VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

BEZPEČNOSTNÍ ANALÝZA FIREWALLU
FIREWALL SECURITY ANALYSIS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Josef Cigánek**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Jan Hajný, Ph.D.**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Josef Cigánek ***ID:*** 174174
Ročník: 3 ***Akademický rok:*** 2016/17

NÁZEV TÉMATU:

Bezpečnostní analýza firewallu

POKYNY PRO VYPRACOVÁNÍ:

Cílem projektu je provedení kompletní bezpečnostní analýzy hardwarového firewallu a provedení testů výkonosti firewallu. Výstupem práce bude testovací prostředí pro odposlech veškeré komunikace firewallu, analýza platformy, nastavení firewallu a realizace scénářů testování výkonosti firewallu na 10 GbE rozhraní.

DOPORUČENÁ LITERATURA:

[1] CASEY, Eoghan. Digital evidence and computer crime: forensic science, computers and the Internet. 3rd ed. Amsterdam: Elsevier, c2011. ISBN 978-0-12-374268-1.

[2] Hillstone Documentation [online]. 2016 [cit. 2016-09-12]. Dostupné z: http://www.hillstonenet.com/resources/

Termín zadání: 1.2.2017 ***Termín odevzdání:*** 8.6.2017

Vedoucí práce: doc. Ing. Jan Hajný, Ph.D.
Konzultant:

doc. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Bakalářská práce pojednává o tématu bezpečnostní a výkonnostní analýzy firewallů. Hlavním úkolem je vytvoření testovacího prostředí pro odposlech veškeré komunikace firewallu a na základě zvolených metod provést bezpečnostní analýzu hardwarového firewallu a dle navržených scénářů provést testy výkonnosti firewallu pomocí zařízení Spirent Avalanche. Teoretická část práce seznamuje čtenáře s problematikou firewallů, bezpečnostního auditu a penetračního testování. Následující praktická část obsahuje komentované výsledky zvolených bezpečnostních a výkonnostních analýz aplikovaných v laboratorním prostředí na hardwarových firewallech Hillstone SG-6000-G2120 a SG-6000-M7260.

KLÍČOVÁ SLOVA

Firewall, Hillstone, bezpečnostní analýza, zátěžové testování, Spirent Avalanche.

ABSTRACT

The bachelor essay is about security analysis and stress testing of firewalls. The main goal is to create a testing environment for eavesdropping of all communication of the firewall, on the principal of security analysis of the hardware firewall and stress testing with device Spirent Avalanche. The theoretical part of the essay is informing the readers about the problems surrounding firewall, security audits and penetration tests. The following practical part consists of commenting on the results of chosen security analysis and stress testing, applied in a laboratory for the hardware firewalls Hillstone SG-6000-G2120 and SG-6000-M7260.

KEYWORDS

Firewall, Hillstone, security analysis, stress testing, Spirent Avalanche.

CIGÁNEK, Josef *Bezpečnostní analýza firewallu*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2016. 71 s. Vedoucí práce byl doc. Ing. Jan Hajný, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Bezpečnostní analýza firewallu“ jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor(ka) uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil(a) autorská práva třetích osob, zejména jsem nezasáhl(a) nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom(a) následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora(-ky)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu doc. Ing. Janu Hajnému, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

podpis autora(-ky)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic
http://www.six.feec.vutbr.cz

PODĚKOVÁNÍ

Výzkum popsaný v této bakalářské 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(-ky)

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OP Výzkum a vývoj
pro inovace

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

V dnešní době, kdy je každodenní využívání internetového připojení samozřejmostí, je síťová bezpečnost stále častěji diskutované téma. Nebezpečí v podobě internetového útoku nebo počítačových virů na nás číhá téměř na každém rohu. Typickým řešením k ochraně síťové bezpečnosti je použití bezpečnostního prvku - firewallu. Pouhé zakoupení a zapojení firewallu náš problém s bezpečností nemusí zcela vyřešit. Důležitá je správná konfigurace a pravidelný bezpečnostní audit firewallu.

Na začátku své bakalářské práce čtenáře seznámíme s obecnou definicí firewallu a představím známé typy a dělení firewallů.

Druhá část je zaměřena na teorii bezpečnostních auditů a penetračního testování. Nalezneme zde také stručný popis aplikací, které se nejčastěji využívají právě k bezpečnostnímu testování firewallů.

Další část práce představuje a popisuje zvolené metody pro bezpečnostní analýzu a navržené scénáře pro výkonnostní testování. Následuje popis testovacího prostředí realizovaného v laboratoři a stručné seznámení a charakteristika testovaných firewallů Hillstone SG-6000-G2120 a SG-6000-M7260 a také testovacího zařízení pro zátěžové testování Spirent Avalanche 3100.

Praktická část práce obsahuje konečné výsledky zvolených metod bezpečnostní a výkonnostní analýzy firewallů.

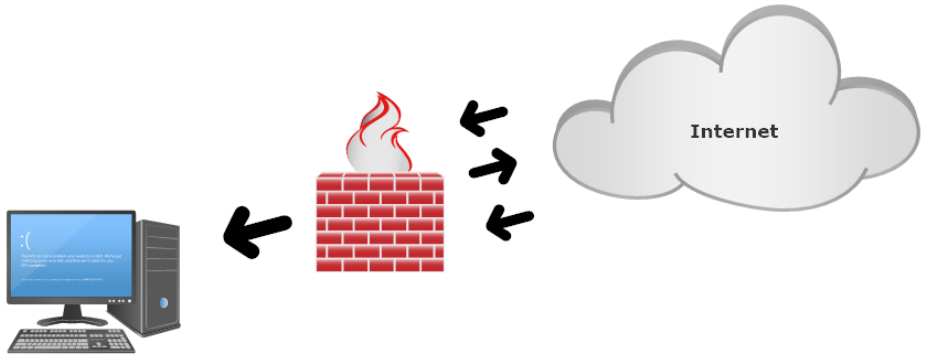
1 SEZNÁMENÍ S FIREWALLY

V následující kapitole čtenáře pro pochopení základních souvislostí bezpečnostních analýz firewallu seznámíme s obecnou definicí firewallu, principy a typy používaných firewallů.

1.1 Definice firewallu

Firewally jsou považované za nejdůležitější bezpečnostní prvky sloužící k řízení a zabezpečení síťového provozu. Jedná se o softwarové programy nebo hardwarová zařízení, která filtrují a řídí datový provoz.

Princip (viz obr. 1.1) je takový, že se na firewallu nadefinují pravidla, podle kterých je následně řízena komunikace mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení, které firewall odděluje. Paket vstupující na rozhraní firewallu je na základě vyhodnocení pravidel bezpečnostní politiky zamítnut, zahozen nebo odeslán na výstupní rozhraní. Primárním účelem firewallů je tedy zabránění neoprávněným průnikům do naší sítě nebo nechtěným odeslání dat ven ze sítě [1],[2].



Obr. 1.1: Principiální schéma umístění firewallu

1.2 Rozdělení firewallů

Firewally obecně lze rozdělit podle mnoha kritérií. Nejčastěji se typy firewallů dělí podle toho, na jakém principu jsou založeny, na které vrstvě síťového modelu pracují nebo podle platformy.

1.2.1 Rozdělení podle funkce

Nestavový firewall (paketový filtr)

Jedná se o nejstarší a zároveň nejjednodušší formu firewallu. Poprvé byl definován v roce 1988, kdy inženýři ze společnosti DEC (Digital Equipment Corporation) vyvinuli filtrační systém, známý jako paketový filtr.

Jeho princip spočívá v přesně definovaných pravidlech, která určují z jaké adresy a portu na kterou adresu a port může být procházející paket doručen. Pokud paket neodpovídá nastaveným filtrovacím pravidlům filtru, bude takový paket odmítnut a zahozen. Naopak v případě, že paket odpovídá naprogramovanému filtru, tak je komunikace povolena a paket firewallem projde. V případě nestavových firewallů se kontrola provádí na třetí a čtvrté vrstvě modelu síťové komunikace OSI.

Výhoda nestavového paketového filtru je ve vysoké rychlosti zpracování. Z tohoto důvodu se využívá zpravidla u vysokorychlostních přenosů velkého množství dat a tam, kde není kladen velký důraz na přesnost a kontrolu dat. Nevýhodou tedy můžeme považovat nízkou úroveň kontroly procházejících spojení, která u složitějších protokolů může být označena za nedostačující [1],[2].

Stavový firewall (stavový paketový filtr)

Stavový firewall je známý jako filtr druhé generace. Na jeho vzniku měli zásluhu kolegové Dave Presotto, Janardan Sharma a Kshitij Nigamz ze společnosti AT & T Bell Laboratories.

Stavový paketový filtr v podstatě vykonává práci předešlého paketového filtru s tím rozdílem, že dokáže pracovat až na 4. vrstvě referenčního modelu OSI. Stavový filtr je schopen udržet pakety v paměti. V paměti jsou pakety drženy tak dlouho, dokud o nich nemá k dispozici dostatek informací k rozhodnutí o jeho následném zařazení. Filtr také zaznamenává všechna procházející spojení a určuje, zda je paket částí stávajícího spojení, nebo se jedná o spojení nové.

Na rozdíl od nestavových paketových filtrů se zvýšila bezpečnost a rychlost kontroly [1],[2].

Aplikační brány

Aplikační brány, označované také jako proxy brány, zcela oddělují sítě, mezi které jsou postaveny. Aplikační brány provádí analýzu paketů na aplikační vrstvě s detailní znalostí konkrétního protokolu a proto mají k rozhodování mnohem více informací. Díky tomu je zřejmé, že jsou aplikační brány považovány za mnohem bezpečnější řešení.

Pro realizaci takové úrovně ochrany musí firewally vstoupit do probíhající komunikace jako prostředník spojení. Všechny uživatelské aplikace komunikují přímo s aplikační branou, nikoliv se skutečnými příjemci, které danou službu poskytují. S příjemci komunikuje právě až bezpečnostní brána, která veškerou komunikaci kontroluje a zabraňuje vykonání nepovolených operací.

Výhodou principu aplikační brány můžeme považovat fakt, že povoluje jen spojení, pro které existuje proxy a vše ostatní blokují. Dále také možnost analýzy a filtrace obsahu paketu. Nevýhodou je zpomalení přenosu dat, které je zapříčiněno dvojí komunikací (síť-proxy, proxy-klient).

Aplikační brány jsou typicky implementovány jako software, jelikož jejich hardwarová implementace je velice náročná [1],[2],[3].

Firewally s kontrolou protokolů a IDS

Nová verze firewallů, označující se jako firewally s hloubkovou inspekcí, podporují mimo stavové kontroly i IDS (Intrusion Detection Systems). Prakticky se jedná o systémy detekce očekávaných útoků, které pracují na podobném principu jako antiviry. Tyto systémy jsou schopné pomocí databáze známých signatur útoků, skenování adresního rozsahu a dalších metod odhalit u zdánlivě korektních spojení vzorce nebezpečných útoků.

Výhodou takových systémů je bezesporu vysoká úroveň bezpečnosti kontroly procházejících protokolů při poměrně vysoké rychlosti kontroly. Oproti klasickým paketovým filtrům je však rychlost zpracování pomalejší [1],[4].

1.2.2 Rozdělení podle platformy

Softwarové firewally

Za softwarový firewall považujeme bezpečnostní software nainstalovaný na osobním počítači, nebo serveru, na kterém však běží i jiné programy a služby. Výhodou takového řešení jsou nízké pořizovací náklady. Pro realizaci můžeme v některých případech využít i zdarma nabízený software a přizpůsobit si ho podle svých představ. Z tohoto důvodu je toto řešení často aplikováno v domácnostech, kde může ve spojení s antivirem, poskytovat dostačující ochranu [3].

Příkladem tohoto řešení jsou:

- Kerio Control,
- Comodo Firewall,
- Oracle SunScreen.

Hardwarové firewally

Hardwarový firewall v podstatě není nic jiného než softwarový firewall, běžící na pro něj vyhrazeném hardwaru. Obrovskou výhodou hardwarového firewallu je to, že hardware oddělí chráněný počítač od zbytku sítě a tím zajistí jeho ochranu. Mnohé z těchto zařízení obsahují i switch, který umožní bez jakýchkoliv dalších nákladů bezpečně propojit více zařízení do sítě.

Výhodu najdeme především v rychlosti, nezávislosti na operačním systému a vyšší poskytované bezpečnosti. Dražší a výkonnější hardwarové firewally najdeme především ve větších firmách a společnostech, kde je kladen velký důraz na bezpečnost [3].

2 TEORIE BEZPEČNOSTNÍ ANALÝZY

V následující kapitole se seznámíme s pojmy bezpečnostního auditu a penetračního testování. Dále bude upřesněno, proč je důležité tyto analýzy vypracovávat a také budou představeny programy sloužící k penetračnímu testovaní firewallu.

2.1 Bezpečnostní audit

Audit se zabývá objektivním vyhodnocením faktu, zda je bezpečnostní charakteristika konkrétního systému v souladu s platnou legislativou nebo s požadavky jeho vlastníků. Audity provádí nezávislí auditoři. S kontrolou informací a událostí je prováděna i analýza rizik s následným vyhodnocením.

Výsledkem bezpečnostního auditu je souhrnný dokument, popisující současný bezpečnostní stav s možnostmi jeho nápravy [2],[5].

Motivace bezpečnostních auditů firewallu

Jak už jsme si mohli přečíst v předchozí kapitole, firewally se již řadu let starají o bezpečnost sítí. Z počátku se používaly jednoduché paketové filtry, které pomocí malého souboru pravidel řídily provoz v síti. Postupem času však začal exponenciální růst síťových provozů a sítí s podporou nových aplikací, webových služeb a nástrojů, které se výrazně projevili na množství možných pravidel firewallu a jeho různých nastavení.

Udržení správné konfigurace pravidel firewallu je obtížný úkol i pro zkušené správce sítě. Jediná chyba v konfiguraci firewallu, může mít za následek obrovské ohrožení bezpečnosti chráněné sítě, které může vést k obrovským ztrátám.

Aby se zabránilo negativním dopadům podobných problémů, musí správci firewallu často firewally a pravidla kontrolovat, měnit jejich nastavení a konfiguraci s cílem zajistit požadovanou bezpečnost. Pravidelný bezpečnostní audit firewallů se tak stal nedílnou součástí práce administrátorů. Frekvence vykonávání bezpečnostních auditů je možné popsat slovy „čím častěji, tím lépe“. V praxi je však důležité najít rozumný kompromis mezi četností a přínosem konání bezpečnostních auditů [2],[3],[5].

2.2 Penetrační testování

Penetrační testy mají za úkol prověřit úroveň zabezpečení síťového prostředí a jsou nedílnou součástí bezpečnostních analýz. Využívají různé techniky pokusů o proniknutí do testovaných systémů pomocí nástrojů, které simulují reálný útok. Tato

činnost je označována jako takzvaný „etický hacking“, který nemá za cíl uškodit, ale naopak pomoci zvýšit míru zabezpečení nalezením zranitelnosti systému. Pomocí penetračních testů jsou auditoři schopni zjistit, jakým způsobem se testovaný systém při určitých útocích zachová. Výsledkem penetračních testů je posudek o odhalených slabinách v zabezpečení systému, který vede k nápravě bezpečnostních chyb a nedostatků. Je důležité zmínit fakt, že penetrační testy nám nikdy nezaručí 100% bezpečnost. Není totiž zaručeno, že případný útočník nenalezne nový způsob útoku, který nebyl součástí obsáhlého penetračního testování. Ale i přesto, jsou penetrační testy velice ceněné, jelikož se jedná o nejreálnější způsob otestovaní bezpečnosti systémů [3],[6].

Penetrační testovaní lze rozdělit podle několika aspektů [6]:

- Způsob provedení:
  - Manuální testy – manuálně vykonávané specifické testy.
  - Automatizované testy – testování pomocí již vytvořených testovacích nástrojů.
  - Semiautomatizované testy – kombinace výše zmíněných typů testování.
- Úroveň znalostí o testovaném systému:
  - Black-box testy – test neznámého systému, ke kterému jsou známé zpravidla jen vstupy a výstupy.
  - White-box testy – test systému, ke kterému jsou k dispozici všechny potřebné informace.
  - Grey-box testy – kombinace výše zmíněných typů.

K penetračnímu testování existuje řada nástrojů i hotových linuxových distribucí:

Kali Linux

Kali je linuxová distribuce využívající architektury Debianu, která je navržená výhradně pro penetrační testování. První verze Kali 1.0.0 byla vydána 13. března 2013 jako přímý nástupce distribuce BackTrack 5R3. Obě bezpečnostní distribuce pochází z dílny vývojářů společnosti Offensive Security. V době psaní této bakalářské práce je aktuální verze Kali Linux 2016.2 vydaná 31. srpna 2016.

Kali linux, stejně jako Backtrack jsou velice uznávané systémy doslova napěchované celou řadou textových i grafických nástrojů a skriptů, určených pro analýzu a mapování internetových sítí, testování hesel, zachytávání paketů, detekci bezpečnostních slabin síťových prvků apod. Velkou výhodou je fakt, že tyto distribuce jsou volně ke stažení a to zdarma [7],[8].

Nmap/Zenpam

Síťový bezpečnostní skener Nmap je open source nástroj určený k průzkumu sítě, který se stal oblíbeným pomocníkem při provádění bezpečnostních kontrol. Nmap odesílá speciální pakety a na základě analýzy odpovědí od cíle je schopen zjistit nejen stavy portů, ale i například operační systém a verzi, rozpoznat druh firewallu a mnoho dalších užitečných informací.

Zenmap je grafická nádstavba Nmap, která se snaží zjednodušit používání aplikace Nmap a zároveň poskytuje pokročilejší funkce. V grafickém rozhraní si uživatelé mohou uložit profily často používaných skenů, ukládat výsledky testů a později se k nim vracet [7],[9].

Nessus

Program Nessus je další bezpečnostní skener, který testuje síťové prvky za účelem nalezení potencionálních bezpečnostních děr. Nessus se skládá ze dvou částí. První částí je démon nessusd, který realizuje všechny bezpečnostní testy a druhou je pak grafické rozhraní v internetovém prohlížeči, kterým je program ovládán.

K analýze můžeme použít již předdefinované šablony testů, které je možné dle potřeby upravovat. Po výběru a nastavení testu je nutné definovat cíl testu. Cíl testu může být reprezentován různými formáty jako konkrétní IP adresa, rozsah IP adres nebo například MAC adresou. Po dokončení testu jsou veškeré informace analýzy uloženy. U testovaného cíle je poté k dispozici detailní výpis a také počet nalezených zranitelností.

Aplikace Nessus rozlišuje stupně bezpečnostních zranitelností následovně:

- nízká závažnost (Low Severity),
- střední závažnost (Medium Severity),
- vysoká závažnost (High Severity),
- kritická závažnost (Critical Severity).

Po vyhodnocení testu jsou také k dispozici veškeré zjištěné informace o skenovaném systému (označovány modrou barvou), které popisují například zjištěnou identifikaci OS, otevřené porty, MAC adresy apod [7],[10].

3 NÁVRH BEZPEČNOSTNÍ ANALÝZY

V této kapitole nalezneme popis zvolených metod bezpečnostní analýzy firewallů.

3.1 Analýza síťové komunikace

Analýza paketů nám umožní podrobně sledovat kompletní síťový provoz, který projde přes síťové rozhraní. Programy, které analýzu paketu zprostředkovávají, dokáží pakety zachytit v reálném čase, případně tyto informace zapsat do souboru pro pozdější zpracování. Analýzou dokážeme určit, které pakety jsou přijaté nebo odeslané, rozpoznat a dekódovat stovky síťových protokolů.

3.2 Externí analýza

Externí analýzy jsou ve většině případů prováděny ze vzdáleného počítače z vnější nebo vnitřní sítě a jeho výsledkem je identifikace zařízení a služeb, sloužící k definování případných bezpečnostních slabin.

3.2.1 Skenování portů

Tato metoda bezpečnostní analýzy hledá otevřené síťové porty na vzdálených zařízeních umístěných v počítačových sítích. Zjištěním, které porty jsou otevřené získáme cenné informace o tom, které služby sledované zařízení poskytuje.

Porty jsou označovány identifikačními čísly z rozsahu 0 až 65535 a rozlišují, kterému programu (aplikaci) mají být data předána. Porty vznikají na transportní vrstvě modelu síťové architektury OSI a dělí se podle toho, jestli využívají protokol UDP, nebo TCP. Rozdíl mezi nimi je především v tom, že protokol TCP zajišťuje spolehlivé doručování ve správném pořadí, na rozdíl od protokolu UDP, který je nasazován v situacích, kdy se počítá se ztrátami.

Skenování portů můžeme provádět programem Nmap, který je možný instalovat na operačním systému Linux i Windows. Výsledkem skenování portů zjistíme, které porty jsou otevřené, zavřené nebo filtrované. Otevřeným port značí dostupnou službu, se kterou lze navázat spojení a může být podrobena nejrůznějším testům a útokům. Se zavřenými porty je navazované spojení odmítáno, tudíž na něm služba neběží. Filtrované spojení na dotaz o spojení neodpovídá vůbec a tím pádem se pravděpodobně jedná o chráněné zařízení [9].

TCP skenování

```
nmap -sT ip_adresa
```

Připojování k TCP portům, které využívá klasické připojení TCP protokolu. Jedná se o nápadné skenovaní, protože připojení k otevřenému portu znamená prozrazení IP adresy v logovacích souborech [9].

TCP SYN skenování

```
nmap -sS ip_adresa
```

Tento typ skenování TCP portů neumožní kompletní TCP spojení a proto nedojde k prozrazení útočníkovi IP adresy [9].

TCP ACK skenování

```
nmap -sA ip_adresa
```

Další typ skenování TCP portů, který neumožní kompletní TCP spojení. TCP ACK skenování ovšem nedokáže zjistit, zda jsou TCP porty otevřené, nebo zavřené. Tento typ skenování dokáže pouze určit, zdali jsou porty filtrované, či ne [9].

UDP skenování

```
nmap -sU ip_adresa
```

Skenování UDP portů probíhá odlišným způsobem než je tomu u TCP skenování. Informace o stavu UDP portů přichází ve formě ICMP zpráv. Jelikož jsou tyto zprávy často blokovány firewally, může se stát, že odpověď nedorazí a nemůžeme tak jednoznačně označit port za otevřený nebo filtrovaný. Jestliže data dorazí, můžeme si být jisti, že port je otevřený. U uzavřených UDP portů je odpovědí ICMP zpráva s označením Port Reachable [9].

3.2.2 Detekce operačního systému

Velice cenou informací pro případného útočníka, který se snaží napadnout vzdálené zařízení je bezesporu zjištění, na jakém operačním systému dané zařízení pracuje. Pomocí aplikace Nmap a zadáním správných parametrů je možné operační systém detekovat [9].

```
nmap -O ip_adresa
```

3.2.3 Analýza programem Nessus

Jak už jsme se mohli dozvědět v kapitole 2.2. Program Nessus slouží k testování síťových prvků za účelem nalezení potencionálních bezpečnostních děr. Pro analýzu zranitelností firewallu Hillstone bude použita verze Nessus Home 6.9.1 a pro detekci zranitelností bude aplikován předvolený Basic Network Scan test.

3.3 Interní analýza

V interní analýze nás bude zajímat, jaký operační systém testovací zařízení používá a jakým způsobem lze zařízení konfigurovat. V příloze bakalářské práce bude také sepsán návod, jak zařízení nainstalovat a jakým způsobem nastavit správně síťová rozhraní. Dále je popsáno, jakým způsobem jsou spravovány uživatelské účty, jak se dají definovat uživatelská práva a jak je řešeno zabezpečení účtu pomocí hesel. Na konci budou uvedeny možné zranitelnosti operačního systému firewallu.

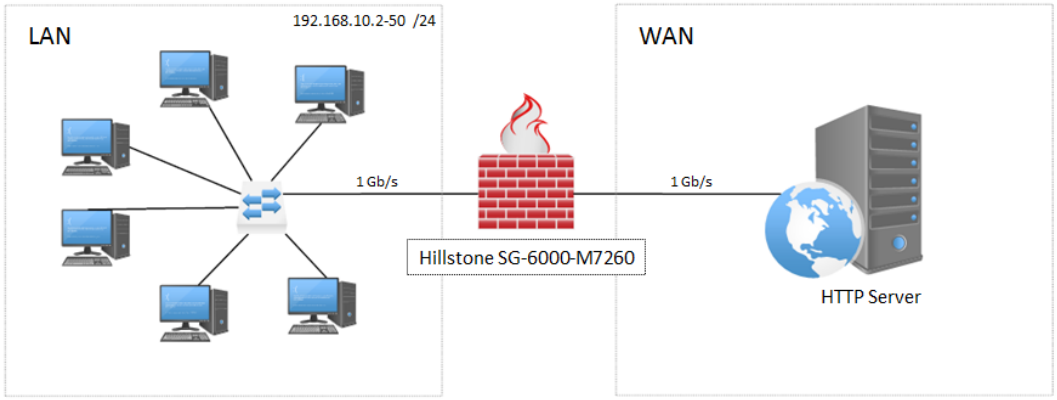
4 NÁVRH VÝKONNOSTNÍHO TESTOVÁNÍ

Následující kapitola bude věnována představení a popisu navržených scénářů pro testování výkonnosti firewallu Hillstone SG6000-M7260 pomocí zařízení Spirent Avalanche M3000, který slouží k simulaci a generování síťového provozu.

První dva navržené scénáře jsou zvoleny tak, aby prověřily schopnost firewallu zvládat provoz pro různé skupiny objektů. První scénář simuluje používání testovaného firewallu v domácnosti, druhý rozšířený scénář reprezentuje podnikovou síť. Ve třetím scénáři bude generován maximálně možný síťový provoz přes 10GbE rozhraní.

4.1 Scénář č. 1: Domácnost

První scénář lze považovat jako základní, který simuluje zapojení firewallu v domácnosti. Firewall je zapojen a nakonfigurován pouze mezi lokální sítí o rozsahu 192.168.10.1-50 obsahující 49 klientských zařízení, komunikující přes firewall s vytvořeným HTTP server na druhém rozhraní. Přes firewall budou procházet požadavky protokolu HTTP o maximální rychlosti 1 Gb/s.

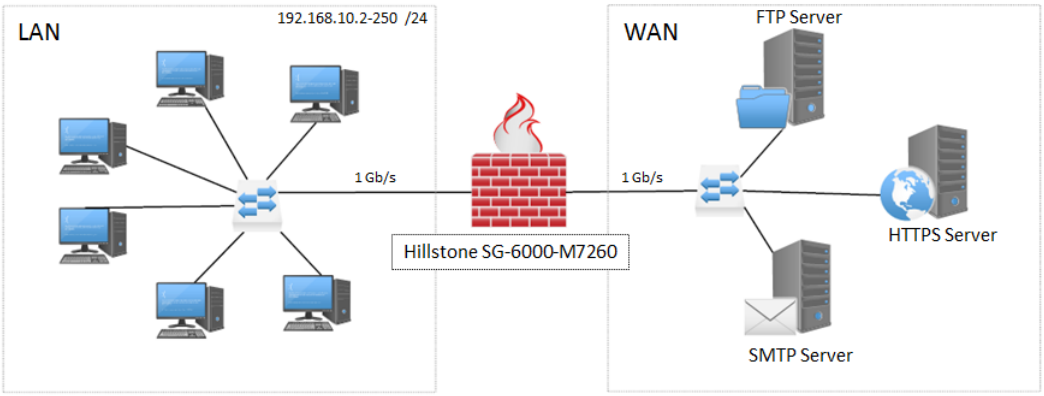


Obr. 4.1: Schéma scénáře č. 1: Domácnost

4.2 Scénář č. 2: Firma

Druhý scénář simuluje zapojení firewallu v malé společnosti. Tento scénář obsahuje rozsáhlejší lokální síť o rozsahu 192.168.10.2-250 obsahující 248 zařízení. Na druhém rozhraní firewallu jsou simulovány 3 různé servery. Jedná se o server HTTPS, FTP a SMTP. Firewall bude testovaný generovanou zátěží všech protokolů simulovaných

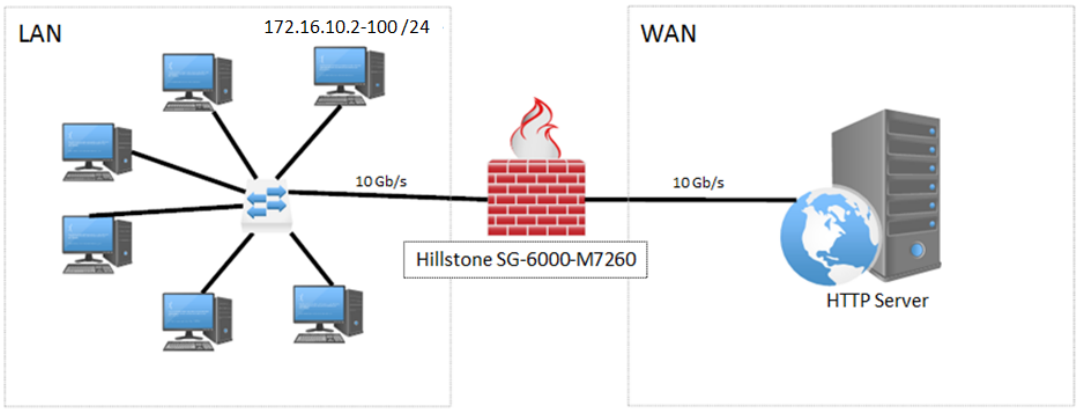
serverů jednotlivě. Stejně jako ve scénáři č. 1 bude použité ethernetové rozhraní o maximální rychlosti 1 Gb/s.



Obr. 4.2: Schéma scénáře č. 2: Malá podniková síť

4.3 Scénář č. 3: Maximální zátěž

Poslední vytvořený scénář bude mít za úkol najít hranici, kdy firewall přestane zvládat generovaný provoz. Na straně klientů bude vytvořena LAN sít o počtu 99 zařízení a na straně serveru bude simulovaný HTTP server. Aby bylo zaručené vytvoření co největší zátěže, tak bude firewall propojen optickými kabely využívající šířku pásma 10Gb/s. Celkem budou provedeny 4 měření. První 3 měření budou zaměřeny na propustnost firewallu a poslední 4. měření bude mít za úkol naleznout maximální hodnotu generovaných transakcí/s.



Obr. 4.3: Schéma scénáře č. 3: Maximální zátěž

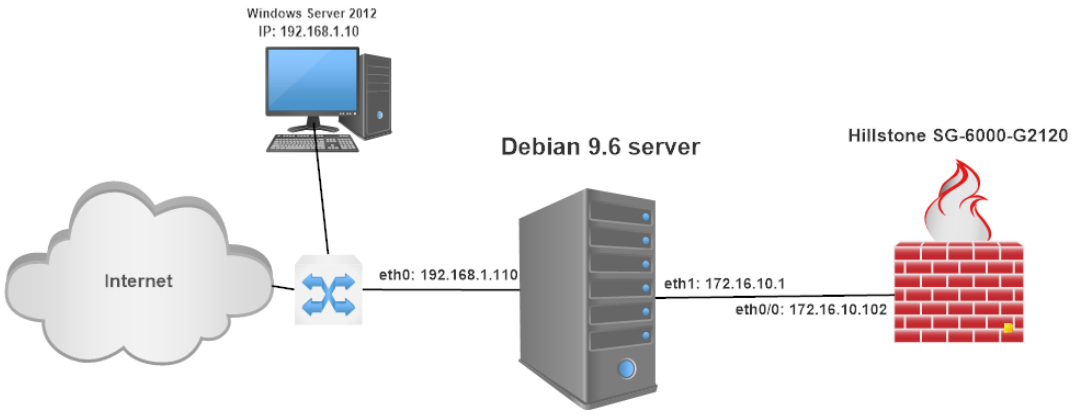
5 PŘEDSTAVENÍ TESTOVACÍHO PROSTŘEDÍ

5.1 Popis testovacího prostředí bezp. analýzy

V laboratoři SC 5.37 Fakulty elektrotechniky a komunikačních technologii VUT v Brně, je na serveru značky IBM nainstalována linuxová distribuce Debian 9.6 Jessie. Tento server je nakonfigurován jako síťová brána, která dokáže přeposílat a zachytávat síťový provoz. Přeposílání paketů je zajištěno pomocí konfiguračního skriptu **rules.sh**, který po spuštění definuje nastavená pravidla iptables. Návod a popis konfigurace je popsán v příloze bakalářské práce.

Server je připojený síťovým rozhraním eth0 do fakultní sítě 192.168.1.0, která má přístup k internetu. Druhé síťové rozhraní eth1 je připojeno k hardwarovému firewallu Hillstone, kterému na linuxovém serveru nainstalovaný DHCP server přiřazuje IP adresu 172.16.10.102. Celkové schéma zapojení reprezentuje obrázek 5.1. Veškerá síťová komunikace testovaného firewallu Hillstone prochází přes nakonfigurovaný server, kde je možné komunikaci zachytávat aplikací Wireshark.

Jelikož na serveru není nainstalované grafické uživatelské prostředí, tak není možné přímo ze serveru konfigurovat firewall Hillstone pomocí webového rozhraní. Proto je v laboratorní síti připojený další server s OS Windows server 2012 s IP adresou 192.168.1.10, který se přes linuxový server dostane až na webové rozhraní firewallu. Zadáním IP adresy 192.168.1.110:80 na vzdáleném serveru je pomocí pravidla PREROUTING v iptables na mezilehlém serveru požadavek přesměrován na skutečnou IP adresu firewallu 172.16.10.102:80. Tento server byl využit i pro vzdálené ovládání programu Nessus, jež je nainstalovaný na linuxovém serveru.



Obr. 5.1: Schéma zapojení

5.2 Hillstone SG-6000-G2120

Bezpečnostní analýza bude prováděna na hardwarovém firewallu Hillstone SG-6000-G2120.

Obr. 5.2: Firewall Hillstone SG-6000-G2120 [11]

Na oficiálních stránkách společnosti Hillstone Networks je tento firewall prezentován jako tzv. firewall nové generace. Firewall dle dokumentace disponuje pokročilými bezpečnostními funkcemi, které poskytují přehlednou kontrolu provozu webových aplikací. Firewall nabízí také aktivní ochranu v reálném čase proti aplikačním a síťovým útokům včetně virů, spyware, DoS/DDoS útokům a trojským koňům.

Tabulka 5.1 obsahuje výpis vybraných specifikací firewallu [12].

Tab. 5.1: Vybrané specifikace firewallu Hillstone SG-6000-G2120

Specifikace	**SG-6000-G2120**
FW Propustnost	4 Gb/s
IPSec Propustnost	1,5 Gb/s
AV Propustnost	350 Mb/s
IPS Propustnost	800 Mb/s
Rozhraní pro management	1 x Console Port, 1 x AUX Port, 1 x USB 2.0 Port
Rozšiřující moduly	IOC-8GE, IOC-8SFP, IOC-4GE-B, Storage Extension Slot
Rozměry (W×D×H)	(436 × 366 × 44 mm)
Váha	19,8 lb (9 kg)

5.3 Hillstone SG-6000-M7260

Hardwarový firewall Hillstone s označením SG-6000-M7260 bude v rámci této bakalářské práce podrobený výkonnostnímu testování.

V porovnání s firewallem SG-6000-G2120 se jedná o výkonnější platformu firewallu, která nabízí téměř čtyřnásobně vyšší parametry vzhledem k propustnosti

Obr. 5.3: Firewall Hillstone SG-6000-M7260 [11]

šířky pásma a počtu spojení za sekundu. Při výkonnostním testování bude otestována především propustnost firewallu v souvislosti s použitím přídavných bezpečnostních prvků jako je IPS a Antivirus. Při měření bude použita v současné době nejnovější verze firmwaru 5.5R3P4.

Tabulka 5.2 obsahuje výpis základních specifikací firewallu [12].

Tab. 5.2: Vybrané specifikace firewallu Hillstone SG-6000-M7260

Specifikace	**SG-6000-M7260**
FW Propustnost	16 [1]/ 20 [2] Gb/s
IPSec Propustnost	9 [1]/ 12 [2] Gb/s
AV Propustnost	1,5 [1]/ 2 [2] Gb/s
IPS Propustnost	2 [1]/ 3 [2] Gb/s
Rozhraní pro management	1 x Console Port, 1 x AUX Port, 1 x USB 2.0 Port
Rozšiřující moduly	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B, IOC-2XFP-Lite-M, IOC-4GE-POE, IOC-8SFP+
Rozměry (W×D×H)	(440 x 520 x 88 mm)
Váha	27,1 lb (12,3 kg)

5.4 Spirent Avalanche 3100

Zařízení Spirent Avalanche 3100 (obr. 5.4) je nástroj sloužící k provádění výkonových a bezpečnostních testů. Testovány mohou být veškerá zařízení v síťové infrastruktuře, stejně tak i webové aplikace a služby. Zařízení Spirent Avalanche 3100 využívá 4 až 7 vrstvu ISO/OSI a dokáže generovat síťový provoz volitelných protokolů, definovaných na straně klienta i serveru, rychlostí až 10 Gb/s. Výkonovým testováním dokážeme zjistit důležité vlastnosti testovaných síťových prvků a aplikací. Zjištění

[1]Hodnota garantované propustnosti při použití základní licence
[2]Hodnota garantované propustnosti při použití speciální licence

hraničních hodnot, u kterých testované prvky přestávají plnit svoji funkci (případ, kdy začínají být zahazovány procházející pakety), bude jedním z cílů této bakalářské práce [13].

Obr. 5.4: Spirent Avalanche 3100 [13]

Pro veškerou konfiguraci zátěže a pro zpracování výsledků testovaní zařízením Avalanche budeme používat programy TestCenter Layer 4-7 Application 4.43 a TestCenter Results Analyzer. Při popisu jednotlivých funkcí následujících programů bylo vycházeno z informacích dostupných v nápovědě těchto programů.

5.4.1 TestCenter Layer 4-7 Application 4.43

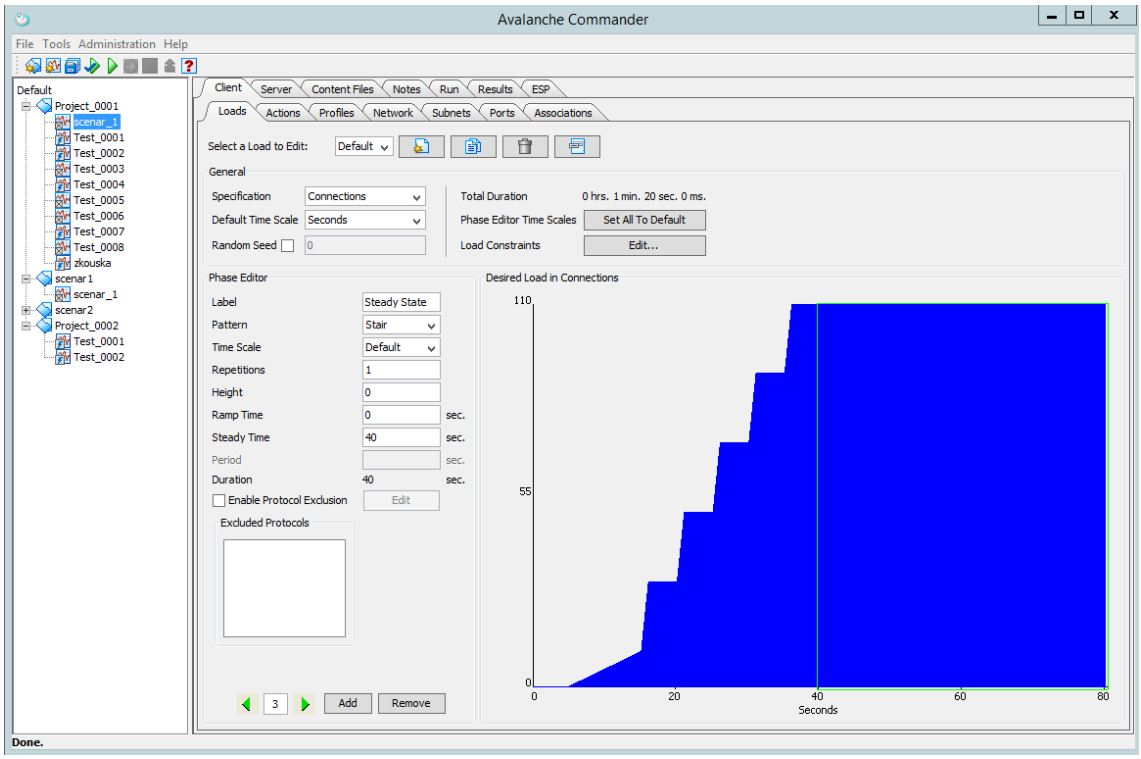
Aplikace TestCenter Layer 4-7 Application 4.43 slouží ke konfiguraci a nastavení veškerých parametrů generovaných zátěží, které jsou simulovány přístrojem Spirent Avalanche. Aplikace nabízí možnost výběru ze dvou kategorií testování, podle toho, zda se testování bude týkat zařízení a bude nutná konfigurace na straně serveru i klientů, nebo aplikací a simulace bude probíhat pouze na straně klienta. Po zvolení typu testování, následuje výběr ze 3 typů specifických testů: Quick, Advanced a EZ test. V našem případě budeme využívat typ Advanced, který umožňuje nejdetailnější konfiguraci.

Na obrázku 5.5 se nachází pohled na grafické rozhraní aplikace TestCenter Layer 4-7Application 4.43. Konfigurace klientské části se nachází pod záložkou *Client*. Zde se nachází další upřesňující konfigurační záložky. Specifikaci generované zátěže klientské části se nastavují v záložce *Client - Load*, kde si v poli *Specification* vybereme mezi následujícími typy generované zátěže:

- Bandwidth – zátěž generována na základě šířky pásma,
- Connections – generování konfigurovaného počtu spojení,

- Connections/second – generování konfigurovaného počtu spojení za sekundu,
- SimUsers/second – zátěž je generována počtem uživatelů za sekundu,
- Transactions – generování nastaveného počtu transakcí,
- Transactions/second – generování nastaveného počtu transakcí za sekundu.

V poli *Phase Editor* poté definujeme různé fáze generování zátěže a jejich velikosti v závislosti na čase. Dalšími důležitými položkami v záložce *Client* je položka *Action* - pro určení příkazů, které definovaní klienti požadují po serverové části, pole *Subnet* - pro definování rozsahu IP adres klientské části a také pole *Ports* a *Associations* - pro přiřazení fyzických portů zařízení Spirent k definovaným klientům.



Obr. 5.5: Vzhled aplikace TestCenter Layer 4-7 Application 4.43

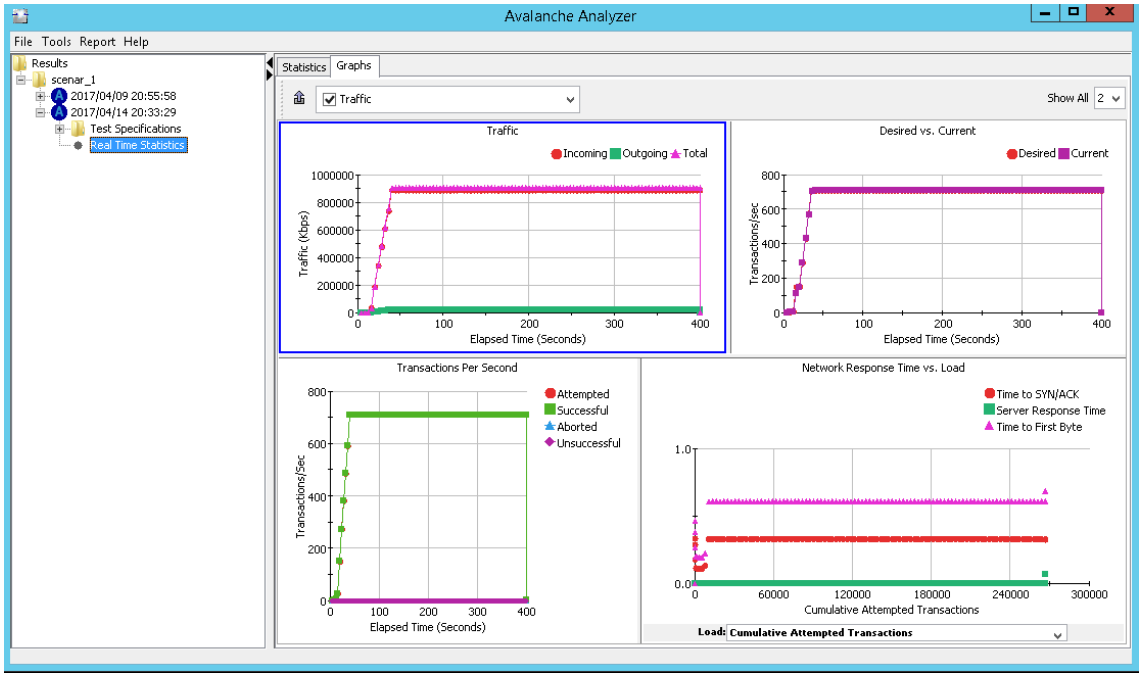
Konfigurace simulované serverové části nalezneme pod záložkou *Server*. Zde v položce *Profiles* a *Transaction* definujeme jednotlivé servery a jejich paramtery. K dispozici máme širokou škálu možných typů serverů, které si můžeme vybrat v poli *Profiles - Type*. V rámci bakalářké práce budou využity typy serverů HTTP, HTTPS, FTP a SMTP. Stejně jako v záložce *Client* i v záložce *Server* je nutné definovat rozsahy IP adres - položka Subnet a přiřadit fyzickým portům definované servery v položkách *Ports* a *Associations*.

Další důležitou částí aplikace Spirent TestCenter jsou záložky *Run* a *Results*. V záložce *Run* můžeme při realizovaní testu v reálném čase sledovat průběh testů a

aktuální výsledky. Po dokončení probíhající testu jsou výsledky uloženy k nahlédnutí právě v záložce *Results*.

5.4.2 TestCenter Results Analyzer

Aplikace TestCenter Results Analyzer slouží k prohlížení a interpretaci výsledků, naměřených pomocí zařízení Spirent Avalanche. Naměřené výsledky lze ukládat do souboru CSV, které obsahují všechny naměřené parametry v přehledných tabulkách, nebo převedené do grafů. Takto naměřené výsledky lze v aplikaci TestCenter Results Analyzer pouze prohlížet, nebo je možné výsledky exportovat do různých formátů jako PDF, HTML. Jednotlivé grafy je možné ukládat do souboru JPG apod. Obrázek 5.6 zobrazuje náhled aplikace TestCenter Results Analyzer.



Obr. 5.6: Vzhled aplikace TestCenter Results Analyzer

6 VÝSLEDKY BEZPEČNOSTNÍCH ANALÝZ

Následující kapitola obsahuje výsledky jednotlivých bezpečnostních analýz, které byly zvoleny v kapitole 5 Návrh bezpečnostních analýz. Cílem analýzy byl hardwarový firewall Hillstone SG-6000-G2120 s verzí firmwaru 5.5R3 nastavený ve výchozím stavu.

6.1 Analýza síťové komunikace

6.1.1 Analýza síťové komunikace při prvním spuštění firewallu

Tato analýza nám ukáže veškerou síťovou komunikaci při startu a ověří nám, jakým způsobem a s kým při startu a prvotním připojení k internetu firewall komunikuje.

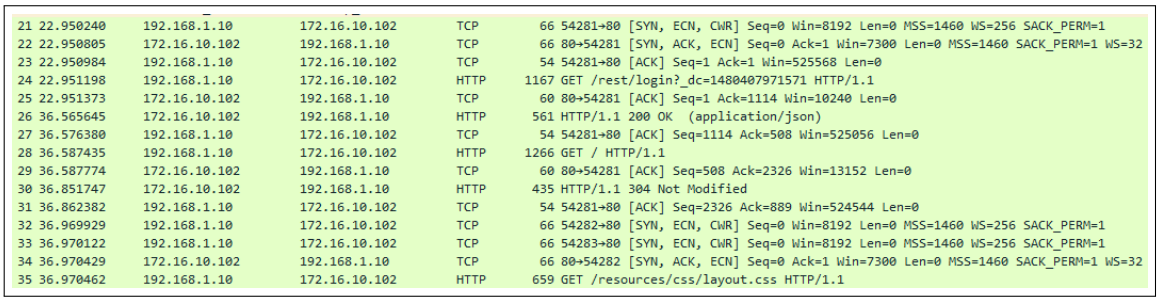
Výsledky:

Při prvním spuštění firewallu byl zachycen požadavek firewallu o přiřazení IP adresy z DHCP serveru vysláním žádosti na broadcastovou adresu 255.255.255.255. Následně DHCP server nainstalovaný na linuxovém serveru žádost přijal, poté firewallu nabídl a přiřadil IP adresu 172.16.10.102. Po přiřazení IP adresy je zachyceno, jak firewall pomocí protokolu DNS získává překlad adresy 192.58.114.5 pro url1.hillstonenet.com (viz. obr. 6.1).

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x7525ff7d
2	0.000201	IbmCorp_41:76:9e	Broadcast	ARP	42	Who has 172.16.10.102? Tell 172.16.10.1
3	0.996631	IbmCorp_41:76:9e	Broadcast	ARP	42	Who has 172.16.10.102? Tell 172.16.10.1
4	1.001442	172.16.10.1	172.16.10.102	DHCP	342	DHCP Offer - Transaction ID 0x7525ff7d
5	1.002322	0.0.0.0	255.255.255.255	DHCP	590	DHCP Request - Transaction ID 0x7525ff7c
6	1.002483	172.16.10.1	172.16.10.102	DHCP	342	DHCP ACK - Transaction ID 0x7525ff7c
7	1.996630	IbmCorp_41:76:9e	Broadcast	ARP	42	Who has 172.16.10.102? Tell 172.16.10.1
8	4.009650	0.0.0.0	255.255.255.255	DHCP	590	DHCP Request - Transaction ID 0x7525ff7c
9	4.009843	172.16.10.1	172.16.10.102	DHCP	342	DHCP ACK - Transaction ID 0x7525ff7c
10	4.010196	Hillston_38:36:86	Broadcast	ARP	60	Who has 172.16.10.102? Tell 0.0.0.0
11	4.640868	Hillston_38:36:86	Broadcast	ARP	60	Gratuitous ARP for 172.16.10.102 (Request)
12	4.640882	Hillston_38:36:86	Broadcast	ARP	60	Gratuitous ARP for 172.16.10.102 (Request)
13	7.173927	Hillston_38:36:86	Broadcast	ARP	60	Who has 172.16.10.1? Tell 172.16.10.102
14	7.173940	IbmCorp_41:76:9e	Hillston_38:36:86	ARP	42	172.16.10.1 is at e4:1f:13:41:76:9e
15	7.174683	172.16.10.102	8.8.8.8	DNS	81	Standard query 0xbb6f A url1.hillstonenet.com
16	7.174712	172.16.10.102	8.8.8.8	DNS	81	Standard query 0xa54d A url2.hillstonenet.com
17	7.180931	8.8.8.8	172.16.10.102	DNS	97	Standard query response 0xa54d A url2.hillstonenet.com A 198.58.114.5

Obr. 6.1: Komunikace při instalaci (získání IP adresy a prvotní komunikace)

V další části (obrázek 6.2) je zaznamenán přístup do webového managementu firewallu Hillstone pomocí vzdáleného serveru s IP adresou 192.168.1.10, umístěného v laboratorní síti. Jelikož připojený linuxový server nevyužívá grafického uživatelského prostředí, ale pracuje jen na úrovni příkazové řádky, tak není schopný firewall Hillstone ovládat pomocí webového rozhraní. Externí server tedy slouží ke konfiguraci firewallu pomocí internetového prohlížeče. Veškerá komunikace mezi vzdáleným serverem a firewallem je zachycena.



21	22.950240	192.168.1.10	172.16.10.102	TCP	66 54281→80 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
22	22.950805	172.16.10.102	192.168.1.10	TCP	66 80→54281 [SYN, ACK, ECN] Seq=0 Ack=1 Win=7300 Len=0 MSS=1460 SACK_PERM=1 WS=32
23	22.950984	192.168.1.10	172.16.10.102	TCP	54 54281→80 [ACK] Seq=1 Ack=1 Win=525568 Len=0
24	22.951198	192.168.1.10	172.16.10.102	HTTP	1167 GET /rest/login?_dc=1480407971571 HTTP/1.1
25	22.951373	172.16.10.102	192.168.1.10	TCP	60 80→54281 [ACK] Seq=1 Ack=1114 Win=10240 Len=0
26	36.565645	172.16.10.102	192.168.1.10	HTTP	561 HTTP/1.1 200 OK (application/json)
27	36.576380	192.168.1.10	172.16.10.102	TCP	54 54281→80 [ACK] Seq=1114 Ack=508 Win=525056 Len=0
28	36.587435	192.168.1.10	172.16.10.102	HTTP	1266 GET / HTTP/1.1
29	36.587774	172.16.10.102	192.168.1.10	TCP	60 80→54281 [ACK] Seq=508 Ack=2326 Win=13152 Len=0
30	36.851747	172.16.10.102	192.168.1.10	HTTP	435 HTTP/1.1 304 Not Modified
31	36.862382	192.168.1.10	172.16.10.102	TCP	54 54281→80 [ACK] Seq=2326 Ack=889 Win=524544 Len=0
32	36.969929	192.168.1.10	172.16.10.102	TCP	66 54282→80 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
33	36.970122	192.168.1.10	172.16.10.102	TCP	66 54283→80 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
34	36.970429	172.16.10.102	192.168.1.10	TCP	66 80→54282 [SYN, ACK, ECN] Seq=0 Ack=1 Win=7300 Len=0 MSS=1460 SACK_PERM=1 WS=32
35	36.970462	192.168.1.10	172.16.10.102	HTTP	659 GET /resources/css/layout.css HTTP/1.1

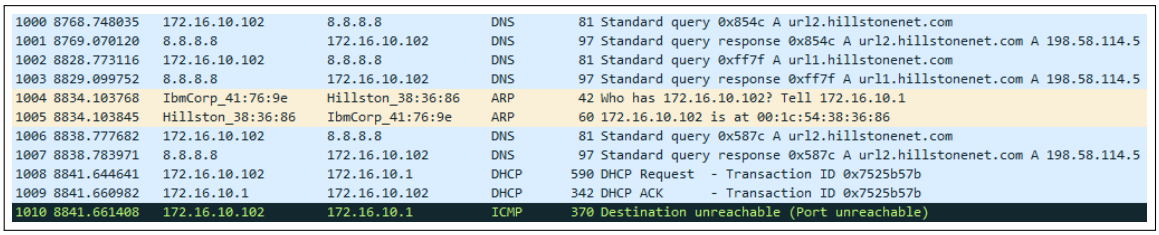
Obr. 6.2: Komunikace při instalaci (přístup do WebUI přes protokol HTTP)

6.1.2 Zachycení komunikace při chodu firewallu

Tato analýza nám ukáže komunikaci firewallu Hillstone SG-6000-G2120 při provozu. Komunikace bude zachytávána po dobu 48 hodin. Následně budou tato data analyzována.

Výsledky:

Za dobu 48 hodin bylo aplikací Wireshark zachyceno celkem 17816 paketů. Dle analýzy zachyceného provozu lze říci, že se v pravidelných intervalech střídá stejná komunikace pomocí 4 síťových protokolů (ARP, DNS, ICMP a DHCP). Názornou ukázku zachycené komunikace nalezneme na obrázku 6.3.



1000	8768.748035	172.16.10.102	8.8.8.8	DNS	81 Standard query 0x854c A url2.hillstonenet.com
1001	8769.070120	8.8.8.8	172.16.10.102	DNS	97 Standard query response 0x854c A url2.hillstonenet.com A 198.58.114.5
1002	8828.773116	172.16.10.102	8.8.8.8	DNS	81 Standard query 0xff7f A url1.hillstonenet.com
1003	8829.099752	8.8.8.8	172.16.10.102	DNS	97 Standard query response 0xff7f A url1.hillstonenet.com A 198.58.114.5
1004	8834.103768	IbmCorp_41:76:9e	Hillston_38:36:86	ARP	42 Who has 172.16.10.102? Tell 172.16.10.1
1005	8834.103845	Hillston_38:36:86	IbmCorp_41:76:9e	ARP	60 172.16.10.102 is at 00:1c:54:38:36:86
1006	8838.777682	172.16.10.102	8.8.8.8	DNS	81 Standard query 0x587c A url2.hillstonenet.com
1007	8838.783971	8.8.8.8	172.16.10.102	DNS	97 Standard query response 0x587c A url2.hillstonenet.com A 198.58.114.5
1008	8841.644641	172.16.10.102	172.16.10.1	DHCP	590 DHCP Request - Transaction ID 0x7525b57b
1009	8841.660982	172.16.10.1	172.16.10.102	DHCP	342 DHCP ACK - Transaction ID 0x7525b57b
1010	8841.661408	172.16.10.102	172.16.10.1	ICMP	370 Destination unreachable (Port unreachable)

Obr. 6.3: Komunikace při chodu firewallu

Zachycená komunikace protokolu ARP ukazuje dotaz na vlastníka IP adresy 172.16.10.102 MAC adresy serveru (IbmCorp_41:76:9e). Tento dotaz je směrován na MAC adresu firewallu (Hillston_38:36:86) a firewall odpovídá, že právě on je vlastníkem této IP adresy.

Komunikace DHCP protokolu obsahuje požadavek firewallu na DHCP server o přiřazení IP adresy a následné vyhovění požadavku ze strany DHCP serveru. Tato komunikace probíhá pravidelně v intervalech odpovídající hodnotě max-lease-time 7200 (maximální době zapůjčení IP adresy) nastavené v konfiguraci DHCP serveru na stanici s OS Debian.

Další komunikace, která byla při odposlechu zachycena je dotaz IP adresy firewalu pomocí DNS protokolu. Firewall žádá nastavený DNS server 8.8.8.8 o překlad

doménového jména url1.hillstonenet.com a ur2.hillstonenet.com. Odpovědí DNS serveru je pro oba dotazy přeložená IP adresa 198.58.114.5.

Poslední zachycený opakující se síťový protokol je ICMP, který slouží k diagnostice IP vrstvy v našem případě informuje o nedosažitelnosti UDP portu.

6.2 Externí analýza

6.2.1 Skenování portů

Pomocí aplikace Nmap bylo provedeno skenování portů firewallu Hillstone. K získaní co nejvíce informací o analyzovaném firewallu bylo nutné volit různé metody, podle kterých bylo skenování portů realizováno.

Výsledky:

Metodou skenování UDP portů (viz obrázek 6.4) se nepodařilo objevit konkrétní otevřený port. Skenovaní pouze nejednoznačně označilo všechny UDP porty firewallu jako otevřené a filtrované.

```
# Nmap 6.47 scan initiated Sun Nov 27 21:20:24 2016 as: nmap -oN nmap-sU.txt -sU 172.16.10.101
Nmap scan report for 172.16.10.101
Host is up (0.00013s latency).
All 1000 scanned ports on 172.16.10.101 are open|filtered

MAC Address: 00:1C:54:38:36:86 (Hillstone Networks)
# Nmap done at Sun Nov 27 21:20:45 2016 -- 1 IP address (1 host up) scanned in 21.51 seconds
```

Obr. 6.4: Skenování portů pomocí metody UDP

Skenování TCP portů již vedlo k nálezu konkrétních otevřených síťových portů. Nejvíce informací se podařilo získat pomocí příkazů pro TCP a TCP SYN skenování (viz obrázek 6.5).

```
# Nmap 6.47 scan initiated Sun Nov 27 21:12:47 2016 as: nmap -oN nmap-sT.txt -sT 172.16.10.101
Nmap scan report for 172.16.10.101
Host is up (0.00030s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
8181/tcp closed unknown

MAC Address: 00:1C:54:38:36:86 (Hillstone Networks)
# Nmap done at Sun Nov 27 21:12:52 2016 -- 1 IP address (1 host up) scanned in 4.99 seconds
```

Obr. 6.5: Skenování portů pomocí TCP

Výsledky těchto metod skenování byly totožné a nalezly otevřený port 22 pro komunikaci protokolu SSH, dále otevřený port 80 a 443 (http a https), sloužící pro vzdálené připojení k managementu firewallu a jeden uzavřený port 8181.

Varianta skenování TCP ACK (viz obrázek 6.6), která ke skenování portů nevyužívá kompletní TCP spojení, označila všechny skenované porty za filtrované.

```
# Nmap 6.47 scan initiated Sun Nov 27 21:16:26 2016 as: nmap -oN nmap-sA.txt -sA 172.16.10.101
Nmap scan report for 172.16.10.101
Host is up (0.00013s latency).
All 1000 scanned ports on 172.16.10.101 are filtered

MAC Address: 00:1C:54:38:36:86 (Hillstone Networks)
# Nmap done at Sun Nov 27 21:16:47 2016 -- 1 IP address (1 host up) scanned in 21.57 seconds
```

Obr. 6.6: Skenování portů metodou TCP ACK

6.2.2 Detekce operačního systému

Jak již bylo zmíněno v kapitole 3.2.2 aplikace Nmap je v některých případech schopna získat informace vedoucí k odhalení operačního systému skenovaného zařízení.

Výsledky:

Při skenování portů firewallu SG-6000-G2120 se nepodařilo přesně detekovat, jaký operační systém firewall používá. Avšak odhalením MAC adresy se aplikaci Nmap podařilo správně určit, že zkoumané zařízení je výrobek firmy Hillstone Networks. Takové zjištění může být případnému útočníkovi velice cennou informací.

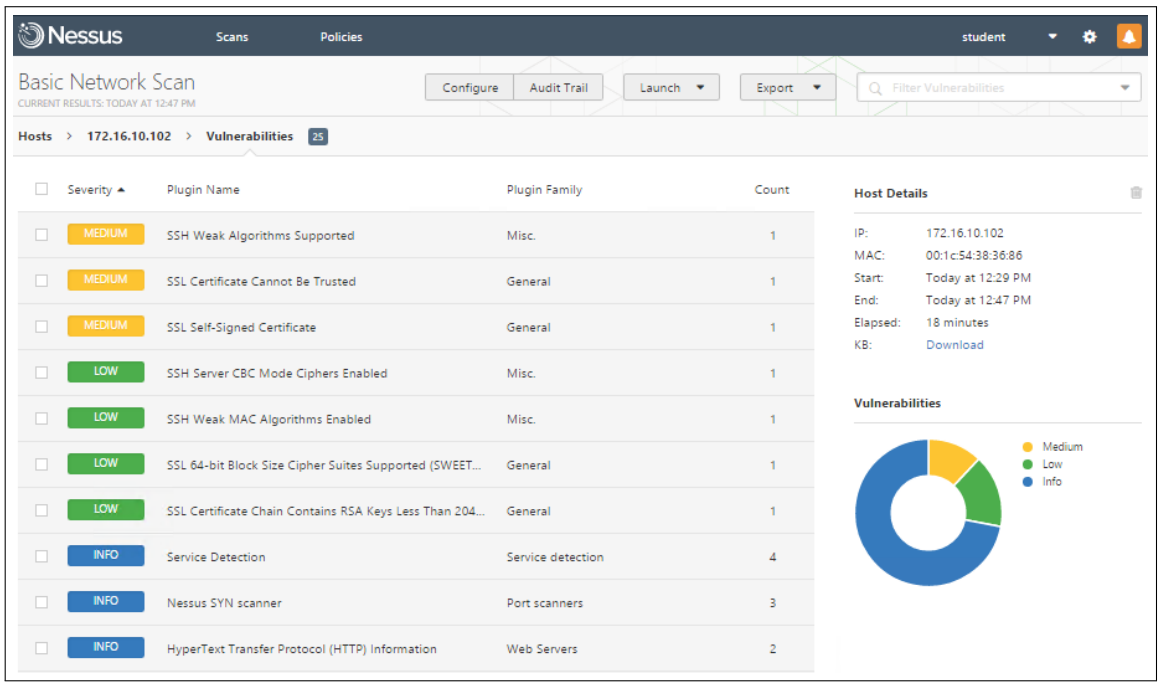
```
# Nmap 6.47 scan initiated Sun Nov 27 21:21:16 2016 as: nmap -oN nmap-O.txt -O 172.16.10.101
Nmap scan report for 172.16.10.101
Host is up (0.00040s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
8181/tcp closed unknown

MAC Address: 00:1C:54:38:36:86 (Hillstone Networks)
OS fingerprint not ideal because: Didn't receive UDP response.
No OS matches for host
Network Distance: 1 hopOS detection performed.
Please report any incorrect results at http://nmap.org/submit/ .
# Nmap done at Sun Nov 27 21:21:43 2016 -- 1 IP address (1 host up) scanned in 27.25 seconds
```

Obr. 6.7: Detekce OS

6.2.3 Analýza aplikací Nessus

Pomocí aplikace Nessus Home verze 6.9.1 byl na IP adresu firewallu Hillstone aplikován Basic Network Scan, který měl za úkol zjistit zranitelností testovaného zařízení.

Analýzou bylo zjištěno celkem 25 potencionálních zranitelností, z nichž 3 jsou označeny střední závažností, 4 závažností nízkou a zbylých 18 záznamů jsou zjištěné informativní zprávy o skenovaném přístroji. Náhled na výsledek Basic Network Testu nalezneme na obrázku 6.8.



Obr. 6.8: Ukázka výpisu zranitelností programem Nessus

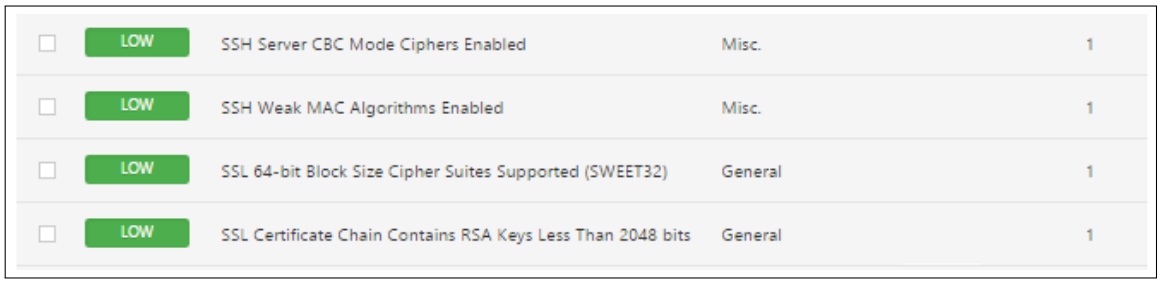
Střední závažností (viz obrázek 6.9) vyhodnotila aplikace Nessus na analyzovaném firewallu zranitelnost ve slabém šifrování SSH připojení, které by mohlo vést ke snadnému zneužití.

Obr. 6.9: Výpis MEDIUM zranitelností programem Nessus

Dále byl nalezen problém s důvěryhodností a šifrováním SSL certifikátů pro přístup do webového managementu pomocí protokolu HTTPS. Tato skutečnost může

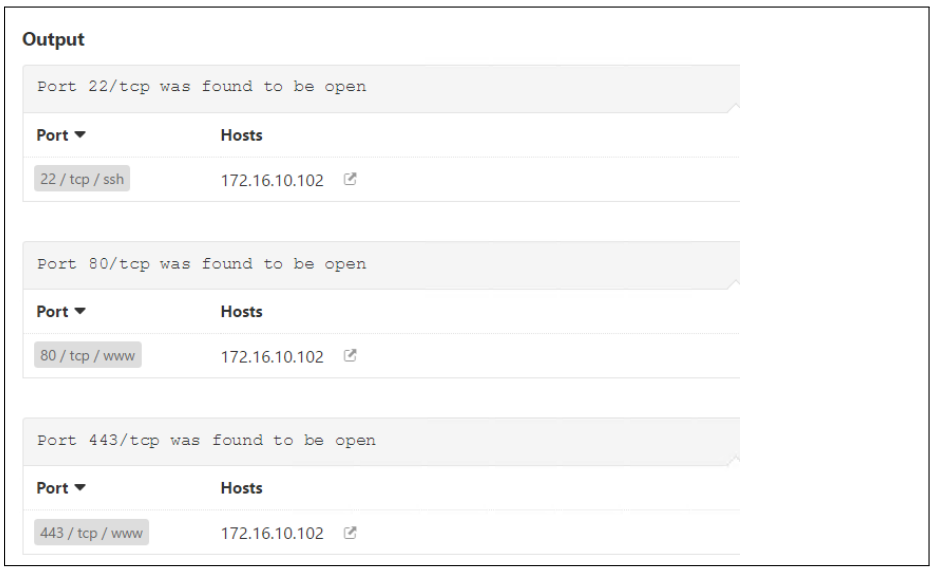
být vodítkem pro případné útočníky, například k útoku MITM (Man in the middle). Jedná se o útok, kde útočník vstoupí do komunikace mezi dva uživatele a využije slabého šifrovaní SSL k podstrčení falešného certifikátu.

Nízkou úrovní zranitelnosti (viz obrázek 6.10) byly označeny 2 nedostatky opět v SSH připojení, které využívá slabé CBC šifrování a slabý algoritmus MAC. Další nedostatky označeny nízkou závažností byly nalezeny v slabém šifrování relace HTTPS a v certifikačním klíči, který je menší než 2048 bitů. Aplikace Nessus považuje blokové šifrování protokolu HTTPS s bloky o velikosti 64 bitů za nebezpečné a doporučuje používat bezpečnější šifrování.



Obr. 6.10: Výpis LOW zranitelností programem Nessus

Další položky, označené jako informativní, poukazují na všechny informace, které byla aplikace Nessus schopna zjistit o připojeném firewallu. Mezi těmito položkami se nachází i skenování portů. Nalezené výsledky se shodují s výsledky aplikace Nmap. Pro názorný příklad uvedu na obrázku 6.11 výstup Nessus SYN scanner, který stejně jako aplikace Nmap nalezl otevřené porty 22, 80 a 433.



Obr. 6.11: Výpis Nessus SYN scanner

6.3 Interní analýza

Operační systém:

Hardwarový firewall Hillstone SG-6000-G2120 používá operační systém StoneOS verze 5.5R3. Operační systém StoneOS zajišťuje chod veškerých funkcí, kterými firewall disponuje. Ovládaní a konfigurace systému je možná pomocí příkazové řádky nebo webovým uživatelským rozhraním.

Způsoby konfigurace:

Konfigurace firewallu Hillstone je možné pomocí následujících přístupů:

- přístup k zařízení přes sériový port konzole,
- přístup k zařízení přes Telnet,
- přístup k zařízení přes SSH,
- přístup k zařízení přes rozhraní WebUI.

Přístup k zařízení přes SSH:

Přístup do přímé konfigurace operačního systému StoneOS je možný pomocí protokolu SSH. Pro připojení přes SSH je potřeba být připojený ethernetovým kabelem s firewallem a mít povolený uživatelský přístup pro SSH. Výchozí uživatelský účet (uživatel: hillstone) má povolený veškerý přístup a proto jej pro připojení můžeme použít. Pro připojení k firewallu přes SSH z připojeného linuxového serveru musíme zadat následující příkaz:

```
ssh hillstone@172.16.10.102
```

Následuje výzva o zadaní hesla, které je: hillstone.

Přístup k zařízení přes webové grafické rozhraní:

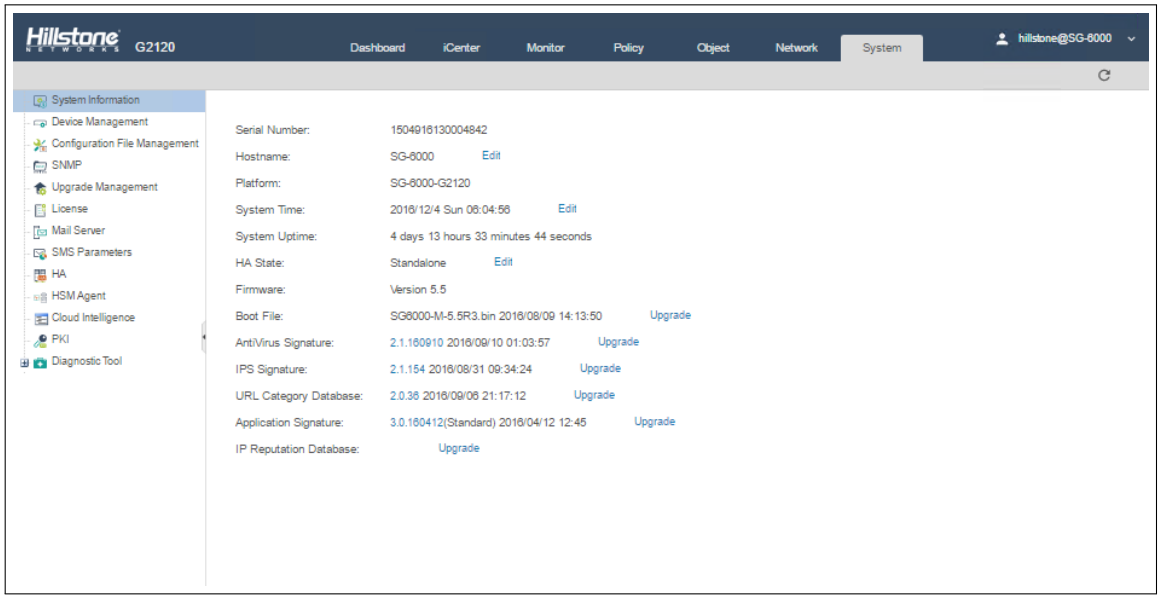
Rozhraní eth0/0 má defaultně nastavenou IP adresu 192.168.1.1/24 a všechny své služby povoleny. Při používání nového zařízení, je pro přístup k webovém managementu nutné postupovat následovně:

- Propojení PC, kterým budeme firewall nastavovat, k rozhraní firewallu eth0/0 pomocí ethernetového kabelu.
- Připojenému počítači se musí nastavit IP adresa stejné podsítě jakou má firewall. Vhodná je například IP adresa 192.168.1.2/24.
- V počítači spusťte webový prohlížeč a přejděte na adresu http://192.168.1.1.
- Zadejte výchozí uživatelské jméno (hillstone) a heslo (hillstone).
- Po stisknutí tlačítka Login budete přihlášeni do webového managementu firewallu Hillstone.

Popis webového grafické rozhraní:

Grafické uživatelské rozhraní (viz obrázek 6.12) poskytuje přímý a efektivní způsob správy a konfigurace firewallu Hillstone. Grafické uživatelské rozhraní je členěno do 7 hlavních záložek:

- Dashboard – domovská informativní stránka shrnující volitelné informace (například o vytížení sítě nebo počtu útoků) pomocí přehledných grafů.
- iCenter – stránka, která informuje uživatele o aktuálních bezpečnostních hrozbách.
- Monitor – položka shrnující statistické informace, které jsou firewallem monitorovány.
- Policy – položka definující bezpečnostní politiky zařízení.
- Object – stránka konfigurující uživatele, jejich role, ale také další připojená zařízení.
- Network – tato záložka obsahuje veškeré nastavení sítě firewallu, jako například nastavení internetových rozhraní, směrovacích pravidel, bezpečnostních zón apod.
- System – záložka obsahující hlavní informace o systému firewallu. Obsahuje důležité nástroje pro diagnostiku firewallu.



Obr. 6.12: Webové grafické rozhraní Hillstone SG-6000-G2120

Správa uživatelských účtů a hesel:

Firewall umožňuje vytvářet účty s různými právy přístupů a možností konfigurace. Účty lze spravovat přes webové rozhraní, ale i přímo z OS pomocí SSH připojení.

Je možné si vybrat z následující základní nabídky typů účtů:

- Administrator – hlavní uživatelský účet, který má veškerá práva pro konfiguraci a správu systému.
- Administrator-read-only – účet umožňující náhled konfigurací, nikoliv však jejich změnu.
- Operator – základní účet s omezenými právy.
- Auditor – účet sloužící auditorům, kterým je umožněn přístup k záznamům logů.

Hesla účtů je možné také konfigurovat. Je možné měnit minimální možnou délku hesla a vyžadovat používaní komplexních hesel. Při používání komplexních hesel musí uživatelské heslo obsahovat minimálně 8 znaků a je nutné použít 2 velká a malá písmena, 2 číslice a 2 speciální znaky (například @,#). V případě, že není komplexní heslo vyžádané, je výchozí minimální délka hesla nastavena pouze na 4 znaky, které lze zvýšit.

U každého účtu je dále možné individuálně povolit typ přístupu (sériový port, telnet, SSH, HTTP nebo HTTPS) a také je možné nastavit maximální počet zadání chybného hesla a následně dobu, po kterou je účet po neplatných pokusech o přihlášení zablokován. Výchozí hodnoty jsou nastaveny na maximálně 3 špatné pokusy a doba blokace účtu je ve výchozím stavu nastavena na 2 minuty.

Na obrázku 6.13 nalezneme přístup do operačního systému firewallu a následný výpis definovaných uživatelů. Pro vyzkoušení vytváření uživatelských účtů firewallu přes SSH připojení byl vytvořen uživatel: uzivatel s právy typu: operator, kterému je povolen přístup pouze přes protokol HTTPS.

```
root@debian:/home/student# ssh hillstone@172.16.10.102
hillstone@172.16.10.102's password:
SG-6000#
SG-6000# show admin user
=============================================================================
Username        Role                Console Telnet SSH HTTP HTTPS
-----------------------------------------------------------------------------
hillstone       admin                Y       Y      Y   Y    Y
uzivatel        operator             -       -      -   -    Y
=============================================================================
```

Obr. 6.13: Výpis def. uživatelů firewallu přes SSH připojení

Zranitelnost firewallu Hillstone SG-6000-G2120:

Dle výsledku externích bezpečnostních analýz je možné analyzovat zranitelnosti testovaného firewallu. Realizované bezpečnostní testy v bakalářské práci sice nebyly

obsáhlé, ale přeci jen bylo pár zranitelností zjištěno.

Vzhledem k zjištěnému slabému šifrování služby SSH aplikací Nessus a k faktu, jak snadné bylo připojení k operačnímu systému firewallu pomocí SSH připojení, vidím hlavní zranitelnost systému StoneOS právě tady. Výchozího uživatele firewallu (hillstone/hillstone), který má veškerá konfigurační a přístupová práva nelze smazat, ale pouze editovat.

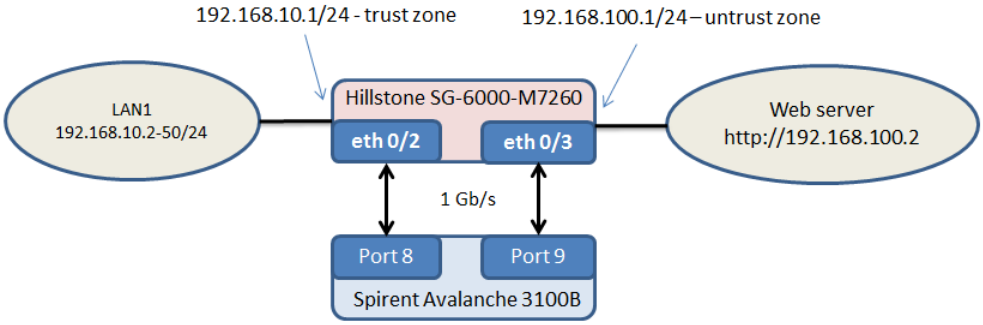
V případě, že by vlastník firewallu neprovedl editaci výchozího uživatele a nechal mu nastavené veškerá práva a především slabé heslo účtu (hillstone), totožné s názvem účtu a značkou firewallu, mohlo by být zneužití zařízení pro případného útočníka poměrně snadné.

7 VÝSLEDKY VÝKONNOSTNÍHO TESTOVÁNÍ

Následující kapitola obsahuje výsledky výkonnostního testování scénářů navržených v kapitole 4 Návrh výkonnostního testování. Cílem analýzy byl hardwarový firewall Hillstone SG-6000-M-7260. Stejně jako bezpečnostní analýza, tak i výkonnostní testování probíhaly v laboratoři SC 5.37. K veškerému nastavení generátoru Spirent Avalanche využijeme aplikaci Spirent TestCenter Layer 4-7 Application 4.43, která je blíže popsána v kapitole 5.4.1

7.1 Scénář č. 1: Domácnost

Cílem výkonnostního testování prvního scénáře, který simuluje použití testovaného firewallu v běžné domácnosti, bude otestovat schopnost firewallu propouštět a zpracovávat generovanou zátěž. Testování 1. scénáře obsahuje 2 měření s postupně zvyšujícím se výkonem zátěže. Schéma konfigurace zátěže, zapojení testovaného firewallu a generátoru Spirent Avalanche je znázorněno na obrázku 7.1). Veškeré kabelové propojení mezi firewallem a generátorem zátěže u prvního scénáře je realizované UTP kabely přes síťová rozhraní 1 Gigabit Ethernet.



Obr. 7.1: Schéma zapojení výkonového testování scénáře č. 1

U obou měření výkonu prvního scénáře bude generována zátěž typu Transactions/second, kterou bude vyvolán požadavek klientské části generátoru o data HTTP serveru a následná odpověď serveru. Příkazem:

```
1 get http://192.168.100.2/index.html
```

zadaného v Actions Listu v aplikaci Spirent TestCenter Layer 4-7 Application 4.43 zaručíme, aby každý definovaný klient (v případě 1. scénáře je počet klientů 49) odeslal žádost GET na URL HTTP serveru http://192.168.100.2/index.html. HTTP server na jednotlivé žádosti odpovídá zasláním požadovaného souboru o definované

velikosti, která je nastavena na 150 kB. Hodnota 150 kB byla zvolena podle velikosti hlavní stránky portálu www.seznam.cz, která je v řadě domácností zvolena jako úvodní stránka ihned po spuštění internetového prohlížeče. Typ protokolu HTTP je vybrán 1.1. Různé konfigurace nastavení klientské části pro generování zátěže jsou podrobně specifikovány u jednotlivých měření.

7.1.1 Měření: 1

Specifikace klientské části generátoru zátěže je nastaveno následujícím způsobem:

- Subnets / IP Adress (Range): 192.168.10.2-50/24 – *rozsah IP adres*
- Loads / Phase Editor / Label: Delay – *počátečního prodlení měření*
  - Pattern: Flat – *typ rovnoměrné zátěže*
  - Repetitions: 1 – *počet opakování*
  - Height: 10 – *velikost navýšení*
  - Duration: 10 sec. – *čas trvání*
- Loads / Phase Editor / Label: Stair Step – *schodovitě zvyšující se zátěž*
  - Pattern: Stair – *typ schodovitě zvyšující se zátěže*
  - Repetitions: 5 – *počet opakování*
  - Height: 40 – *velikost navýšení*
  - Duration: 25 sec. – *čas trvání*
- Loads / Phase Editor / Label: Steady State – *ustáleně generující se zátež*
  - Pattern: Stair – *typ schodovitě zvyšující se zátěže*
  - Repetitions: 1 – *počet opakování*
  - Height: 0 – *velikost navýšení*
  - Duration: 360 sec. – *čas trvání*

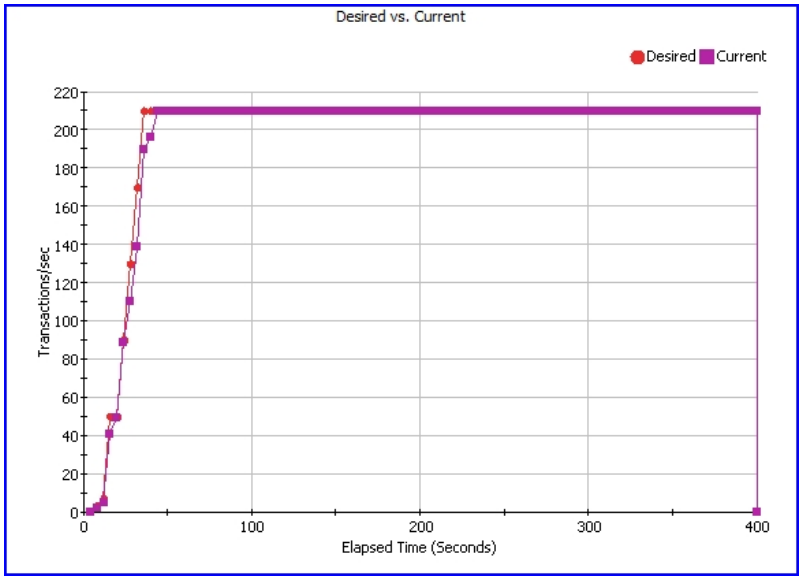
Výsledky:

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	78606	196	Minimum	1.0	1.0	0.104	0.08	0.0	Attempted	78606
	Successful	78606	196	Maximum	1.0	1.0	0.523	0.393	0.248	Established	78606
	Unsuccessful	0	0	Average	1.0	1.0	0.112	0.084	0.0		
	Aborted	0	0								

User Profile Definitions	Test							
	Profile	Percentage	Think Time (seconds)	Aborted	Protocol	Persistent Connection	Transactions Per Connection	Connections Per Server
	Default_0	100.000%	0.0	0 % after 0 seconds	HTTP 1.1	Enabled	50	2

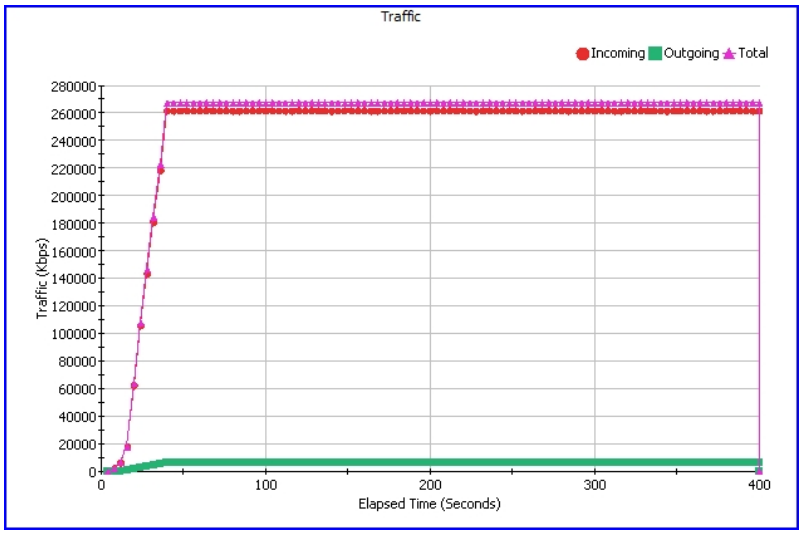
Obr. 7.2: Počet úspěšných transakcí při 1. měření

Na obrázku 7.2 je patrný celkový počet vygenerovaných transakcí (78606) a také úspěšnost jejich zpracování firewallem, která je 100%.



Obr. 7.3: Počet vygenerovaných transakcí/s při 1. měření

Další obrázek 7.3 ukazuje závislost požadovaných a zpracovaných transakcí za sekundu, jehož maximální hodnota reprezentovala 210 transakci/s.



Obr. 7.4: Vytížení linky při 1. měření

Obrázek 7.4 reprezentuje velikost vytížení linky, které bylo při testování naměřeno.

7.1.2 Měření: 2

Při druhém měření bude konfigurace obdobná jako u prvního měření. Lišit se budou pouze následující hodnoty v nastavení klientské části generátoru:

- Loads / Phase Editor / Label: Stair Step – *schodovitě zvyšující se zátěž*
  - Pattern: Stair – *typ schodovitě zvyšující se zátěže*
  - Repetitions: 5 – *počet opakování*
  - Height: 80 – *velikost navýšení*
  - Duration: 25 sec. – *čas trvání*

Zvýšením parametru Height na hodnotu 80 na dostaneme dvojnásobný počet generovaných transakcí za vteřinu a to přesně 410 transakcí/s.

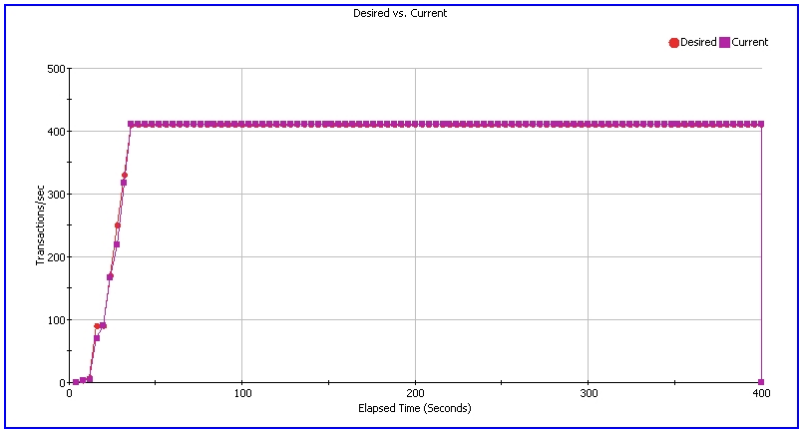
Výsledky:

Při druhém měření bylo vygenerováno celkově transakcí 154105 viz obrázek 7.5. Úspěšnost zpracování transakcí je opět 100%.

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	154105	385	Minimum	1.0	1.0	0.103	0.08	0.0	Attempted	154105
	Successful	154105	385	Maximum	1.0	1.0	0.524	0.4	0.291	Established	154105
	Unsuccessful	0	0	Average	1.0	1.0	0.109	0.083	0.0		
	Aborted	0	0								

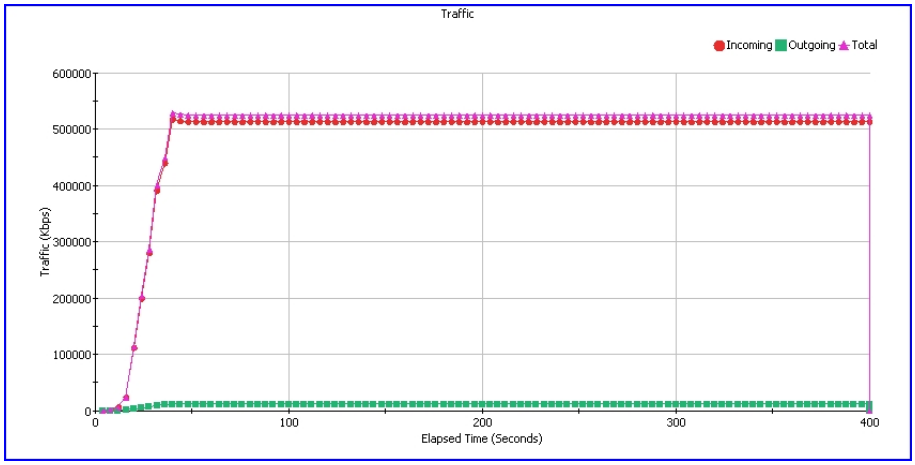
User Profile Definitions	Test							
	Profile	Percentage	Think Time (seconds)	Aborted	Protocol	Persistent Connection	Transactions Per Connection	Connections Per Server
	Default_0	100.000%	0.0	0 % after 0 seconds	HTTP 1.1	Enabled	50	2

Obr. 7.5: Počet úspěšných transakcí při 2. měření



Obr. 7.6: Počet vygenerovaných transakcí/s při 2. měření

Závislost požadovaných a zpracovaných transakcí znázorňuje obrázek 7.6. Velikost vytížení linky, které bylo při testování naměřeno, reprezentuje obrázek 7.7.



Obr. 7.7: Vytížení linky při 2. měření

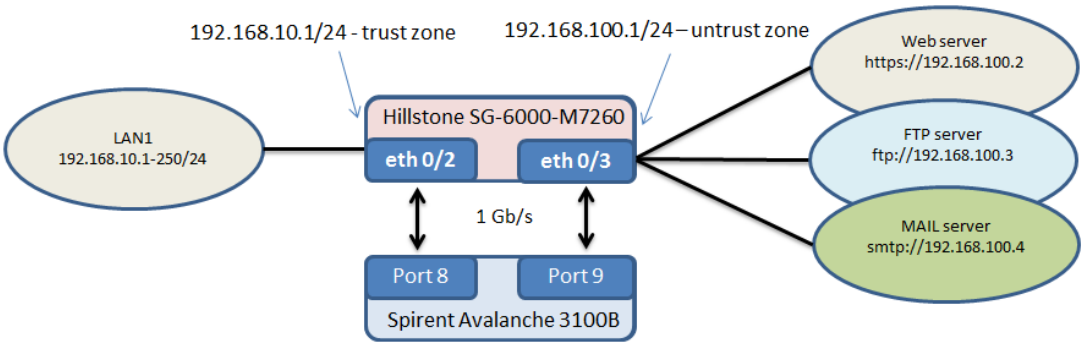
7.1.3 Hodnocení výkonového měření 1. scénáře: Domácnost

Z výše naměřených hodnot a výsledků můžeme usoudit, že při prvním výkonovém testování, kde byla simulována zátěž domácí sítě, firewall generovanou zátěž při obou měřeních se značnou rezervou bez jediné chyby propustil. Tudíž můžeme konstatovat, že testovaný firewall Hillstone SG-6000-M7260 je po výkonové stránce dostačující pro využití v domácnosti.

7.2 Scénář č. 2: Firma

Druhý vytvořený scénář, simuluje použití firewallu Hillstone SG-6000-M7260 v menší společnosti. Firewall bude připojený k LAN o počtu 248 klientů.

Na druhé straně v tzv. untrust zóně bude pomocí zařízení Spirent Avalanche nasimulovaný FTP server, webový HTTPS server a také poštovní SMTP server. Jednotlivá měření otestují schopnost firewallu propouštět generovaný provoz na jednotlivých serverech. Schéma zapojení testovaného firewallu a generátoru Spirent Avalanche reprezentuje obrázek 7.8. Stejně jako u prvního scénáře jsou síťové porty firewallu a generátoru zátěže propojeny UTP kabely přes síťová rozhraní Gigabit Ethernet. Proto musí být pro generování zátěže brána v potaz maximální možná přenosová rychlost 1 Gb/s.



Obr. 7.8: Schéma zapojení výkonového testování scénáře č. 2

7.2.1 Měření: FTP serveru

Při výkonovém testování FTP bude generována zátěž typu SimUsers/second, kterou bude generována zátěž o požadovaném počtu současně připojených uživatelů. Požadavkem klientské části generátoru od FTP serveru bude načtení souboru o velikosti 1 MB jednotlivých generovaných uživatelů. Příkazem:

```
1 ftp://192.168.100.3/1m
```

zadaném v Actions Listu v aplikaci Spirent TestCenter Layer 4-7 Application 4.43 definujeme adresu FTP serveru a také předdefinovanou velikost souboru.

Klientská část je nakonfigurována následovně:

- Subnets / IP Adress (Range): 192.168.10.2-250/24 – *rozsah IP adres*
- Loads / Phase Editor / Label: Delay – *počátečního prodlení měření*
  - Pattern: Flat – *typ rovnoměrné zátěže*
  - Repetitions: 1 – *počet opakování*
  - Height: 0 – *velikost navýšení*
  - Duration: 5 sec. – *čas trvání*
- Loads / Phase Editor / Label: Stair Step – *typ schodovitě zvyšující se zátěže*
  - Pattern: Stair – *typ schodovité zátěže*
  - Repetitions: 5 – *počet opakování*
  - Height: 10 – *velikost navýšení*
  - Duration: 25 sec. – *čas trvání*
- Loads / Phase Editor / Label: Steady State – *ustáleně generující se zátež*
  - Pattern: Stair – *typ schodovité zátěže*
  - Repetitions: 1 – *počet opakování*
  - Height: 0 – *velikost navýšení*
  - Duration: 360 sec. – *čas trvání*

Výsledky:

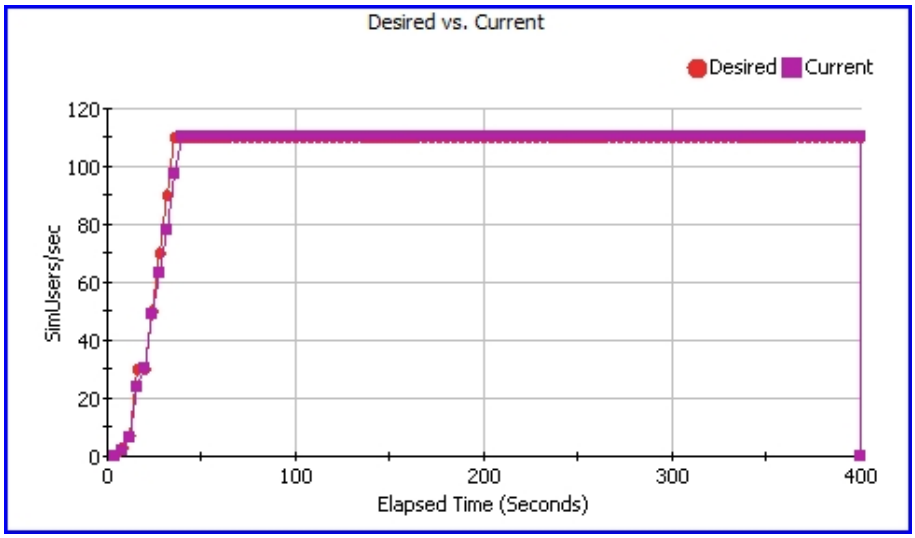
Při druhém měření FTP serveru bylo vygenerováno celkově 41286 viz obrázek 7.9. Úspěšnost zpracování transakcí se dá považovat téměř za 100%, pouze jedna transakce byla přerušena.

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	41286	-	Minimum	0.0	139.0	0.098	0.0	0.0	Attempted	82572
	Successful	41285	-	Maximum	0.0	146.0	1.422	0.0	1.119	Established	82572
	Unsuccessful	0	-	Average		141.675	0.389	0.0	0.04		
	Aborted	1	-								

User Profile Definitions	Test							
	Profile	Percentage	Think Time (seconds)	Aborted	Protocol	Persistent Connection	Transactions Per Connection	Connections Per Server
	Default_0	100.000%	0.0	0 % after 0 seconds	FTP	Enabled	50	2

Obr. 7.9: Počet úspěšných transakcí při měření FTP serveru

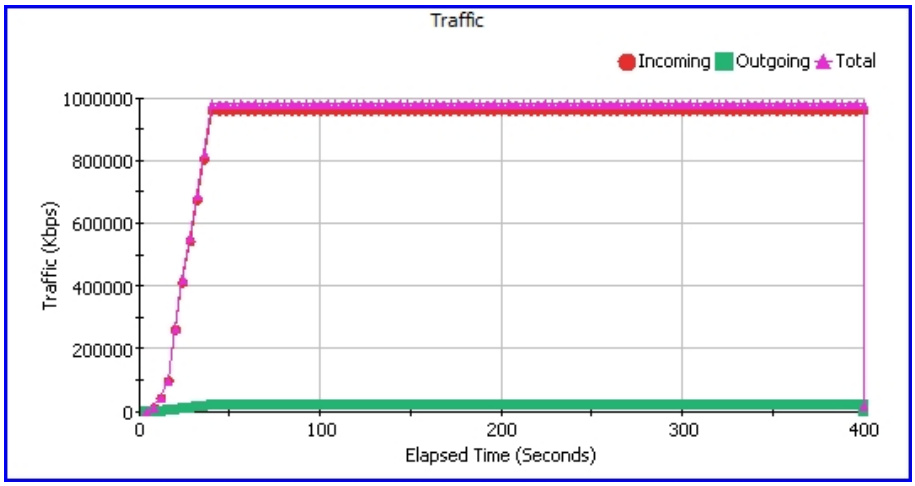
Další obrázek 7.10 ukazuje závislost počtu vytvořených a zpracovaných uživatelů za sekundu, který se pohyboval okolo 110 generovaných uživatelů za sekundu.



Obr. 7.10: Počet vygenerovaných uživatelů/s při měření FTP serveru

Vytížení linky, které bylo při měření FTP serveru obsazené je znázorněno na obrázku 7.11.

Hodnota se pohybuje na hranici možné přenosové rychlost, kterou umožní použité síťové rozhraní o maximální rychlosti 1 Gb/s. Z tohoto důvodu můžeme usoudit, že testovaný firewall zvládne zpracovat všechny FTP požadavky, které je možné vygenerovat přes dostupné síťové rozhraní.



Obr. 7.11: Vytížení linky při měření FTP serveru

7.2.2 Měření: SMTP serveru

Při výkonovém měření SMTP serveru budeme přes testovaný firewall odesílat mailové požadavky z klientské části generátoru Spirent Avalanche přes vytvořený SMTP server na druhém rozhraní firewallu.

Příkazem:

```
smtp://192.168.100.4
FROM=<uzivatel@test-vutbr.cz>
TO=<a@test-vutbr.cz,b@test-vutbr.cz,c@test-vutbr.cz>
DATA=<FIXED,500>
```

zadaném v Actions Listu v aplikaci Spirent TestCenter Layer 4-7 Application 4.43 definujeme adresu SMTP serveru, dále v poli FROM vytvořeného odesílatele a v poli TO 3 adresáty, kterým bude e-mailová zpráva odeslána. V poli DATA definujeme fixní velikost textu zprávy, nastavenou na 500 alfa-numerických znaků. Typ generované zátěže bude Transaction/s.

Klientská část je nakonfigurována následovně:

- Subnets / IP Adress (Range): 192.168.10.2-250/24 – *rozsah IP adres*
- Loads / Phase Editor / Label: Delay – *počátečního prodlení měření*
  - Pattern: Flat – *typ rovnoměrné zátěže*
  - Repetitions: 1 – *počet opakování*
  - Height: 0 – *velikost navýšení*
  - Duration: 5 sec. – *čas trvání*
- Loads / Phase Editor / Label: Stair Step – *schodovitě zvyšující se zátěž*
  - Pattern: Stair – *typ schodovitě zvyšující se zátěže*
  - Repetitions: 5 – *počet opakování*

  - Height: 1000 – *velikost navýšení*
  - Duration: 25 sec. – *čas trvání*
- Loads / Phase Editor / Label: Steady State – *ustáleně generující se zátěž*
  - Pattern: Stair – *typ schodovitě zvyšující se zátěže*
  - Repetitions: 1 – *počet opakování*
  - Height: 0 – *velikost navýšení*
  - Duration: 360 sec. – *čas trvání*

Výsledky:

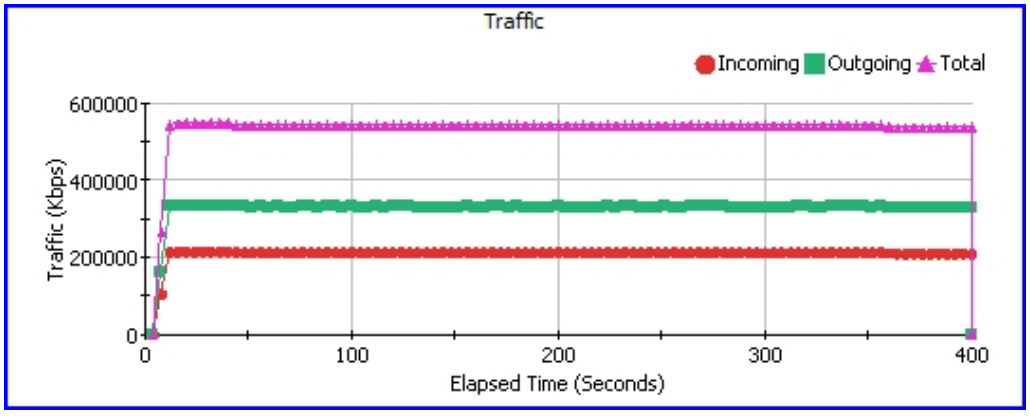
Na obrázku 7.12 je patrný celkový počet 11096100 vygenerovaných transakcí a také úspěšnost 100% jejich zpracování firewallem.

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	11096100	-	Minimum	0.0	0.0	0.097	0.0	0.0	Attempted	11096100
	Successful	11096100	-	Maximum	0.0	2.0	0.636	0.0	0.171	Established	11096100
	Unsuccessful	0	-	Average		0.0	0.111	0.0	0.0		
	Aborted	0	-								

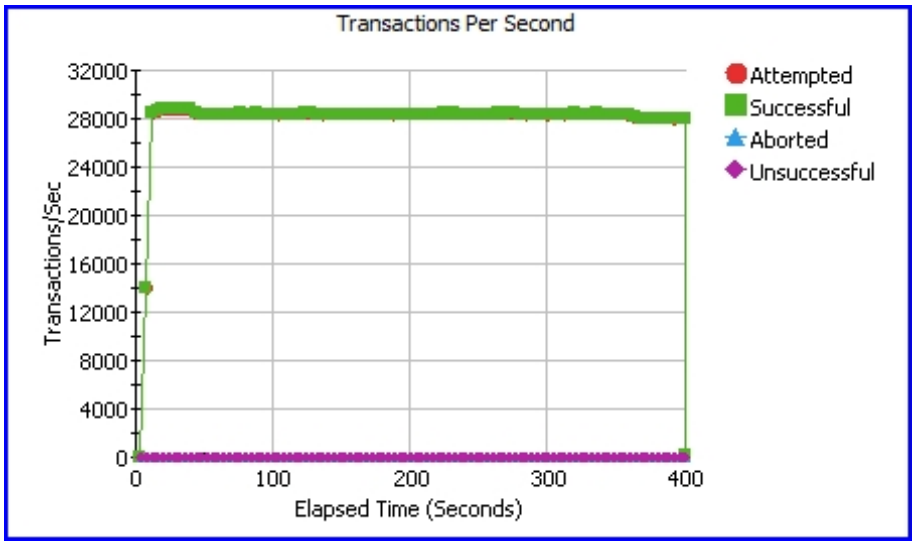
User Profile Definitions	Test							
	Profile	Percentage	Think Time (seconds)	Aborted	Protocol	Persistent Connection	Transactions Per Connection	Connections Per Server
	Default_0	100.000%	0.0	0 % after 0 seconds	SMTP	Enabled	50	2

Obr. 7.12: Počet úspěšných transakcí při měření SMTP serveru

Počet vygenerovaných transakcí/s nalezneme na obrázku 7.14 a velikost výsledné přenosové rychlosti na obrázku 7.13.



Obr. 7.13: Vytížení linky při měření SMTP serveru



Obr. 7.14: Počet vygenerovaných transakcí/s při měření SMTP serveru

7.2.3 Měření: HTTPS serveru

Při výkonovém měření HTTPS serveru ve druhém scénáři bude vygenerovaná síťová zátěž, která bude dosahovat téměř maximálního vytížení linky pro použité síťové rozhraní Gigabit Ethernet, tedy zátěž okolo 1 Gb/s. Generována zátěž bude typu Transaction/s.

Příkazem:

```
1 get https://192.168.100.3/index.html
```

zadaném v Actions Listu v aplikaci Spirent TestCenter Layer 4-7 Application 4.43 definujeme adresu HTTPS serveru. Velikost požadovaného souboru index.html, je stejně jako při měření HTTP serveru v prvním scénáři, nastavena na 150 kB. Typ generované zátěže bude Transaction/s.

Klientská část je nakonfigurována následovně:

- Subnets / IP Adress (Range): 192.168.10.2-250/24 – *rozsah IP adres*
- Loads / Phase Editor / Label: Delay – *počátečního prodlení měření*
  - Pattern: Flat – *typ rovnoměrné zátěže*
  - Repetitions: 1 – *počet opakování*
  - Height: 0 – *velikost navýšení*
  - Duration: 5 sec. – *čas trvání*
- Loads / Phase Editor / Label: Stair Step – *schodovitě zvyšující se zátěž*
  - Pattern: Stair – *typ schodovitě zvyšující se zátěže*
  - Repetitions: 5 – *počet opakování*
  - Height: 100 – *velikost navýšení*

  - Duration: 25 sec. – *čas trvání*
- Loads / Phase Editor / Label: Steady State – *ustáleně genereující se zátež*
  - Pattern: Stair – *typ schodovité zátěže*
  - Repetitions: 1 – *počet opakování*
  - Height: 0 – *velikost navýšení*
  - Duration: 360 sec. – *čas trvání*

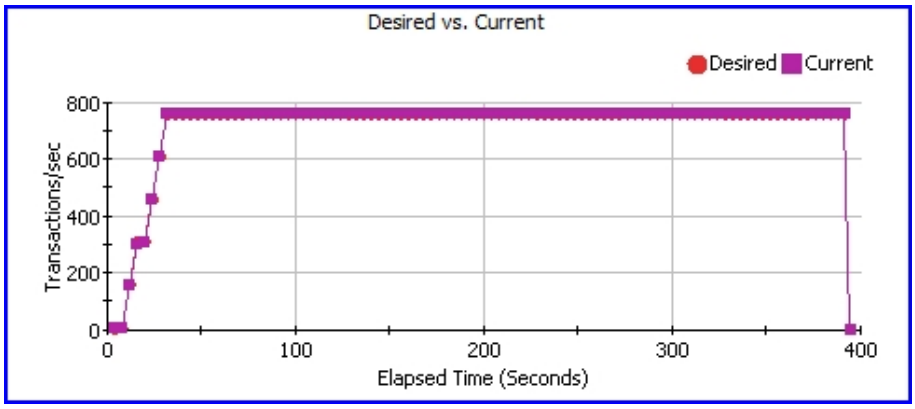
Výsledky:

Při měření HTTPS serveru bylo vygenerováno celkově 285127 transakcí, viz obrázek 7.15. Úspěšnost zpracování transakcí je 100%. Žádná generovaná transakce nebyla odmítnutá ani zahozená. Závislost požadovaných a zpracovaných transakcí znázorňuje obrázek 7.16. Požadovanou velikost přenosové rychlosti (pohybující se na hranici 1 Gb/s) reprezentuje obrázek 7.17.

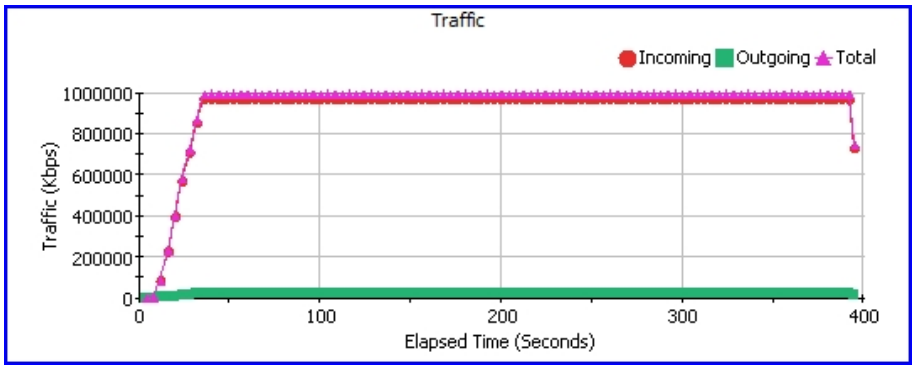
Test Results Summary	Transactions			Time (ms)						TCP Connections	
		Total	Rate Per Second		Page Response	URL Response	To TCP SYN/ACK	To First Data Byte	Est. Server Response		Total
	Attempted	285127	721	Minimum	1.0	1.0	0.104	0.114	0.0	Attempted	285127
	Successful	285127	721	Maximum	7.0	7.0	1.241	1.503	0.883	Established	285127
	Unsuccessful	0	0	Average	5.99	5.989	0.884	0.775	0.168		
	Aborted	0	0								

User Profile Definitions	Test							
	Profile	Percentage	Think Time (seconds)	Aborted	Protocol	Persistent Connection	Transactions Per Connection	Connections Per Server
	Default_0	100.000%	0.0	0 % after 0 seconds	HTTP 1.1	Enabled	50	2

Obr. 7.15: Počet úspěšných transakcí při měření HTTPS serveru



Obr. 7.16: Počet vygenerovaných transakcí/s při měření HTTPS serveru



Obr. 7.17: Vytížení linky při měření HTTPS serveru

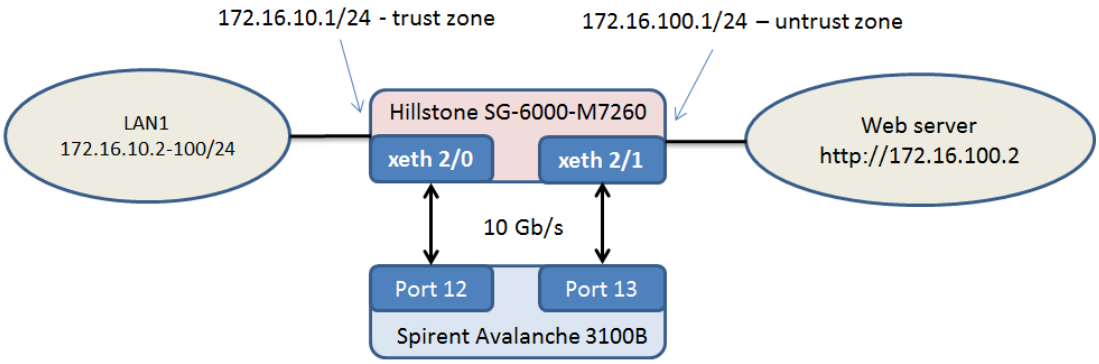
7.2.4 Hodnocení výkonového měření 2. scénáře: Firma

Z výše naměřených hodnot a výsledků je patrné, že i při druhém výkonovém testování, kde byla simulována síťová zátěž ve firmě, firewall generovanou zátěž při všech 3 typech připojených serverů (FTP, SMTP a HTTPS) dokázal bez chyby propustit. Při generování FTP a HTTPS požadavků byla generována maximální možná zátěž, které umožňuje využité 1000Base-T síťové rozhraní.

Jelikož úspěšnost transakcí při takové zátěži byla 100%, tak můžeme konstatovat, že testovaný firewall Hillstone SG-6000-M7260 je po výkonové stránce dostačující pro využití ve firmě, využívající síťová rozhraní technologie Gigabit Ethernet.

7.3 Scénář č. 3: Maximální zátěž

Jak jsme se dozvěděli v kapitole 4.3, v posledním testovacím scénáři bude generovaná zátěž dosahovat přenosové rychlosti až 10 Gb/s. Schéma zapojení měření nalezneme na obrázku 7.18.



Obr. 7.18: Schéma zapojení výkonového testování scénáře č. 3

Generovaná zátěž bude nastavena tak, že v 5 krocích bude skokově růst až na limitní hodnotu transakcí/s, která bude přesahovat přenosovou rychlost 10 Gb/s. Probíhajícími transakcemi bude probíhat požadavek klientské části generátoru o data HTTP serveru a následná odpověď serveru. Adresu HTTP serveru definujeme zadáním následujícího příkazu v poli Actions List:

```
1 get http://172.16.100.2/index.html
```

Probíhat budou HTTP transakce o velikosti 150 kB, což představuje velikost souboru index.html. Další konfigurace pole *Phase Editor* v klientské části aplikace Spirent TestCenter Layer 4-7 Application 4.43 je následující:

- Subnets / IP Adress (Range): 172.16.10.2-100/24 – *rozsah IP adres*
- Loads / Phase Editor / Label: Delay – *počáteční prodlení měření*
  - Pattern: Flat – *rovnoměrný typ zátěže*
  - Repetitions: 1 – *počet opakování*
  - Height: 0 – *velikost navýšení*
  - Duration: 5 sec. – *doba trvání*
- Loads / Phase Editor / Label: Stair Step – *schodovitě zvyšující se zátěž*
  - Pattern: Stair – *typ schodovité zátěže*
  - Repetitions: 5 – *počet opakování skoků*
  - Height: 1800 – *velikost navýšení*
  - Ramp Time: 40 sec. – *doba trvání navýšení jednoho skoku*
  - Steady Time: 70 sec. – *doba rovnoměrného generování jednoho skoku*

S výše uvedenou konfigurací generátoru Spirent budou probíhat pouze měření propustnosti 3. scénáře. Poslední měření 3. scénáře, které bude mít za úkol zjistit hodnotu maximálního počtu úspěšně procházejících transakcí/s bude konfigurace generátoru přenastavena dle hodnot uvedených v kapitole 7.3.4, obhajující přímo výsledky daného měření.

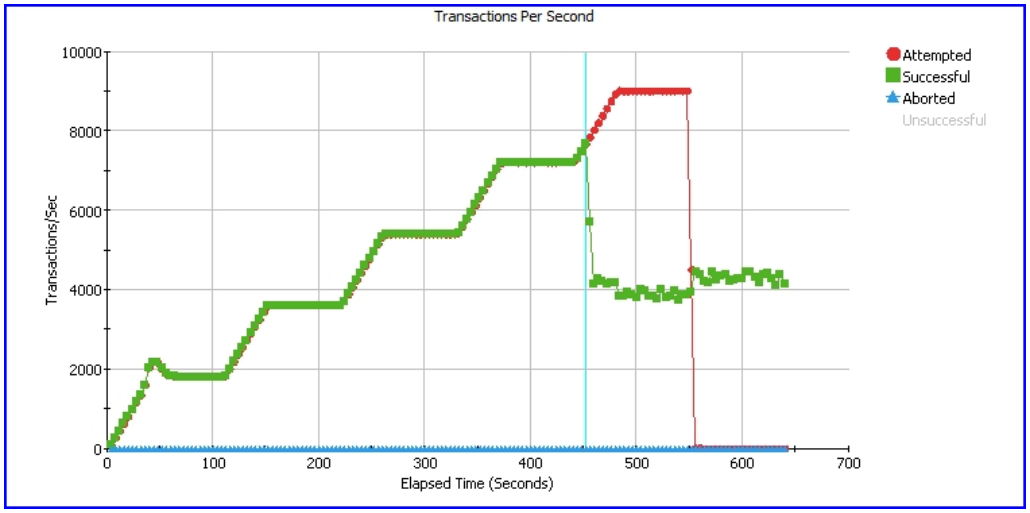
7.3.1 Měření propustnosti bez přidaných bezp. prvků

Při měření výkonosti firewallu bez zapnutých přídavných bezpečnostních prvků, tedy ve výchozím stavu byly naměřeny následující výsledky.

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	2801159	4374	Minimum	0.0	0.0	0.119	0.066	0.0	Attempted	2801159
	Successful	2717338	4242	Maximum	101250.0	101250.0	6053.602	98644.453	98606.18	Established	2801111
	Unsuccessful	83821	126	Average	14254.363	14254.362	27.763	14236.214	14205.265		
	Aborted	0	0								

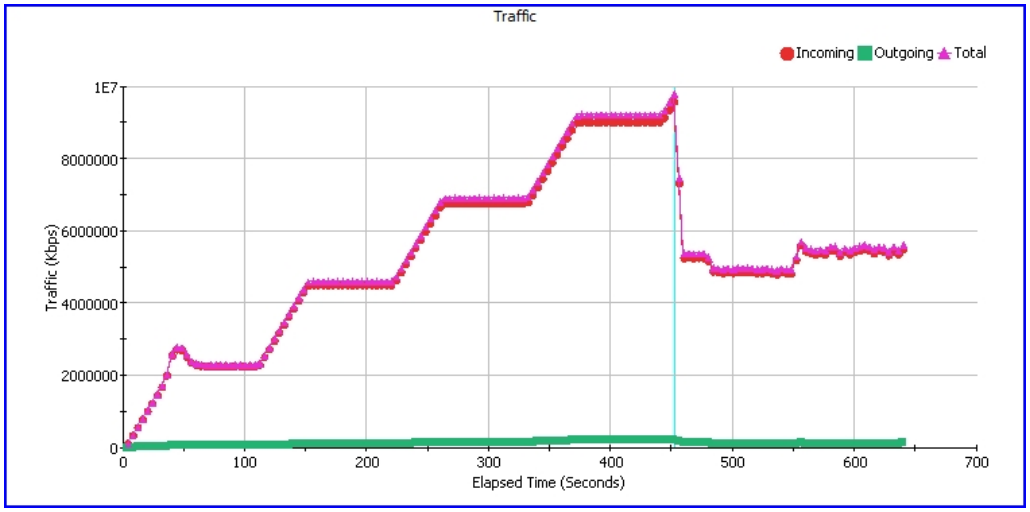
Obr. 7.19: Počet úspěšných transakcí při 1. měření 3. scénáře

Obrázek 7.19 reprezentuje celkový počet úspěšných a neúspěšných transakcí. Celkově bylo při prvním měření 3. scénáře vygenerováno 2801159 transakcí, z toho bylo 2717338 úspěšných a 83821 transakcích bylo neúspěšných. Procentuální hodnota úspěšnosti transakcí je 97,01%.



Obr. 7.20: Počet vygenerovaných transakcí/s při 1. měření 3. scénáře

Další obrázek 7.20 ukazuje závislost vygenerovaných transakcí/s a jejich úspěšnosti v čase. Z výsledného grafu je patrné, že v čase 452 sekund trvání měření, kdy generovaná zátěž dosáhla hodnoty 7668 transakcí/s, začíná firewall pakety zahazovat a probíhající transakce začínají být neúspěšné.



Obr. 7.21: Vytížení linky při 1. měření 3. scénáře

Při pohledu na obrázek 7.21, který vyobrazuje průběh přenosové rychlosti, je patrný fakt, že ve stejný čas, kdy firewall začal pakety zahazovat a transakce začínají

být neúspěšné (v čase 452 sekund), dosahuje velikost přenosové rychlosti 9,799892 Gb/s, což se dá považovat za reálnou hranici možného vytížení linky při použití 10GbE portů.

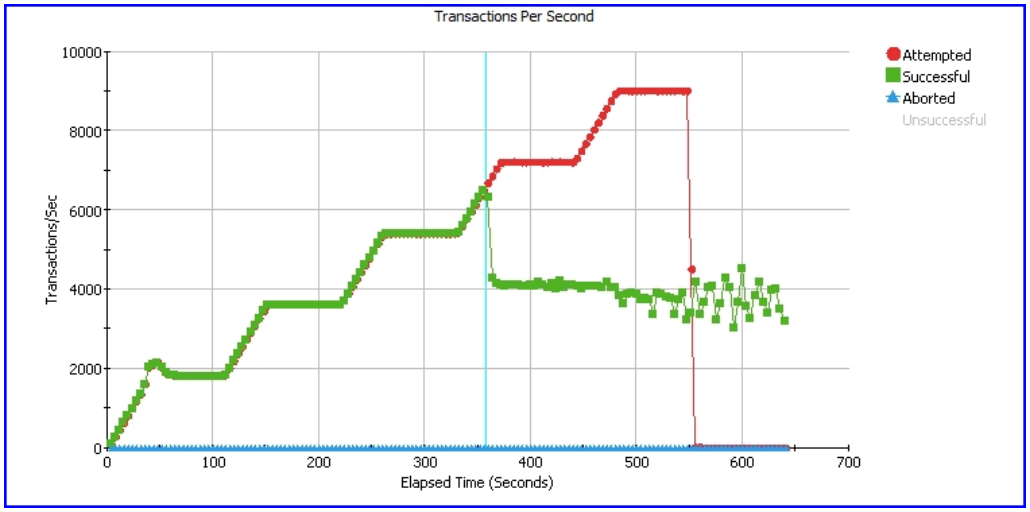
Můžeme tedy konstatovat, že při používání firewallu ve výchozím stavu, tedy bez zapnutých přídavných bezpečnostních prvků IPS a Antiviru, byl firewall schopný propouštět generovaný provoz, který byl v našem případě limitovaný propustností připojených 10GbE portů. Při pohledu do vybraných specifikací firewallu Hillstone SG-6000-M7260 v tabulce 5.2 je propustnost firewallu ve výchozím stavu stanovena na 16/20 Gb/s. Při testovaní firewallu pomocí zařízení Spirent Avalanche s využitím dvou 10GbE portů však není možné definovanou hranici propustnosti firewallu reálně otestovat.

7.3.2 Měření propustnosti s funkcí IPS

Při zapnutí bezpečnostního prvku IPS došlo k ovlivnění výkonnosti firewallu. Při generovaní totožné zátěže, jako v předešlém měření, byly naměřeny odlišné hodnoty. Na obrázku 7.22 je znázorněn celkový počet úspěšných a neúspěšných transakcí.

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	2800853	4368	Minimum	1.0	1.0	0.137	0.142	0.0	Attempted	2800853
	Successful	2358350	3677	Maximum	143818.0	143818.0	6055.023	136542.594	136494.875	Established	2799673
	Unsuccessful	442503	688	Average	28948.557	28948.556	50.694	29065.529	28963.777		
	Aborted	0	0								

Obr. 7.22: Počet úspěšných transakcí při druhém měření 3. scénáře

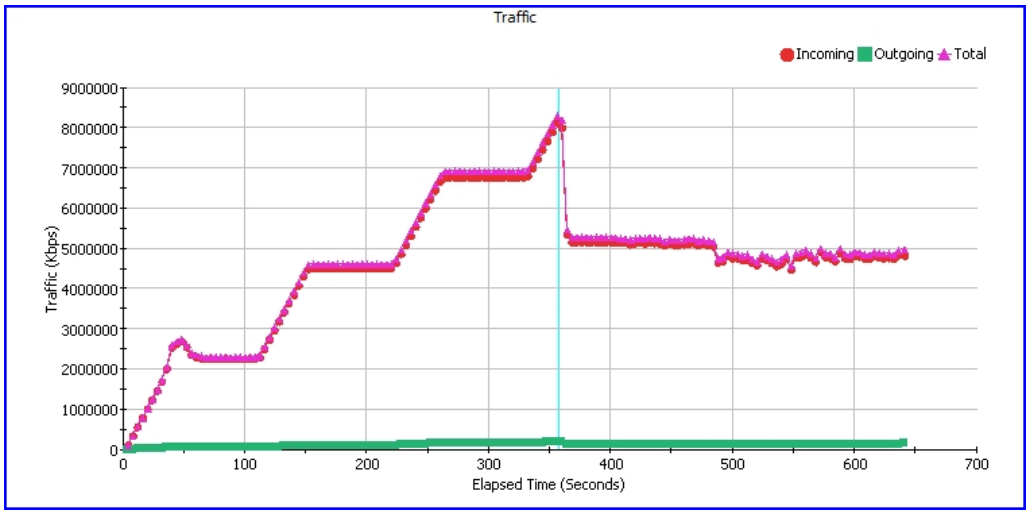


Obr. 7.23: Počet vygenerovaných transakcí/s při druhém měření 3. scénáře

Při druhém měření 3. scénáře bylo vygenerováno celkem 2800853 transakcí. 2358350 transakcí bylo úspěšných a 442503 transakcích neúspěšných. Procentuální úspěšnost transakcí se snížila na 84,20%.

Obrázek 7.23 ukazuje závislost úspěšnosti vygenerovaných transakcí/s v čase. I zde byly naměřeny odlišné hodnoty. K výraznému zahazování probíhajících paketů dochází již v čase 356 s, kdy generovaná zátěž dosáhla hodnoty 6677 transakcí/s.

Jak je patrné na obrázku 7.24, který zobrazuje celkové vytížení linky, hranice kde firewall v čase 356 sekund začíná mít problém se zahazováním paketů je na hodnotě 8,315362 Gb/s.



Obr. 7.24: Vytížení linky při druhém měření 3. scénáře

Naměřená maximální hodnota přenosové rychlosti 8,315362 Gb/s je menší než reálná hranice možné propustnosti 10GbE rozhraní. Výsledek tudíž nemohl být limitovaný nedostatečnou propustností linky. Sledováním vytížení CPU firewallu Hillstone SG-6000-M7260 při generování zátěže byla zjištěna informace, že v okamžiku, kdy začaly být transakce neúspěšné, bylo CPU vytíženo na 94,7 %. Zatížení CPU bylo v reálném čase měření sledováno přes SSH připojení, viz obrázek 7.25.

```
SG-6000# show cpu
Average cpu utilization : 0.9%
Current cpu utilization :94.7%
Last 1 minute :93.3%
Last 5 minutes :85.1%
Last 15 minutes :36.5%
```

Obr. 7.25: Vytížení CPU firewallu při druhém měření 3. scénáře

Ze zjištěných skutečností je patrné, že při používání bezpečnostní funkce IPS je

CPU firewallu vytíženo natolik, že výsledná propustnost firewallu při druhém měření 3. scénáře dosahuje hraniční hodnoty 8,315362 Gb/s.

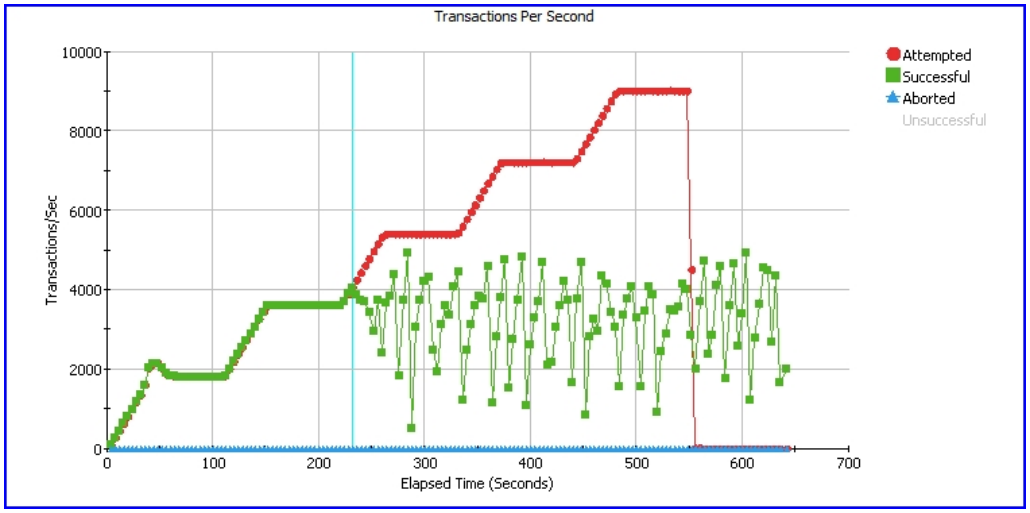
7.3.3 Měření propustnosti s funkcí IPS a Antiviru

Při třetím měření 3. scénáře byla na firewallu Hillstone k bezpečnostní funkci IPS zapnuta i funkce Antiviru. Vzájemné používání IPS a Antiviru značně ovlivnilo výkonnost propustnosti firewallu, což se projevilo na výsledných hodnotách třetího měření.

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	2800892	4365	Minimum	2.0	2.0	0.139	0.219	0.0	Attempted	2800892
	Successful	1904030	2965	Maximum	199671.0	199671.0	13532.634	183800.578	183748.047	Established	2795299
	Unsuccessful	896862	1395	Average	58319.928	58319.926	284.122	56892.442	56511.59		
	Aborted	0	0								

Obr. 7.26: Počet úspěšných transakcí při třetím měření 3. scénáře

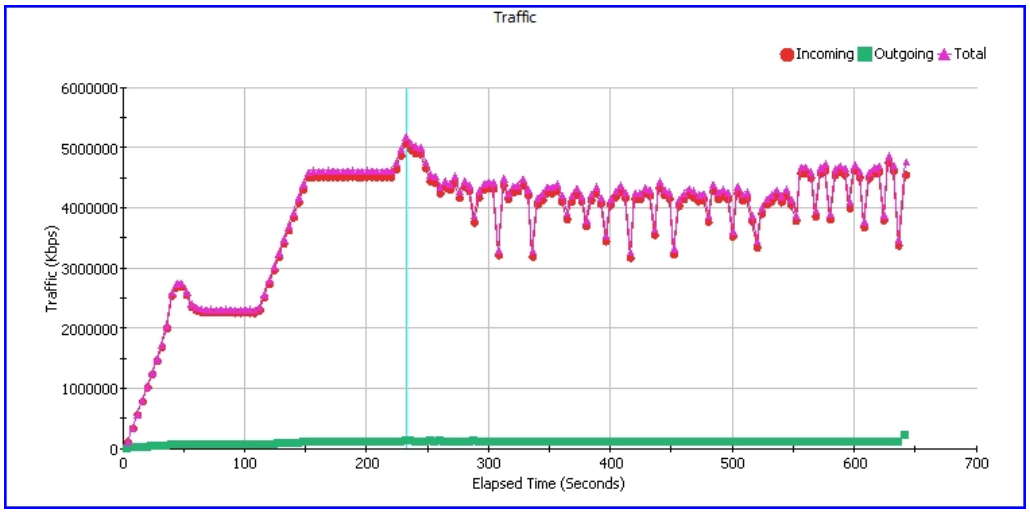
Počet úspěšných transakcí (obrázek 7.26) se snížil na hodnotu 1904030 z celkového počtu 2800892 vygenerovaných transakcí. Počet neúspěšných transakcí naopak vzrostl na hodnotu 896862 transakcí. Procentuální úspěšnost transakcí klesla na 67,97 %.



Obr. 7.27: Počet vygenerovaných transakcí/s při třetím měření 3. scénáře

Při pohledu na graf na obrázku 7.27 je zřejmé, že firewall začal zahazovat pakety již v čase 232 sekund. Generovaná zátěž v tento čas dosáhla hodnoty 4068 transakcí/s.

Maximální hodnota přenosové rychlosti se při použití funkce IPS a Antiviru na firewallu, dle obrázku 7.28, zastavila na hodnotě 5,191655 Gb/s.



Obr. 7.28: Vytížení linky při třetím měření 3. scénáře

Stejně jako při druhém měření je výsledná propustnost menší než reálná hranice možného vytížení linky 10GbE rozhraní. Opět se potvrdila skutečnost, že při vytížení CPU firewallu okolo 95 %, začínají být požadované transakce firewallu neúspěšné. Vzájemné používání bezpečnostních funkcí IPS a Antiviru má tedy za následek výrazné vytížení CPU firewallu přídavnými funkcemi a detailnější kontrolou procházející komunikace a tím pádem snížení dostupné síťové propustnosti a to přibližně na polovinu možného vytížení linky 10GbE rozhraní.

7.3.4 Měření hraniční hodnoty transakcí/s

V předchozích měřeních 3. scénáře jsme byli v počtu generovaných transakcí/s omezeni velikostí přenosové rychlosti probíhající zátěže. Abychom mohli otestovat, kolik transakcí/s je firewall schopen zpracovávat, budeme muset upravit velikost souboru index.html, definovaného na straně HTTP serveru. V předchozích měřeních byla velikost souboru index.html nastavena na 150 kB, kterou pro měření maximální hodnoty úspěšných transakcí/s snížíme (záložka *Server - Transaction - Size*) na hodnotu 150 B. Oproti předchozích měření 3. scénáře upravíme také velikost a tvar generované zátěže.

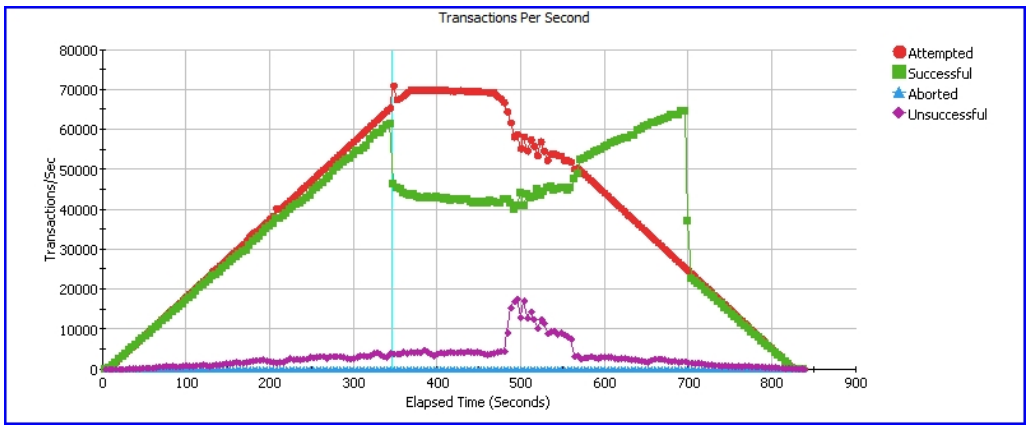
Důležité je také zmínit, že při měření budou na firewallu vypnuté přídavné bezpečnostní funkce IPS a Antiviru a bude tedy ve výchozím stavu. Klientská část aplikace Spirent TestCenter Layer 4-7 Application 4.43 je nastavena následovně:

- Subnets / IP Adress (Range): 172.16.10.2-100/24 – *rozsah IP adres*
- Loads / Phase Editor / Label: Stair Step – *schodovitě zvyšující se zátěž*
  - Pattern: Stair – *typ schodovité zátěže*
  - Repetitions: 1 – *počet opakování skoků (schodů)*

  - Height: 70000 – *velikost navýšení*
  - Ramp Time: 360 sec. – *doba trvání navýšení jednoho skoku*
  - Steady Time: 100 sec. – *doba rovnoměrného generování jednoho skoku*
- Loads / Phase Editor / Label: Ramp Down – *klesající zátěž*
  - Pattern: Flat – *typ zátěže*
  - Repetitions: 1 – *počet opakování skoků (schodů)*
  - Height: 0 – *velikost navýšení*
  - Ramp Time: 360 sec. – *doba trvání navýšení jednoho skoku*
  - Steady Time: 100 sec. – *doba rovnoměrného generování jednoho skoku*

Výsledky:

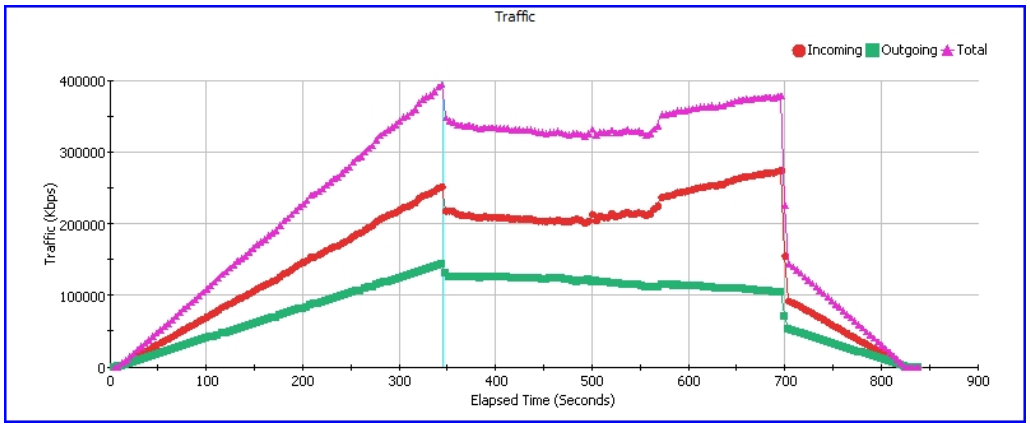
Generovaný provoz byl nastavený, aby lineárně vzrůstal počet generovaných transakcí/s až na hodnotu 70000 transakcí/s. Na obrázku 7.29 vidíme průběh generovaných transakcí a také jejich úspěšnost.



Obr. 7.29: Počet vygenerovaných transakcí/s při čtvrtém měření 3. scénáře

Při pohledu na výsledný graf je vidět, že s rostoucí hodnotou generovaných transakcí/s počet úspěšných transakcí/s mírně klesá. Do hodnoty 65499 transakcí/s se ovšem jedná o minimální chybovost. V tomto intervalu linka představující úspěšné transakce/s pouze s mírnou odchylkou opisuje linku transakcí generovaných. V čase 344 sekund, kdy hodnota generovaných transakcí/s dosáhla hodnoty 65499, je ovšem patrný velký propad úspěšných transakcí/s, který se projevil i na grafu reprezentující vytížení linky, viz obrázek 7.29.

Velikost přenosové rychlosti, která dosáhla maximální hodnoty 394,714 Mb/s zdaleka nedosáhla hranice dostupné propustnosti použitých síťových rozhraní. Důvodem propadu zpracovávaných transakcí bylo podobně jako při druhém a třetím



Obr. 7.30: Vytížení linky při čtvrtém měření 3. scénáře

měření 3. scénáře přetížení CPU firewallu. Z výsledných grafů daného měření 3. scénáře je tedy zřejmé, že pro firewall Hillstone SG-6000-M7260 je hraniční hodnota 65499 generovaných transakcí/s, které je firewall schopen úspěšně zpracovat.

7.3.5 Hodnocení výkonového testování 3. scénáře: Maximální zátěž

Při měřeních 3. scénáře, použitím optických kabelů a síťových rozhraní 10GbE, již byly zjištěny hodnoty generované zátěže, při kterých byl firewall Hillstone SG-6000-M7260 vytížen natolik, že procházející síťovou zátěž nedokázal úspěšně zpracovat. Jak již bylo uvedeno u jednotlivých měření, při použití přídavných funkcí firewallu byl značně ovlivněn výkon CPU firewallu a tím i výsledná propustnost. Tabulka 7.1 obsahuje souhrn výsledků, které byly naměřeny při testování propustnosti 3. scénáře.

Tab. 7.1: Souhrn výsledných parametrů při měření propustnosti 3. scénáře

Aktivované bezp. funkce firewallu	**Max. počet transakcí/s**	**Max. propustnost**	**Celková úspěšnost transakcí**
Firewall	7668	9,799892 Gb/s	97,01 %
Firewall + IPS	6677	8,315362 Gb/s	84,20 %
Firewall + IPS + Antivirus	4068	5,191655 Gb/s	67,97 %

Je nutné podotknout, že získané výsledné hodnoty prvního měření 3. scénáře, kde byl firewall ve výchozím nastavení bez přídavných bezpečnostních funkcí, nebyly způsobené chybou firewallu, nýbrž maximálním vytížením dostupné 10GbE linky při měření. Dle dokumentace je firewall Hillstone SG-6000-M7260 ve výchozím nastavení s použitím základních licencí schopný propouštět zátěž o přenosové rychlostí 16 Gb/s, kterou nebylo možné pomocí dvou 10GbE síťových portů na zařízení

Spirent Avalanche vygenerovat. Měřením propustnosti s přidanými bezpečnostními funkcemi IPS i Antiviru, již bylo možné zjistit hraniční hodnoty výkonnosti firewallu. Dle dokumentace testovaného firewallu můžeme porovnat hodnotu propustnosti IPS uvedené v dokumentaci a hodnotu naměřenou, při použití základních licencí. Při porovnání zjistíme, že naměřená hodnota maximální propustnosti 8,315362 Gb/s je mnohem větší, než je uvedená hodnota v dokumentaci 2 Gb/s (při použití základní licence). Při hledání souvislostí byl zjištěn fakt, že jediná dostupná dokumentace testovaného firewallu, ze které byly specifikace firewallu čerpány nebyla nikdy aktualizována a data uvedené v ní, odpovídají nejstaršímu firmwaru firewallu s označením StoneOS 5.0R3. Firma Hillstone od této verze vydala již několik updatů, které vedly k zlepšení výkonnostních parametrů. Z tohoto důvodu je výsledná hodnota naměřené IPS propustnosti větší, než uvedená hodnota. Měření probíhalo na nejnovější verzi firmwaru StoneOS 5.5R3P4. Ze stejného důvodu je větší i výsledná hodnota propustnosti IPS + Antiviru, než zvlášť uvedené hodnoty propustnosti IPS a Antiviru. Dalším parametrem výkonnosti firewallu, kterou se podařilo zjistit, byla hodnota maximálního počtu transakcí/s, který je firewall schopen úspěšně zpracovávat. Po snížení maximální přenosové rychlosti pro generování velkého počtu transakcí, byl získaný počet 65499 transakcí/s označen jako hraniční hodnota daného měření pro firewall Hillstone SG-6000-M7260.

8 ZÁVĚR

V teoretické části práce jsme se pro pochopení souvislostí bezpečnostní analýzy firewallu seznámili s obecnou definicí firewallu a s jeho možným rozdělením v závislosti, na které vrstvě síťového modelu pracují a na jakém principu jsou založeny. U každé varianty jsem se snažil popsat princip a uvést výhody a nevýhody použití daného typu firewallu.

Následující teoretická část bakalářské práce je věnována tématu bezpečnostních auditů a penetračního testování. V případě bezpečnostních auditů je vysvětlen jejich princip a také je zde nastíněn důvod, proč je důležité bezpečnostní audity u firewallů vykonávat. Dále jsou čtenáři seznámeni s penetračním testováním a s jejich dělením dle různých aspektů. Nalezneme zde také stručný popis nástrojů, které se nejčastěji využívají právě k bezpečnostnímu testování síťových prvků.

Další část bakalářské práce obsahuje návrh bezpečnostní analýzy, kde najdeme zvolené metody, které budou pro bezpečnostní analýzu firewallu použity a také návrh výkonnostního testování, kde jsou čtenářům představené scénáře pro testování výkonosti firewallu pomocí zařízení Spirent Avalanche.

V následující kapitole práce se nachází popis testovacího prostředí, které je realizované v laboratoři SC 5.37, dále stručná charakteristika testovaných firewallů Hillstone a představení zařízení Spirent Avalanche pro výkonnostní testování.

Závěrečná část práce patří výsledkům zvolených metod bezpečnostní analýzy firewallu Hillstone SG-6000-G2120 a výsledkům navržených scénářů výkonnostního testování firewallu Hillstone SG-6000-M7260. Výsledky bezpečnostní analýzy jsou rozděleny do tří částí. V první části byla analyzována síťová komunikace firewallu Hillstone ve dvou scénářích. První scénář je analýza komunikace při prvotní instalaci firewallu a druhý zachycuje komunikaci firewallu při chodu po dobu 48 hodin. Při analýze síťové komunikace nebyla nalezena žádná nevyžádaná komunikace ze strany firewallu, kterou by firewall například prozrazoval 3. straně soukromé informace. Druhá část obsahuje výsledky externí analýzy, kde byly oskenovány porty pomocí aplikace Nmap a vyhledávány možné bezpečnostní zranitelnosti vyhodnocené aplikací Nessus. V případě skenování portů, obě použité aplikace shodně nalezly otevřené TCP porty 22, 80 a 443. Aplikace Nessus navíc objevila možné zranitelnosti ve slabém šifrování protokolu SSH a HTTP. V poslední části výsledků nalezneme interní analýzu, která popisuje jakým způsobem je možné operační systém firewallu Hillstone konfigurovat a nastavovat. Dále jsou popsány možné přístupy do zařízení, řešení bezpečnosti uživatelských účtů a hesel a také jsou zmíněny možné zranitelnosti operačního systému. Výsledky měření navržených scénářů výkonnostního testování firewallu obsahují vždy popis konfigurace jednotlivých měření a komentované výsledky, opírající se především o údaje z výsledných grafů. Při testování prvních dvou

scénářů byl simulovaný síťový provoz domácnosti a malé podnikové sítě. Oba tyto scénáře využívali připojení pomocí rozhraní gigabitového Ethernetu a veškerý generovaný provoz testovaný firewall bez problému zpracoval. Při měření 3. scénáře, již byly použiti 10GbE porty a pomocí jejich měření, se podařilo zjistit hraniční hodnoty propustnosti firewallu, ale také úspěšnosti transakcí a maximálního počtu úspěšně zpracovatelných transakcí/s. Dále byl sledován vliv přidaných bezpečnostních funkcí IPS a Antiviru na celkovou výkonnost firewallu. Výsledné hodnoty byly porovnány s hodnotami, uvedenými v dostupné dokumentaci firewallu Hillstone SG-6000-M7260.

LITERATURA

[1] STREBE, Matthew PERKINS, Charles. *Firewally a proxy-servery: Praktický průvodce.* Brno: Computer Press, 2003, 450 stran. ISBN 80-7726-983-6

[2] KRAJÍČEK, J. *Bezpečnostní audit firewallu: diplomová práce.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 76 stran. Vedoucí práce Ing. Radim Pust.

[3] HONTAÑÓN, Ramón J. *Linux: praktická bezpečnost.* Praha: Grada, 2003, 438s. ISBN 80-247-0652-0.

[4] *IPS (Intrusion Prevention System) and IDS (Intrusion Detection Systems)* [online]. © 2008 – 2011 [cit. 29. 11. 2016]. Dostupné z:<`http://www.internet-computer-security.com/Firewall/IPS.html`>.

[5] CASEY, Eoghan. *Digital evidence and computer crime: forensic science, computers and the Internet. 3rd ed.* Amsterdam: Elsevier, c2011. ISBN 978-0-12-374268-1

[6] SELECKÝ, Matúš. *Penetrační testy a exploitace.* 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.

[7] *SecTools.Org Top Network Security Tools. SECTOOLS.ORG* [online]. 2014 [cit. 29. 11. 2016]. Dostupné z:<`http://sectools.org/`>

[8] *Kali Linux Tools* [online]. © 2016 [cit. 29. 11. 2016]. Dostupné z:<`http://tools.kali.org/tools-listing`>.

[9] *Port Scanning Techniques* [online]. © 2016 [cit. 29. 11. 2016]. Dostupné z:<`https://nmap.org/book/man-port-scanning-techniques.html`>.

[10] *Tenable Network Security* [online]. 2014 [cit. 29. 11. 2016]. Dostupné z:<`http://www.tenable.com/`>.

[11] *Hillstone Documentation* [online]. © 2016 [cit. 29. 11. 2016]. Dostupné z:<`http://www.hillstonenet.com/resources/`>.

[12] *Hillstone M/G Series Next-Generation Firewall* [cit. 15. 5. 2017]. Dostupné z:<`http://www.hillstonenet.com/`>.

[13] *Spirent Support* [online]. 2017 [cit. 15. 5 2017]. Dostupné z:<`http://support.spirentcom.com`>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

10GbE	10 Gigabit Ethernet
ACK	Acknowledgment
ARP	Address Resolution Protocol
CPU	Central Processing Unit
CSV	Comma-Separated Values
DHCP	Dynamic Host Configuration Protocol
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection Systems
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol security
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
MAC	Media Access Control
NAT	Network Address Translation
OS	Operating System
OSI	Open Systems Interconnection
PC	Personal Computer
PDF	Portable Document Format
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell

SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WebUI	Web User Interfaces

SEZNAM PŘÍLOH

A INSTALACE SERVERU PRO ODPOSLECH SÍŤOVÉ KOMUNIKACE

Následující návod slouží k ukázce instalace a nastavení serveru používající linuxovou distribuci Debian 9.4. Jessie. Tato konfigurace umožní serveru přesměrovávat a zachytit veškerý síťový provoz připojeného zařízení.

A.1 Nastavení pravidel iptables

Pro nastavení přeposílání paketů mezi rozhraními musíme v souboru /etc/sysctl.conf odkomentovat řádek:

```
net.ipv4.ip_forward = 1
```

Změnu nastavení je nutné uložit pomoci příkazu:

```
sysctl -p
```

Kontrola povolení přeposílání paketů. Výstupem následujícího příkazu musí být 1.

```
cat /proc/sys/net/ipv4/ip_forward
```

Dále vytvoříme soubor rules.sh:

```
vi /rules.sh
```

Soubor bude obsahovat následující kód:

```
iptables -F
iptables -t nat -F
iptables -t mangle -F

iptables -X
iptables -t nat -X
iptables -t mangle -X

iptables -t nat -A PROUTROUTING -p tcp -i eth0 -j DNAT --to 172.16.10.102
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Povolení spuštění souboru zajistí příkaz:

```
chmod 777 /rules.sh
```

Soubor spustíme příkazem:

```
./rules.sh
```

A.2 Nastaveni DHCP serveru

Příkaz pro instalaci DHCP serveru:

```
apt-get install isc-dhcp-server
```

Soubor /etc/dhcp/dhcpd.conf je nakonfigurován následovně:

```
subnet 172.16.10.0 netmask 255.255.255.0 {
range 172.16.10.100 172.16.10.105;
option domain-name-server 8.8.8.8;
option subnet-mask 255.255.255.0;
option routerss 172.16.10.1;
option broudcast-address 172.16.10.255;
default-lease-time 600;
max-lease-time 7200;
}
```

A.3 Instalace programu Wireshark

Program Wireshark nainstaluje následujícím příkazem:

```
apt-get install wireshark
```

Ukázka příkazu pro zachycení komunikace z příkazového řádku po dobu 60 sekund na rozhraní eth1 a následné zapsaní do souboru capture.pcap:

```
dumpcap -i eth1 -a duration:60 -w capture.pcap
```

B OBSAH PŘILOŽENÉHO DVD

- `/` ..... kořenový adresář přiloženého DVD
  - `Bezpečnostní analýza firewallu.pdf` ..... bakalářská práce v PDF
  - `Výsledky analýzy síťové komunikace` ..... adresář s příslušnými výsledky
    - `zachyceni_48hod.pcap` ..... soubor se zachycenou komunikací
    - `zachyceni_instalace.pcap` ..... soubor se zachycenou komunikací
  - `Výsledky skenování portů` ..... adresář s příslušnými výsledky
    - `nmap-O.txt` ..... soubor s výstupem příkazu nmap -O
    - `nmap-sA.txt` ..... soubor s výstupem příkazu nmap -sA
    - `nmap-sS.txt` ..... soubor s výstupem příkazu nmap -sS
    - `nmap-sT.txt` ..... soubor s výstupem příkazu nmap -sT
    - `nmap-sU.txt` ..... soubor s výstupem příkazu nmap -sU
  - `Výsledky analýzy programem Nessus` ..... adresář s příslušnými výsledky
    - `Basic_Network_Scan.html` ..... soubor s výsledky zranitelností
    - `výpisy_jednotlivých_zranitelností.zip` .. archív obsahující html soubory jednotlivých zranitelností
  - `Výsledky výkonového testování` ..... adresář s příslušnými scénáři
    - `Měření prvního scénáře` ..... adresář s výsledky prvního měření
      - `sc1_mereni1` ..... adresář s výsledky 1. měření 1. scénáře
        - `realtime.csv` ..... soubor s konfigurací a výsledky
        - `client-summary.csv` ..... soubor s konfigurací a výsledky
        - `server-summary.csv` ..... soubor s konfigurací a výsledky
      - `sc1_mereni2` ..... adresář s výsledky 2. měření 1. scénáře
        - `realtime.csv` ..... soubor s konfigurací a výsledky
        - `client-summary.csv` ..... soubor s konfigurací a výsledky
        - `server-summary.csv` ..... soubor s konfigurací a výsledky
    - `Měření druhého scénáře` ..... adresář s výsledky druhého měření
      - `sc2_mereni1_ftp` ..... adresář s výsledky 1. měření 2. scénáře
        - `realtime.csv` ..... soubor s konfigurací a výsledky
        - `client-summary.csv` ..... soubor s konfigurací a výsledky
        - `server-summary.csv` ..... soubor s konfigurací a výsledky
      - `sc2_mereni2_smtp` ..... adresář s výsledky 2. měření 2. scénáře
        - `realtime.csv` ..... soubor s konfigurací a výsledky
        - `client-summary.csv` ..... soubor s konfigurací a výsledky
        - `server-summary.csv` ..... soubor s konfigurací a výsledky
      - `sc2_mereni3_https` ..... adresář s výsledky 3. měření 2. scénáře
        - `realtime.csv` ..... soubor s konfigurací a výsledky
        - `client-summary.csv` ..... soubor s konfigurací a výsledky
        - `server-summary.csv` ..... soubor s konfigurací a výsledky
    - `Měření třetího scénáře` ..... adresář s výsledky třetího měření
      - `sc3_mereni1_m7260` ..... adresář s výsledky 1. měření 3. scénáře
        - `realtime.csv` ..... soubor s konfigurací a výsledky
        - `client-summary.csv` ..... soubor s konfigurací a výsledky
        - `server-summary.csv` ..... soubor s konfigurací a výsledky
      - `sc3_mereni2_m7260_ips` ..... adresář s výsledky 2. měření 3. scénáře

```
    ├── realtime.csv ..................... soubor s konfigurací a výsledky
    ├── client-summary.csv ............... soubor s konfigurací a výsledky
    └── server-summary.csv ............... soubor s konfigurací a výsledky
├── sc3_mereni3_m7260_ips+av ......adresář s výsledky 3. měření 3. scénáře
    ├── realtime.csv ..................... soubor s konfigurací a výsledky
    ├── client-summary.csv ............... soubor s konfigurací a výsledky
    └── server-summary.csv ............... soubor s konfigurací a výsledky
└── sc3_mereni4_m7260_transaction  adresář s výsledky 4. měření 3. scénáře
    ├── realtime.csv ..............soubor s výsledky a konfigurací měření
    ├── client-summary.csv ............... soubor s konfigurací a výsledky
    └── server-summary.csv ............... soubor s konfigurací a výsledky
```