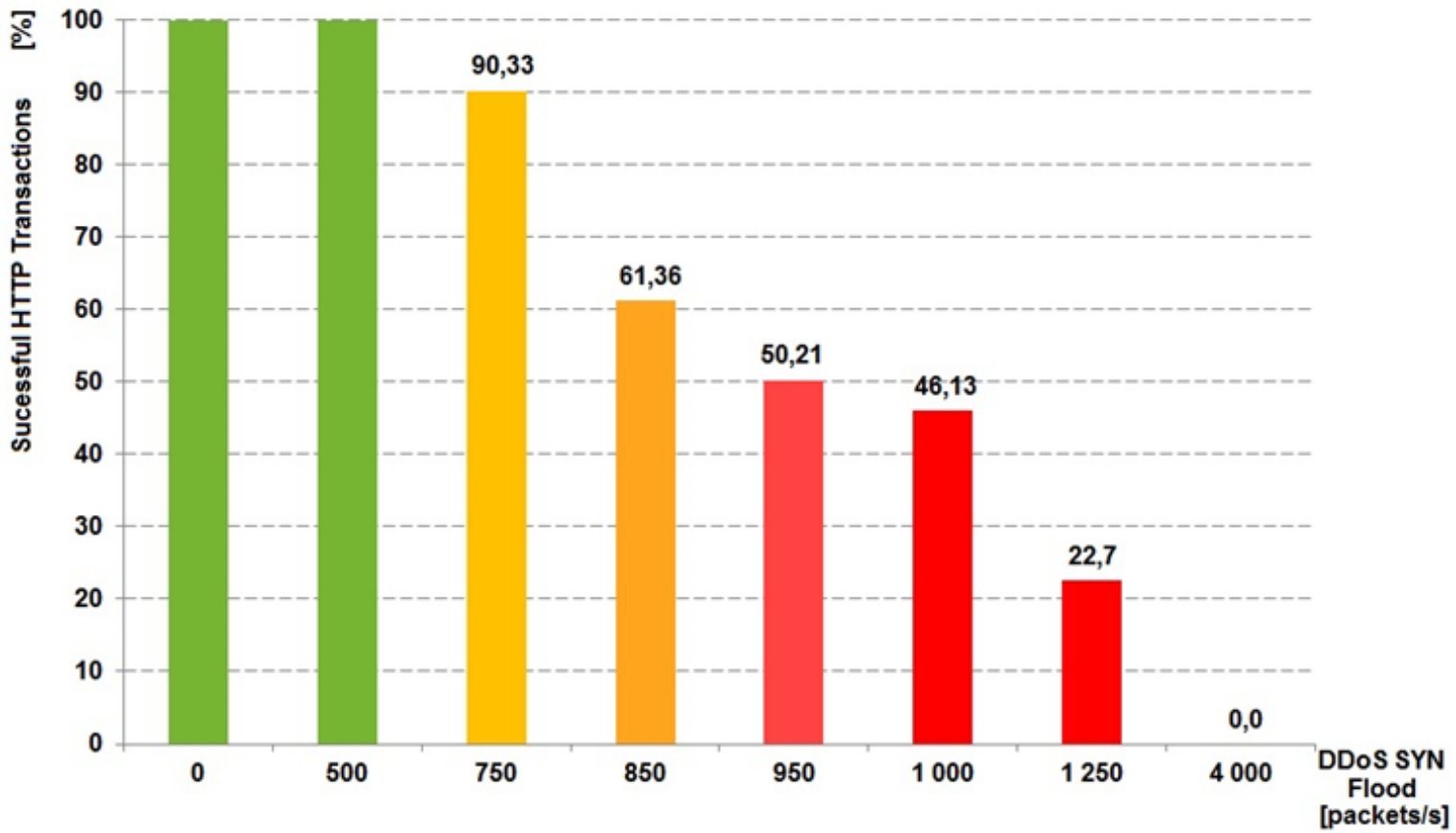
Testovací topologie s HW testerem a testovaným firewallem





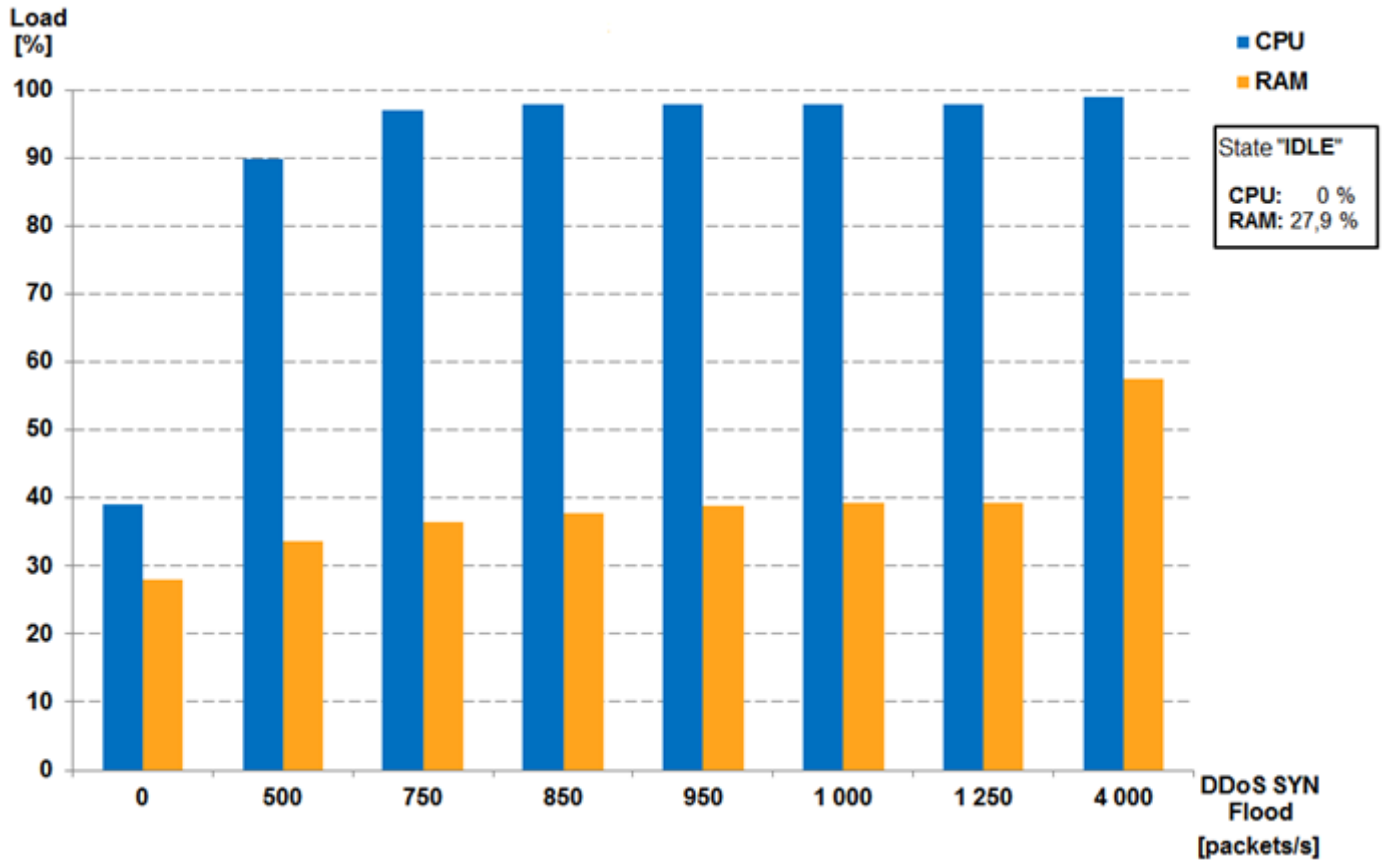
Výsledky testování firewallu - SYN flood

Procentuální podíl úspěšných HTTP transakcí při útoku TCP-SYN flood attack:



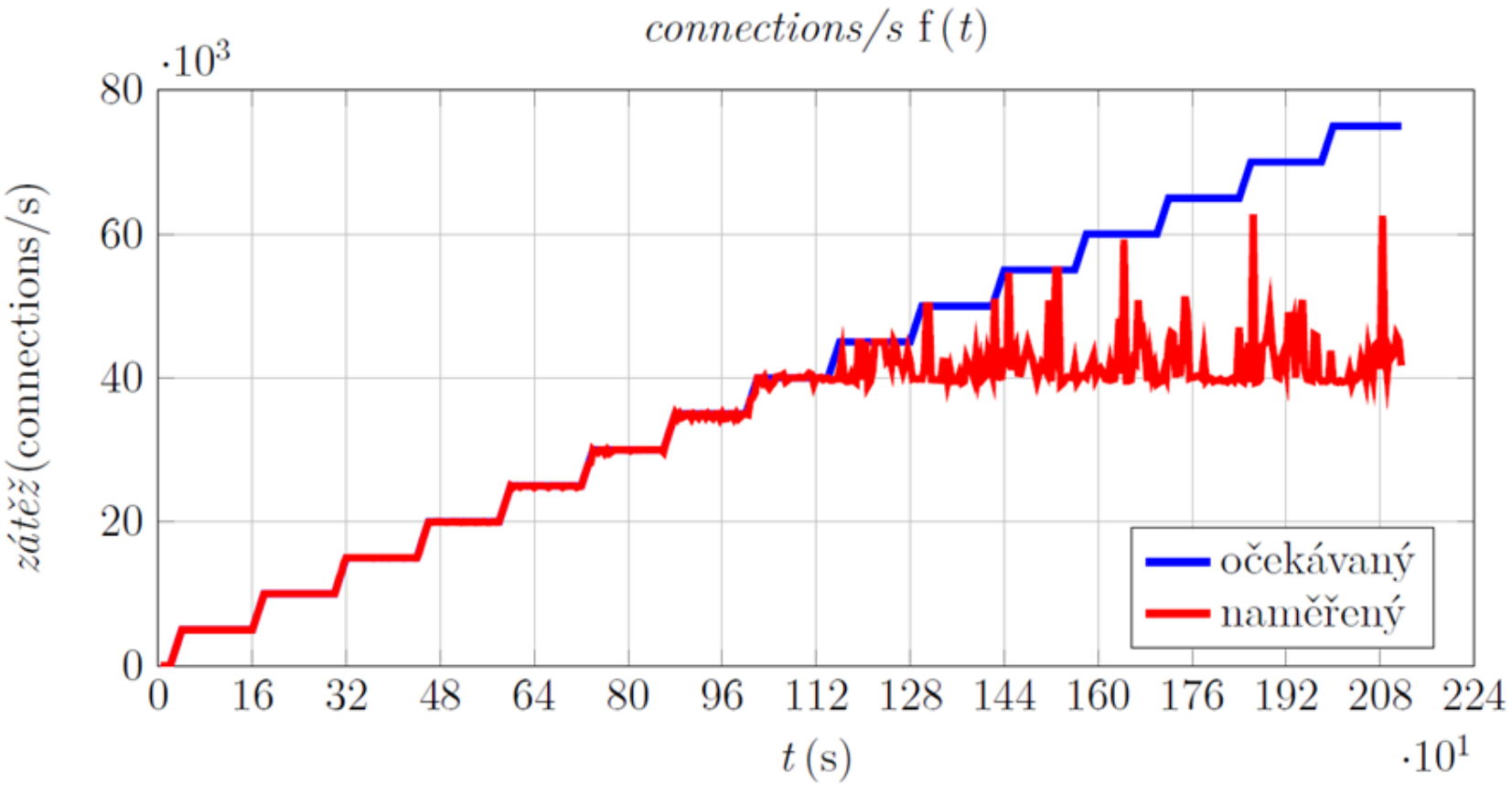
Výsledky testování firewallu - SYN flood

Zatížení paměti a CPU na firewallu ASA5510 během útoku TCP-SYN flood attack:



Výsledky testování firewallu - test zátěže

TCP connection test (ASA 5510 poskytuje max. 50000 TCP spojení/s):



Zátěžové testovaní - zhodnocení

- Výhodou je **zjištění limitů zařízení, sítí, služeb** atd.
- **Ověření správnosti konfigurace a propustnosti sítě, zařízení a služeb**.
- Testování scénářů při netypickém zatížení webových služeb (např. slevové akce, významné události, atd.).
- Využití zátěžového testeru s generováním (emulací) provozu a sledováním odezvy (analýza provozu).

Děkuji za pozornost!
Dotazy ?

malina@feec.vutbr.cz

Reference I


Steve Manzuik, Andre Gold, Chris Gatford
Network Security Assessment: From Vulnerability to Patch.
2006.


B. B. Gupta.
An Introduction to DDoS Attacks and Defense Mechanisms: An Analyst's Handbook
LAP LAMBERT Academic Publishing, 2011.


Harris, Shon.
CISSP exam guide.
Logical Security, 2007.