VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

VÝKONNOSTNÍ A BEZPEČNOSTNÍ TESTY SÍŤOVÝCH APLIKACÍ

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

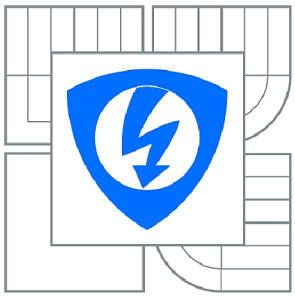
AUTOR PRÁCE
AUTHOR

Bc. MICHAL MATEJ

BRNO 2013

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

VÝKONNOSTNÍ A BEZPEČNOSTNÍ TESTY SÍŤOVÝCH APLIKACÍ

PERFORMANCE AND SECURITY TESTING OF NETWORK APPLICATIONS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

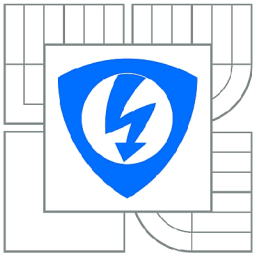
AUTOR PRÁCE — Bc. MICHAL MATEJ

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. VÁCLAV ZEMAN, Ph.D.

SUPERVISOR

BRNO 2013



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student: Bc. Michal Matej ***ID:*** 106625
Ročník: 2 ***Akademický rok:*** 2012/2013

NÁZEV TÉMATU:

Výkonnostní a bezpečnostní testy síťových aplikací

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte a popište bezpečnostní hrozby síťových aplikací na vrstvách L4 až L7. Při popisu hrozeb využijte publikované seznamy CVE (Common Vulnerabilities and Exposures). Dále vytvořte laboratorní síťovou infrastrukturu, na které by bylo možné jednotlivé typy bezpečnostních hrozeb testovat. Jádrem laboratorní sítě bude tester Avalanche 31000. V laboratorní síti proveďte testování jednotlivých síťových prvků při simulovaném síťovém provozu, výsledky testů statisticky zpracujte a vyhodnoťte.

DOPORUČENÁ LITERATURA:

[1] Scambray, J., McClure, S., Kurtz G. Hacking bez tajemství. COMPUTER PRESS, 2003.
[2] LeBlanc, D., Howard, M. Bezpečný kód, COMPUTER PRESS, 2008.

Termín zadání: 11.2.2013 ***Termín odevzdání:*** 29.5.2013

Vedoucí práce: doc. Ing. Václav Zeman, Ph.D.
Konzultanti diplomové práce:

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Cieľom tejto diplomovej práce je navrhnúť a realizovať bezpečnostný test na základe skúmania odolnosti testovaného zariadenia voči pôsobeniu distribuovaného útoku odoprenia služby *DDoS SYN Flood*. Následne, po spracovaní výsledkov testu, je vypracovaný protokol o vykonaní bezpečnostného testu testovaného zariadenia. V práci sú testované 2 zariadenia, konkrétne firewall CISCO ASA5510 a server s určeným názvom Server.

V teoretickej časti práce sú popisované primárne typy sieťových útokov ako rekognoskácia, získanie prístupu a útoky odoprenia služby. Vysvetlený je pojem DoS a jeho princíp, ďalej typy útokov odoprenia služby DoS a útoky distribuovaného odoprenia služby DDoS.

KĽÚČOVÉ SLOVÁ

Útok, DoS, DDoS, Avalanche 3100B, DDoS SYN Flood, firewall, server.

ABSTRACT

The aim of this Master's thesis is to design and to implement the security test in considering a resistance of the device under test to the effects of the distributed denial of service attack DDoS SYN Flood. After processing the test results is developed a protocol about security test of the device under test. In this thesis are tested two devices, namely CISCO ASA5510 firewall and a server with the specified name Server.

The theoretical part of the thesis discusses the primary types of network attacks such as reconnaissance, gain access and denial of service attacks. Explained the concept of DoS and its principle, further types of DoS attacks and distributed denial of service attacks DDoS.

KEYWORDS

Attack, DoS, DDoS, Avalanche 3100B, DDoS SYN Flood, firewall, server.

MATEJ, Michal *Výkonnostní a bezpečnostní testy síťových aplikací*: diplomová práca. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2013. 76 s. Vedúci práce bol doc. Ing. Václav Zeman, Ph.D.

PREHLÁSENIE

Prehlasujem, že som svoju diplomovoú prácu na tému „Výkonnostní a bezpečnostní testy síťových aplikací“ vypracoval samostatne pod vedením vedúceho diplomovej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej diplomovej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto diplomovej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/nebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona č. 121/2000 Sb., o právu autorském, o právoch súvisejúcich s právom autorským a o zmeně niektorých zákonov (autorský zákon), vo znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhé, hlavy VI. diel 4 Trestného zákoníka č. 40/2009 Sb.

Brno ....

(podpis autora)

POĎAKOVANIE

Na tomto mieste by som sa chcel poďakovať svojmu vedúcemu diplomovej práce, pánovi docentovi Ing. Václavovi Zemanovi, Ph.D., a pánovi Ing. Janovi Hajnému, Ph.D.

Brno . . . . . .

. . . . . .

(podpis autora)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic

http://www.six.feec.vutbr.cz

POĎAKOVANIE

Výzkum popsaný v této diplomové práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno . . . . . .

. . . . . .

(podpis autora)

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ÚVOD

Výkonnostné a bezpečnostné testy sieťových aplikácií predstavujú azda najdôležitejší proces hneď po vybudovaní sieťovej infraštruktúry a jej konfigurácie. Avšak zaobstarať reálne zariadenia, ktoré v definovaný čas vytvoria okamžitú záťaž na danú sieťovú infraštruktúru, predstavuje problém finančný, časový a je náročný z hľadiska realizácie. Odpoveď na tento problém nesie spoločnosť *Spirent Communications, Inc.*, ktorá vyvinula zariadenie *Avalanche 3100B*, umožňujúce generovanie reálnej sieťovej prevádzky na vrstvách L4-L7 sieťového modelu ISO/OSI, a umožňuje spracovávať výsledky definovaného testu výkonnosti a bezpečnosti.

V prvej kapitole diplomovej práce sú stručne popísané primárne typy sieťových útokov ako rekognoskácia, získanie prístupu a útoky odoprenia služby. Druhá kapitola je venovaná pojmu DoS a na túto kapitolu naväzuje kapitola venujúca sa typmi útokov DoS. V tejto kapitole sú jednotlivé typy útokov rozobrané z hľadiska princípu, z ktorého vychádzajú a ich vplyv na zariadenie obete útoku. V štvrtej kapitole je vysvetlený pojem DDoS, jeho princíp a uvedené príklady. Piata kapitola pokladá základ pre prácu s generátorom/testerom sieťovej prevádzky-Avalanche 3100B a taktiež tvorí odrazový most pre realizáciu bezpečnostných a výkonnostných testov. V tejto kapitole je popísaná laboratórna sieť, na ktorej sú realizované základné formy komunikácie medzi Avalanche 3100B a prepojenými zariadeniami-riadiaci terminál, smerovač, server a klient. Je tu špecifikovaná samotná konfigurácia týchto zariadení a vykonané funkčné testy laboratórnej siete realizované na protokoloch ICMP, HTTP a FTP.

Siedma a ôsma kapitola predstavuje výstup praktickej časti diplomovej práce v podobe dvoch protokolov o vykonaní bezpečnostného testu testovaných zariadení na základe odolnosti voči distribuovanému útoku odoprenia služby *DDoS SYN Flood*. Tieto protokoly je možné použiť ako dve samostatné časti, preto sú niektoré časti textu v protokoloch opakované. Siedma kapitola teda predstavuje protokol o vykonaní bezpečnostného testu firewall-u CISCO ASA5510, ôsma kapitola protokol o vykonaní bezpečnostného testu servera. V každom protokole je uvedená špecifikácia testu, vysvetlený pojem *DDoS SYN Flood*, technické špecifikácie testovaného zariadenia a jeho konfigurácia, ďalej výsledky testu testovaného zariadenia a v závere celkové zhrnutie testu.

1 PRIMÁRNE TYPY SIEŤOVÝCH ÚTOKOV

Sieťový útok je proces, pri ktorom osoba iniciujúca útok, nazývaná útočník, protiprávne postupuje voči systému siete, sieťovému prvku alebo koncovému zariadeniu užívateľa s cieľom jeho narušenia, obmedzenia alebo úplného odstavenia z prevádzky. Medzi primárne typy sieťových útokov patrí rekognoskácia, ktorá predznačuje počiatočnú fázu samotného útoku, ďalej proces získavania prístupu, prostredníctvom ktorého útočník získa kontrolu nad systémom obete. Odoprenie služby značí tretí typ sieťového útoku, kedy útočník doslova odoprie funkčnosť systému jeho legitímneho užívateľa.

1.1 Rekognoskácia

Rekognoskácia znamená neoprávnené objavovanie a mapovanie sietí, ich systémov, služieb a bezpečnostných medzier. Jedná sa o získavanie informácií, ktoré sú ďalej využívané v prospech útočníka a predznačujú samotný počiatok útoku [1].

K rekognoskácií patria:

- získavanie informácií z internetových zdrojov,
- skenovanie sietí,
- paketové analyzátory.

1.1.1 Internetové zdroje informácií

Prostredníctvom služieb internetu je možné nájsť na internetových stránkach voľne dostupné informácie, akými sú napr. vlastníci domén, aké adresy resp. adresný priestor bol danej doméne pridelený, kedy bola doména registrovaná, kedy vyprší jej platnosť, kontakty na zodpovedné osoby. Sú to všetko citlivé informácie, ktoré útočníkovi veľa napovedia pri plánovaní útoku. Útočník si môže taktiež zobraziť zdrojový kód webovej stránky obete, v ktorom často nájde zakomentované skryté informácie [1].

Príklad:
WHOis.net (http://www.whois.net)

1.1.2 Skenovanie sietí

Skenovať sieť znamená zistiť prítomnosť tzv. „živých“ sieťových zariadení na danom rozsahu adries, ďalej determinovať o aké zariadenie ide, aké služby na danom zariadení sú spustené na základe TCP a UDP portov, na akom operačnom systéme

je dané zariadenie realizované. Ku skenovaniu sietí patria techniky „ping sweep“ a „Port scan“ [1]. Pomocou ping-u útočník zistí prítomnosť sieťového zariadenia, následne prostredníctvom skenovania portov determinuje aké služby sú spustené na tomto zariadení.

Príklad:

- príkaz *ping* [2],
- ARP scan [1],
- nmap [1],
- ZENMAP (user-friendly nádstavba nmap) [1].

1.1.3 Paketové analyzátory

Paketový analyzátor je softwareová aplikácia, ktorá odchytáva a spracováva kompletnú komunikáciu na sieťovej karte. Umožňuje tak hĺbkovo analyzovať dáta a pakety odoslané zo sieťového zariadenia a prijaté sieťovým zariadením. Analýza môže predstavovať časovo náročnú operáciu, ktorá vyžaduje znalosti útočníka na odbornej úrovni [1]. Príkladom paketového analyzátora je software Wireshark organizácie Wireshark Foundation [3].

1.2 Získanie prístupu

Získať prístup pre útočníka znamená schopnosť infiltrovať sa do systému, na ktorý nemá oprávnenie prístupu, nemá svoj užívateľský účet, ďalej odcudziť alebo inak pozmeniť dáta a v neposlednom rade znamená zvýšenie úrovne prístupových práv užívateľa [1].
K získaniu prístupu patria:
Útoky k získaniu hesla – Slúžia k získaniu hesla systému obete. Môžu byť implementované formou brute-force útoku (útok hrubou silou), Trojskými koňmi a taktiež paketovými analyzátormi.
Využitie dôvery – útočník sa neinfiltruje do systému obete priamo, ale využije pri útoku iné zariadenie, ktorému obeť dôveruje.
Presmerovanie portu – Využíva tzv. „spreneverený“ hostiteľský počítač, ktorý slúži ako vstupno/výstupný prvok medzi firewall-om a vonkajšiou sieťou, z ktorej je realizovaný útok. Bez tohto prvku by bol kompletný prenos dát firewall-om zamietnutý. Na tomto prvku dochádza k presmerovaniu portov z vnútornej siete na porty vonkajšej siete, ktoré by inak boli firewallom blokované.
„Man-in-the-Middle“ – Útočník je prostredníkom komunikácie medzi 2 entitami.

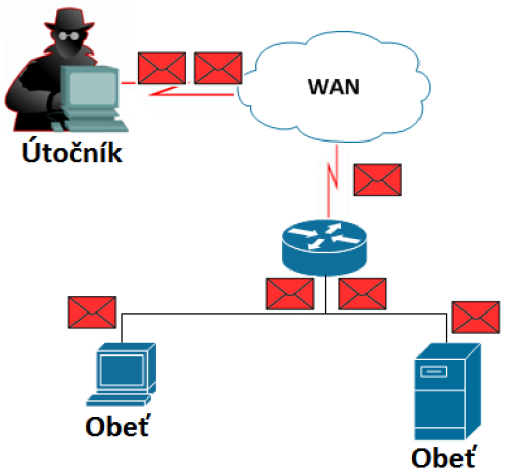
To znamená, že ním prechádza celá komunikácia týchto entít, ktorú je schopný modifikovať a zneužiť.

1.3 Útoky odoprenia služby

Narušenie činnosti siete alebo iného sieťového zariadenia je pre útočníka oveľa jednoduchšie než získanie samotného prístupu či už do sieťovej infraštruktúry, sieťového prvku alebo jediného počítača užívateľa. Ubehlo už niekoľko rokov od doby, kedy bola navrhnutá protokolová sada TCP/IP [5]. V dávnych rokoch sa počítalo s dôveryhodným systémom, ktorý bude korektne fungovať podľa dohodnutých pravidiel. Avšak týmto časom odzvonilo a práve útočníci tvoria skupinu ľudí, ktorí využívajú nedostatkov a medzier tejto protokolovej sady v podobe sieťových útokov. Útoky predstavujú zahltenie cieľa útoku obrovským množstvom žiadostí za jednotku času, ktoré spôsobia neoptimálne chovanie cieľa, v najhoršom prípade až jeho nedostupnosť pre prístup a použitie legitímnymi užívateľmi. Do skupiny útokov odoprenia služby patria útoky realizované jedinou entitou na jediný cieľ-DoS a distribuované útoky, realizované viacerými entitami produkujúcimi útok na jediný cieľ-DDoS [1],[6].

2 DOS - DENIAL OF SERVICE

„*Denial of Service*“ v preklade znamená odoprenie služby. Princíp útoku teda spočíva v tom, že útočník ním odoprie, zneprístupní alebo inak zamedzí funkčnosť služby jej legitímnemu užívateľovi, resp. užívateľom [1], [6], [8]. Schéma princípu útoku DoS je zobrazená na Obr. č. 2.1.



Obr. 2.1: Princíp útoku DoS [1].

Príklady DoS:

- Zahltenie siete brániace jej správnej funkčnosti,
- zabránenie prístupu k službe legitímnemu užívateľovi,
- narušenie služby konkrétneho systému alebo užívateľa.

Účinkom DoS útoku je zamedzenie prevádzky počítača alebo siete. DoS útoky existujú v rôznych formách a ich cieľom je široké spektrum obmedzenia služieb. Základné formy útoku [8]:

1. Spotreba zdrojov.
2. Deštrukcia alebo modifikácia konfiguračných informácií.

2.1 Spotreba zdrojov

Pripojenie k sieti – Hlavným cieľom je zabránenie komunikácie medzi užívateľom a sieťou, resp. komunikácií na sieti. Príkladom je SYN Flood útok [8].

Použitie svojich vlastných zdrojov proti sebe samému – Útočník na napadnutie obete využije jej vlastné zdroje. Príkladom je UDP Port útok [8].

Spotreba šírky pásma – Útočník zahltí voľnú šírku pásma generovaním obrovského množstva paketov smerovaných do napádanej siete. Príkladom je zahltenie ICMP „Echo“ paketmi, ale v podsate útočník môže využiť akýkoľvek typ paketu [8].

Spotreba ne-sieťových zdrojov – Útočník môže mimo zdroje dôležité pre chod siete napadnúť zdroje zabezpečujúce chod systému samotného klienta alebo servera, t.j. využitie procesora a procesov, operačnej pamäte, diskového poľa vo svoj prospech spustením skriptov inicializujúcich útok [8].

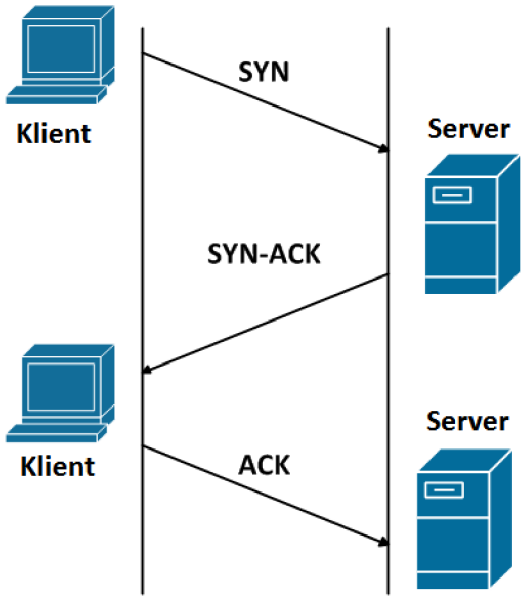
Deštrukcia alebo modifikácia konfiguračných informácií – Pokial získa útočník kontrolu nad počítačom alebo iným sieťovým prvkom, môže zmeniť jeho konfiguráciu vo svoj prospech a tým zamedziť v komunikácií legitímneho užívateľa so sieťou, pri zmene konfigurácie smerovača napr. zamedziť intranetu komunikovať s ISP atď [8].

3 ÚTOKY DOS

DoS útoky vychádzajú z princípu popísaného v kap.2. V tejto kapitole sú rozobrané jednotlivé typy DoS útokov koncipované na sieťovej a transportnej vrstve referenčného modelu ISO/OSI [7].

3.1 TCP SYN Flood

Cieľom útoku je znemožniť korektný proces naviazania TCP spojenia „Three-Way-Handshake“ medzi klientom a serverom. Schéma Three-Way-Handshake je znázornená na Obr. č. 3.1,[4].

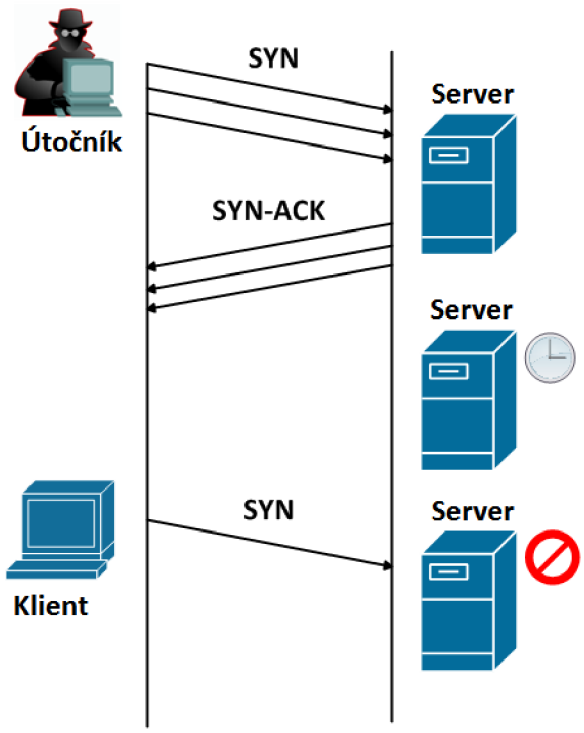


Obr. 3.1: Three-Way-Handshake [4].

Princíp útoku [1]:

1. Útočník posiela naraz množstvo falošných „Spoofed-SYN“ žiadostí na server.
2. Server odpovedá posielaním „SYN-ACK“ odpovedí a čaká na dokončenie Three-Way-Handshake. V tejto dobe sa na serveri plní fronta neuzavretých spojení a dochádza k vyčerpaniu voľných zdrojov servera.
3. Klient zahajuje spojenie so serverom odoslaním nefalšovanej „SYN“ žiadosti na server ale v dôsledku zahltenia servera nedôjde k spojeniu, server má preplnenú frontu, žiadosť ignoruje, stáva sa nedostupný.

Princíp útoku je znázornený na Obr.č.3.2.



Obr. 3.2: SYN Flood.[1]

Tab. 3.1: TCP „SYN“ Flood - parametre [10]

Parameter	**Popis**	**Hodnota (pr.)**
RepeatCount	Počet opakovaní sekvencie útoku	120
PacketsToGenerate	Počet paketov generovaných v jednej sekvencií útoku	1000
PacketRate	Rýchlosť generovania paketov (paket/s)	1000
TCPSourcePort	Číslo portu zdroja (TCP záhlavie)	1024
TCPDestPort	Číslo portu cieľa (TCP záhlavie)	80 (HTTP)

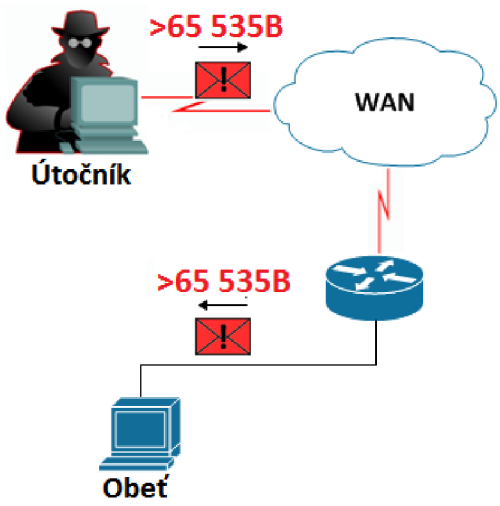
3.2 Ping of Death

Jeden z najstarších útokov vôbec. Využíva zraniteľnosť starých operačných systémov (Windows 98, 2000, NT). Útok zahrňuje odosielanie nesprávnej veľkosti ICMP „Echo“ paketu - „ping“, za účelom pretečenia vstupnej vyrovnávajúcej pamäte počítača obete, čo má za následok zrútenie operačného systému [1],[11].

Princíp útoku:

1. Útočník upraví veľkosť paketu ICMP ECHO žiadosti na veľkosť väčšiu ako 65535 bajtov. Tento paket následne odošle na adresu cieľovej obete.
2. Po prijatí neštandardizovanej veľkosti paketu počítačom obete dôjde k pretečeniu vyrovnávacej pamäte a tým k pádu operačného systému.

Princíp útoku je znázornený na Obr.č.3.3.



Obr. 3.3: Ping of Death.[1]

Tab. 3.2: Ping of Death - parametre.[10]

Parameter	**Popis**	**Hodnota (pr.)**
RepeatCount	Počet opakovaní sekvencie útoku	120
PacketsToGenerate	Počet paketov generovaných v jednej sekvencií útoku	1000
PacketRate	Rýchlosť generovania paketov (paket/s)	1000

3.3 LAND attack

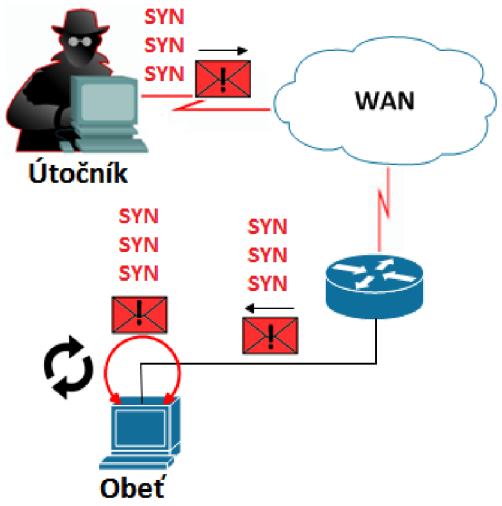
LAND je skratka pre „Local Area Network Denial“. Útok spočíva vo vytvorení lokálnej slučky na klientskom počítači a následnom zahájení prenosu TCP SYN paketov vo vytvorenej slučke [12].

Princíp útoku:

1. Útočník odosiela svojej obeti infikované pakety, ktoré sú nositeľmi rovnakej IP adresy a rovnakého čísla portu pre cieľ aj zdroj, t.j. dochádza k vytvorení lokálnej slučky. Počítač obete vlastne sám sebe sústavne odpovedá.

2. Dochádza k vlastnému zahlteniu systému obete množstvom SYN paketov inicializujúcich spojenie - dochádza k vyčerpaniu zdrojov a pretečeniu fronty, systém nie je schopný korektnej provádzky.

Princíp útoku je znázornený na Obr.č.3.4.



Obr. 3.4: LAND attack [1].

Tab. 3.3: Land Attack - parametre [10]

Parameter	**Popis**	**Hodnota (pr.)**
RepeatCount	Počet opakovaní sekvencie útoku	120
PacketsToGenerate	Počet paketov generovaných v jednej sekvencií útoku	1000
PacketRate	Rýchlosť generovania paketov (paket/s)	1000
TCPDestPort	Rovnaké číslo portu zdroja aj cieľa	80 (HTTP)

3.4 ARP Flood

Útok generuje pakety protokolu ARP (Address Resolution Protocol) cielené na sieťový prvok z rozsahu virtuálnych zdrojových adries. Útočník pritom generované ARP pakety - „ARP Request“ a „ARP Reply“ konfiguruje. Cieľom útoku je zneužiť limitované schopnosti v riadení protokolu ARP sieťovým prvkom a preplnení jeho pamäte cache dotazmi ARP [13].

Tab. 3.4: ARP Flood - parametre.[10]

Parameter	**Popis**	**Hodnota (pr.)**
RepeatCount	Počet opakovaní sekvencie útoku	120
PacketsToGenerate	Počet paketov generovaných v jednej sekvencií útoku	1000
PacketRate	Rýchlosť generovania paketov (paket/s)	1000
ARPHSourceEthAddr	Počiatočná „spoofed“ fyzická adresa zdroja	0A:05:00:00:00:01
ARPHDestEthAddr	Fyzická adresa cieľa	0A:0D:00:00:00:01
ARPHSourceIPAddr	Počiatočná „spoofed“ IP adresa zdroja	10.5.0.1
ARPHDestIPAddr	IP adresa cieľa	10.13.0.1
ARPHeaderOperation	Operačný kód v ARP záhlaví	2

3.5 Evasive UDP

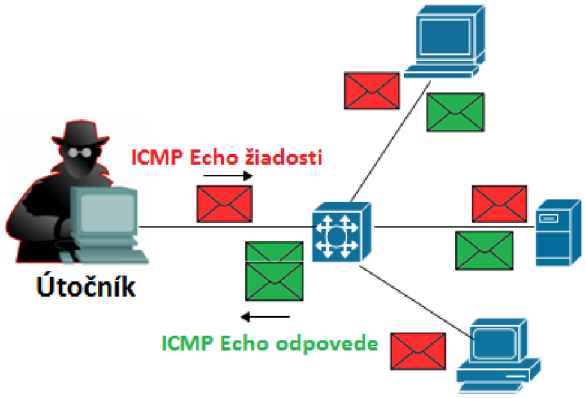
Útok je založený na princípe generovania prúdu UDP rámcov s variabilnou veľkosťou rámca a náhodnými zdrojovými IP adresami. Výsledkom útoku je zahltenie systému veľkým množstvom prijatých rámcov [10].

Tab. 3.5: Evasive UDP Attack - parametre. [10]

Parameter	**Popis**	**Hodnota (pr.)**
RepeatCount	Počet opakovaní sekvencie útoku	120
PacketsToGenerate	Počet paketov generovaných v jednej sekvencií útoku	1000
PacketRate	Rýchlosť generovania paketov (paket/s)	1000
UDPSourcePort	Číslo portu zdroja (UDP záhlavie)	1024
UDPDestPort	Číslo portu cieľa (UDP záhlavie)	512

3.6 Ping Sweep

Ping sweep je využívaný na indetifikáciu dostupnosti sieťových zariadení na danom rozsahu adries. Ako útok predstavuje generovanie množstva ICMP „Echo“ žiadostí smerujúce širokému rozsahu cieľových adries [10]. Princíp útoku je znázornený na Obr.č.3.5.



Obr. 3.5: Ping Sweep [1].

Tab. 3.6: Ping Sweep - parametre. [10]

Parameter	**Popis**	**Hodnota (pr.)**
RepeatCount	Počet opakovaní sekvencie útoku	120
PacketsToGenerate	Počet paketov generovaných v jednej sekvencií útoku	1000
PacketRate	Rýchlosť generovania paketov (paket/s)	1000

3.7 Smurf attack

Útok generuje ICMP ping žiadosti na špecifický sieťový prvok z rozsahu virtuálnych zdrojových adries s cieľom zahltiť sieť ping žiadosťami na broadcastové adresy. Zariadenia na sieti tak odpovedajú na ping žiadosti a tým dochádza k záplave siete a plytvaniu prenosovej kapacity liniek [10].

Tab. 3.7: Smurf attack - parametre.[10]

Parameter	**Popis**	**Hodnota (pr.)**
RepeatCount	Počet opakovaní sekvencie útoku	120
PacketsToGenerate	Počet paketov generovaných v jednej sekvencií útoku	1000
PacketRate	Rýchlosť generovania paketov (paket/s)	1000

3.8 Unreachable Host

Útok je postavený na princípe odosielania chybnej ICMP správy „Zariadenie nedostupné“. Systém si tak myslí, že entita na druhej strane je naozaj nedostupná

a preto dôjde k rozpadu spojenia. Generovanie týchto správ v malom množstve za jednotku času už môžu paralyzovať systém [10].

Tab. 3.8: Unreachable Host - parametre. [10]

Parameter	**Popis**	**Hodnota (pr.)**
RepeatCount	Počet opakovaní sekvencie útoku	120
PacketsToGenerate	Počet paketov generovaných v jednej sekvencií útoku	1000
PacketRate	Rýchlosť generovania paketov (paket/s)	1000
UnreachableHAddr	IP adresa nedosiahnuteľného host-a	10.0.0.1

3.9 Reset Flood

Útok generuje pakety TCP „RST“ zasielané rozsahu cieľových adries. Kľúčovou úlohou útoku je prerušiť aktívne-už naviazané TCP spojenia na sieti alebo na sieťových zariadeniach [10].

Tab. 3.9: Reset Flood - parametre. [10]

Parameter	**Popis**	**Hodnota (pr.)**
RepeatCount	Počet opakovaní sekvencie útoku	120
PacketsToGenerate	Počet paketov generovaných v jednej sekvencií útoku	1000
PacketRate	Rýchlosť generovania paketov (paket/s)	1000
TCPSourcePort	Číslo portu zdroja (TCP záhlavie)	1024
TCPDestPort	Číslo portu cieľa (TCP záhlavie)	80

3.10 TCP Port Scan

TCP Port Scan je podľa správnosti využívaný na identifikáciu TCP portov, ktorých služby sú k dispozícií. Ako útok generuje pakety TCP „SYN“ z rozsahu portov TCP na IP adresy cieľov. Kľúčovou úlohou útoku je zamedziť korektné naviazanie TCP spojenia, spôsobené vyčerpaním voľných zdrojov cieľových sietí a sieťových prvkov (buffer-y, pamäť RAM) [10].

Tab. 3.10: TCP Port Scan - parametre.[10]

Parameter	**Popis**	**Hodnota (pr.)**
TargetsToHit	Počet skenovaných cieľov (adries)	1
PortsToScan	Počet skenovaných portov každého cieľa	65535
PacketRate	Rýchlosť generovania paketov (paket/s)	1000
TCPSourcePort	Číslo portu zdroja (TCP záhlavie)	1024
StartingTCPDestP	Štartovné číslo skenovaného portu cieľa	0

3.11 Teardrop

Útok predstavuje odosielanie fragmentovaných IP paketov s odlišnou veľkosťou offsetu a veľkosťou jedného fragmentovaného paketu v porovnaní s predošlým paketom. Dochádza k overlapingu-prekrývaniu paketov. Cieľová stanica nie je schopná správne rekonštruovať záhlavie týchto paketov a dochádza k zrúteniu alebo neodpovedaniu systému [10].

Tab. 3.11: Teardrop - parametre. [10]

Parameter	**Popis**	**Hodnota (pr.)**
RepeatCount	Počet opakovaní sekvencie útoku	120
PacketsToGenerate	Počet paketov generovaných v jednej sekvencií útoku	1000
PacketRate	Rýchlosť generovania paketov (paket/s)	1000
UDPSourcePort	Číslo portu zdroja (UDP záhlavie)	1024
UDPDestPort	Číslo portu cieľa (UDP záhlavie)	512

3.12 UDP Flood

Útok generuje sekvenciu UDP paketov cielených na špecifický sieťový prvok z rozsahu virtuálnych zdrojových adries. Jeho poslaním je zahltenie šírky pásma siete a zamedzenie schopnosti sieťových prvkov naviazať nové UDP spojenia. Taktiež je útok využitý na vyčerpanie prostriedkov siete a sieťových zariadení (buffer) [10].

Tab. 3.12: UDP Flood - parametre.[10]

Parameter	**Popis**	**Hodnota (pr.)**
RepeatCount	Počet opakovaní sekvencie útoku	200
PacketsToGenerate	Počet paketov generovaných v jednej sekvencií útoku	255
PacketRate	Rýchlosť generovania paketov (paket/s)	1000
UDPSourcePort	Číslo portu zdroja (UDP záhlavie)	1024
UDPDestPort	Číslo portu cieľa (UDP záhlavie)	512

3.13 UDP Port Scan attack

UDP Port Scan je primárne určený na identifikovanie UDP portov, na ktorých sú prístupné služby. Avšak v podobe útoku generuje sekvenciu UDP paketov zo škály cieľových UDP portov na rozsahu cieľových adries. Podobne ako UDP Flood attack aj UDP Port scan attack má za úlohu zahltiť šírku pásma siete a zamedziť schopnosti sieťových prvkov naviazať nové UDP spojenia. Taktiež je využitý na vyčerpanie prostriedkov siete a sieťových zariadení (buffer) [10].

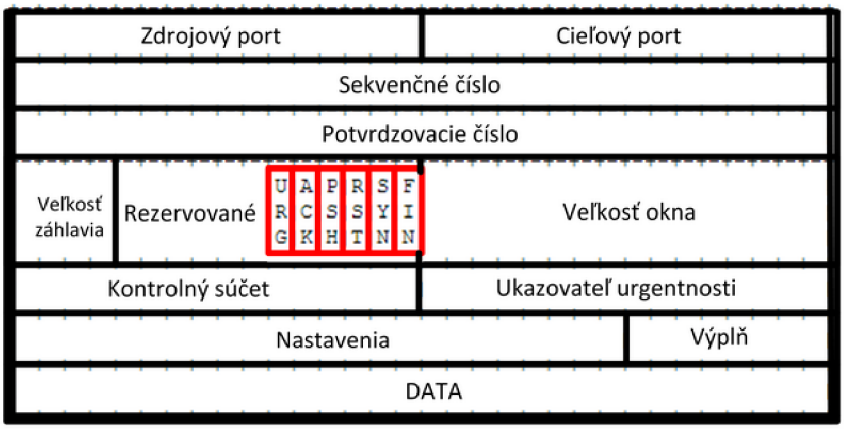
Tab. 3.13: UDP Port Scan attack - parametre.[10]

Parameter	**Popis**	**Hodnota (pr.)**
TargetsToHit	Počet skenovaných cieľov (adries)	1
PortsToScan	Počet skenovaných portov každého cieľa	65535
PacketRate	Rýchlosť generovania paketov (paket/s)	1000
UDPSourcePort	Číslo portu zdroja (UDP záhlavie)	1024
StartingUDPDestP	Štartovné číslo skenovaného portu cieľa	0

3.14 XMasTree attack

Útok generuje sekvenciu TCP paketov, ktoré majú v TCP záhlaví nastavených všetkých 6 kontrolných bitov(Flags), t.j. *URG*, *ACK*, *PSH*, *RST*, *SYN* a *FIN* na hodnotu 1. Z toho vyplýva pseudonymum útoku-TCP záhlavie je ovešané bitmi ako vianočný stromček. Pakety sú cielené na špecifický sieťový prvok z rozsahu virtuálnych zdrojových adries. Zariadenia, ktoré nemajú ošetrený systém proti prijatiu tohto „znetvoreného“ paketu, zlyhajú [10].

Obr. č. 3.6 ilustruje polia TCP záhlavia s vyznačenými kontrolnými bitmi, ktorých hodnoty sú nastavené na 1.



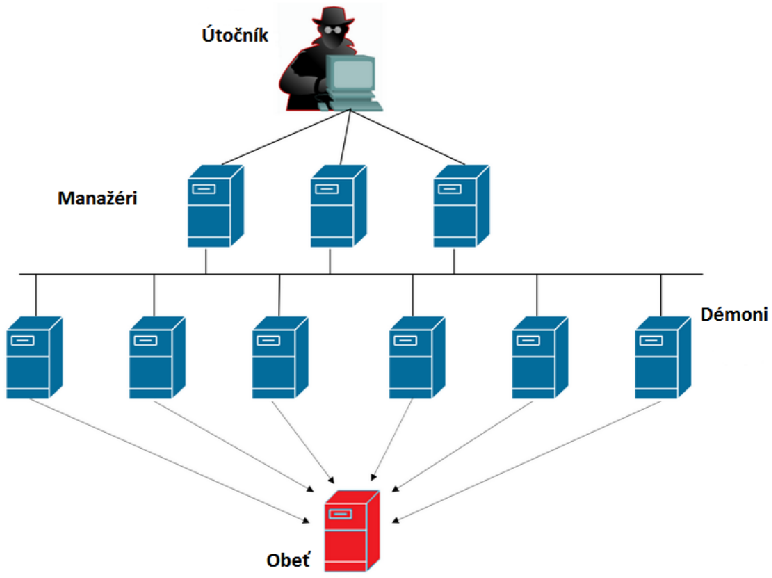
Obr. 3.6: TCP záhlavie-vyznačené kontrolné bity [5].

Tab. 3.14: XMasTree attack - parametre.[10]

Parameter	**Popis**	**Hodnota (pr.)**
RepeatCount	Počet opakovaní sekvencie útoku	120
PacketsToGenerate	Počet paketov generovaných v jednej sekvencií útoku	1000
PacketRate	Rýchlosť generovania paketov (paket/s)	1000

4 DDOS - DISTRIBUTED DENIAL OF SERVICE

Distribuované odoprenie služby vychádza z princípu DoS, avšak odlišnosť spočíva vo využití viacerých koordinovaných zdrojov sústreďujúcich útok na jediný cieľ. Útočník v prvom rade vytvorí sieť útočných počítačov-„Démoni“, a poprípade ich koordinačných počítačov-„Manažéri“.
Manažér a démon je zraniteľný, len málo zabezpečený alebo vôbec nezabezpečený systém, do ktorého útočník prenikne. Bez povšimnutia užívateľa na tento systém prenesie a spustí na pozadí nástroje, pomocou ktorých získa útočník kontrolu nad napadnutým počítačom. Pomocou infiltrovaných nástrojov je spustený skript, ktorý na povel útočníka vykoná príslušnú operáciu-v podobe generovania nežiadúcej prevádzky zo strany démona na cieľ alebo riadiace príkazy manažérov pre podskupinu démonov. Obr. č. 4.1 ilustruje princíp útoku DDoS [1].



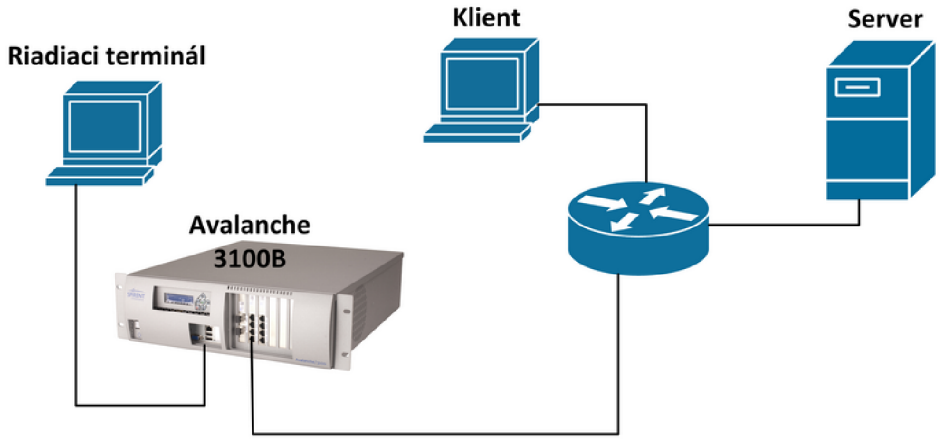
Obr. 4.1: Princíp útoku DDoS.[1]

Útok DDoS predstavuje využitie jedného alebo kombináciu viacerých útokov DoS. Medzi známe útoky patria [6]:
TFN (Tribe Flood Network) - zahŕňa útok SYN Flood, UDP Flood, Smurf a útoky realizované protokolom ICMP.
Trinoo - komunikácia medzi útočníkom a manažérom na špecifickom TCP porte 27665, komunikácia medzi manažérom a démonom na UDP porte 27444. Démoni útočia na systém obete zaplavovaním UDP Flood útoku.
Stacheldraht - kombinácia TFN a Trinoo, pridané šifrovanie komunikácie medzi

manažerom a démonom.
TFN2K - nástupca TFN, umožňuje randomizovať komunikačné porty, využitá šifrovaná komunikácia medzi manažérom a démonom, útoky SYN Flood, UDP Flood, Smurf attack-náhodné prepínanie.

5 LABORATÓRNA SIEŤ

Na praktické realizovanie výkonnostných testov bola podľa návrhu zostavená laboratórna sieť, ktorá predstavuje zmenšený model reálnej siete a slúži na interpretáciu využitia kľúčového zariadenia-testeru Avalanche 3100B. Návrh laboratórnej siete je zobrazený na Obr. č. 5.1. Pripojený tester v sieti generuje reálnu komunikáciu zastupujúcu veľký počet skutočných zariadení, ktoré by inak museli byť pripojené v tejto sieti pre získanie výsledkov.



Obr. 5.1: Návrh laboratórnej siete.

Laboratórna sieť je zostavená z:

- tester Spirent Avalanche 3100B,
- riadiaci terminál pre Avalanche 3100B,
- server s operačným systémom MS Windows Server 2003 Standard Edition x86 [20],
- smerovač MikroTik RouterBOARD 1200 [16],
- klientský počítač.

5.1 Avalanche 3100B

Avalanche 3100B je generátor a emulátor sieťovej infraštruktúry v jednom, kompletné testovacie prostredie umožňujúce záťažové testovanie vrátane generovania reálnej prevádzky na vrstvách L4 až L7. Zariadenie je schopné simulovať až 30 miliónov spojení, čím komplexne nahradzuje nutnosť realizovať testovanie pomocou reálneho hardwaru. Technické špecifikácie testeru sú uvedené v prílohe.

Pre účel testovania je využitý jeden Gigabit Ethernet port Eth0, ktorý je prepojený so smerovačom MikroTik. Na tento port sú generovaní klienti z rozsahu adries 192.168.1.3-192.168.1.254 siete 192.168.1.0/24. Port je nakonfigurovaný na maximálne využitie šírky pásma, pokiaľ to bude generovaná prevádzka vyžadovať.

5.2 Riadiaci terminál

Riadiaci terminál je realizovaný na platforme MS Windows 7 Professional [15] a slúži na riadenie testeru Avalanche 3100B prostredníctvom management portu na báze ethernetu pomocou aplikácií:

- Spirent TestCenter Layer 4-7 Application [9],
- Spirent TestCenter Layer 4-7 Results Analyzer [9].

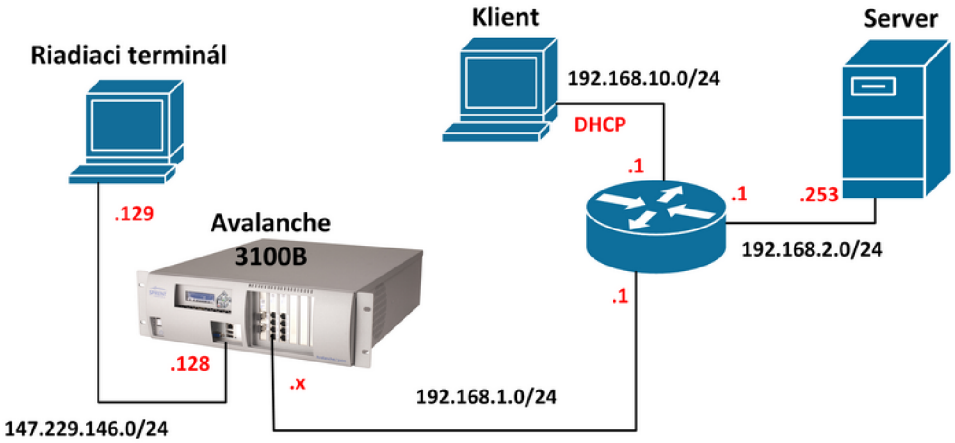
TestCenter Layer 4-7 Application je aplikácia slúžiaca na riadenie komplexnej činnosti testeru, t.j. samotnú administráciu, vytváranie a spúšťanie testov.
Spirent TestCenter Layer 4-7 Results Analyzer je aplikácia slúžiaca na analýzu a spracovanie výsledkov dosiahnutých na výstupe programu *TestCenter Layer 4-7 Application*.

5.3 RouterBOARD 1200

RouterBoard 1200 je 10 portový smerovač rozhrania Ethernet s podporou rýchlostí prenosu dát 10/100/1000 Mbit/s, každý port s funkciou Auto-MDI/X. Na testovanie sú využité 3 porty, z nich 1 je určený na konfiguráciu samotého smerovača[16].

Konfigurácia:
Port ETH1: IP adresa siete 192.168.1.0, IP adresa portu 192.168.1.1/24. Na tento port je pripojený tester Avalanche portom Eth0 s IP adresou 192.168.1.2.
Port ETH2: Sieť 192.168.2.0, IP adresa portu 192.168.2.1/24. Port je konfigurovaný ako DHCP server. Pripojený server obdrží IP adresu automaticky.
Port ETH10: Sieť 192.168.10.0, IP adresa portu 192.168.10.1/24. Tento port je využívaný na kofiguráciu smerovača pomocou klientského počítača s nainštalovaným nástrojom *WinBox*.

Obr. č. 5.2 ilustruje topológiu laboratórnej siete a Tab. č. 5.1 pripojené zariadenia na jednotlivé porty smerovača spolu s IP adresami.



Obr. 5.2: Topológia laboratórnej siete.

Tab. 5.1: Pripojené zariadenia na porty smerovača.

Port smerovača	Adresa portu	Pripojené zariadenie / Port
ETH1	192.168.1.1/24	Avalanche 3100B / Eth0
ETH2	192.168.2.1/24	Server / GiE
ETH10	192.168.10.1/24	Klient / FE

5.4 Server

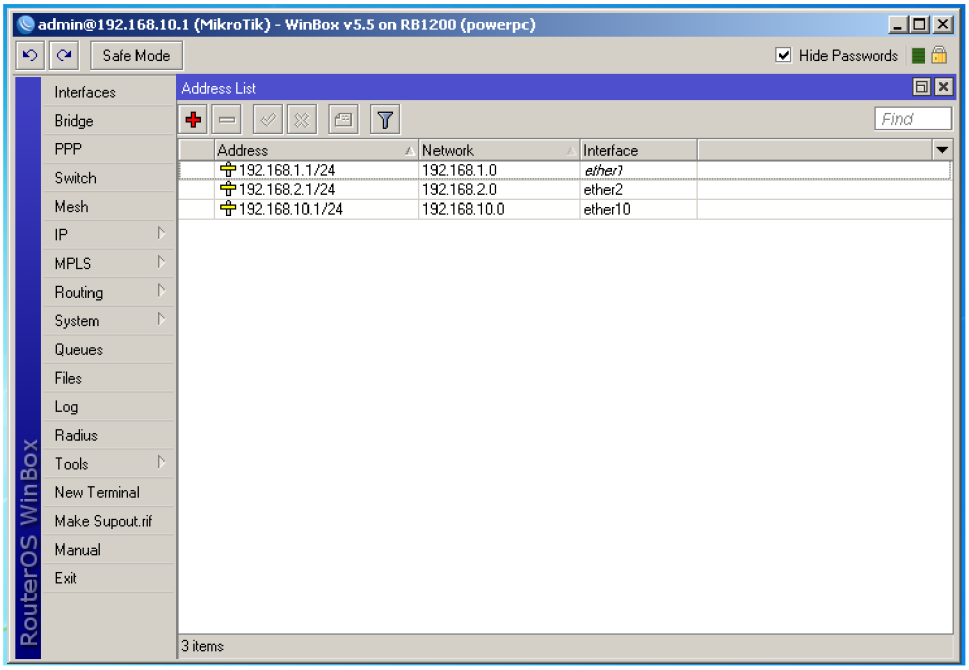
Server je realizovaný na platforme operačného systému MS Windows Server 2003 Standard Edition [20]. Hardware tvorí 2-jadrový procesor intel Xeon, 4GB RAM a sieťová karta Gigabit Ethernet. Na serveri je spustená aplikácia FTP server-FileZilla Server v0.9.41(freeware), a HTTP server-Apache v2.0.64(freeware).

FTP server je v aktívnom režime a čaká na pripojenie anonymného užívateľa, ktorému sprístupňuje textový súbor *TestFile.txt* o veľkosti 100kB na stiahnutie.

HTTP server emuluje úvodnú stránku serveru www.vutbr.cz, ktorej celková veľkosť je 1,74MB.

5.5 Klient

Klientský počítač je realizovaný na platforme operačného systému MS Windows 7 Professional SP1. Jeho funkciou je konfigurácia smerovača MikroTik pomocou nástroja WinBox [16] a overenie správnosti konfigurácie servera, t.j. klientskú pripojiteľnosť k službám FTP a HTTP. Okno konfiguračného nástroja WinBox je zobrazené na Obr. č. 5.3. Klientská pripojiteľnosť k FTP serveru je otestovaná pomocou freeware klienta FileZilla Client v3.6.0.2 a zobrazenie HTTP stránky je otestované pomocou webového prehliadača Internet Explorer v8.



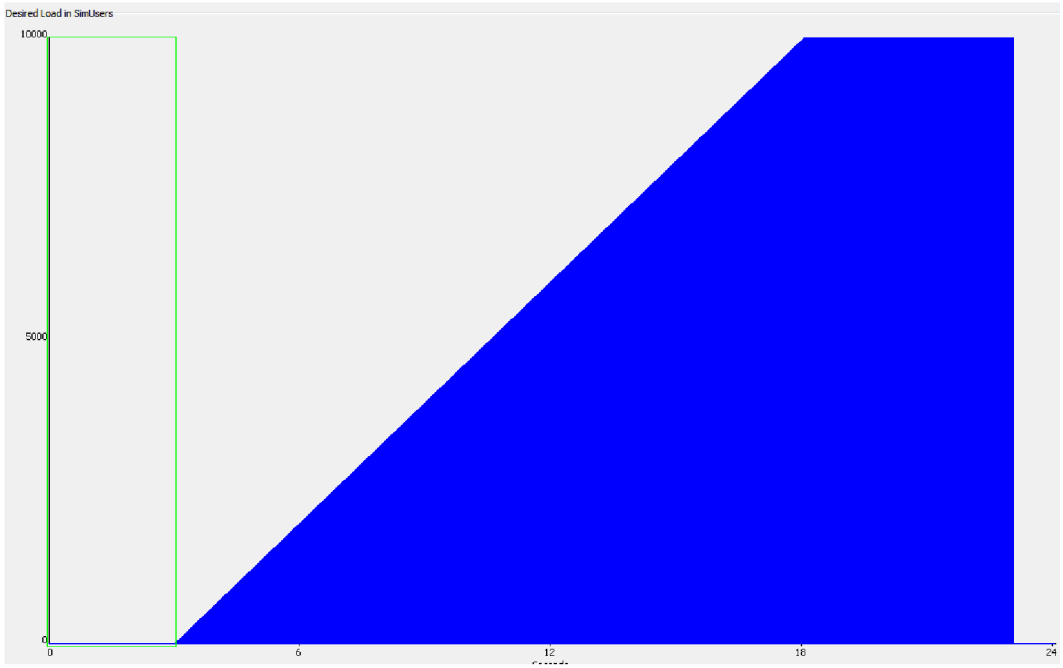
Obr. 5.3: Konfiguračný nástroj WinBox [16].

6 TESTY LABORATÓRNEJ SIETE

Na realizáciu záťažových testov laboratórnej siete bolo potrebné v aplikácií *Test-Center Layer 4-7 Application* vytvoriť vlastný profil, nazývaný *MyProfile*, v ktorom je obsiahnutá hardware-ová konfigurácia samotného testeru Avalanche, ďalej definovaný záťažový profil, vyjadrujúci počet generovaných klientov v čase priebehu testu a postupnosť príkazov pre príslušný typ testu. V tomto profile sa taktiež mení forma záťaže asociovanej služby na definovanom protokole. Celkom boli realizované 3 typy záťažových testov, konkrétne test reakcie servera na prúd ICMP *Echo* žiadostí generovaných klientami, test obsluhy pripojených klientov sťahujúcich textový súbor zo servera a test obsluhy pripojených klientov prezerajúcich si webovú stránku.
V záťažovom profile je definovaný graf závislosti počtu užívateľov na čase. Každý test vychádza z definovaného profilu a celková doba trvania testu je 24 sekúnd. Graf záťažového profilu je zobrazený na Obr. č. 6.1.

Popis grafu záťažového profilu:

1. **DELAY** – Štartovný čas, tzv. „nulová úroveň“, kedy prístroj Avalanche zahajuje fázu inicializácie prevádzky. Doba trvania: t=3s.
2. **RAMP Up** – Nábeh záťaže. Dochádza k pripájaniu klientov predstavujúcich záťaž. Začiatok nábehu v čase t=3s. Doba trvania narastania záťaže po dosiahnutie maximálnej úrovne: t=15s.
3. **STEADY** – Dosiahnutie požadovaného počtu klientov. Počiatok v čase t=18s, doba trvania t=5s.
4. **RAMP Down** – Náhly pokles záťaže na nulovú hodnotu. Počiatok v čase t=23s. Po dosiahnutí nulovej úrovne test ešte 1s trvá s nulovou záťažou.



Obr. 6.1: Graf záťažového profilu *MyProfile*.

Prístroj Avalanche 3100B je nakonfigurovaný na generovanie záťaže o celkovom počte 10 000 klientov. Záťažový profil pre konkrétny test obsahuje postupnosť príkazov *Action List*-u, ktoré sú vykonávané pre každého generovaného klienta. Na výstupnom porte Eth0 testeru Avalanche je definovaná sieť s rozsahom 253 dostupných adries a rýchlosťou linky 1Gb/s. Počas testovania dochádza k monitoringu priebehu testovania na výstupe programu *TestCenter Layer 4-7 Application* a k výsledkom testovania na výstupe programu *TestCenter Results Analyzer*.

TestCenter Layer 4-7 Application informuje o fázach testu, počtoch pokusných, úspešných, neúspešných a prerušených operáciach, ďalej o uplynulom a zostávajúcom čase testu. Taktiež informuje o štatistikách linkovej vrstvy - počet odoslaných paketov, počet prijatých paketov, počet odoslaných a prijatých bajtov, momentálny počet odosielaných (prijatých) paketov za jednotku času, maximálny počet odoslaných (prijatých) paketov za jednotku času a priemerný počet odosielaných (prijatých) paketov za jednotku času.
TestCenter Results Analyzer zobrazuje kompletné sumarizované výsledky po skončení testu. Tieto výsledky je schopný exportovať do súboru s príponou *pdf* a *html*.

V jednotlivých testoch sú zachytené snímky z oboch programov informujúce o priebehu a výsledkoch testu.

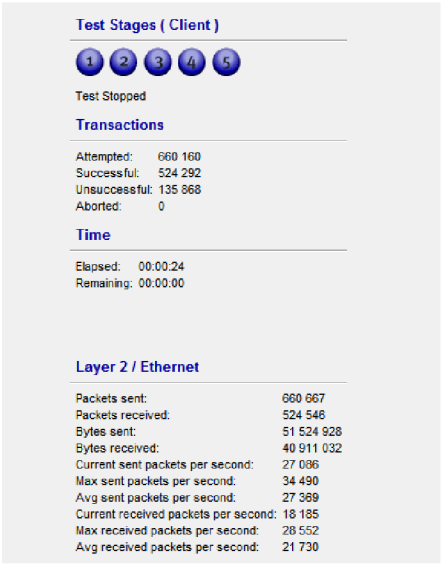
6.1 ICMP Ping Test

V tomto teste je na prístroji Avalanche 3100B definovaný scenár, podľa ktorého sú generované „ping“ žiadosti na server definovaného počtu užívateľov. Každý užívateľ odosiela 4 ICMP Echo žiadosti, každá o veľkosti 32bajtov, t.j. presne podľa *cmd* príkazu ping v operačnom systéme Windows.

Definované príkazy v **Action List**-e programu TestCenter:
ICMP://192.168.2.253 ECHO LENGTH=32
ICMP://192.168.2.253 ECHO LENGTH=32
ICMP://192.168.2.253 ECHO LENGTH=32
ICMP://192.168.2.253 ECHO LENGTH=32

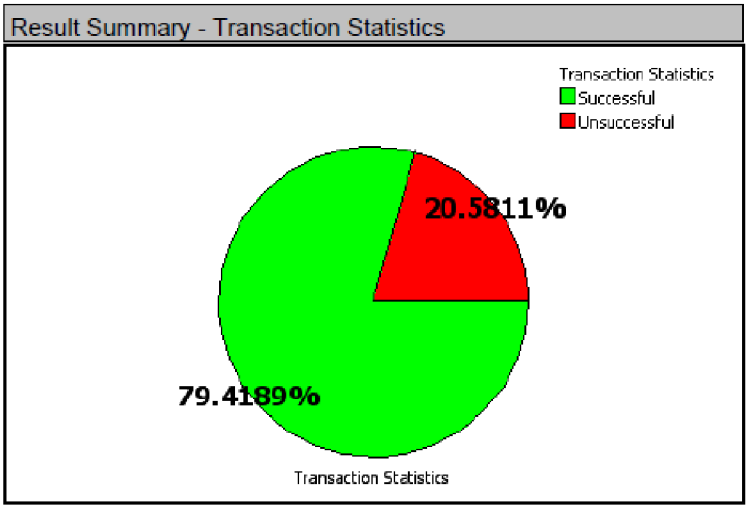
6.1.1 Výstup programu TestCenter a Results Analyzer

Nasledujúce obrázky ilustrujú výstup programov TestCenter, Obr. č. 6.2 a Results Analyzer, Obr. č. 6.3,6.4,6.5. Pri definovanej záťaži došlo k 79% úspešnosti prevedenia príkazu ping jedným užívateľom, 21% bolo neúspešných a žiadna žiadosť nebola serverom prerušená.



Obr. 6.2: TestCenter-monitoring priebehu testu.

Obr. č. 6.3 – graf *Results Summary - Transactions Statistics* vyjadrujúci percentuálnu úspešnosť a neúspešnosť prevedených transakcií.



Obr. 6.3: Results Analyzer-graf.

Obr. č. 6.4 – tabuľka *Test Results Summary* predstavuje sumarizované výsledky testu.

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	660160	27506	Minimum	0.0	0.0	0.0	0.0	0.0	Attempted	0
	Successful	524292	21845	Maximum	0.0	1049.0	0.0	0.0	0.0	Established	0
	Unsuccessful	135868	5661	Average							
	Aborted	0	0								

Obr. 6.4: Results Analyzer-sumár výsledkov testu.

Obr. č. 6.5 – tabuľka *Transaction Summary* predstavuje sumár o počte prevedených príkazov v definovanom profile a dobu odozvy (ms) vykonaných príkazov.

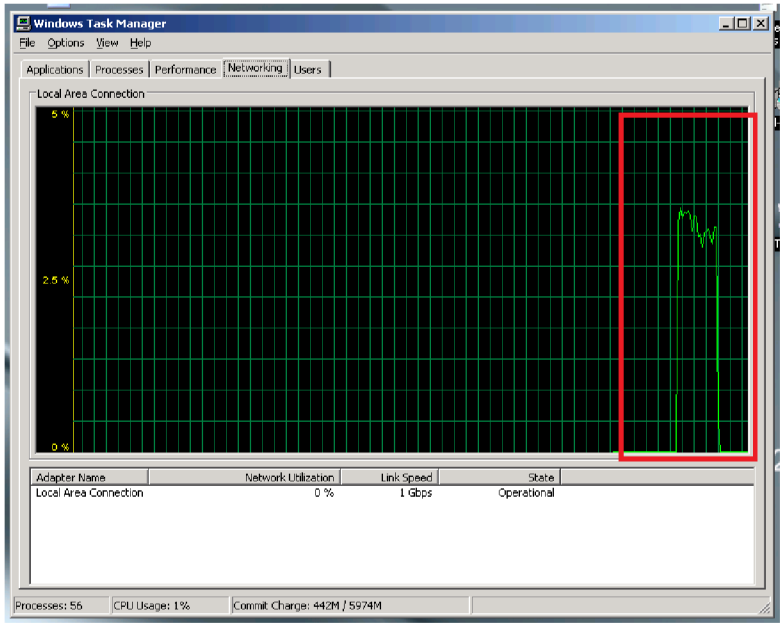
Transaction Summary	Test	Count	Transactions (Sub-Commands included)							
	Profile	URL	Average Successful Per Second	Attempted	Successful	Unsuccessful	Aborted	Percent Successful	Percent Unsuccessful	Percent Aborted
	User_0001_0	4	0	0	0	0	0	0.0	0.0	0.0
	Totals	4		0	0	0	0	0.0	0.0	0.0

Response Time (ms)		
Minimum	Maximum	Average
0.0	1049.0	199.481

Obr. 6.5: Results Analyzer-sumár transakcií.

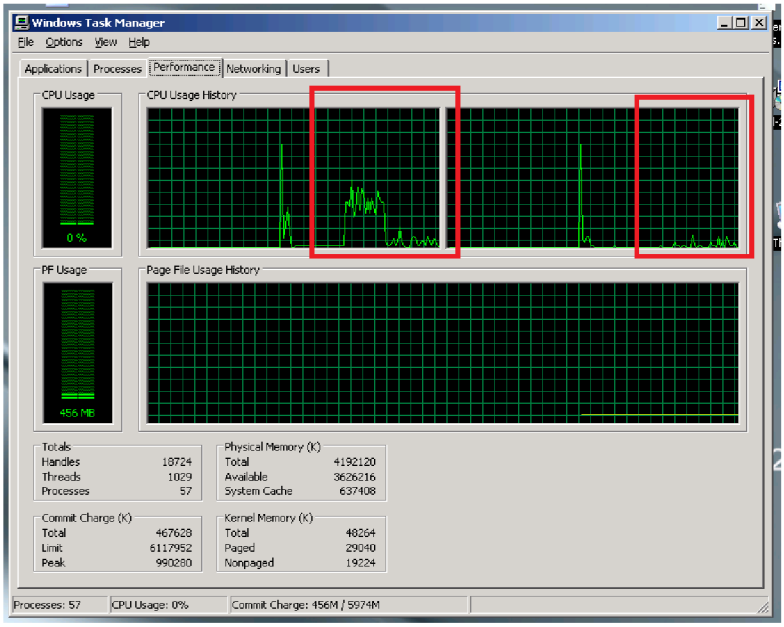
6.1.2 Monitoring servera

Obr. č. 6.6 znázorňuje histogram percentuálneho vyťaženia sieťovej karty po dobu testu. Špička dosiahla hodnotu 3%, čomu zodpovedá hodnota prenosovej rýchlosti 30,72Mbit/s.



Obr. 6.6: Správca úloh-vyťaženie sieťového pripojenia.

Obr. č. 6.7 znázorňuje histogram percentuálneho vyťaženia jadier procesora.



Obr. 6.7: Správca úloh-vyťaženie procesora.

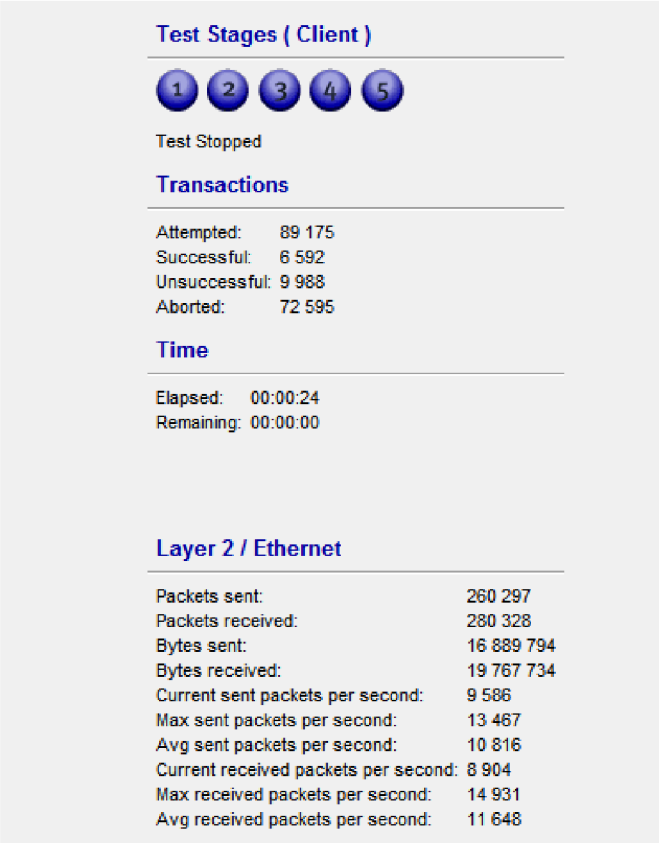
6.2 FTP Test

Test predstavuje generovanie definovaného počtu anonymných klientov pripojujúcich sa na FTP server FileZilla. Každým pripojeným užívateľom je zo serveru sťahovaný 100kB textový súbor *TestFile.txt*.

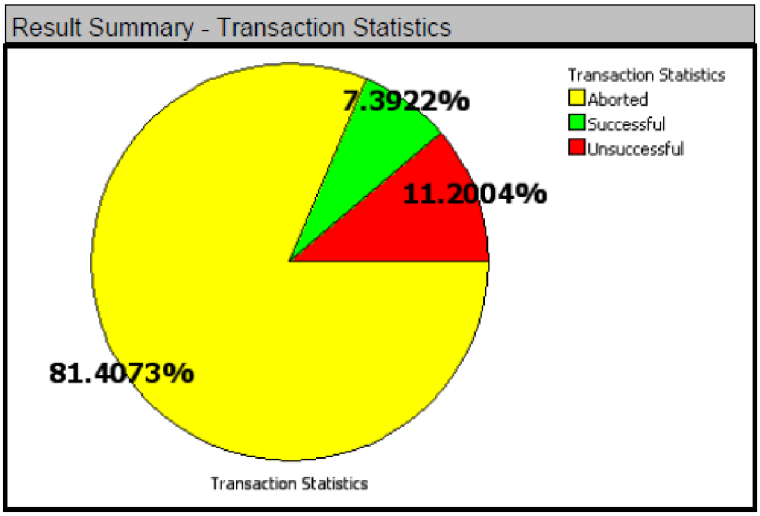
Definované príkazy v *Action List*-e programu TestCenter:
FSTREE=TestDirectory
1 ftp://192.168.2.253 <USER=anonymous PASSWD=anonymous> <GET=TestFile.txt>

6.2.1 Výstup programu TestCenter a Results Analyzer

Z grafu na Obr. č. 6.9 je zrejmé, že pri tomto type testu dosiahol server len 7,4% úspešnosť prevedených transakcií, 11,2% ich bolo neúspešných a 81,4% ich bolo prerušených. Obr. č. 6.10 a Obr. č. 6.11 znázorňuje výsledky testu s načerveno vyznačeným oknom s počtom neúspešných transakcií.



Obr. 6.8: TestCenter-monitoring priebehu testu.



Obr. 6.9: Results Analyzer-graf.

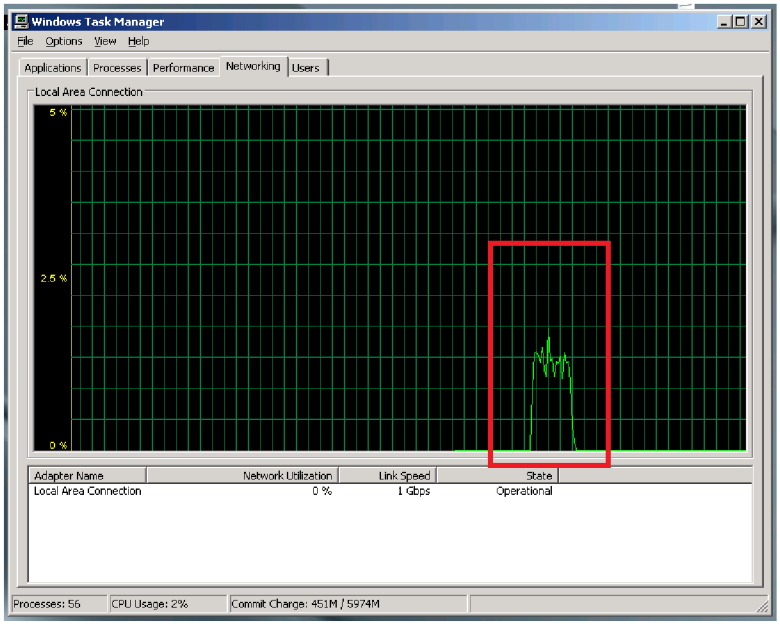
Test Results Summary	Transactions			Time (ms)						TCP Connections	
		Total	Rate Per Second		Page Response	URL Response	To TCP SYN/ACK	To First Data Byte	Est. Server Response		Total
	Attempted	89175	-	Minimum	0.0	0.0	0.079	0.0	0.0	Attempted	95767
	Successful	6592	-	Maximum	0.0	6529.0	3792.815	0.0	3786.192	Established	95767
	Unsuccessful	9988	-	Average							
	Aborted	72595	-								

Obr. 6.10: Results Analyzer-sumár výsledkov testu.

Transaction Summary	Test	Count	Transactions (Sub-Commands included)						
	Profile	URL	Average Successful Per Second	Attempted	Successful	Unsuccessful	Aborted	Percent Successful	Percent Unsuccessful	Percent Aborted
	User_0001_0	1	274	89175	6592	9988	72595	7.39	11.2	81.4
	Totals	1		89175	6592	9988	72595	7.39	11.2	81.4

Response Time (ms)		
Minimum	Maximum	Average
0.0	6529.0	158.901

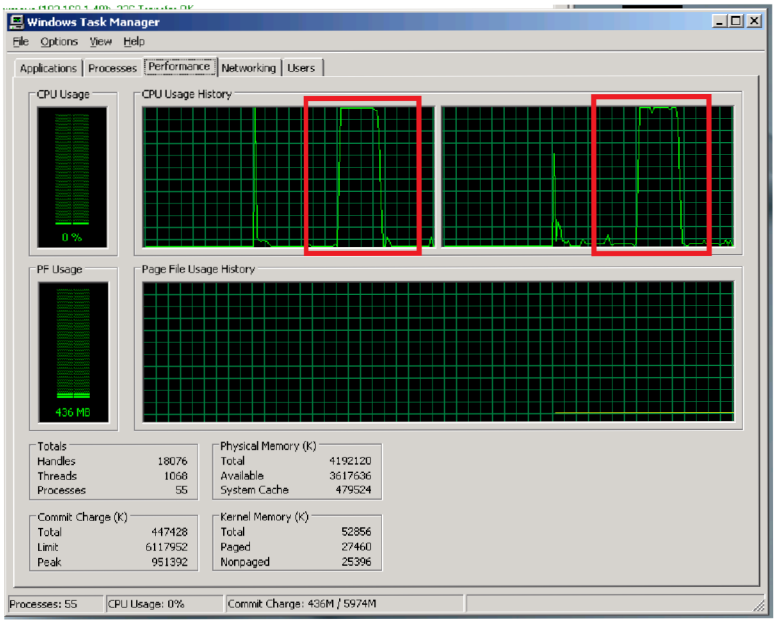
Obr. 6.11: Results Analyzer-sumár operácií.



Obr. 6.12: Správca úloh-vyťaženie sieťového pripojenia.

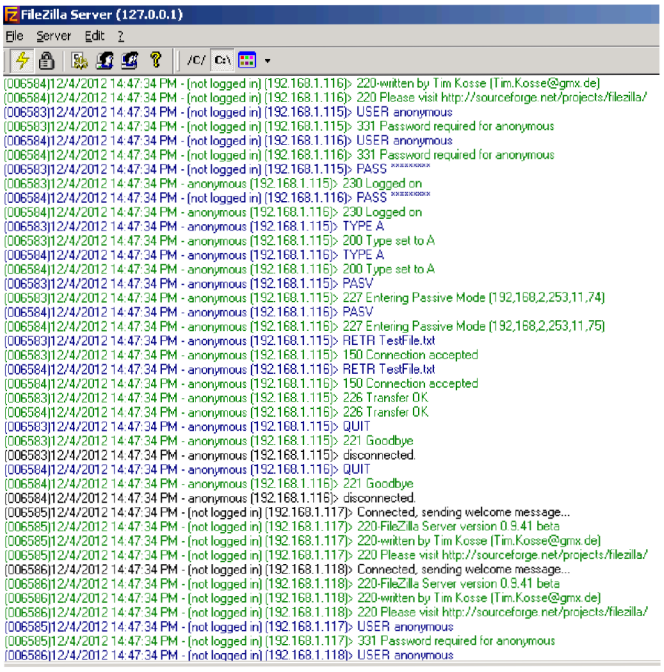
6.2.2 Monitoring servera

Obr. č. 6.14 znázorňuje log prístupov užívateľov pripájaných na FTP server FileZilla. Z logu je zrejmé, že napr. anonymný užívateľ pripájaný s adresy 192.168.1.116



Obr. 6.13: Správca úloh-vyťaženie procesora.

úspešne stiahol súbor *TestFile.txt*.



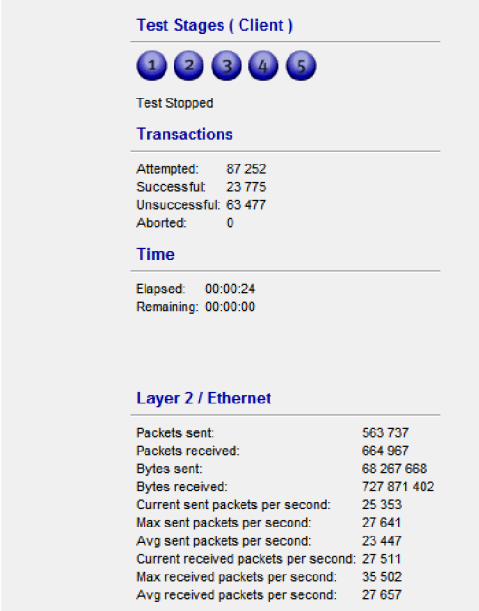
Obr. 6.14: FileZilla Server-log prístupov.

6.3 HTTP Test

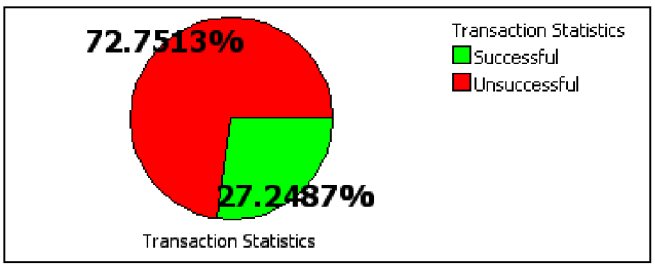
Test predstavuje generovanie definovaného počtu užívateľov pripojujúcich sa na web server Apache. Zo servera je načítaná úvodná stránka portálu *vutbr.cz* s celkovou veľkosťou 1,74MB.

Definované príkazy v *Action List*-e programu TestCenter:
1 get http://192.168.2.253/index.html

6.3.1 Výstup programu TestCenter a Results Analyzer



Obr. 6.15: TestCenter-monitoring priebehu testu.



Obr. 6.16: Results Analyzer-graf.

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								

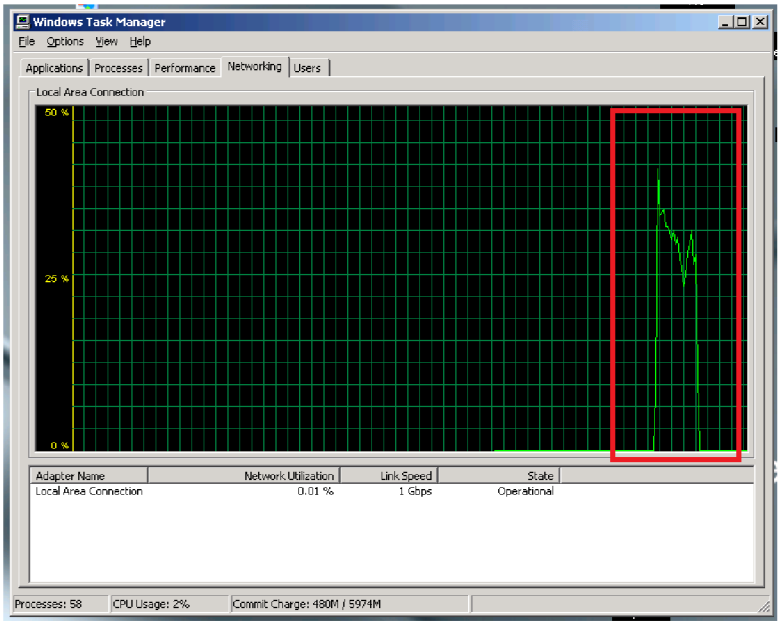
Obr. 6.17: Results Analyzer-sumár výsledkov testu.

Transaction Summary	Test	Count	Transactions (Sub-Commands included)							
	Profile	URL	Average Successful Per Second	Attempted	Successful	Unsuccessful	Aborted	Percent Successful	Percent Unsuccessful	Percent Aborted
	User_0001_0	1	990	87252	23775	63477	0	27.24	72.75	0.0
	Totals	1		87252	23775	63477	0	27.24	72.75	0.0

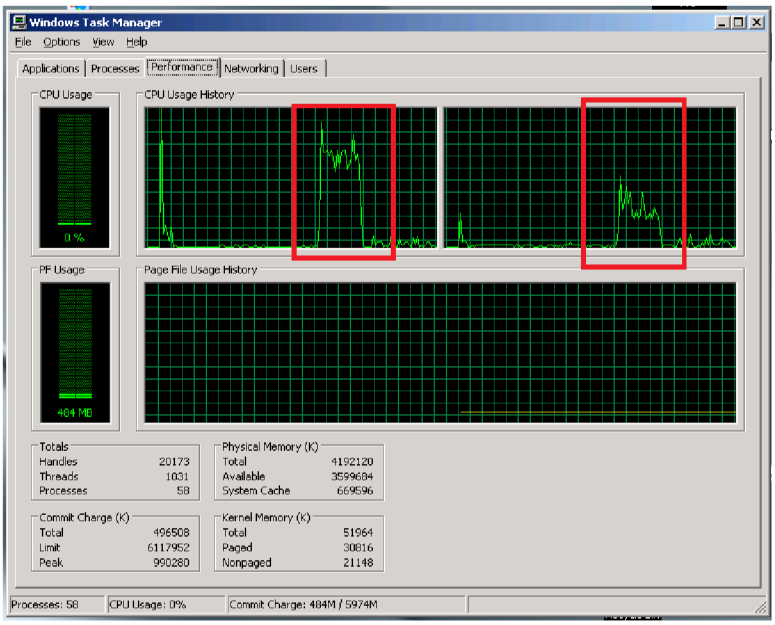
Response Time (ms)		
Minimum	Maximum	Average
1.0	9104.0	366.67

Obr. 6.18: Results Analyzer-sumár operácií.

6.3.2 Monitoring servera



Obr. 6.19: Správca úloh-vyťaženie sieťového pripojenia.



Obr. 6.20: Správca úloh-vyťaženie procesora.

Obr. č. 6.21 znázorňuje log prístupov užívateľov pripájaných na web server Apache.

```
192.168.1.96 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.172 - - [04/Dec/2012:13:38:32 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.98 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.97 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.95 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.252 - - [04/Dec/2012:13:38:32 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.25 - - [04/Dec/2012:13:38:32 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.24 - - [04/Dec/2012:13:38:32 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.71 - - [04/Dec/2012:13:38:32 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.159 - - [04/Dec/2012:13:38:32 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.162 - - [04/Dec/2012:13:38:32 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.156 - - [04/Dec/2012:13:38:32 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.174 - - [04/Dec/2012:13:38:32 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.68 - - [04/Dec/2012:13:38:32 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.157 - - [04/Dec/2012:13:38:32 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.155 - - [04/Dec/2012:13:38:32 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.111 - - [04/Dec/2012:13:38:32 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.58 - - [04/Dec/2012:13:38:23 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.90 - - [04/Dec/2012:13:38:31 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.71 - - [04/Dec/2012:13:38:29 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.70 - - [04/Dec/2012:13:38:29 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.72 - - [04/Dec/2012:13:38:29 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.74 - - [04/Dec/2012:13:38:29 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.73 - - [04/Dec/2012:13:38:29 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.219 - - [04/Dec/2012:13:38:29 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.214 - - [04/Dec/2012:13:38:29 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.215 - - [04/Dec/2012:13:38:29 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.216 - - [04/Dec/2012:13:38:29 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.218 - - [04/Dec/2012:13:38:29 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.217 - - [04/Dec/2012:13:38:29 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.203 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.204 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.202 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.205 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.206 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.248 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.5 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.252 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.2 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.253 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.4 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.240 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.246 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
192.168.1.254 - - [04/Dec/2012:13:38:30 +0100] "GET /index.html HTTP/1.1" 200 28532
```

Obr. 6.21: Apache Server-log prístupov.

7 BEZPEČNOSTNÝ TEST CISCO ASA5510

V tomto teste je na základe generátora/testera sieťovej prevádzky, ďalej len *GT*, Spirent Avalanche 3100B zistená odolnosť testovaného zariadenia, ďalej len *TZ*, firewall-u CISCO ASA5510 voči pôsobeniu útoku *DDoS SYN Flood*. V teste je realizovaný HTTP prenos web stránky o definovanej veľkosti z emulovaného HTTP servera ku emulovaným klientom podľa 2 scenárií:

1. bez pôsobenia útoku *DDoS SYN Flood*,
2. s útokom *DDoS SYN Flood*.

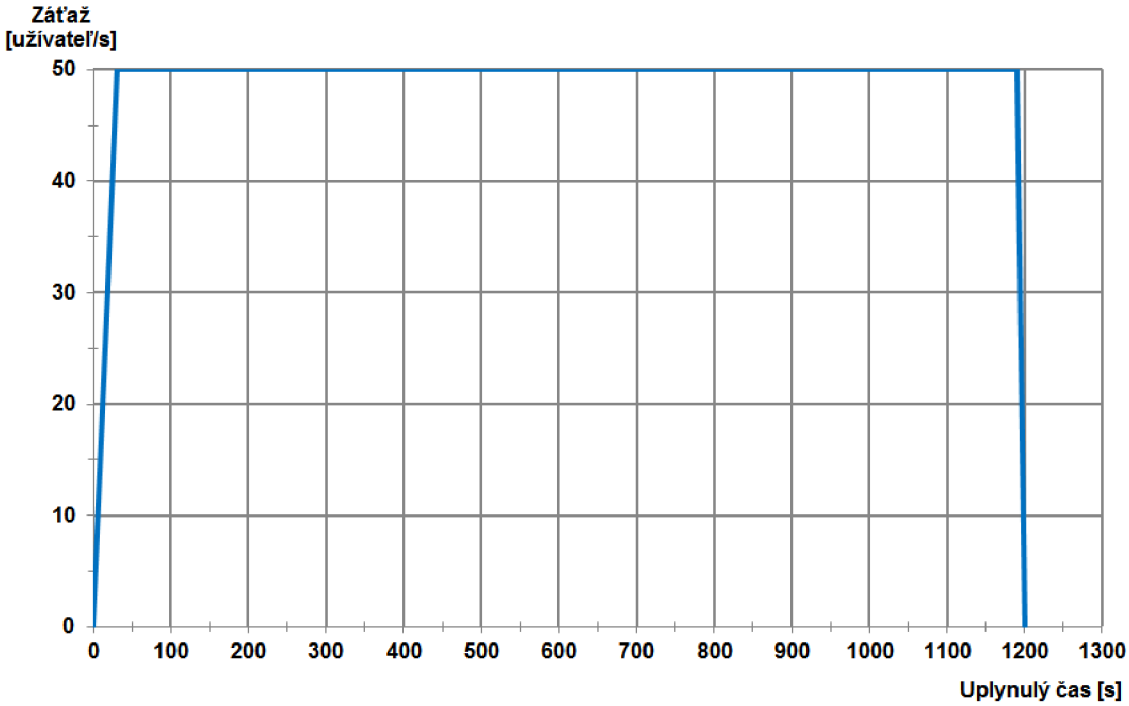
Test bez pôsobenia útoku *DDOS SYN Flood* bude nakonfigurovaný tak, aby bola zabezpečená 100% úspešnosť vykonaných HTTP transakcií od emulovaného servera ku emulovaným klientom. Tento test bude slúžiť ako referenčný bod pre test s útokom *DDoS SYN Flood*, v ktorom bude skúmaná odolnosť TZ voči útoku na základe percentuálnej úspešnosti vykonaných HTTP transakcií. Kľúčovým účelom druhého scenária testu bude zistenie maximálnej škály pôsobenia útoku, počas ktorej bude 100% úspešnosť vykonaných HTTP transakcií, t.j. TZ bude schopné útoku odolávať bez degradácie požadovanej prevádzky. Následne bude postupne zvyšovaná škála pôsobenia útoku až po hranicu úplnej degradácie požadovanej HTTP prevádzky a tak určený limit TZ.

7.1 Špecifikácia testu

GT využitím dvoch portov Gigabit Ethernet generuje sieťovú prevádzku na aplikačnom protokole HTTP. *Port0* GT je nakonfigurovaný na generovanie klientskej záťaže privátnej IPv4 siete, *Port1* GT na emuláciu HTTP servera vo verejnej IPv4 sieti, ktorý poskytuje na štandardom definovanom porte *80* web stránkový súbor. Požadovaná záťaž je definovaná na počte úžívateľov, prevádzajúcich HTTP transakciu, za jednu sekundu po dobu trvania testu a je špecifikovaná záťažovým profilom. Každým užívateľom je vykonaná HTTP transakcia len raz, t.j. načítanie(stiahnutie) web stránky je každým užívateľom vykonané 1 krát. Graf záťažového profilu zobrazuje krivku doby nábehu „*Ramp Up*“ po požadovanú záťaž počtu užívateľov za sekundu, krivku doby pretrvávajúcej záťaže „*Steady State*“ a krivku poklesu záťaže „*Ramp Down*“ na nulovú hodnotu. Graf záťažového profilu je uvedený na Obr. č. 7.1. Súhrné informácie o špecifikácií testu sú uvedené v Tab. č. 7.1.

Tab. 7.1: Špecifikácia testu.

Klient	
Priradený port GT	Port0
Rýchlosť linky	1Gb/s
Frekvencia strátovosti paketov	0%
Špecifikácia záťaže	50 užívateľov/s
Záťaž na protokole	HTTP
Adresa siete/maska	192.168.10.0/24
Adresný priestor	192.168.10.2-192.168.10.254
Server	
Priradený port GT	Port1
Rýchlosť linky	1Gb/s
Frekvencia strátovosti paketov	0%
Typ servera	Apache/2.0.49
Port servera	HTTP(80)
Max počet žiadostí na spojenie	64
Adresa siete/maska	10.10.10.0/24
Adresa servera	10.10.10.2
Zdieľaný súbor	index.html
Veľkosť súboru	566kB
Test	
Celková doba trvania testu (s)	1200
Celková doba trvania testu (hh:mm:ss)	00:20:00
Doba nábehu po požadovanú záťaž (s)	30
Doba trvania požadovanej záťaže(s)	1170
Doba ukončenia záťaže (s)	0

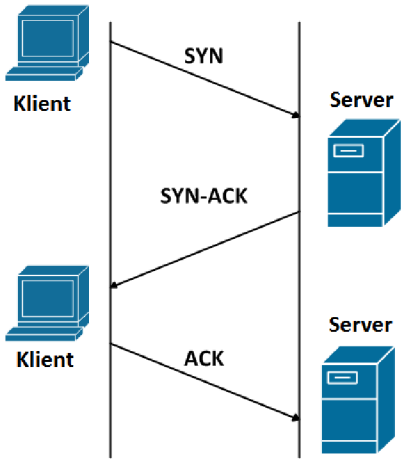


Obr. 7.1: Graf záťažového profilu.

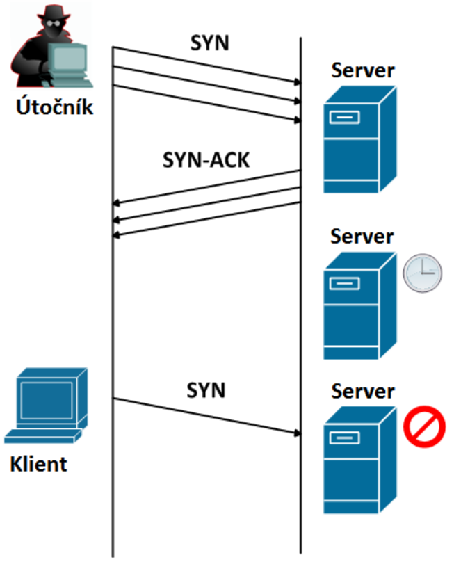
7.1.1 O útoku DDoS SYN Flood

DDoS SYN Flood je záplavový typ distribuovaného útoku odoprenia služby, ktorého cieľom je zahltenie cieľového zariadenia množstvom žiadostí paketov *SYN* nadväzujúcimi TCP spojenie. Cieľové zariadenie na tieto žiadosti odpovedá paketmi *SYN-ACK* a u jednotlivých spojení je spustený časovač, ktorý predstavuje dobu pre príjem odpovede *ACK*, vyslanej od stanice žiadosť-odosielajúcej k cieľovej stanici. Avšak odosielajúca stanica cieľovej stanici žiadnu odpoveď neposiela a preto nedochádza ku korektnému naviazaniu TCP spojenia metódou Three-Way-Handshake. Dochádza k vyčerpaniu prostriedkov cieľového zariadenia, zariadenie sa stáva zahltené a dochádza k odopreniu poskytovanej služby. Klientská stanica, ktorá je schopná korektného nadviazania TCP spojenia, na takto zahltené zariadenie nie je schopná sa pripojiť.

Schéma Three-Way-Handshake je uvedená na Obr. č. 7.2,[4]. Schéma útoku *DDoS SYN Flood* je uvedená na Obr. č. 7.3 [1].



Obr. 7.2: Korektné naviazanie TCP spojenia Three-Way-Handshake [4].



Obr. 7.3: DDoS SYN Flood [1].

7.2 Technické špecifikácie TZ

CISCO ASA5510 Adaptive Security Appliance poskytuje pokročilé bezpečnostné a sieťové služby pre malé a stredne veľké firmy, vzdialené/pobočkové kancelárie v ľahko nasaditeľnom, nákladovo efektívnom zariadení. Tieto služby môžu byť jednoducho riadené a monitorované integrovanou aplikáciou CISCO ASDM, čím sa zníži celkové nasadenie a prevádzkové náklady spojené s poskytovaním tejto vysokej úrovne bezpečnosti. ASA5510 poskytuje vysoko-výkonný firewall, VPN služby, 5 integrovaných rozhraní Fast Ethernet a 2 integrované rozhrania Gigabit Ethernet [17].

Informácie o hardware a software TZ sú uvedené v Tab. č. 7.2 a Tab. č. 7.3.

Tab. 7.2: CISCO ASA5510-Hardware.

HARDWARE	
CPU	Intel Pentium 4 @ 1600MHz
RAM	1024 MB
Flash pamäť	256MB (interná), 128MB (v slote)
Rozhrania	2x Gigabit Ethernet
	5x Fast Ethernet
Priepustnosť FW	<= 300Mbps
Max. priepustnosť FW s IPS	<= 150Mbps

Tab. 7.3: CISCO ASA5510-Software.

SOFTWARE	
OS	Cisco Adaptive Security Appliance Software
Verzia OS	v9.0(2)
Riadiaca App	Cisco Adaptive Security Device Manager
Verzia App	v7.1(2)

7.3 Konfigurácia TZ

TZ CISCO ASA5510 firewall je konfigurovaný a monitorovaný prostredníctvom *java* aplikácie CISCO ASDM v7.1(2), bežiacej na protokole HTTP. Pre prístup na TZ je nakonfigurovaný *Management port* s IPv4 adresou 192.168.1.2/24. Firewall pracuje v móde smerovača–*Routed Mode*, v ACL je povolená komunikácia na aplikačnom protokole HTTP, ostatná komunikácia je implicitne zakázaná. Nie je definované žiadne pravidlo ani obranný mechanizmus pre útoky DDoS, je len nastavená detekcia útokov pre výstupný monitoring firewall-u. Na TZ sú využité 2 rozhrania Gigabit Ethernet pre komunikáciu medzi klientami a serverom generovaných GT. *Port0* GT pre generovanie klientov je prepojený s portom TZ Ethernet0/0 a *Port1* GT pre emulovanie HTTP servera je prepojený s portom TZ Ethernet0/1.

Konfigurácia rozhraní TZ je uvedená v Tab. č. 7.4, ACL pravidlá pre prichádzajúce dáta v Tab. č. 7.5, ACL pravidlá pre odchádzajúce dáta v Tab. č. 7.6.

Tab. 7.4: ASA5510: Rozhrania

Rozhranie	**Názov**	**IP adresa**	**Maska**	**MAC adresa**
Ethernet0/0	Eth0	192.168.10.1	255.255.255.0	f684.38f2.b6fd
Ethernet0/1	Eth1	10.10.10.1	255.255.255.0	Default

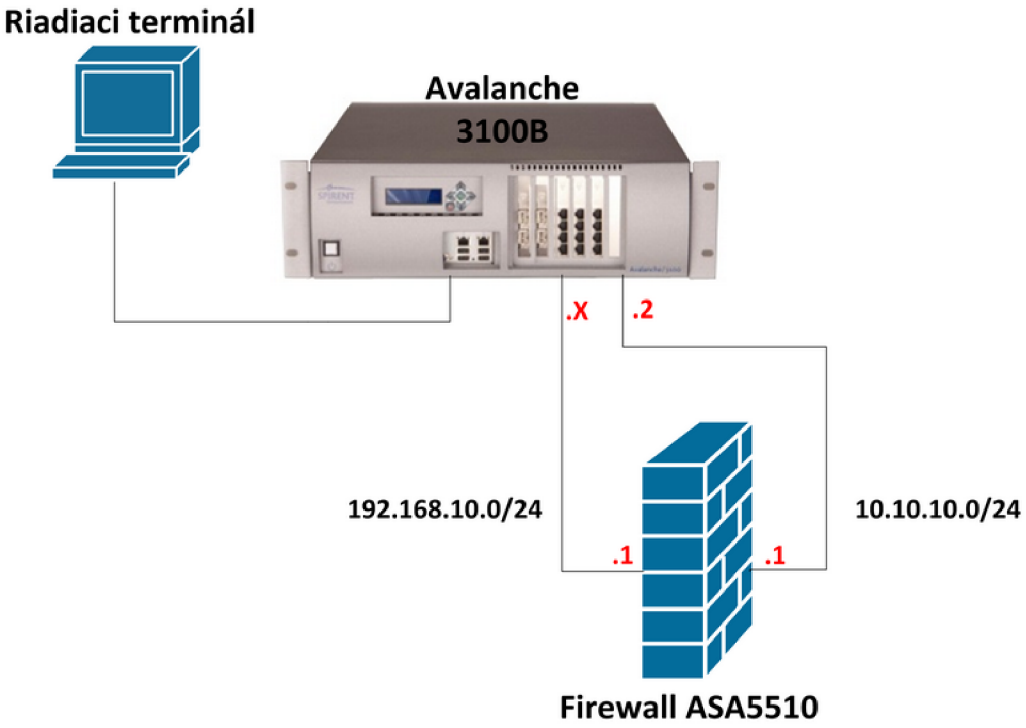
Tab. 7.5: ACL: Pravidlá pre prichádzajúce dáta

Rozhranie	**Zdroj**	**Cieľ**	**Služba**	**Akcia**
Eth0	všetko (IPv4)	všetko (IPv4)	http	Povoliť
Eth1	všetko (IPv4)	všetko (IPv4)	http	Povoliť

Tab. 7.6: ACL: Pravidlá pre odchádzajúce dáta

Rozhranie	**Zdroj**	**Cieľ**	**Služba**	**Akcia**
Eth0	všetko (IPv4)	všetko (IPv4)	http	Povoliť
Eth1	všetko (IPv4)	všetko (IPv4)	http	Povoliť

Topológia GT s pripojeným TZ spolu s popisom adries je zobrazená na Obr. č. 7.4.



Obr. 7.4: Topológia GT + TZ.

Prepojovacia kabeláž:
Na prepojenie GT s TZ boli použité 2 sieťové káble *UTP CAT6 LSZH patch cord* s dĺžkou 3,0m v súlade s ROHS a REACH/SVHC [18],[19].

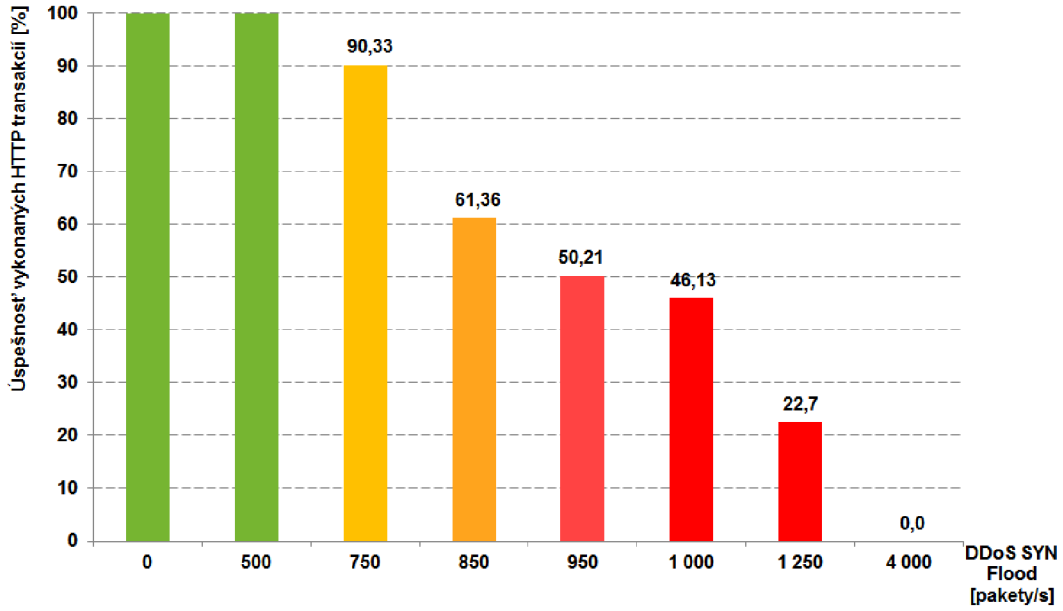
7.4 Výsledky testu TZ

Výsledky bezpečnostného testu TZ sú spracované na základe výstupu programov Spirent Avalanche Commander, Spirent Avalanche Analyzer a CISCO ASDM. V Tab. č. 7.7 sú zosumarizované hodnoty jednotlivých výsledkov testu, najprv bez útoku DDoS-nulová hodnota paketov DDoS za jednotku času, a následne s pôsobením útoku DDoS v škálach 500, 750, 850, 950, 1000 a 1250 paketov DDoS za jednotku času. V tabuľke sú uvedené transakcie prenosu web stránky od servera ku klientom v hodnotách celkového počtu uskutočnených pokusov, ďalej počtu úspešných a neúspešných pokusov prenosu web stránky, štatistika úspešnych a neúspešných pokusov za jednotku času a percentuálna úspešnosť, resp. neúspešnosť vykonaných transakcií.

Závislosť percentuálnej úspešnosti vykonaných HTTP transakcií podľa škály pôsobenia útoku DDoS bola vynesená do grafu úspešnosti vykonaných HTTP transakcií, zobrazenom na Obr. č. 7.5. Z grafu je zrejmé, že i napriek škály pôsobenia útoku *DDoS SYN Flood* o hodnote 500 paketov/s je úspešnosť vykonaných transakcií 100%. Postupným zvyšovaním škály pôsobenia útoku *DDoS SYN Flood* bolo spôsobené degradovanie úspešnosti vykonaných HTTP transakcií: pri 750 *DDoS SYN Flood* paketov za sekundu o 9,66%, pri 850 o 38,64%, pri 950 o 49,79%, 1 000 *DDoS SYN Flood* paketov za sekundu už degradovalo úspešnosť vykonaných HTTP transakcií o viac ako 50% a pri škále 1 250 paketov za sekundu o 77,3%. Pri škále 4 000 *DDoS SYN Flood* paketov za sekundu bolo TZ úplne zahltené a došlo k úplnej degradácií HTTP prenosu. Táto hodnota predstavuje limit TZ, ktorý bol zistený na základe správnosti ukazateľa prechodu TCP paketov TZ za jednotku času podľa aplikácie ASDM. Zvýšením škály pôsobenia útoku *DDoS SYN Flood* spôsobilo nekorektné informácie v monitoringu TZ a anomálie v riadení prenosu dát TZ.

Tab. 7.7: Štatistiky testu.

DDoS [pakety/s]	0	500	750	850	950	1 000	1 250
Transakcie *HTTP*							
Pokusov	59 216	59 214	59 209	59 208	59 207	59 208	59 208
Úspešných	59 216	59 214	53 488	36 332	29 729	27 318	13 444
Neúspešných	0	0	5 721	22 876	29 478	31 890	45 764
Úspešných/s	50	50	44	30	24	22	11
Neúspešných/s	0	0	4	18	24	26	37
Úspešnosť [%]	100	100	90,338	61,363	50,212	46,139	22,706
Neúspešnosť [%]	0	0	9,662	38,637	49,788	53,861	77,294



Obr. 7.5: Graf úspešnosti vykonaných HTTP transakcií.

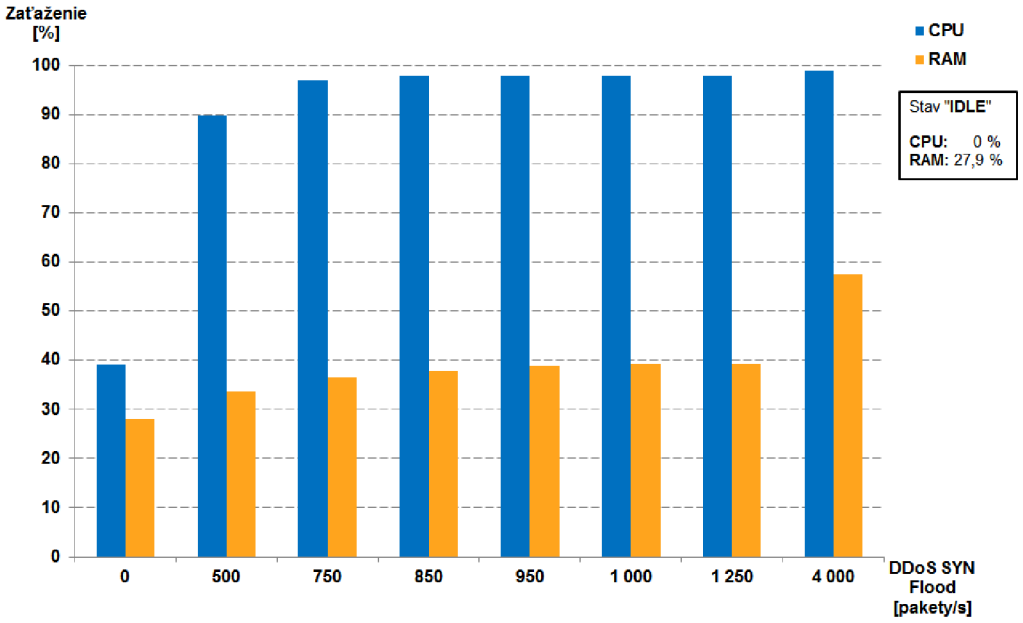
Z monitoringu TZ bol spracovaný graf percentuálneho vyťaženia CPU a pamäti RAM v jednotlivých fázach testu, uvedenom na Obr. č. 7.6. V kolonke *Stav „IDLE“* je pre názornosť uvedený stav CPU a RAM TZ v dobe nečinnosti. Uvedené hodnoty boli počas fázy testu *SteadyState* nemenné.

Hodnota vyťaženia CPU TZ bez pôsobenia útoku *DDoS SYN Flood* bola udržovaná na 39% a pamäti RAM na 28%. Pri škále pôsobenia útoku 500 *DDoS SYN Flood* paketov za sekundu došlo k nárastu vyťaženia CPU o 51% a pamäti RAM o 5,56% voči referenčnému testu bez pôsobenia útoku. Pri záťaži so škálou útoku 750 *DDoS SYN Flood* paketov za sekundu došlo k vyťaženiu CPU na 97% (nárast o 58%) a pamäti RAM na 36,43% (nárast o 8,4%). Pri škálach útoku v rozsahu 850-1250 *DDoS SYN Flood* paketov za sekundu bolo CPU TZ vyťažené na 98% (nárast o 59%) a vyťaženie pamäti RAM bol v rozahu od 37,7% do 39,4% (nárast o 9,67%-11,33%).

Maximálna škála pôsobenia útoku *DDoS SYN Flood* bez degradácie požadovanej HTTP komunikácie bola testom určená na hodnotu 500 *DDoS SYN Flood* paketov za sekundu. Limit TZ bol dosiahnutý pri škále pôsobenia útoku 4000 *DDoS SYN Flood* paketov za sekundu, počas ktorého bolo CPU TZ vyťažené na 99% a pamäť RAM na 57,52%.

Poznámka: Na základe testovania TZ bol zistený limit vyťaženia CPU na 99%, pričom 1% výkonu CPU je rezervované na monitoring a logging TZ. Z tohto dôvodu

CPU nebolo vyťažené na 100% ani pri väčšej škále pôsobenia útoku ako 4000 *DDoS SYN Flood* paketov za sekundu.

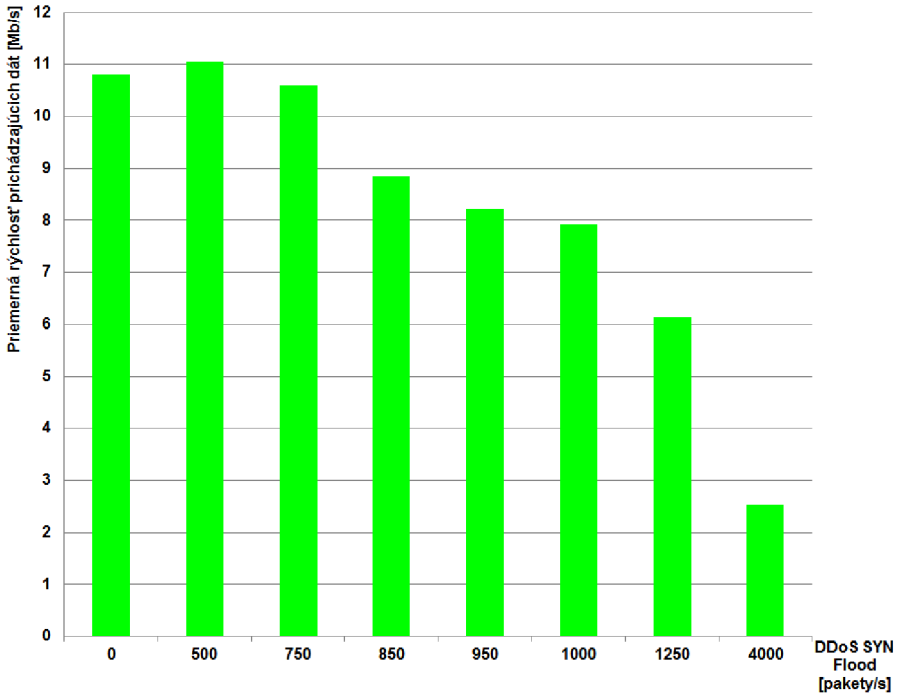


Obr. 7.6: TZ: Graf zaťaženia CPU a RAM.

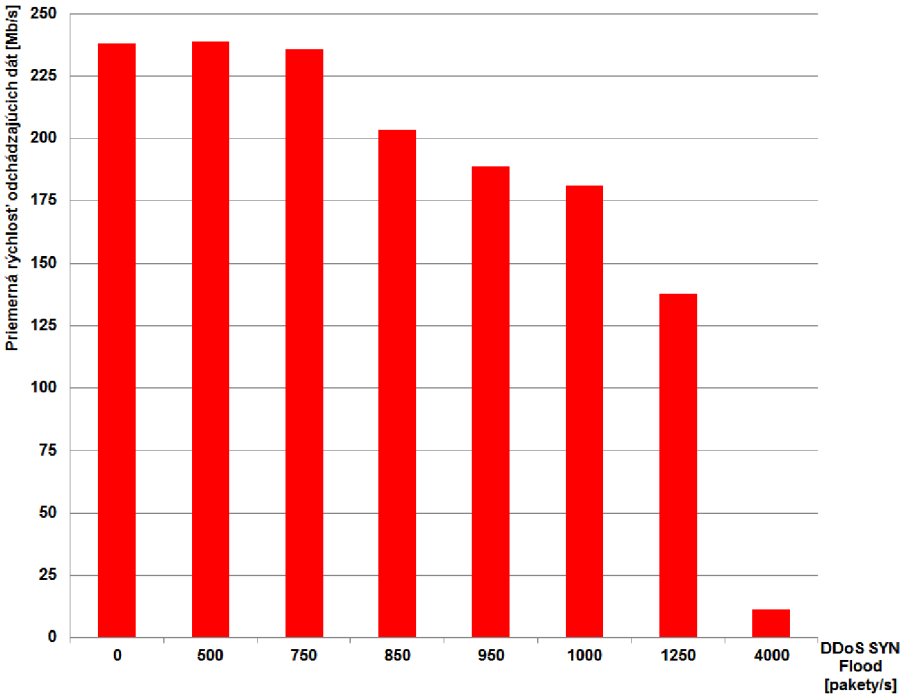
V Tab. č. 7.8 sú uvedené priemerné rýchlosti dát prichádzajúcich na HTTP server a odchádzajúcich od HTTP servera v závislosti na škále pôsobenia útoku *DDoS SYN Flood*. Tieto hodnoty sú vynesené do grafu priemernej rýchlosti dát prichádzajúcich na server, zobrazenom na Obr. č. 7.7, a grafu priemernej rýchlosti dát odchádzajúcich od servera, zobrazenom na Obr. č. 7.8.

Tab. 7.8: Server: Priemerné rýchlosti prichádzajúcich/odchádzajúcich dát

DDoS SYN Flood [pakety/s]	**Prichádzajúce dáta priem. rýchlosť [Mbps]**	**Odchádzajúce dáta priem. rýchlosť [Mbps]**
0	10,808	238,29
500	11,043	238,787
750	10,595	235,798
850	8,853	203,285
950	8,23	188,786
1000	7,925	181,252
1250	6,138	137,945
4000	2,528	11,481



Obr. 7.7: Graf priemernej rýchlosti dát Klient » Server.



Obr. 7.8: Graf priemernej rýchlosti dát Server » Klient.

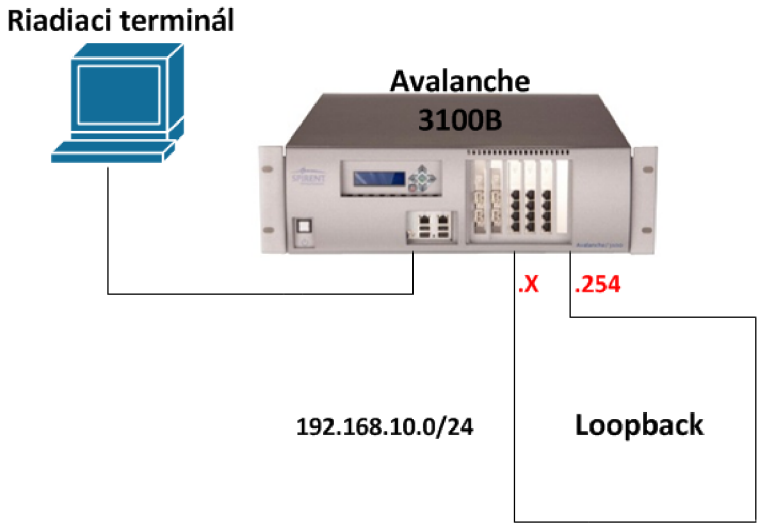
7.4.1 TZ vs. Loopback

Pre porovnanie degradácie prenosu HTTP transakcií zariadením TZ bol vykonaný test bez TZ-tzv. slučkový test „Loopback“ z portu-na-port zariadenia GT. *Port0* bol teda priamo prepojený s *Port1* GT. Rovnako ako v teste s TZ bola generovaná klientská záťaž a emulovaný HTTP server s pôsobením útoku *DDoS SYN Flood* v škále 1 250 paketov za sekundu. Bolo však nutné pozmeniť sieťovú konfiguráciu GT kôli slučkovému prepojeniu portov GT.

V skratke ku zmene konfigurácie GT:

- Použitá jedna IPv4 adresa siete, 192.168.10.0/24, kôli chýbajúcemu aktívnemu medziprvku,
- klientská časť generovaná na rozsahu IPv4 adries 192.168.10.2–192.168.10.252,
- HTTP server emulovaný na adrese 192.168.10.253,
- ostatné parametre testu nezmenené.

Topológia GT s prepojením portov spolu s popisom adries je znázornená na Obr. č.7.9.



Obr. 7.9: Topológia GT + Loopback.

V Tab. č. 7.9 sú uvedené štatistiky testu TZ a Loopback s pôsobením útoku 1 250 *DDoS SYN Flood* paketov za sekundu. Z výsledkov je zrejmé, že pri Loopback nedochádza ku žiadnej degradácií prenosu HTTP transakcií i napriek pôsobeniu útoku. Z testu vyplýva, že pri použití TZ dochádza približne k 77% degradácií prenosu HTTP prevádzky, spôsobenej hardware-ovým limitom TZ. Tento limit je

daný výkonom CPU, procesom inšpekcie prijímaných paketov na vstupnom rozhraní porovnávaním s definovaným ACL, réžiou na sieťovej vrstve spojenou so zmenou IPv4 adresy pre preposielanie paketov zo vstupného rozhrania na výstupné rozhranie a prepočtom CRC paketu.

Tab. 7.9: Štatistiky testu TZ vs Loopback.

	TZ	**Loopback**
DDoS [pakety/s]	1 250	1 250
Transakcie *HTTP*		
Pokusov	59 208	59 211
Úspešných	13 444	59 211
Neúspešných	45 764	0
Úspešných/s	11	50
Neúspešných/s	37	0
Úspešnosť [%]	22,706	100,0
Neúspešnosť [%]	77,294	0,000

7.5 Záver

V tomto bezpečnostnom teste bola zistená škála odolnosti TZ, firewall-u CISCO ASA5510 voči pôsobeniu útoku *DDoS SYN Flood*. Podľa jednotlivých výsledkov[1] testu bola 100% úspešnosť vykonaných HTTP transakcií pri škále útoku stanovenom na 500 *DDoS SYN Flood* paketov za sekundu, ktoré muselo byť TZ schopné preposielať zo vstupného portu pripojenej klientskej siete na výstupný port siete pripojeného HTTP servera. Na druhej strane, najhoršia úspešnosť vykonaných HTTP transakcií v percentuálnej hodnote 22,7% bola v škále útoku 1 250 *DDoS SYN Flood* paketov za sekundu. Limit TZ podľa škály pôsobenia útoku *DDoS SYN Flood* bol na základe monitoringu TZ stanovený na 4 000 SYN paketov za sekundu. Podľa výsledkov testu *TZ vs. Loopback* bola na TZ zistená 77% degradácia HTTP prevádzky (s pôsobením útoku 1 250 *DDoS SYN Flood* paketov za sekundu) v porovnaní s testom Loopback. Na základe tohto faktu je ovplyvnenie výsledkov TZ zariadením GT vylúčené.

[1] Po každom jednotlivom teste bolo TZ reštartované, vymazaná jeho ARP cache a boli resetované počítadlá prístupov na jednotlivé rozhrania podľa ACL.

8 BEZPEČNOSTNÝ TEST SERVER

V tomto teste je na základe generátora/testera sieťovej prevádzky, ďalej len *GT*, Spirent Avalanche 3100B zistená odolnosť testovaného zariadenia, ďalej len *TZ*, Servera voči pôsobeniu útoku *DDoS SYN Flood*. V teste je realizovaný HTTP prenos web stránky o definovanej veľkosti z TZ ku emulovaným klientom GT podľa 2 scenárií:

1. bez pôsobenia útoku *DDoS SYN Flood*,
2. s útokom *DDoS SYN Flood*.

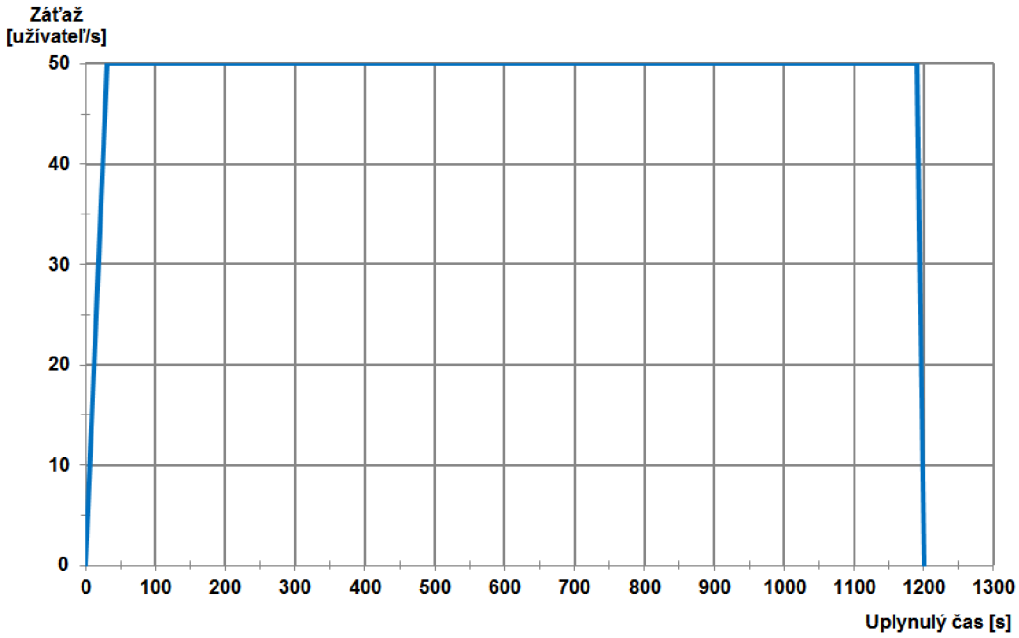
Test bez pôsobenia útoku *DDOS SYN Flood* bude nakonfigurovaný tak, aby bola zabezpečená 100% úspešnosť vykonaných HTTP transakcií od *Servera* ku emulovaným klientom. Tento test bude slúžiť ako referenčný bod pre test s útokom *DDoS SYN Flood*, v ktorom bude skúmaná odolnosť TZ voči útoku na základe percentuálnej úspešnosti vykonaných HTTP transakcií. Kľúčovým cieľom druhého scenária testu bude zistenie maximálnej škály pôsobenia útoku, počas ktorej bude 100% úspešnosť vykonaných HTTP transakcií, t.j. TZ bude schopné útoku odolávať bez degradácie požadovanej prevádzky. Následne bude postupne zvyšovaná škála pôsobenia útoku až po hranicu úplnej degradácie požadovanej HTTP prevádzky a tak určený limit TZ.

8.1 Špecifikácia testu

GT využitím jedného portu Gigabit Ethernet generuje sieťovú prevádzku na aplikačnom protokole HTTP. *Port0* GT je nakonfigurovaný na generovanie klientskej záťaže verejnej IPv4 siete. Požadovaná záťaž je definovaná na počte úžívateľov, prevádzajúcich HTTP transakciu, za jednu sekundu po dobu trvania testu a je špecifikovaná záťažovým profilom. Každým užívateľom je vykonaná HTTP transakcia len raz, t.j. načítanie(stiahnutie) web stránky je každým užívateľom vykonané 1 krát. Graf záťažového profilu zobrazuje krivku doby nábehu „*Ramp Up*“ po požadovanú záťaž počtu užívateľov za sekundu, krivku doby pretrvávajúcej záťaže „*Steady State*“ a krivku poklesu záťaže „*Ramp Down*“ na nulovú hodnotu. Graf záťažového profilu je uvedený na Obr. č. 8.1. Súhrné informácie o špecifikácií testu sú uvedené v Tab. č. 8.1.

Tab. 8.1: Špecifikácia testu.

Klient	
Priradený port GT	Port0
Rýchlosť linky	1Gb/s
Frekvencia strátovosti paketov	0%
Špecifikácia záťaže	50 užívateľov/s
Záťaž na protokole	HTTP
Adresa siete/maska	10.10.10.0/24
Adresný priestor	10.10.10.3-10.10.10.0.254
Test	
Celková doba trvania testu (s)	1200
Celková doba trvania testu (hh:mm:ss)	00:20:00
Doba nábehu po požadovanú záťaž (s)	30
Doba trvania požadovanej záťaže(s)	1170
Doba ukončenia záťaže (s)	0

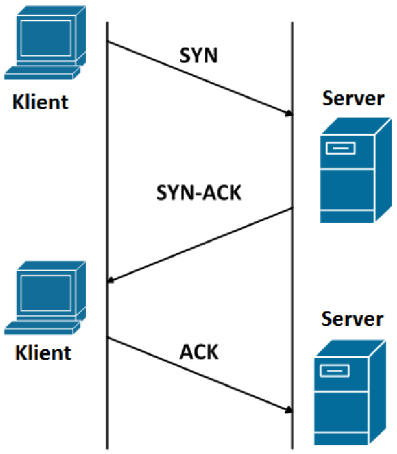


Obr. 8.1: Graf záťažového profilu.

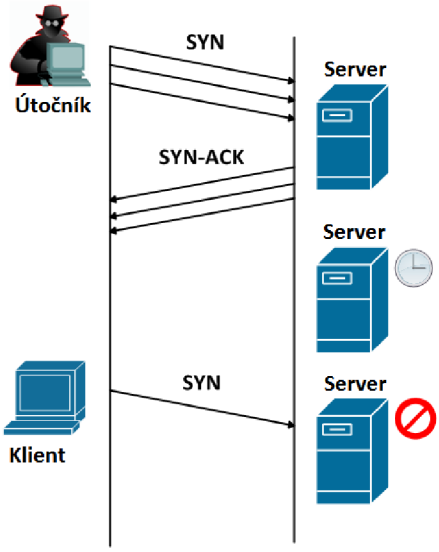
8.1.1 O útoku DDoS SYN Flood

DDoS SYN Flood je záplavový typ distribuovaného útoku odoprenia služby, ktorého cieľom je zahltenie cieľového zariadenia množstvom žiadostí paketov *SYN* nadväzujúcimi TCP spojenie. Cieľové zariadenie na tieto žiadosti odpovedá paketmi

SYN-ACK a u jednotlivých spojení je spustený časovač, ktorý predstavuje dobu pre príjem odpovede *ACK*, vyslanej od stanice žiadosť-odosielajúcej k cieľovej stanici. Avšak odosielajúca stanica cieľovej stanici žiadnu odpoveď neposiela a preto nedochádza ku korektnému naviazaniu TCP spojenia metódou Three-Way-Handshake. Dochádza k vyčerpaniu prostriedkov cieľového zariadenia, zariadenie sa stáva zahltené a dochádza k odopreniu poskytovanej služby. Klientská stanica, ktorá je schopná korektného nadviazania TCP spojenia, na takto zahltené zariadenie nie je schopná sa pripojiť. Schéma Three-Way-Handshake je uvedená na Obr. č. 8.2,[4]. Schéma útoku *DDoS SYN Flood* je uvedená na Obr. č. 8.3 [1].



Obr. 8.2: Korektné naviazanie TCP spojenia Three-Way-Handshake [4].



Obr. 8.3: DDoS SYN Flood [1].

8.2 Technické špecifikácie TZ

Server je zariadenie pre poskytovanie služieb prevažne menším firmám alebo organizáciam. Tieto služby, akými sú napríklad HTTP, FTP, IMAP, DHCP, DNS, atď., môžu byť spravované administrátorom servera prostredníctvom inštalovaných aplikácií bežiacich na inštalovanom operačnom systéme Microsoft Windows Server 2003 [20]. TZ v inštalovanej konfigurácií poskytuje HTTP služby, ktorým základ tvorí aplikácia *Apache HTTP Server*[21].

Informácie o hardware a software TZ sú uvedené v Tab. č. 8.2 a Tab. č. 8.3.

Tab. 8.2: Server-Hardware.

HARDWARE	
CPU	Intel Xeon 3040 @ 1,86GHz
RAM	4,0 GB
HDD	320 GB
NIC	HP NC320i PCIe Gigabit Server Adapter

Tab. 8.3: Server-Software.

SOFTWARE	
OS	Microsoft Windows Server 2003 Standard Edition SP2
App HTTP server	Apache 2.0.64 (x86)

Apache HTTP Server je 32bitová *open-source* aplikácia pre operačné systémy Microsoft Windows, UNIX a Mac OS, poskytujúca služby webového servera na aplikačnom protokole HTTP. Apache je od roku 1996 zaradený medzi najpopulárnejší web server, poskytujúci klientom internetové stránky [21].

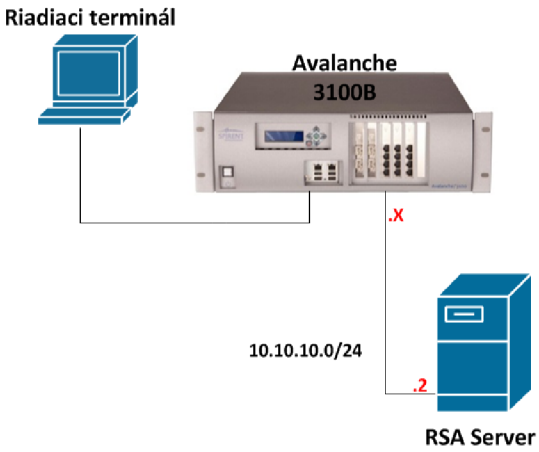
8.3 Konfigurácia TZ

TZ Server je nakonfigurovaný konfiguračným súborom *httpd.conf* aplikácie Apache 2.0.64 (x86) na poskytovanie web stránky o veľkosti 566kB, uloženej na lokálnom disku TZ. Serverom je táto služba poskytovaná na verejnej IPv4 adrese 10.10.10.2 a štandardom definovanom porte 80. Všetky konfiguračné nastavenia sú zapísané v textovej forme podľa definovaných pravidiel v súbore *httpd.conf*. Informácie o konfigurácií aplikácie *Apache* sú zhrnuté v Tab. č. 8.4.

Tab. 8.4: Apache-konfigurácia.

IP adresa/Maska	10.10.10.2/24
Port	80 (HTTP)
Poskytovaný súbor	index.html
Veľkosť súboru	566kB
Max počet žiadostí na spojenie	64

Topológia GT s pripojeným TZ spolu s popisom adries je zobrazená na Obr. č. 8.4.



Obr. 8.4: Topológia GT + TZ.

Prepojovacia kabeláž:
Na prepojenie GT s TZ boli použité 2 sieťové káble *UTP CAT6 LSZH patch cord* s dĺžkou 3,0m v súlade s ROHS a REACH/SVHC [18],[19].

8.4 Výsledky testu TZ

Výsledky bezpečnostného testu TZ sú spracované na základe výstupu programov Spirent Avalanche Commander, Spirent Avalanche Analyzer, Windows Task Manager operačného systému Microsoft Windows Server 2003 a log súborov prístupu aplikácie Apache 2.0.64 (x86). V Tab. č. 8.5 a Tab. č. 8.6 sú zosumarizované hodnoty jednotlivých výsledkov testu, najprv bez útoku DDoS-nulová hodnota paketov DDoS za jednotku času, a následne s pôsobením útoku DDoS v škálach 50 000, 100 000, 125 000, 130 000, 135 000, 135 500 a 137 000 paketov DDoS za jednotku času. V tabuľke sú uvedené transakcie prenosu web stránky od TZ ku emulovaným klientom v hodnotách celkového počtu uskutočnených pokusov, ďalej počtu úspešných a neúspešných

pokusov prenosu web stránky, štatistika úspešnych a neúspešných pokusov za jednotku času a percentuálna úspešnosť, resp. neúspešnosť vykonaných transakcií.

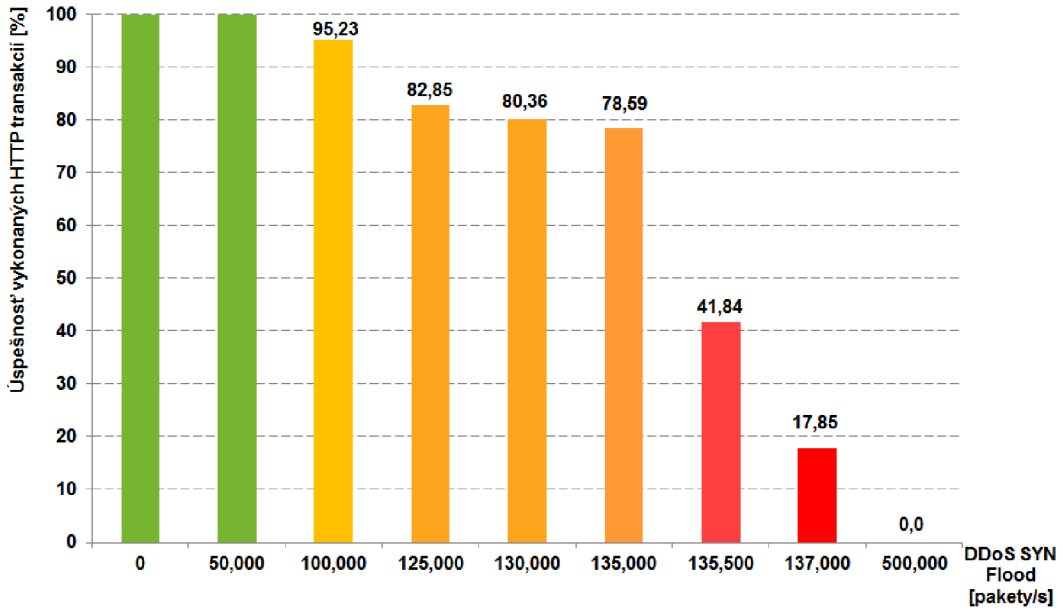
Tab. 8.5: Štatistiky testu, 1/2.

DDoS [pakety/s]	0	50 000	100 000	125 000	130 000	135 000
Transakcie *HTTP*						
Pokusov	59 216	59 206	59 204	59 203	59 203	59 203
Úspešných	59 216	59 206	56 380	49 051	47 578	46 529
Neúspešných	0	0	2 824	10 152	11 625	12 674
Úspešných/s	50	50	46	40	39	38
Neúspešných/s	0	0	2	8	9	10
Úspešnosť [%]	100	100	95,23	82,85	80,36	78,59
Neúspešnosť [%]	0	0	4,77	17,15	19,64	21,41

Tab. 8.6: Štatistiky testu, 2/2.

DDoS [pakety/s]	135 500	137 000
Transakcie *HTTP*		
Pokusov	59 202	59 201
Úspešných	24 771	10 572
Neúspešných	34 431	48 629
Úspešných/s	20	8
Neúspešných/s	28	40
Úspešnosť [%]	41,84	17,86
Neúspešnosť [%]	58,16	82,14

Závislosť percentuálnej úspešnosti vykonaných HTTP transakcií podľa škály pôsobenia útoku DDoS je vynesená do grafu úspešnosti vykonaných HTTP transakcií, zobrazenom na Obr. č. 8.5. Z grafu je zrejmé, že i napriek škále pôsobenia útoku *DDoS SYN Flood* o hodnote 50 000 paketov/s je úspešnosť vykonaných transakcií 100%. Postupným zvyšovaním škály pôsobenia útoku *DDoS SYN Flood* bolo spôsobené degradovanie úspešnosti vykonaných HTTP transakcií: pri 100 000 *DDoS SYN Flood* paketov za sekundu o 4,77%, pri 125 000 o 17,15%, pri 130 000 o 19,64%, pri 135 000 o 21,41%, 135 500 *DDoS SYN Flood* paketov za sekundu už degradovalo úspešnosť vykonaných HTTP transakcií o viac ako 50% a pri škále 137 000 paketov za sekundu o 82,14%. Pri škále 500 000 *DDoS SYN Flood* paketov za sekundu bolo TZ úplne zahltené a došlo k úplnej degradácií HTTP prenosu.



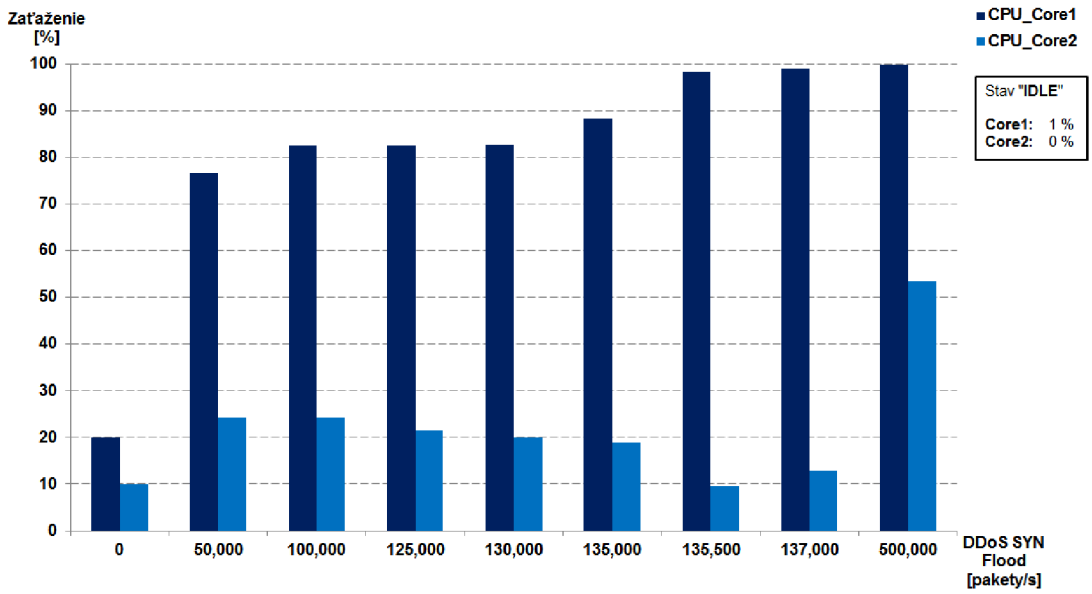
Obr. 8.5: Graf úspešnosti vykonaných HTTP transakcií.

Z monitoringu TZ bol podľa Windows Task Manager-a štatisticky spracovaný graf percentuálneho vyťaženia jadier CPU, *Core1* a *Core2*, v jednotlivých fázach testu, Obr. č. 8.6. V kolonke *Stav „IDLE“* je pre názornosť uvedený stav vyťaženia jadier CPU TZ v dobe nečinnosti.

Hodnota vyťaženia jadra CPU_Core1 bez pôsobenia útoku *DDoS SYN Flood* bola priemerne udržovaná do 20% a jadra CPU_Core2 do 10%. Pri škále pôsobenia útoku 50 000 *DDoS SYN Flood* paketov za sekundu došlo k nárastu vyťaženia CPU_Core1 o 56,7% a CPU_Core2 o 14,4% voči referenčnému testu bez pôsobenia útoku. Pri záťaži so škálou útoku 100 000 *DDoS SYN Flood* paketov za sekundu došlo k vyťaženiu CPU_Core1 do 82,6% (nárast o 62,6%), CPU_Core2 do 24,4% (nárast o 14,4%). Pri škálach útoku v rozsahu 125 000-130 000 *DDoS SYN Flood* paketov za sekundu bolo jadro CPU_Core1 vyťažené do 82,6%-82,9%, jadro CPU_Core2 do 21,5%. Škálou 135 000 bolo spôsobené vyťaženie jadra CPU_Core1 blížiacemu sa hranici 90%, jadro CPU_Core2 do 18,9%. 135 500-137 000 *DDoS SYN Flood* paketov za sekundu malo za následok vyťaženie jadra CPU_Core1 do 98,5%-99%, jadra CPU_Core2 9,6%-12,8%.

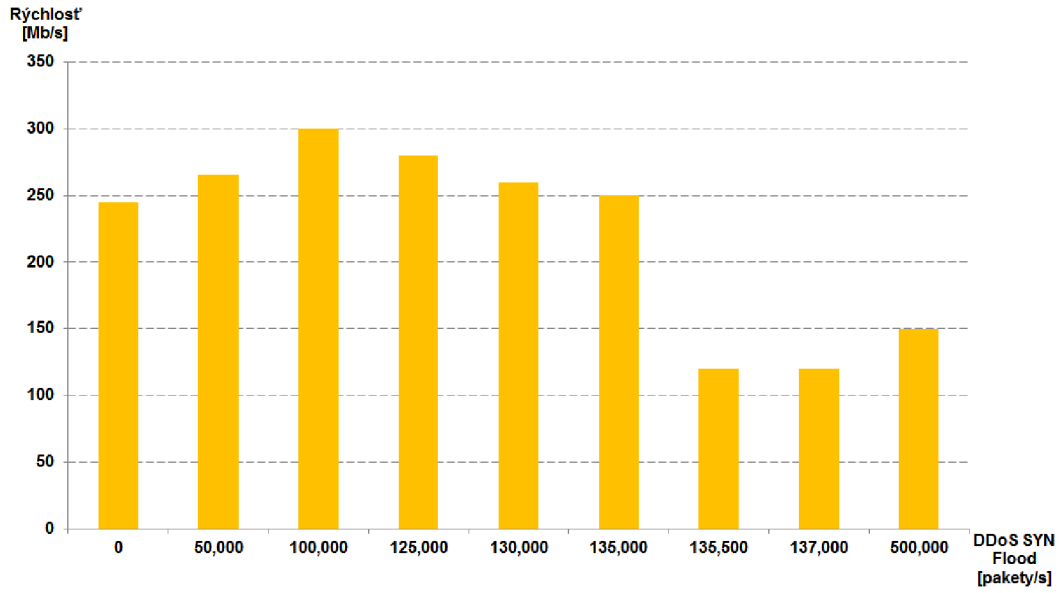
Pri škále 500 000 *DDoS SYN Flood* paketov za sekundu bolo TZ úplne zahltené, pretrvávajúce vyťaženie jadra CPU_Core1 na 100%, jadra CPU_Core2 do 54%, a došlo k úplnej degradácií HTTP prenosu. Na TZ boli pozorované oneskorené reakcie

pohybov ukazovateľa myši, prepínania sa medzi oknami a pri zachytávaní obrazovky funkciou *Print Screen*. Táto hodnota predstavuje limit TZ.



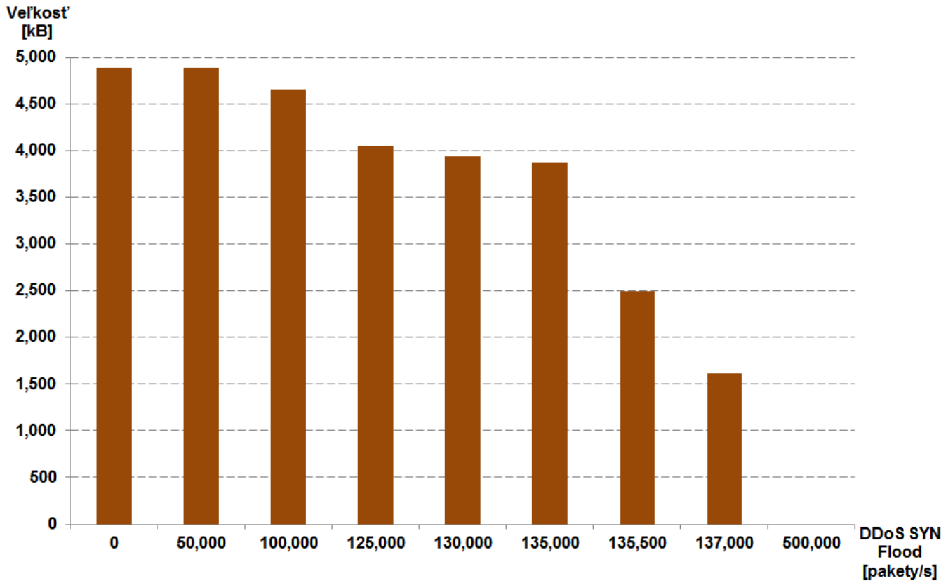
Obr. 8.6: TZ: Graf zaťaženia jadier CPU.

Z monitoringu TZ bol podľa Windows Task Manager-a štatisticky spracovaný graf sumáru rýchlostí prichádzajúcich a odchádzajúcich dát v jednotlivých fázach testu. Graf je zobrazený na Obr. č. 8.7.



Obr. 8.7: TZ: Graf sumáru rýchlosti prichádzajúcich a odchádzajúcich dát.

Podľa veľkosti súboru *access.log*, v ktorom sú zaznamenané prístupy na HTTP server, bol vypracovaný graf závislosti veľkosti tohto súboru podľa škál pôsobenia útoku *DDoS SYN Flood*. Graf je zobrazený na Obr. č. 8.8.



Obr. 8.8: Apache: Veľkosť súboru log.

Veľkosť súboru *access.log* bez pôsobenia útoku DDoS dosiahla hodnotu 4 891kB. Táto hodnota bola rovnaká aj pri škále pôsobenia útoku 50 000 *DDoS SYN Flood* paketov za sekundu. Pri zvyšovaní škály pôsobenia útoku sa veľkosť tohto súboru zmenšovala kôli zvyšovaniu percenta degradácie HTTP prenosu.

8.5 Záver

V tomto bezpečnostnom teste bola zistená škála odolnosti TZ Servera voči pôsobeniu útoku *DDoS SYN Flood*. Podľa jednotlivých výsledkov[1] testu bola 100% úspešnosť vykonaných HTTP transakcií pri škále útoku stanovenom na 50 000 *DDoS SYN Flood* paketov za sekundu, ktorému muselo TZ byť schopné odolávať bez degradácie prenosu web stránky ku emulovaným klientom. Na druhej strane, najhoršia úspešnosť vykonaných HTTP transakcií v percentuálnej hodnote 17,86% bola v škále útoku 137 000 *DDoS SYN Flood* paketov za sekundu. Limit TZ podľa škály pôsobenia útoku *DDoS SYN Flood* bol na základe monitoringu TZ stanovený na hodnotu 500 000 SYN paketov za sekundu, pri ktorom boli spôsobené oneskorené

[1]Po každom jednotlivom teste bola aplikácia Apache reštartovaná, vymazaný log súbor prístupov a reštartovaný Windows Task Manager.

reakcie operačného systému Windows 2003 Server ale nedošlo k jeho zrúteniu. Pri pôsobení tejto škály útoku by bol ešte administrátor schopný zabrániť zrúteniu OS zastavením služby HTTP aplikácie Apache HTTP Server.

9 ZÁVER

V tejto diplomovej práci boli objasnené primárne typy sieťových útokov ako rekognoskácia, získanie prístupu a útoky odoprenia služby. Podrobne boli rozobrané jednotlivé typy útokov odoprenia služby DoS, a to TCP SYN Flood, Ping of Death, LAND attack, ARP Flood, Evasive UDP, Ping Sweep, Smurf attack, ďalej Unreachable Host, Reset Flood, TCP Port Scan, Teardrop, UDP Flood, UDP Port Scan attack a XMasTree attack. Následne bol vysvetlený princíp útoku distribuovaného odoprenia služby DDoS s uvedenými príkladmi. V praktickej časti diplomovej práce bola navrhnutá laboratórna sieťová infraštruktúra pre testovanie jednotlivých typov bezpečnostných hrozieb. Táto ifraštruktúra bola realizovaná prvkami: firewall CISCO ASA5510, Server, klientský počítač a smerovač MikroTik RouterBoard 1200.

V práci boli vypracované 2 vzorové protokoly o vykonaní bezpečnostného testu odolnosti sieťových prvkov, konkrétne firewall-u CISCO ASA5510 a Servera, voči pôsobeniu útoku distribuovaného odoprenia služby *DDoS SYN Flood*. Na základe výsledkov jednotlivých testov boli určené limity testovaných zariadení podľa škály pôsobenia útoku *DDoS SYN Flood*.

Škála odolnosti firewall-u CISCO ASA5510 voči pôsobeniu útoku *DDoS SYN Flood* bez degradácie úspešnosti vykonaných HTTP transakcií, bola stanovená na 500 *DDoS SYN Flood* paketov za sekundu. Limit tohto zariadenia podľa škály pôsobenia útoku *DDoS SYN Flood* bol na základe monitoringu stanovený na 4 000 *DDoS SYN Flood* paketov za sekundu. Zvýšením škály pôsobenia útoku spôsobilo nekorektné informácie v monitoringu firewall-u a anomálie v riadení prenosu dát týmto firewall-om. Škála odolnosti Serveru voči pôsobeniu útoku *DDoS SYN Flood* bez degradácie úspešnosti vykonaných HTTP transakcií, bola stanovená na 50 000 *DDoS SYN Flood* paketov za sekundu. Limit tohto zariadenia podľa škály pôsobenia útoku *DDoS SYN Flood* bol na základe monitoringu stanovený na 500 000 *DDoS SYN Flood* paketov za sekundu, pri ktorom boli spôsobené oneskorené reakcie operačného systému ale nedošlo k jeho zrúteniu. Pri pôsobení tejto škály útoku by bol ešte administrátor schopný zabrániť zrúteniu OS zastavením služby HTTP aplikácie Apache HTTP Server.

Z výsledkov testov je zrejmé, že firewall CISCO ASA5510 dokáže odolávať podstatne nižšej škále pôsobenia útoku *DDoS SYN Flood* v porovnaní so Serverom. Limit firewall-u je daný hlavne procesom inšpekcie prijímaných paketov na vstupnom rozhraní porovnávaním s definovaným ACL, réžiou na sieťovej vrstve spojenou so zmenou IPv4 adresy pre preposielanie paketov zo vstupného rozhrania na výstupné rozhranie a prepočtom CRC paketu. U Servera tieto procesy odpadajú a preto je jeho limit rádovo vyšší.

LITERATÚRA

[1] BARKER, Keith a Scott MORRIS. *CCNA Security 640-554 official cert guide*. 1. vyd. Indianapolis, Ind: Cisco Press, 2012. ISBN 15-872-0446-0.

[2] *Online Ping, Traceroute, DNS lookup, WHOIS, Port check, Reverse lookup, Proxy checker, Bandwidth meter, Network calculator, Network mask calculator, Country by IP, Unit converter: Ping* [online]. © 2013 [cit. 20. 05. 2013]. Dostupné z URL:<`http://ping.eu/ping/`>.

[3] *Wireshark · Go Deep.* [online]. © 2013 [cit. 20. 05. 2013]. Dostupné z URL: <`http://www.wireshark.org/`>.

[4] MARK A. DYE, Mark A.Rick McDonald. *Network fundamentals: CCNA exploration companion guide*. Indianapolis, Ind: Cisco Press, 2012. ISBN 15-871-3348-2.

[5] The Internet Engineering Task Force. *RFC: 793 Transmission Control Protocol* [online]. [cit. 10. 12. 2012]. Dostupné z URL:<`http://www.ietf.org/rfc/rfc793.txt`>.

[6] SCAMBRAY, Joel, Stuart MCCLURE a George KURTZ. *Hacking bez tajemství*. 2. vyd. Praha: Computer Press, 2002. ISBN 80-7226-644-6.

[7] *ISO - ISO Standards - ICS 35.100: Open systems interconnection (OSI)* [online]. [2013] [cit. 20. 05. 2013]. Dostupné z URL:<`http://www.iso.org/iso/products/standards/catalogue_ics_browse.htm?ICS1=35&ICS2=100&`>.

[8] Denial of Service Attacks. CERT: Software Engineering Institute [online]. 1997, 04.06.2001 [cit. 10. 12. 2012]. Dostupné z URL: <`http://www.cert.org/tech_tips/denial_of_service.html`>.

[9] *Spirent - A leader in test, measurement and service assurance solutions*[online]. © 2013 [cit. 20. 05. 2013]. Dostupné z URL:<`http://www.spirent.com/`>.

[10] SPIRENT COMMUNICATIONS, Inc. *Spirent Avalanche: The Layer 4-7 Application Online Help*. ©2012.

[11] Ping of Death. Javvin: *Network management & security* [online]. [cit. 10. 12. 2012]. Dostupné z URL: <`http://www.javvin.com/networksecurity/PingDeath.html`>.

[12] Land Attack. Javvin: *Network management & security* [online]. [cit. 10. 12. 2012]. Dostupné z URL: <http://www.javvin.com/networksecurity/LandAttack.html>.

[13] ARP Poisoning. Javvin: *Network management & security* [online].[cit. 10. 12. 2012]. Dostupné z URL:<http://www.javvin.com/networksecurity/ARPPoisoning.html>.

[14] Spirent Discussion Forums: Spirent Forums [online]. 2012 [cit. 20. 05. 2013]. Dostupné z URL:<http://forums.spirent.com/index.html>.

[15] *Windows 7 - Microsoft Windows* [online]. © 2013 [cit. 20. 05. 2013]. Dostupné z URL:<http://windows.microsoft.com/cs-CZ/windows7/products/home>.

[16] *RouterBoard.com : RB1200*[online]. [2013] [cit. 20. 05. 2013]. Dostupné z URL:<http://routerboard.com/RB1200>.

[17] Cisco ASA 5500 Series Next Generation Firewalls: *Cisco ASA 5510 Adaptive Security Appliances* [online]. [cit. 20. 05. 2013]. Dostupné z URL:<http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html>.

[18] ROHS2. *RoHS compliance: BOMcheck.net* [online]. [cit. 20. 05. 2013]. Dostupné z URL:<https://www.bomcheck.net/rohs>.

[19] REACH. *REACH compliance: BOMcheck.net* [online]. [cit. 20. 05. 2013]. Dostupné z URL:<https://www.bomcheck.net/reach>.

[20] *Microsoft Windows Server: Windows Server 2003 technical documentation, downloads, and additional resources* [online]. © 2013 [cit. 20. 05. 2013]. Dostupné z URL:<http://technet.microsoft.com/en-us/windowsserver/bb512919.aspx>.

[21] *Apache Software Foundation: Apache HTTP Server* [online]. ©1999-2013 [cit. 20. 05. 2013]. Dostupné z URL:<http://projects.apache.org/projects/http_server.html>.

ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK

DoS Denial of Service (Odoprenie služby)

DDoS Distributed Denial of Service (Distribuované odoprenie služby)

GT Generátor/Tester

FW Firewall

TZ Testované zariadenie

ZOZNAM PRÍLOH

A PRILOŽENÉ CD

Na priloženom kompaktnom disku sa nachádzajú zdrojové súbory programu LaTeX pre kompiláciu elektronickej verzie diplomovej práce a výstupný súbor „*.pdf*“ tejto práce.