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

METODIKA TESTOVÁNÍ BEZPEČNOSTI A VÝKONNOSTI FIREWALLŮ
METHODOLOGY FOR TESTING THE SECURITY AND PERFORMANCE OF FIREWALLS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — Dominik Sasko
AUTHOR

VEDOUCÍ PRÁCE — Ing. Jakub Frolka
SUPERVISOR

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Dominik Sasko ***ID:*** 187518
Ročník: 3 ***Akademický rok:*** 2017/18

NÁZEV TÉMATU:

Metodika testování bezpečnosti a výkonnosti firewallů

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s hardwarovým firewallem, prostudujte jeho funkce, proveďte rozbor jeho hardwaru a softwaru. Vytvořte si experimentální pracoviště pro zachytávání provozu firewallu. Navrhněte scénář pro výkonnostní testování firewallu. Podle navrženého scénáře proveďte základní měření a výsledky zpracujte do přehledných grafů. Vytvořte metodiku testování firewallu. Výkonost i bezpečnost firewallu důkladně otestujte a výsledky prezentujte v přehledné formě se závěry a doporučeními na zlepšení.

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: 5.2.2018 ***Termín odevzdání:*** 29.5.2018

Vedoucí práce: Ing. Jakub Frolka
Konzultant:

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

ABSTRAKT

Cieľom tejto bakalárskej práce je analyzovať bezpečnosť a výkon firewallov a navrhnúť metodiku ich testovania. Teoretická časť sa venuje vysvetleniu firewallov a ich rozdeleniu a opisu funkcií firewallov novej generácie. Začiatok praktickej časti sa zameriava na testovanie bezpečnosti pomocou penetračných programov a ukazuje výsledky jednotlivých bezpečnostných testov. Pokračovanie praktickej časti sa zaoberá záťažovými skúškami pri rôznych scenároch pomocou zariadenia Spirent Avalanche a porovnáva výsledky s hodnotami udávanými výrobcom firewallu Hillstone.

KĽÚČOVÉ SLOVÁ

firewall, Hillstone, Spirent Avalanche, testovanie zabezpečenia, testovanie výkonu

ABSTRACT

This bachelor thesis focuses on analysis of security and performance of firewalls and designing a methodology for testing them. Theoretical part is devoted to explaining firewalls and its' division and describing functions of next generation firewalls. Beginning of practical part focuses on testing security using penetration programs and shows results of each security test. Practical part continues with performance tests in various scenarios using Spirent Avalanche and compares the results with values stated by the manufacturer of firewall Hillstone.

KEYWORDS

firewall, Hillstone, performance testing, security testing, Spirent Avalanche

SASKO, Dominik. *Metodika testování bezpečnosti a výkonnosti firewallů*. Brno, 2018, 59 s. Bakalárska práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedúci práce: Ing. Jakub Frolka

VYHLÁSENIE

Vyhlasujem, že som svoju bakalársku prácu na tému „Metodika testování bezpečnosti a výkonnosti firewallů“ vypracoval samostatne pod vedením vedúceho bakalárskej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákoníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora

POĎAKOVANIE

Rád by som poďakoval pánovi Ing. Jakubovi Frolkovi za čas a trpezlivosť pri vedení tejto bakalárskej práce a za poskytovanie cenných rád počas celého školského roku.

Brno ....

podpis autora

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

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

POĎAKOVANIE

Výskum popísaný v tejto bakalárskej práci bol realizovaný v laboratóriách podporených projektom SIX; registračné číslo CZ.1.05/2.1.00/03.0072, operačný program Výzkum a vývoj pro inovace.

Brno ....

podpis autora

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OBSAH

ZOZNAM OBRÁZKOV

ÚVOD

Internet sa každým rokom stáva dostupnejší. To dokazuje aj počet ľudí, ktorí k nemu majú prístup. K roku 2018 sa odhaduje až 40 % svetovej populácie, v porovnaní s rokom 1995, kedy malo prístup k internetu iba 1 % ľudstva [1].
Vďaka internetu majú ľudia k dispozícii také množstvo informácií, že už pre nich nie je pripojenie len výhodou, ale nevyhnutnosťou. Tu sa ale naskytá problém. Pretože nielenže informácie z internetu získavajú, ale sami ich tam aj nahrávajú. Mnoho ľudí si neuvedomuje, aké hrozby na nich číhajú a myslia si, že nie sú pre potenciálnych útočníkov zaujímaví. Avšak niektoré osobné informácie môžu byť dôverné a nemali by sa dostať do nesprávnych rúk. Práve proti takýmto krádežiam dát a neoprávneným vniknutiam napomáhajú firewally.

Začiatok bakalárskej práce je venovaný základnému opisu firewallu. Opisuje ich rozdelenie a to, ako sa vyvíjali v priebehu rokov. Taktiež popisuje funkcie firewallov novej generácie a hardware a software firewallu Hillstone, ktorý je testovaný v tejto práci.

Druhá časť je zameraná na metodiku testovania bezpečnosti firewallu pomocou penetračných nástrojov. Čitateľa zoznamuje s operačným systémom vytvoreným práve na takéto testovanie. Pokračuje popisom základných kybernetických útokov a metodiky zachytávania prevádzky siete.

V nasledujúcej časti je popísaná metodika testovania výkonnosti firewallu. Nasleduje popis zariadenia na záťažové testovanie Spirent Avalanche.

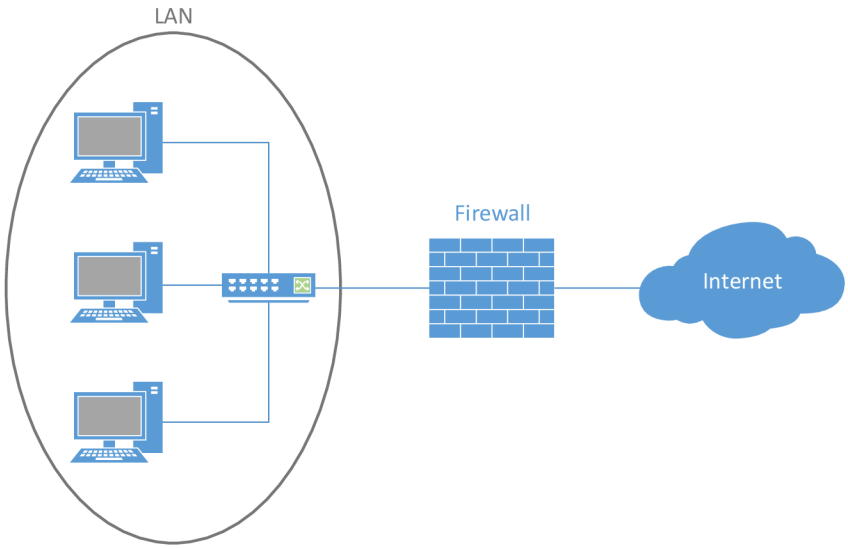
Posledná časť práce zobrazuje vykonávanie bezpečnostného testovania spolu s komentármi k jednotlivým výsledkom. Nasledujú výkonnostné testy realizované pri rôznych scenároch. Výsledky sú nakoniec porovnávané s ich teoretickými hodnotami udanými výrobcom.

1 ÚVOD DO FIREWALLOV

Ako už samotný preklad naznačuje, firewall, alebo aj „protipožiarna stena“ má hlavnú úlohu chrániť. V tomto prípade to ale nie je pred požiarom, ale proti osobám, ktoré sa snažia bez dovolenia dostať do siete s väčšinou zlými úmyslami. Tieto osoby sa nazývajú hackeri.

Firewall je sieťový prvok, ktorý je umiestnený medzi vnútornou (bezpečnou) a vonkajšou (neznámou) sieťou (obr. 1.1). Možno ho prirovnať ku hraničnej polícii, ktorá sleduje a kontroluje všetko, čo prechádza touto hranicou medzi dvoma sieťami. Ak nájde niečo, čo je proti pravidlám, zablokuje alebo odmietne sieťový tok, prípadne len upozorní administrátora siete. Tieto pravidlá si užívateľ nastavuje sám a je veľmi dôležité aby boli nastavené správne, pretože nesprávne nakonfigurovaný firewall môže byť niekedy horší, ako keby sme nemali žiadny [2]. Tieto pravidlá sú definované podľa bezpečnostnej politiky firmy, čo je vlastne súbor pravidiel a nariadení, ktoré definujú postoj danej organizácie k otázkam bezpečnosti. Každá spoločnosť môže mať túto politiku nastavenú inak, preto sa s ňou administrátor siete musí oboznámiť pred nastavovaním jednotlivých pravidiel.

Väčšina bežných užívateľov sa už stretla s firewallom, aj keď o tom nemusia ani vedieť. Jedná sa o softwarový firewall predinštalovaný v operačnom systéme, ktorý má užívateľa chrániť pred základnými hrozbami. Existujú aj samostatne stojace zariadenia, nazývané hardwarové firewally. ktoré sa využívajú predovšetkým vo firemných prostrediach. Oba tieto typy firewallov budú opísané v časti 2.2.



Obr. 1.1: Topológia siete s firewallom.

1.1 Rozbor hardwaru

V tejto sekcii je popísaný hardware firewallu. Konkrétne firewallu od firmy Hillstone.

Firma Hillstone bola založená v roku 2006 profesionálmi na internetovú bezpečnosť z firiem ako NetScreen, Cisco a Juniper. Špecializuje sa na výrobu „Next Generation Firewalls“, čo v preklade znamená „firewally novej generácie“. Sú to firewally, ktoré používajú techniky strojového učenia (zariadenie sa učí samo bez potreby výslovného naprogramovania) a umelej inteligencie na skúmanie správania sieťovej prevádzky a identifikáciu nezvyčajných aktivít [3].
V práci bude opísaný konkrétny typ Hillstone SG-6000-M7260, na ktorom budú následne vykonávané bezpečnostné a záťažové testovania.

Hillstone SG-6000-M7260

V laboratórnej učebni je k dispozícii firewall Hillstone SG-6000-M7260.

Obr. 1.2: Hillstone SG-6000-M7260 [4].

Je to firewall novej generácie na použitie predovšetkým do stredne veľkých až veľkých firiem vzhľadom na maximálnu priepustnosť firewallu 25 Gb/s, viď tab 1.1.

Tab. 1.1: Základné parametre firewallu Hillstone SG-6000-M7260 [4].

Špecifikácie	**SG-6000-M7260**
FW priepustnosť	25 Gb/s
IPsec priepustnosť	15 Gb/s
AV priepustnosť	7 Gb/s
IPS priepustnosť	12 Gb/s
Porty pre manažment	1 x konzolový port, 1 x AUX port, 1 x USB port, 1 x HA, 1 x MGT
Zabudované I/O porty	4 x GE, 4 x SFP
Rozmery (Š x H x V)	(440 x 520 x 88 mm)
Hmotnosť	12,3 kg

Pre objasnenie budú v jednoduchosti opísané jednotlivé parametre uvedené vyššie v tabuľke. Všetky tieto parametre sú udávané za časový úsek jednej sekundy.

- **FW priepustnosť:** Maximálna priepustnosť paketov firewallom.
- **IPsec priepustnosť:** Udáva maximálne množstvo prechádzajúcich dát zabezpečených pomocou protokolu IPsec. Tento protokol zvyšuje bezpečnosť paketov posielaných cez internet a to tak, že je nevyhnutná autentizácia oboch strán pred začatím spojenia a šifrovanie tohoto spojenia.
- **AV priepustnosť:** Maximálna priepustnosť paketov pri zapnutej funkcii antivírusovej ochrany.
- **IPS priepustnosť:** Udáva maximálne množstvo prechádzajúcich dát pri zapnutej funkcii IPS. Táto funkcia analyzuje celý paket, hlavičku a taktiež dáta, a hľadá v nich abnormality. Ak nejaké nájde, firewall paket odmietne. Podobne pracuje aj IDS (Intrusion Detection System), ktorý ale pri nájdenej abnormalite vypíše záznam o jej detekovaní [4].

1.2 Rozbor softwaru

Firma Hillstone používa proprietárny software nazvaný **StoneOS**. V tejto práci bude využívaná verzia StoneOS 5.5.

Tento software disponuje mnohými funkciami. Je možné v ňom nastaviť smerovanie, a tak bude firewall vstupná brána do vnútornej siete. Typ SG-6000-M7260 je schopný využívať viacero smerovacích protokolov, ako napríklad OSPF, BGP alebo RIPv2. Takisto na ňom možno využiť funkciu NAT na preklad súkromných adries na verejnú adresu a naopak, alebo na ňom nastaviť DHCP a DNS server.
Nakoľko je tento typ firewallom novej generácie, jeho software podporuje **Intrusion Prevention System**. Tomuto systému a firewallom novej generácie bude venovaná časť 2.3.

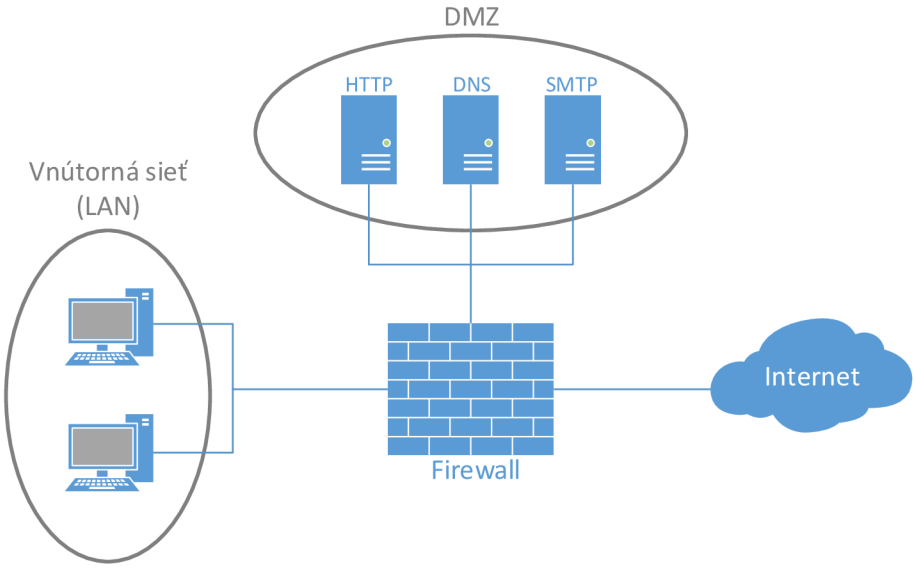
1.3 Demilitarizovaná zóna

Demilitarizovaná zóna, skrátene DMZ, je všeobecné označenie pre pásmo, kam nemôžu vstúpiť vojenské jednotky. V problematike počítačovej bezpečnosti sa takto nazýva miesto v sieti (podsieť), ktorá je pomocou firewallu oddelená od ostatných zariadení. Táto časť siete je vo všeobecnosti náchylnejšia na útoky hackerov, ako zbytok siete.
Prečo by si ale administrátori siete chceli spraviť časť siete menej bezpečnú? Vo väčšine prípadov pri ktorých je zvolené takéto riešenie ide o organizácie, ktoré poskytujú svoje služby užívateľom mimo lokálnu sieť, ako napríklad webové služby [2].

Ako príklad môže slúžiť napríklad malá firma na výrobu a predaj čokolády. Aby svoj produkt mohli predať, majú vlastné webové stránky a internetový obchod na servery vo vlastnej sieti. K tomuto webovému serveru sa ľudia musia pripojiť z vonkajšej (neznámej siete) aby získali informácie o produktoch. Je nutné im dať možnosť dostať sa do vnútornej siete, a to povolením určitých portov, v tomto prípade to bude HTTP port číslo 80. Na druhú stranu ale majiteľ firmy nechce, aby sa im niekto dostal na druhý server, kde sú uložené citlivé informácie o firme ako finančné záznamy alebo postup výroby produktov. Táto situácia sa dá vyriešiť viacerými spôsobmi – najčastejšie pomocou jedného, alebo dvoch firewallov.

1.3.1 DMZ pomocou jedného firewallu

Ak je použitý jeden firewall na vytvorenie DMZ, bude musieť mať aspoň tri sieťové rozhrania. Prvé rozhranie pre externú sieť medzi firewallom a ISP (poskytovateľom internetového pripojenia), druhé rozhranie tvorené vnútornou sieťou a posledné s DMZ. Cez tento firewall sa dostaneme priamo ku webovému serveru v demilitarizovanej zóne, aj ku serveru vo vnútornej sieti.

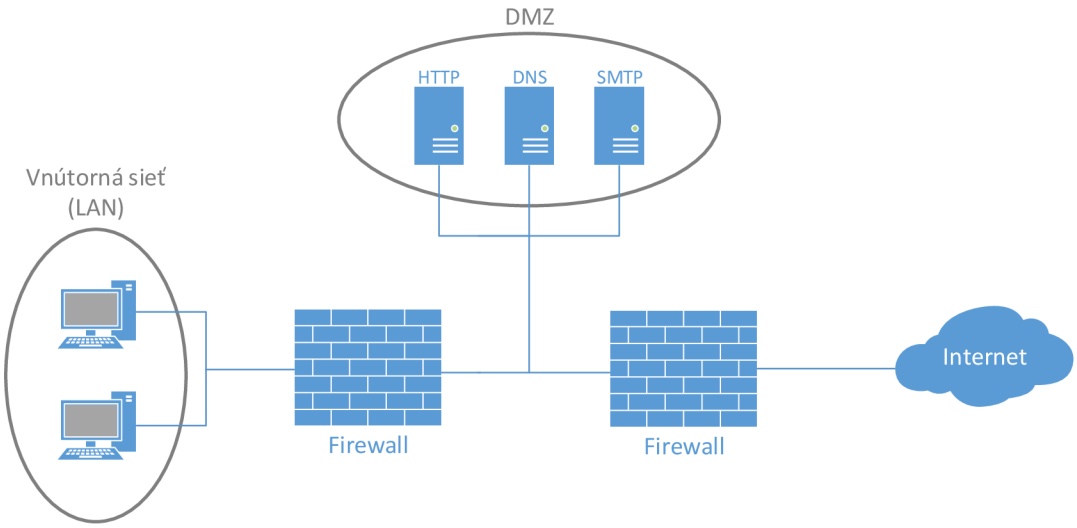


Obr. 1.3: DMZ s použitím jedného firewallu.

1.3.2 DMZ pomocou dvoch firewallov

Pri topológii s dvoma firewallmi sa za prvým nachádza DMZ, nasleduje druhý firewall a nakoniec vnútorná sieť. Zabezpečuje sa tak väčšia bezpečnosť vnútornej siete a zariadení v nej na úkor vyššej ceny za dva sieťové prvky. Využívajú sa firewally

od rôznych výrobcov. Takže ak útočník nájde a využije bezpečnostnú chybu prvého firewallu, zastaví ho druhý do prístupu k vnútornej sieti [5].



Obr. 1.4: DMZ s použitím dvoch firewallov.

2 ROZDELENIE FIREWALLOV

Firewally možno rozdeliť podľa viacerých kritérií, najčastejšie sa ale rozdeľujú podľa typu a podľa platformy na ktorej pracujú.

2.1 Rozdelenie firewallov podľa typu

Podľa typu budú ukázané tri najzákladnejšie firewally. Toto rozdelenie môže byť nazývané aj ako rozdelenie podľa vrstvy OSI modelu, na ktorej jednotlivé firewally pracujú. Patria sem nestavové paketové filtre, stavové paketové filtre a aplikačné brány.

2.1.1 Nestavové paketové filtre

Paketové filtre, nazývané tiež nestavové firewally, sú najstaršie a najjednoduchšie spomedzi všetkých typov firewallov. Skúmajú zdrojovú a cieľovú IP adresu a číslo portu a podľa vopred stanovených pravidiel sa rozhodujú, čo ďalej s paketom urobia. Kontrola teda nastáva na tretej vrstve modelu OSI, tj. sieťovej vrstve. Výhodou takejto jednoduchej kontroly je vysoká rýchlosť spracovania veľkého množstva dát, ktoré prechádzajú cez takýto typ firewallu. Nachádzajú sa napríklad implementované v sieťových prvkoch ako sú smerovače alebo prepínače.

Paketové filtre majú ale jednu veľkú nevýhodu. V určitých prípadoch musia na serveri fungovať služby, ktoré pri komunikácii využívajú náhodne vybraté porty (napr. prenos súborov pomocou FTP). V takomto prípade firewall nevie, či môže alebo nemôže takýto paket prejsť, pretože v nich nevidí súvislosti a každý analyzuje samostatne. Vtedy ostávajú dve možnosti. Povoliť celý rozsah portov (nebezpečné), alebo zakázať tieto služby a vôbec ich nepoužívať (niekedy nemožné). V takýchto prípadoch je nutné zvoliť iný typ firewallu, konkrétne stavový paketový filter [7].

2.1.2 Stavové paketové filtre

Stavový paketový filter pracuje veľmi podobne ako paketový filter, má ale vylepšenia, ktoré zefektívňujú kontrolu sieťovej prevádzky a pracuje aj so štvrtou (transportnou) vrstvou referenčného modelu OSI. Aby sa predošlo už vyššie spomenutému problému zo samostatnou inšpekciou každého paketu s náhodne vybratými portami, stavový firewall si ukladá informácie o relácií. Reláciou (anglicky session) sa nazýva nadviazané spojenie a všetky pakety, ktoré k nemu patria.
Ako príklad je možné ukázať problém s FTP protokolom. Protokol FTP môže pracovať v dvoch režimoch – pasívnom a aktívnom. Pri pasívnom režime server pošle klientovi číslo portu (väčšie ako 1024) a klient sa následne na neho pripojí. Aktívny

režim funguje opačne, a to tak, že klient začína spojenie. Odošle na port 21 serveru číslo portu (väčšie než 1024). Následne sa server zo svojho portu (číslo 20) pripojí na klienta. Pasívny režim je považovaný za bezpečnejší kvôli nadviazaniu dátového spojenia v rovnakom smere ako pôvodná požiadavka [6].
Problém ale vytvára fakt, že pracovný port nie je statický a mení sa s každým spojením. Kvôli tomu je nemožné nastaviť pravidlá na filtrovanie FTP spojenia, ktoré by nestavový firewall rozpoznal ako jednu reláciu. Preto si stavový firewall tvorí tabuľku, v ktorej si udržuje nadviazané spojenia.
Výhodou je rýchlosť spracovania požiadavok oproti nestavovým paketovým filtrom. K nevýhodám patrí nižšia úroveň zabezpečenia ako u aplikačných brán a vyššia záťaž zariadenia kvôli udržovaniu informácií o spojení [7].

2.1.3 Aplikačné brány

Stavový firewall by útokom na vyšších vrstvách ako na transportnej nezabránil. Na to slúžia aplikačné brány. Ako už samotný názov naznačuje, aplikačné brány (nazývané aj proxy brány) pracujú na siedmej – aplikačnej – vrstve OSI modelu a tak môžu kontrolovať celý paket. Pri takomto riešení dochádza k úplnému rozdeleniu sietí, medzi ktorými sa nachádza brána, a tak sa stáva medzičlánkom spojenia.
Princíp fungovania aplikačných brán je nasledovný:

1. Klient iniciuje spojenie na server → najprv je pripojený na aplikačnú bránu.
2. Brána otvorí nové spojenie ku serveru (brána sa z pohľadu serveru stáva klientom).
3. Sever pošle dáta aplikačnej bráne.
4. Pôvodný klient dostáva dáta od aplikačnej brány.

Takýmto spôsobom sa klient anonymizuje voči severu, pretože aplikačná brána vystupuje ako klient. Preto sa používa názov proxy, čo v preklade z angličtiny znamená „zástupca/splnomocnenec“.

Proxy brány majú ale aj svoje nevýhody. Vzhľadom na to, že všetka sieťová prevádzka musí prechádzať jedným bodom a taktiež sa musí kontrolovať celý paket, stáva sa tento typ firewallu veľmi pomalým v porovnaní s ostatnými. Ďalšou nevýhodou je nutnosť nastavenia proxy pre každú aplikáciu, pretože neexistujú univerzálne pravidlá ako pri paketových filtroch [7].

2.2 Rozdelenie firewallov podľa platformy

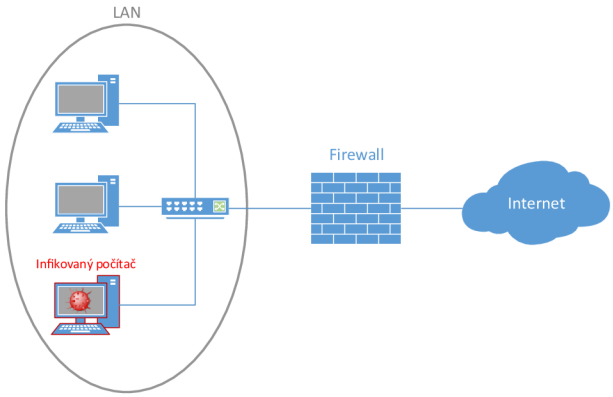
Firewally sa podľa platformy rozdeľujú na hardwarové a softwarové firewally. Osobitne možno zaradiť firewally novej generácie, ktoré môžu byť ako softwarové aplikácie, tak hardwarové zariadenia.

2.2.1 Hardwarový firewall

Hardwarový firewall možno nájsť ako samostatne stojace zariadenie, alebo v mnohých prípadoch tiež ako súčasť smerovačov. Je to vlastne softwarový firewall pracujúci na určitom hardwary. Ak je použitý v smerovačoch, zaistí sa vyššia bezpečnosť siete, ale nemôžme od takéhoto riešenia očakávať rovnaké zabezpečenie, ako keď je zvolený samostatne stojaci firewall. Sú to väčšinou lacnejšie smerovače, ktoré sú používané tiež ako prepínače a využívajú sa v menších sieťach, napr. v rodinných domoch. Použitie drahšieho firewallu, ktorý je zhotovený ako samostatné zariadenie je častejšie vo veľkých firmách, ktoré dbajú na zvýšenú bezpečnosť vo svojej sieti.

2.2.2 Softwarový firewall

Mnoho domácich používateľov internetu volí možnosť softwarového firewallu. Je to software nainštalovaný na počítači (ako akýkoľvek iný software), ktorý je možné nastavovať podľa predstáv užívateľa. Môže mať mnoho funkcií, cez ochranu voči počítačovým vírusom až po nastavenie bezpečného zdieľania súborov alebo tlačiarní v sieti. Prečo je ale softwarový firewall nutný na každom počítači vo vnútornej sieti, keď sa v nej nachádza hardwarový, ktorý ju ochráni pred útokmi z vonkajšej siete? Situáciu objasňuje obrázok 2.1. Je to už použitý obrázok z úvodu do firewallov, ale obsahuje určité zmeny.



Obr. 2.1: Útok na sieť z vnútra siete.

Červená „mína“ na obrazovke počítača znázorňuje napadnutie vírusom. Tento vírus tam neprenikol z vonkajšej siete, dostal sa tam napríklad pripojením infikovaného USB kľúča. Týmto spôsobom by sa mohol vírus šíriť vo vnútri sieti a hardwarový firewall na okraji sieti by tomu nezabránil. Ak je ale na ostatných počítačoch nainštalovaný softwarový firewall, je menšia možnosť, že sa vírus bude ďalej šíriť vo vnútornej sieti.

2.2.3 Porovnanie HW a SW firewallu

Pri použití hardwarového firewallu je nutné len jedno zariadenie, ktoré má za úlohu chrániť celú sieť. Tento typ firewallu je rýchlejší a bezpečnejší, nakoľko má vlastný operačný systém, určený práve na ochranu proti útokom. Pri konfigurácii či aktualizácií systému stačí tieto akcie vykonať len na jednom zariadení, narozdiel od softwarového firewallu, pri ktorom je nutné vykonať tieto akcie na každej stanici. Softwarový firewall konkuruje hardwarovému najmä v cene, keďže býva zdarma zahrnutý v operačnom systéme. Zvyčajne je ľahko rozšíritelný o prídavné funkcionality, ktoré už ale môžu byť spoplatnené. Nevýhodou je delenie sa o výkon zariadenia, na ktorom je firewall spustený – to môže znížiť výkonnosť obom stranám.

2.3 Firewally novej generácie

Ďalší druh firewallov predstavujú „firewally novej generácie“. Ich práca bola naznačená v opise Hillstone produktov, viď časť 1.1. Kombinujú funkcie štandardných firewallov s novými, bezpečnejšími funkciami ako napríklad dešifrovanie a inšpekcia zašifrovanej SSL a SSH prevádzky. Firewally novej generácie zvyčajne ponúkajú prídavné možnosti ako antivírus, antispam alebo systémy IDS a IPS, ktoré budú opísané v nasledujúcich sekciách. Poskytujú sledovanie a kontrolu webových aplikácií nezávisle na čísle portu alebo použitom protokole. Na základe zvolenej politiky môžu upravovať šírku pásma pre jednotlivé aplikácie (funkcia QoS) a zároveň môžu blokovať nevhodné alebo škodlivé aplikácie [8].

2.3.1 Intrusion Detection System

IDS alebo „Intrusion Detection System“ možno voľne preložiť ako systém na detekciu narušenia. Takýto systém môže pracovať na samostatne stojacom zariadení alebo môže predstavovať softwarovú aplikáciu nainštalovanú napríklad vo firewalle. Má za úlohu monitorovať sieťovú prevádzku a pokúša sa odhaliť podozrivé aktivity v sieti. Využíva na to rôzne detekčné metódy. Jedna z týchto metód je detekcia podľa vzoru.

Princíp spočíva v rozpoznávaní určitých vzorov škodlivého kódu, nazývaných signatúry. Ak takýto vzor zaznamená, vykoná sa príslušná aktivita – napr. oznámenie možnej hrozby bezpečnostnému administrátorovi. Ako aj pri konfigurácii pravidiel firewallu aj tu je nutné dať pozor na to, čo má systém detekovať ako útok a na čo nereagovať, pretože zlá konfigurácia by administrátora siete mohla nechať v pocite bezpečia, aj keď by na jeho sieť útočili. Systémy IDS sa rozlišujú na dva typy:

- **Sieťový detekčný systém NIDS** – Systém umiestnený priamo v chránenej sieti, ktorý sleduje všetku sieťovú prevádzku, ktorá ňou prechádza. Kontroluje prichádzajúce a odchádzajúce dáta zo siete, ako aj dáta medzi hosťami v sieti.
- **Hostiteľský detekčný systém HIDS** – Špeciálna softwarová aplikácia nainštalovaná priamo na hostiteľský počítač (často sú to servery). Sleduje prichádzajúce a odchádzajúce dáta a zmeny súborového systému [2].

2.3.2 Intrusion Prevention System

IPS systémy sú považované za rozšírenie IDS systémov, väčšina výrobcov firewallov ale IDS a IPS kombinujú. Oba systémy sledujú sieťovú premávku a hľadajú v nej nezvyčajné aktivity, ale z názvu IPS (systém na prevenciu narušenia) vyplýva, že tento typ aktívne chráni sieť tým, že bráni aby sa útok úspešne dokončil.
Na ochranu sa využívajú dve techniky:

- **Snipping** – Systém ukončí podozrivý útok pomocou paketu TCP Reset alebo pomocou ICMP Unreachable správy o nedostupnosti.
- **Shunning** – Systém zmení konfiguráciu vstupného smerovaču alebo firewallu a tak tomuto zariadeniu nariadi zamietať premávku daného spojenia. Systém vytvorí prístupový zoznam (ACL), v ktorom nastaví blokovanie IP adresy útočníka [2].

Firewall Hillstone obsahuje funkciu IPS, pri ktorej je možné nastavovať profily s rôznymi typmi signatúr, ktoré ponúka priamo výrobca z jeho databázy. V tejto databáze sa nachádza viac ako 8000 signatúr pre IPS a 4 milióny signatúr pre antivírus [4]. Taktiež je možné nastaviť, aká akcia sa má pri detekcii vykonať – vytvoriť záznam, resetovať spojenie, zablokovať IP adresu alebo zablokovať službu.

3 METODIKA TESTOVANIA ZABEZPEČENIA

Každý majiteľ firmy, ktorý chce ochrániť svoju sieť pred útokmi, by mal rozmýšľať nad kúpou firewallu na zvýšenie ochrany jeho siete. Na trhu je množstvo rozličných výrobcov a typov z ktorých si môže vybrať. Prvá dôležitá vec je priepustnosť firewallu, ktorá bola opísaná v časti 1.1. Ďalšia vlastnosť, pre ktorú si tento sieťový prvok zákazník primárne zadováži, je bezpečnosť. Rôzne typy firewallov poskytujú iný stupeň ochrany, konkrétny typ Hillstone SG-6000-M7260 patrí medzi najbezpečnejšie kvôli funkciám firewallu novej generácie.

V súčasnej dobe by pri úspešnom útoku na firemnú sieť mohol útočník napadnutú firmu úplne položiť. Hlavným dôvodom je obrovský rozvoj digitalizácie – firma už nemá sklady plné papierov s citlivým obsahom, ale namiesto toho dátové centrá s týmito informáciami, ktoré môže hacker napríklad znehodnotiť či odcudziť. To záleží na tom, aký útok využije. Základné útoky budú opísané v časti 3.1. Ak už firma má zriadené zabezpečenie siete a chce overiť, či spĺňa požiadavky kladené na toto zabezpečenie, môže využiť tzv. „audit informačnej bezpečnosti“, ktorý bude opísaný v časti 3.2.

3.1 Kybernetické útoky

Oblasť kybernetických útokov je veľmi rozsiahla a hackeri stále vyvíjajú iné metódy na preniknutie do systémov svojich obetí. V tejto časti sú opísané základné kybernetické útoky proti ktorým sa vie firewall Hillstone SG-6000-M7260 chrániť.

SYN Flood

Pomenovanie SYN Flood je odvodené od funkcie tohoto útoku. Flood, v preklade záplava, je uskutočňovaná pri nadväzovaní TCP spojenia medzi dvoma bodmi (napr. klient a server). Je to druh útoku označovaný ako „Denial of Service“, ktorý má za úlohu znefunkčniť cieľovú službu a zneprístupniť ju ostatným užívateľom. Pre pochopenie tohoto útoku je dôležité najprv vedieť ako sa TCP spojenie zostavuje.

1. Klient začína spojenie zaslaním SYN správy na server.
2. Server obdrží tento segment, alokuje si určitú časť pamäte na spojenie s týmto klientom a odpovedá so SYN-ACK (acknowledgement – potvrdenie).
3. Akonáhle dostane klient potvrdenie od serveru, posiela ACK na server a týmto sa končí nadväzovanie spojenia, nazývané „3-way handshake“ a začína sa prenos dát.

Útočník využíva fakt, že server alokuje pamäť pri obdržaní SYN správy. Začne teda tieto správy posielať a neodpovedá na ne. Takto sa na serveri po určitom čase zaplní pamäť a nemôže „obslúžiť“ čestného klienta, ktorý by chcel nadviazať spojenie.

Existuje mnoho riešení ako sa ochrániť pred takýmto útokom. Pri využití firewallu sa musí zostavenie TCP spojenia najprv úspešne uskutočniť s firewallom, až potom sa spája zo serverom a vybavuje sa požiadavka klienta [9].

DDoS útok

Tak isto ako už spomenutý SYN Flood, aj DDoS útok má za úlohu odoprieť službu klientovi, ktorý ju chce využívať. V tomto prípade ale nekoná útočník sám. Je buď dohodnutý s viacerými komplicmi, alebo sa zmocní viacerých počítačov, z ktorých vykonáva útok bez vedomia vlastníka počítača (takáto sieť ovládnutých počítačov sa nazýva „botnet“). Preto sa v názve pred DoS pridalo písmeno „D“, ktoré označuje slovo „Distributed“, v preklade distribuovaný. Takto napr. server dostane viac požiadaviek, ako je schopný riešiť a tak musí hosť čakať, poprípade nie je obslúžený vôbec z dôvodu znefunkčnenia serveru.

Typický príklad je vidieť každý semester pri vyberaní športu. Všetci žiaci VUT v Brne, ktorý si chcú registrovať šport, začnú posielať požiadavku na server v rovnakom čase. Tým pádom musí zvládať veľký nápor a server vybavuje požiadavky s veľkým oneskorením – webová stránka sa buď načíta veľmi pomaly, alebo sa vôbec nenačíta. V tomto prípade nemožno označiť študentov za hackerov alebo útočníkov, kvôli tomu že nekonajú zo zlými úmyslami.

Jednou z ochrán proti DDoS útokom môže byť zvýšenie šírky pásma, čo zaručí možnosť vybavovania omnoho viac klientov súčasne. To je ale len odsunutie problému do budúcna a nie jeho koncové riešenie. Tiež je možnosť zakázať prístup na jednotlivé porty, napríklad HTTP. To by ale spôsobilo nedostupnosť HTTP serveru pred ktorým by bol umiestnený firewall [9].

Spyware

Spyware patrí medzi škodlivé programy nazývané aj „malware“. Jeho úlohou je sledovať rôzne aktivity na hostiteľskom počítači, bez vedomia majiteľa tohto počítača. Tento malware sa zvykne nainštalovať ako súčasť iného softwaru, a je využívaný na získavanie informácií o obeti. Môžu to byť údaje o navštívených webových stránkach, ale aj veľmi citlivé informácie ako prihlasovacie mená či heslá do internetového bankovníctva. Na práve takéto získavanie dát slúžia tzv. „keyloggery“, ktoré zaznamenávajú všetky stlačené klávesy a tým aj napísané heslá.

Spyware sa netýka len počítačov, môže postihnúť taktiež mobily. Pri zneužití sledovacieho softwaru môže útočník podstatne narušiť naše súkromie, a to tak, že sa zmocní kamery a mikrofónu, môže nahrávať hovory a taktiež sledovať polohu infikovaného mobilného zariadenia.

Príznaky, ktoré môžu nasvedčovať, že je na zariadení spyware, môžu byť znížený výkon procesoru alebo rýchlosť pripojenia. Ako ochrana slúžia antivírové programy, ktorých súčasťou je antispyware, ktorý nájde spyware a odstráni ho [10].

3.2 Bezpečnostný audit

Ako bolo už v úvode do metodiky testovania zabezpečenia povedané, bezpečnostný audit má ohodnotiť zabezpečenie napr. počítačovej siete zákazníka a upozorniť na možné riziká, ktorým je táto sieť a dáta v nej vystavené. Takýto audit má za úlohu odhaliť nedostatky zabezpečenia a nájsť slabé miesta v sieti, ktoré by útočník mohol použiť na preniknutie do siete.
Mnohé bezpečnostné firmy ponúkajú službu bezpečnostného auditu, ako napríklad Slovenská firma ESET, ktorá sa špecializuje na antivírusové softwary. Ponúka špecialistov s CISA certifikátmi, ktorý využívajú rôzne techniky, ako napríklad penetračné testovanie na vyhodnotenie bezpečnostného auditu [11].

3.3 Penetračné testovanie

Na overenie bezpečnosti, či už celej siete alebo firewallu, slúžia takzvané „penetračné testy“. Sú vykonávané špecialistami pri bezpečnostnom audite. Ich konanie sa nazýva aj „etický hacking“. Znamená to, že hľadajú zraniteľnosti a snažia sa dostať do siete – penetrovať ju – s úmyslom upozorniť majiteľa na nedostatky zabezpečenia, nie využiť tieto zraniteľnosti vo svoj prospech.
Pri vykonávaní penetračného testovania je možné skúšať útoky zvnútra siete – vystupovať ako zlomyseľný zamestnanec alebo útočník, ktorý sa dostal do vnútra siete. Druhá možnosť je útok zvonku siete cez Internet. Spôsob testovania závisí hlavne na klientovi. Možno použiť aj tzv. „social engineering“. To zahŕňa manipulovanie so zamestnancami, mnohokrát spolu s ich vydieraním, k účelu získania prístupu do siete cez nich (napr. vložia USB so škodlivým kódom do firemného počítaču a infikujú sieť zvnútra) [12].

Kali Linux

Pri penetračnom testovaní je vhodné mať operačný systém, ktorý môže človeku uľahčiť prácu. Kali Linux je distribúcia Linuxu odvodená od Debianu, ktorá v sebe zahŕňa široký výber nástrojov na forenznú analýzu a penetračné testovanie. Je to open source projekt spravovaný a financovaný spoločnosťou Offensive Security. Obsahuje viac ako 600 penetračných a analytických nástrojov, ktoré sú predinštalované v systéme [13]. Medzi najznámejšie patria napríklad [12]:

- *Aircrack-ng* – testovanie zabezpečenia Wi-Fi,
- *Metasploit Framework* – nástroj na simulovanie rozličných útokov na sieť,
- *Nmap* – skenovanie siete, otvorených portov a mnoho ďalšieho,
- *Wireshark* – zachytávanie sieťovej prevádzky a analýza jednotlivých paketov.

Veľkou výhodou Kali Linux je jeho dostupnosť. Je voľne dostupný aj s predinštalovanými nástrojmi na domovskej stránke `www.kali.org`.

Firewalk

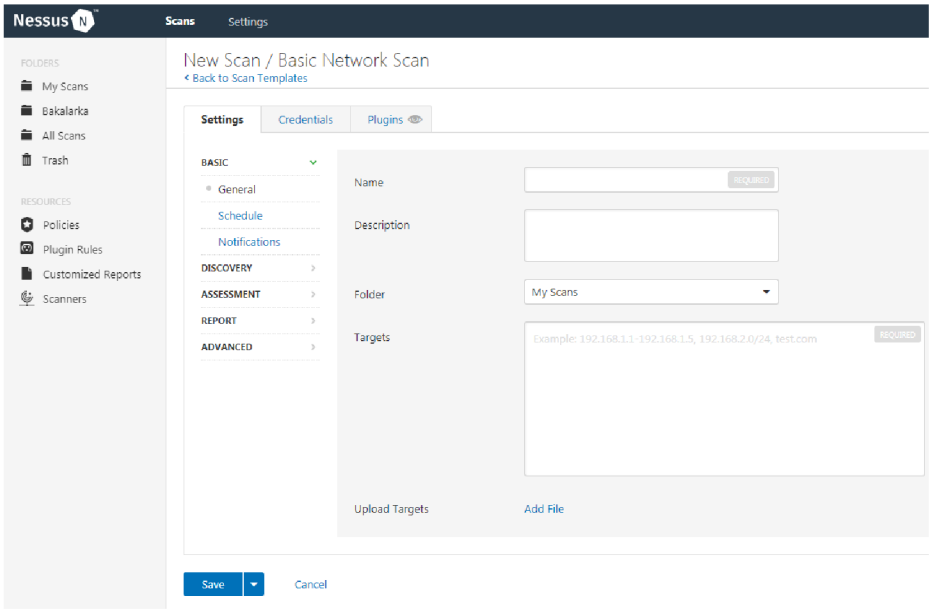
Firewalk je bezpečnostný nástroj, ktorý pomáha zisťovať, či sieťový prvok ako smerovač alebo firewall vykonávajú svoju prácu správne. Administrátor siete ho môže použiť na skontrolovanie správnej konfigurácie ktorú vykonal. Firewalk vyhodnocuje, ktoré protokoly zo štvrtej vrstvy OSI modelu prejdú cez sieťový prvok. Pracuje na základe posielania TCP a UDP paketov s číslom TTL o jedno väčším ako je cieľová východzia brána. Ak východzia brána povolí tento paket, prejde až na ďalší uzol kde bude mať hodnotu TTL nula a zobrazí hlášku „ICMP_TIME_EXCEEDED“. Ak by brána nepovolila tento paket, s najväčšou pravdepodobnosťou by ho zahodila a administrátor by nedostal žiadnu hlášku [14].

V tejto práci bude Firewalk využívaný na kontrolovanie nastavenia ACL pre TCP port 139, ktorý využíva protokol NetBIOS. Tento port môže byť terčom útoku, nakoľko býva vo Windows operačných systémoch otvorený. Systém IPS vo firewally Hillstone používaný v tejto práci obsahuje vo svojej databáze až 207 signatúr útokov na protokol NetBIOS.

Nessus

Pri výbere nástroja pre penetračných testerov, hackerov alebo aj domácich užívateľov, ktorí chcú zistiť či je ich sieť bezpečná, je možné obrátiť sa na Nessus.

Je to software, ktorý sa ľahko používa, rýchlo pracuje a dokáže urobiť podrobný prehľad siete pomocou pár kliknutí. Patrí medzi produkty Americkej firmy Tenable, ktorá sa zameriava na kybernetickú bezpečnosť. Obrázok 3.1 zobrazuje webové rozhranie nástroja Nessus.



Obr. 3.1: Grafické rozhranie nástroju Nessus.

Je dostupný pre rozličné operačné systémy ako Windows, Mac OS a mnohé distribúcie Linuxu. Licenciu pre Nessus Professional je nutné si zakúpiť, alebo je možné využiť bezplatnú skúšobnú verziu na týždeň [15].

Nástroj Nessus je možné použiť na viacero účelov. V tejto práci budú využité funkcie na vyhľadávanie hostov v sieti, hľadanie zraniteľných portov a zraniteľností v sieti. Obsahuje ale aj mnohé iné funkcie, ako napríklad zisťovanie slabých hesiel v sieti alebo prítomnosť malwaru v systémoch.

3.4 Zachytávanie sieťovej prevádzky

Existuje mnoho nástrojov na zachytávanie sieťovej prevádzky ako *Wireshark, tcpdump* alebo *dsniff*. V tejto práci bude využitý Wireshark kvôli rozšírenosti a prehľadnému GUI. S Wiresharkom je možné zachytávať ethernetovú, bezdrôtovú alebo Bluetooth prevádzku a následne ju analyzovať. Taktiež dokáže dekódovať rozličné protokoly, čo sa dá využiť napríklad na rekonštrukciu záznamu VoIP telefonátov.

Wireshark zobrazuje len pakety určené pre MAC/IP adresu používateľa. Ak ale chce vidieť a analyzovať prevádzku na sieti, musí dostávať všetky pakety, ktoré v nej sú. Prvá dôležitá vec je nastavenie sieťovej karty do „promiskuitného módu“ v ktorom bude akceptovať všetku prevádzku v lokálnej sieti, tj. aj pakety smerujúce na inú MAC/IP adresu.
Druhá potrebná vec je, aby sa ku používatelovi táto prevádzka dostala. V sieti, kde je rozbočovač (HUB) to nie je problém, pretože rozbočovač rozpošle pakety na všetky porty okrem toho, z ktorého prišli. Problém nastáva pri použití prepínača, ktorý si uchováva v ARP tabuľke preklady IP adries na MAC adresy, a v CAM tabuľke prekľady MAC adries na fyzické porty podľa ktorých posiela rámce. Tu je nutné využiť *ARP Spoofing* na prepísanie ARP tabuľky. Po tomto útoku bude používateľ dostávať presmerovanú prevádzku a stane sa „Man-in-the-middle“ (z angličtiny „človek v strede“) [12].

Ak si bude chcieť sieťový administrátor zistiť, akú prevádzku zariadenie generuje a aká do neho prichádza, môže využiť sieťový prvok, napríklad prepínač, na ktorom nastaví funkciu port mirroring. Názornú ukážku, ako táto topológia môže vyzerať a ako bude odpočúvanie premávky vykonávané v tejto práci, možno vidieť v časti 5.1.

4 METODIKA TESTOVANIA VÝKONU

Testovanie výkonu sieťových prvkov je možné vykonávať pomocou tzv. „packet crafting tools“. Sú to softwarové nástroje, ktoré generujú sieťovú prevádzku a posielajú ju cez testovaný prvok siete. Ďalšia možnosť je využitie hardwarového prvku. V tejto práci bude na toto testovanie využité zariadenie Spirent Avalanche 3100.

Topológie na testovanie výkonu a bližšie popisy k jednotlivým testom budú uvedené v nasledujúcej kapitole v časti 5.3.

4.1 Spirent Avalanche 3100

Zariadenie Spirent Avalanche 3100 je využívané ako na výkonnostné, tak aj bezpečnostné testovanie sieťových prvkov. Pracuje na 4. až 7. vrstve OSI modelu a preto je možné testovať aj webové aplikácie alebo cloudové služby. Dokáže generovať až 10 Gb/s dát cez určené zariadenie a to tak, že sa nastaví zvlášť strana klienta a zvlášť strana serveru [16].

Obr. 4.1: Spirent Avalanche 3100 [17].

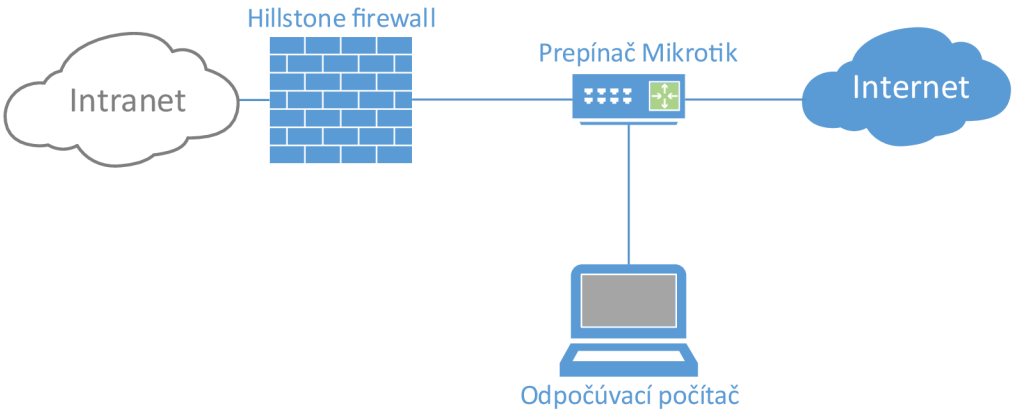
Na konfiguráciu jednotlivých výkonnostných scenárov bude využívaný software *Spirent TestCenter Layer 4-7 Application 4.43*, ktorý ponúka komplexné nastavenie druhu a veľkosti záťaže. Následné výsledky zobrazí software *Spirent TestCenter Layer 4-7 Result Analyzer 4.43*.

5 PREDSTAVENIE TOPOLÓGIÍ

Táto kapitola oboznamuje čitateľa s jednotlivými topológiami na odpočúvanie sieťovej premávky a na testovanie bezpečnosti firewallu. Taktiež predstavuje scenáre na výkonnostné testovanie.

5.1 Odpočúvanie premávky

Aby bolo možné odchytávať pakety vychádzajúce von zo siete, je potrebné dostať sa medzi vonkajšie rozhranie firewallu a pomyselného poskytovateľa internetu. Ako poskytovateľ internetu bude slúžiť firewall Palo Alto pripojený do VUT siete. Medzi týmito dvoma spojmi bude zapojený prepínač *Mikrotik CRS226-24G-25+RM*, kde bude nastavený port mirroring – to znamená, že všetky dáta odoslané na port ether2 budú teraz preposielané na port ether3, kde je umiestnený počítač s nainštalovaným Wiresharkom na odpočúvanie sieťovej premávky. Celú topológiu možno vidieť na obr. 5.1. Pre zjednodušenie je vnútorná sieť zamenená za oblak s názvom „Intranet“.

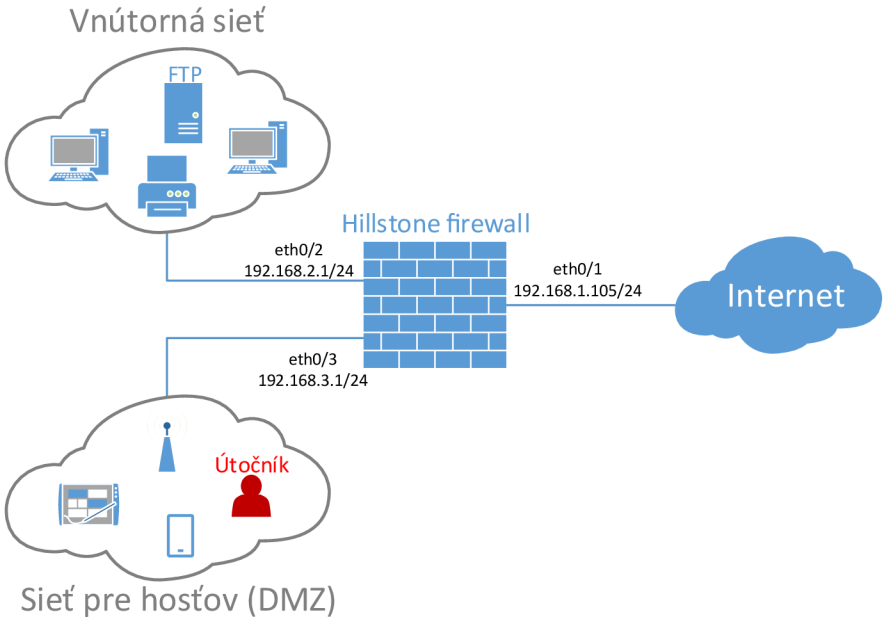


Obr. 5.1: Topológia siete na odchytávanie premávky.

5.2 Testovanie bezpečnosti

Ak firma potrebuje zabezpečiť prístup na internet pre svojich hostí, môže zvoliť bezpečnejšie riešenie ako len pripojiť ich priamo do vnútornej siete. Môže využiť demilitarizovanú zónu, v ktorej obmedzí hosťom prístup do vnútornej siete firmy. Práve túto topológiu možno vidieť na obrázku 5.2. V oboch častiach siete (vnútornej aj DMZ) sú na ukážku umiestnené zariadenia, ktoré možno v týchto častiach siete mať. Topológia v tejto práci bude mať pripojený len jeden počítač – útočníka –

v rozhraní eth0/3 a druhý počítač – hosťa – vo vnútornej sieti. Bude sa tak testovať bezpečnosť z demilitarizovanej zóny.



Obr. 5.2: Topológia siete na testovanie zabezpečenia.

5.3 Testovanie výkonu

V tejto sekcii bude predstavený návrh topológie na testovanie výkonu firewallu Hillstone pomocou zariadenia Spirent Avalanche. Celkovo bude vykonaných šesť testov, kde pri dvoch z nich bude nasimulovaný HTTP server, a na ostatných štyroch FTP server.

5.3.1 Testovanie výkonu pomocou HTTP serveru

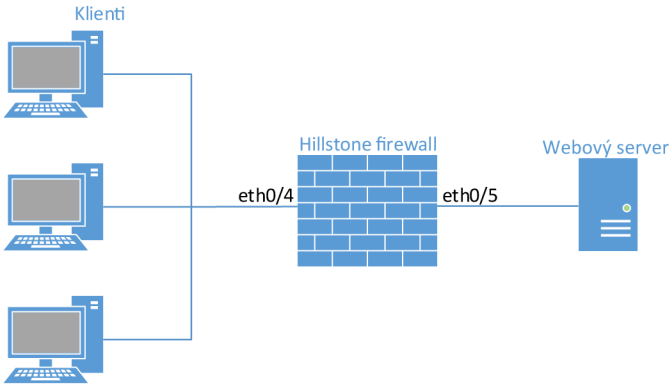
Testovanie s malým počtom užívateľov

Pri tomto teste bude odskúšaný praktický príklad, ktorý môže nastať pri otvorení stránky `https://www.vutbr.cz/` študentmi v jednej učebni.

Nastane situácia s päťdesiatimi študentmi, ktorým učiteľ nariadi prihlásiť sa do školského systému. Tí naraz posielajú požiadavok HTTP GET na server (v tomto prípade fiktívny sever vytvorený zariadením Spirent Avalanche). Ten im posiela HTML súbor `vut.html` so zdrojovým kódom o veľkosti 30,2 kB. S týmto by nemal mať firewall problém a všetky transakcie by mali byť úspešné. Ako táto topológia vyzerá možno vidieť na obrázku 5.3.

Testovanie s veľkým počtom užívateľov

Tento test bude obdobný s predošlým, ale na rozdiel od 50 študentov, budú klienti pribúdať až na hranicu 1000 za sekundu. Topológia bude zostavená ako v predošlom prípade podľa obrázku 5.3.



Obr. 5.3: Topológia siete s webovým serverom.

Testovanie maximálneho počtu transakcií.

Pri metodike testovania výkonu firewallu je možné testovať, koľko transakcií je zariadenie schopné spracovať za určitý čas. Takýto test nie je obmedzený maximálnou priepustnosťou firewallu, ale zameriava sa len na transakcie za sekundu. Toto testovanie hraničnej hodnoty transakcií je vykonané v bakalárskej práci „Bezpečnostní analýza firewallu“ [18].

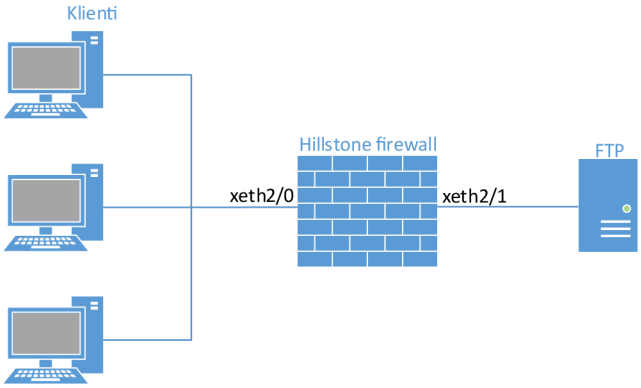
5.3.2 Testovanie výkonu pomocou FTP serveru

Testovanie bude prebiehať podobne ako v predchádzajúcom prípade. Zmeny nastanú zámenou HTTP serveru z obrázku 5.3 za FTP server a zmenou rozhraní na xeth2/0 na strane klienta a xeth2/1 na strane severu. Topológia je ukázaná na obrázku 5.4.

Všetky testy budú využívať rozširujúci modul *IOC-2XFP-Lite-M*, ktorý slúži na pripojenie 2 x XFP optických modulov s maximálnou priepustnosťou 10 Gb/s.
Zariadenie Spirent Avalanche bude simulovať 100 užívateľov sťahujúcich súbor s rozličnou veľkosťou. Veľkosť súboru sa bude odvíjať od požadovanej záťaže, ktorú je nutné vytvoriť na overenie výrobcom udávanej priepustnosti.
Pri všetkých výkonnostných testoch bude sledovaná a porovnávaná maximálna priepustnosť a využitie a teplota CPU.

Testovanie bez funkcií IPS a antivíru

Prvý záťažový test pomocou FTP serveru bude vykonávaný s vypnutými funkciami firewallu novej generácie. Výrobca udáva priepustnosť firewallu až 25 Gb/s. Kvôli



Obr. 5.4: Topológia siete s FTP serverom.

obmedzeniu XFP modulov na rýchlosť 10 Gb/s nebude možné dosiahnuť túto prevádzku. Preto bude test prebiehať pri rýchlosti 10 Gb/s. Túto rýchlosť zabezpečí 100 používateľov, ktorý budú sťahovať súbor o veľkosti 12,5 MB.

Testovanie s funkciou IPS

Ďalší z testov bude využívať funkciu IPS, pri ktorej by mala byť priepustnosť až 12 Gb/s. Tu taktiež nastáva problém s maximálnou priepustnosťou XFP modulov, a preto bude záťaž zhodná s predošlým testovaním, tj. 12,5 MB na klienta.

Testovanie s antivírom

Pri tomto teste bude zapnutá funkcia firewallu novej generácie, konkrétne funkcia antivíru. Tabuľková hodnota maximálnej priepustnosti pri tejto funkcii je 7 Gb/s. Testovanie bude prebiehať pri vyššej rýchlosti, a to až o 1 Gb/s. Každý užívateľ teda bude sťahovať súbor o veľkosti 10 MB/s.

Testovanie s funkciou IPS a antivírom

Posledný záťažový test bude vykonávaný so zapnutou funkciou IPS a tak isto aj antivírom. Výrobcom udávaná priepustnosť je pri zapnutí funkcie antivíru 7 Gb/s a pri IPS 12 Gb/s, preto možno zvoliť prevádzku o rýchlosti 8 Gb/s, ako to bolo v predošlom prípade a sledovať, ako firewall zvláda kombináciu týchto funkcií.

6 VÝSLEDKY TESTOVANIA

V tejto kapitole bude ukázané praktické prevedenie testov, ktoré boli stručne opísané v kapitole číslo 5 a budú popísané jednotlivé výsledky každého z nich.

6.1 Odpočúvanie premávky

Pri zachytávaní premávky bolo zostavené pracovisko podľa topológie na obrázku 5.1 a 24 hodín sa zachytávala programom Wireshark. Ako prvé sa zapne odpočúvanie a firewall bude zapojený do elektrickej siete. DHCP server priradil IP adresu `192.168.1.128`. Túto akciu je vidieť na obrázku 6.1, kde pri zapnutí firewallu Hillstone zariadenie posiela zo zdrojovej adresy `0.0.0.0` požiadavku na broadcast adresu `255.255.255.255`, tj. na všetky zariadenia v sieti, a hľadá DHCP server, ktorý mu adresu priradí. Okrem IP adresy mu priradí aj adresu predvolenej brány a DNS serveru. Ďalej nasleduje požiadavka na preklad IP adresy (3. vrstva ISO/OSI modelu) na MAC adresu (2. vrstva) pomocou protokolu ARP.

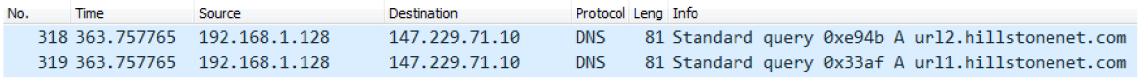
No.	Time	Source	Destination	Protocol	Leng	Info
304	357.763657	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0xa2d1fee8
305	357.764107	192.168.1.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xa2d1fee8
306	357.764710	0.0.0.0	255.255.255.255	DHCP	590	DHCP Request - Transaction ID 0xa2d1fee3
307	357.765080	192.168.1.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xa2d1fee3
310	360.765206	0.0.0.0	255.255.255.255	DHCP	590	DHCP Request - Transaction ID 0xa2d1fee3
311	360.765654	192.168.1.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xa2d1fee3
312	360.766300	Hillston_3b:08:d7	Broadcast	ARP	60	Who has 192.168.1.128? Tell 0.0.0.0
313	362.016532	Hillston_3b:08:d7	Broadcast	ARP	60	Gratuitous ARP for 192.168.1.128 (Request)
314	362.016532	Hillston_3b:08:d7	Broadcast	ARP	60	Gratuitous ARP for 192.168.1.128 (Request)
316	363.756999	Hillston_3b:08:d7	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.128
317	363.757112	PaloAlto_08:39:01	Hillston_3b:08:d7	ARP	60	192.168.1.1 is at 00:1b:17:08:39:01

Obr. 6.1: Žiadosť o IP adresu a následný preklad IP adries na MAC adresy.

Aby bola zobrazená len premávka, ktorá prichádza a odchádza z firewallu Hillstone, je nutné ju filtrovať pomocou príkazu `ip.src == 192.168.1.128 or ip.dst == 192.168.1.128`.
Takto sa vyfiltruje nepotrebná premávka, ktorú vytvára napríklad prepínač Mikrotik, alebo firewall Palo Alto, ktorý simuluje poskytovateľa internetu.

Po pridelení IP adresy je vidieť, ako sa zariadenie dopytuje po preklad domén `url1.hilstonenet.com` a `url2.hilstonenet.com`, na ktorých si kontroluje aktualizácie. Je nutné preložiť doménové meno na IP adresu pomocou DNS, takže posiela požiadavku na doménový server VUT, ako je vidieť na obrázku 6.2. Táto požiadavka sa opakuje zhruba každú minútu.

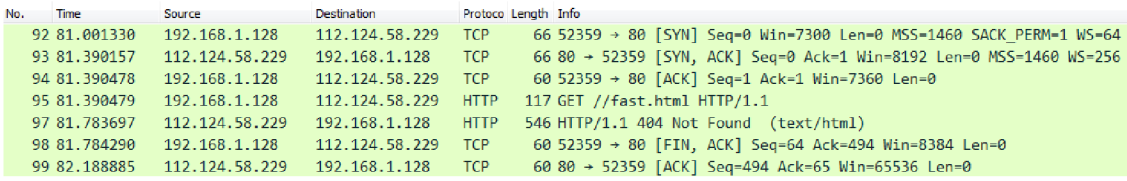
Ďalšiu vec, ktorá sa v zachytenej premávke opakuje každých 20 minút, je snaha firewallu kontaktovať IP adresu `112.124.58.229`, z ktorej sa snaží získať súbor



No.	Time	Source	Destination	Protocol	Leng	Info
318	363.757765	192.168.1.128	147.229.71.10	DNS	81	Standard query 0xe94b A url2.hillstonenet.com
319	363.757765	192.168.1.128	147.229.71.10	DNS	81	Standard query 0x33af A url1.hillstonenet.com

Obr. 6.2: Žiadosť o preklad doménového mena na IP adresu.

`fast.html`. Táto akcia je neúspešná – server na požiadavku `GET` od klienta odpovedá stavovým kódom `404 Not Found`, čo znamená že požadovaný dokument nebol nájdený. Všetko zachycuje obrázok 6.3.



No.	Time	Source	Destination	Protoco	Length	Info
92	81.001330	192.168.1.128	112.124.58.229	TCP	66	52359 → 80 [SYN] Seq=0 Win=7300 Len=0 MSS=1460 SACK_PERM=1 WS=64
93	81.390157	112.124.58.229	192.168.1.128	TCP	66	80 → 52359 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256
94	81.390478	192.168.1.128	112.124.58.229	TCP	60	52359 → 80 [ACK] Seq=1 Ack=1 Win=7360 Len=0
95	81.390479	192.168.1.128	112.124.58.229	HTTP	117	GET //fast.html HTTP/1.1
97	81.783697	112.124.58.229	192.168.1.128	HTTP	546	HTTP/1.1 404 Not Found (text/html)
98	81.784290	192.168.1.128	112.124.58.229	TCP	60	52359 → 80 [FIN, ACK] Seq=64 Ack=494 Win=8384 Len=0
99	82.188885	112.124.58.229	192.168.1.128	TCP	60	80 → 52359 [ACK] Seq=494 Ack=65 Win=65536 Len=0

Obr. 6.3: Kontaktovanie serveru a dopyt HTML súboru.

6.2 Testovanie bezpečnosti

Prvá skúška zabezpečenia firewallu bude zisťovanie otvorených portov. Na to bude slúžiť nástroj *Nmap*, ktorý už je v Kali Linuxe predinštalovaný. Druhý test bude vykonaný použitím *Hping3*, ktorý bude vytvárať DDoS útok, pri ktorom bude sledovaná záťaž procesoru. Ďalším testovacím nástrojom bude *Firewalk*, a posledný test bude vykonávaný nástrojom *Nessus*. Pri všetkých testoch okrem tretieho bude počítač útočníka pripojený ethernet káblom do rozhrania v demilitarizovanej zóne, ako na obrázku 5.2. Pri použití Firewalku bude útočník vo vonkajšej sieti Internet.

Ako prvý krok je nutné vo WebUI nastaviť zabezpečenie demilitarizovanej zóny, aby pri každej podozrivej akcii urobil firewall záznam:

1. Záložka Policy → dmz → Protection → Antivirus: Enable
   → Profile: predef_high
   → IPS: Enable
   → Profile: predef_loose
2. Záložka Network → dmz → Threat protection → Antivirus: Enable
   → Profile: predef_high
   → IPS: Enable
   → Profile: predef_loose
   → Defense Direstion: bidirect
   → Attack Defense: enable

6.2.1 Nmap

Najprv je nutné otvoriť terminál v Kali Linux a zistiť IP adresu východzej brány príkazom:

```
route -n
```

Po zadaní príkazu bolo zistené, že adresa východzej brány je `192.168.3.1` – tú je teraz možné skenovať príkazom:

```
nmap 192.168.3.1
```

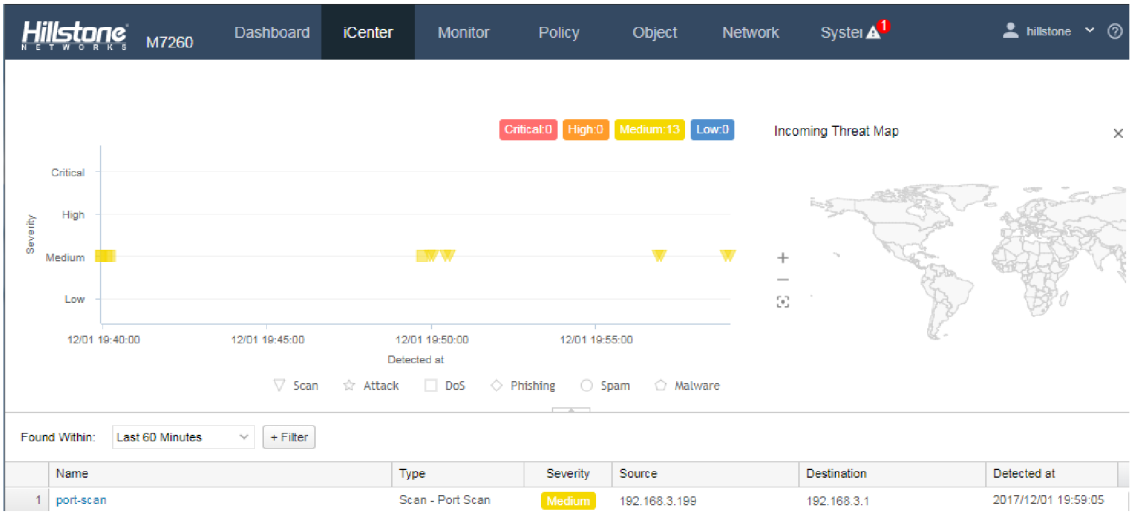
```
root@sklad-NB:~# nmap 192.168.3.1

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-12-01 19:59 CET
Nmap scan report for 192.168.3.1
Host is up (0.00019s latency).
Not shown: 999 filtered ports
PORT     STATE  SERVICE
8181/tcp closed unknown
MAC Address: 00:1C:54:3B:08:D9 (Hillstone Networks)

Nmap done: 1 IP address (1 host up) scanned in 4.89 seconds
```

Obr. 6.4: Skenovanie otvorených portov.

Ako je vidieť na obrázku 6.4, bol nájdený iba jeden TCP port číslo 8181, ktorý je ale zavretý, takže nemá zmysel na neho útočiť. Ďalší problém pre útočníka je, že firewall o ňom zistil, že skenoval sieť. Hneď ako zaznamenal skenovanie portov, urobil záznam, ktorý je vidieť vo WebUI v záložke Policy, ako ukazuje obrázok 6.5. Je tu jasne vidieť zdroj (IP adresa `192.168.3.199`), cieľ a druh útoku.



Obr. 6.5: Záznam útoku – skenovanie portov.

Ak by sa útočník chcel vyhnúť priamemu odhaleniu, je možnosť „skryť sa v dave“. Príkazom:

```
nmap 192.168.3.1 -D 192.168.3.198,192.168.3.197
```

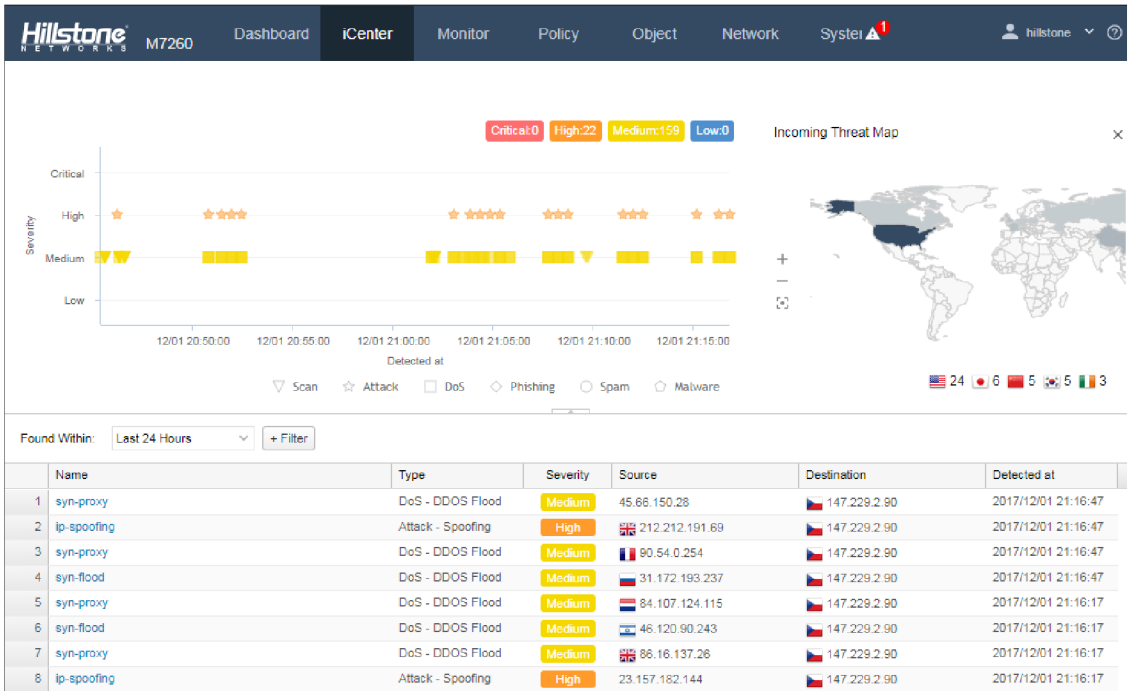
pridá ďalšie adresy ako zdroje skenovania, a tak nebude administrátor siete vedieť, kto je pravý útočník, pretože mu firewall ukáže ako útočníkov aj pravým útočníkom zvolené adresy. Výsledné adresy by boli zaznamenané podobne ako na obrázku 6.6 v stĺpci „Source“.

6.2.2 Hping3

Pri tomto teste sa bude posielať príkazom

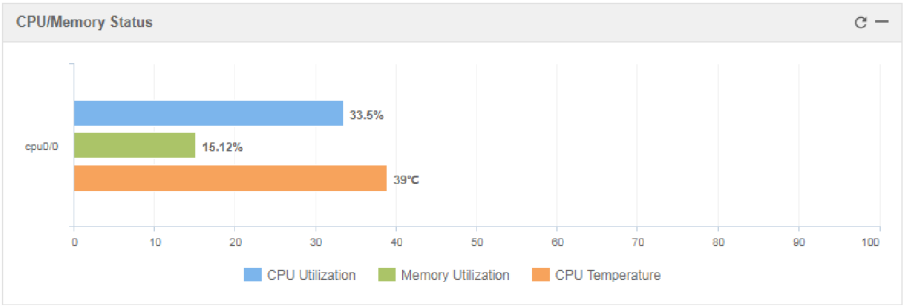
```
hping3 -c 10000 -d 120 -S -w 64 -p 80 --flood
       --rand-source www.vutbr.cz
```

10000 paketov o veľkosti 120 kilobitov na port 80 serveru VUT Brno. Aby firewall nezistil, kto je strojcom útoku, je nutné nastaviť „random-source“, čiže náhodný zdroj. Týmto spôsobom bude firewall označovať pakety ako DoS útok, ale zdrojová IP adresa bude náhodná. -S znamená posielanie SYN paketov a -w je určenie veľkosti TCP okna.



Obr. 6.6: Záznam útoku – skenovanie portov.

Označených útočníkov a oblasti odkiaľ sú, je možné vidieť na obrázku 6.6. V niektorých možnostiach označil firewall správne útok ako IP Spoofing – podvrhnutie IP adresy útočníka.



Obr. 6.7: Využitie procesora firewallu pri DDoS útoku.

Pri sledovaní využitia procesoru v záložke Monitor → Device je vidieť že v pokojnom stave sa využitie CPU pohybuje okolo 1 %. Avšak ak sa začne útok, zvýši sa na viac ako 30 %. Ak by bolo viac pripojených užívateľov, ktorí by začali útok v ten istý moment, mohli by zahltiť firewall. Na ochranu takéhoto útoku by administrátor nastavil prerušenie tohoto spojenia pri náznaku útoku. To je v tomto prípade vypnuté, preto môže útok pokračovať.

6.2.3 Firewalk

Ako bolo naznačené na začiatku sekcie 6.2, počítač administrátora siete, ktorý chce skontrolovať či nastavil ACL správne, bude umiestnený vo vonkajšej „untrusted“ zóne, odkiaľ bude testovať priechodnosť paketov firewallom. V prvom teste bude cez firewall prechádzať všetka prevádzka na ukážku otvoreného TCP portu 139. Pred druhým testom bude nastavený prístupový zoznam, v ktorom bude komunikácia na tomto porte s vonkajšou sieťou zakázaná. Konfigurácia firewallu je nasledovná:
Záložka Policy → Security Policy → New → Source → Zone: untrust
→ Destination → Zone: dmz
V kolónke Service je nutné pridať novú možnosť, kde sa nastaví Destination Port: 139 a typ spojenia TCP. Nakoniec treba vyberať akciu „Deny“ a potvrdiť tlačidlom OK. Týmto sa obmedzí prechod komunikácie z vonkajšej siete na TCP porte 139.

Nástroj Firewalk nie je predinštalovaný v najnovšej verzii Kali Linux, takže je nutné nainštalovať ho príkazom:

```
apt-get install firewalk
```

Po inštalácii je už možné vykonávať testy. Prvý test TCP portu bude vykonaný bez nastavenia ACL. Príkaz vyzerá nasledovne:

```
firewalk -S139 -i eth0 -pTCP 192.168.100.1 192.168.3.200
```

kde -S139 znamená číslo portu, -i eth0 rozhranie, na ktorom bude test vykonaný, -pTCP určenie typu protokolu, prvá IP adresa je adresa východzej brány počítača administrátora a druhá je adresa hosťa, ku ktorému je nutné sa dostať. V tomto prípade má túto adresu počítač, ale je možné takto testovať prístup k rozličným serverom. Na obrázku 6.8 možno vidieť výsledok tohto testu.

```
dominik@sklad-NB:/$ sudo firewalk -S139 -i eth0 -pTCP 192.168.100.1 192.168.3.200
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 53, destination port: 33434
Hotfoot through gateway using 192.168.3.200 as a metric.
Ramping Phase:
 1 (TTL  1): expired [gateway]
Binding host reached.
Scan bound at 2 hops.
Scanning Phase:
port 139: A! open (port listen) [192.168.3.200]

Scan completed successfully.

Total packets sent:                2
Total packet errors:               0
Total packets caught               2
Total packets caught of interest   2
Total ports scanned                1
Total ports open:                  1
Total ports unknown:               0
```

Obr. 6.8: Testovanie pomocou nástroju Firewalk.

Z tohto obrázku je vidieť, že Firewalk poslal 2 pakety, prvý s TTL rovným jedna, ktorým sa dostal na firewall. Druhý paket mal hodnotu TTL o jednu vyššiu, aby sa dostal až ku hosťovi. Testovaný bol port 139, ktorý je zobrazený ako otvorený. Druhý test je vykonávaný s nakonfigurovaným prístupovým listom a komunikácia na porte by mala byť zakázaná. Administrátor si to môže skontrolovať zadaním toho istého príkazu ako pri prvom teste.

```
Scanning Phase:
port 139: *no response*

Scan completed successfully.

Total packets sent:                2
Total packet errors:               0
Total packets caught               1
Total packets caught of interest   1
Total ports scanned                1
Total ports open:                  0
Total ports unknown:               0
```

Obr. 6.9: Testovanie pomocou nástroju Firewalk s nakonfigurovaným ACL.

Výsledok tohto testu ukazuje, že port 139 neodpovedá. Tým je overené že konfigurácia bola úspešná. Týmto spôsobom je možné presvedčiť o nastavení prístupových listov na sieťovom prvku a zmenšiť riziko napadnutia rozličných portov útočníkmi.

6.2.4 Nessus

Na skenovanie siete pomocou nástroja Nessus je nutné najprv jeho stiahnutie. To je možné priamo na webovej stránke `www.tenable.com`. V prípade používania Kali Linux je nutné stiahnuť súbor *Nessus-7.0.3-debian6_amd64.deb*. Po stiahnutí je potrebné jeho následné rozbalenie a nainštalovanie príkazom:

```
dpkg -i Nessus-7.0.3-debian6_amd64.deb
```

a ďalej spustenie príkazom:

```
/etc/init.d/nessusd start
```

Po spustení je treba registrovať sa, po čom užívateľ získa aktivačný kód na prihlásenie sa do Nessusu. Následne otvorí internetový prehliadač a napíše do neho URL adresu `https://localhost:8834/`, kde sa užívateľ prihlási a zadá kód. Teraz môže nastavovať jednotlivé skeny a ich parametre.

Zisťovanie hosťov v sieti

Prvý test, ktorý môže užívateľ využiť, je skenovanie siete s účelom získania informácií o hosťoch v sieti. Ako prvá sa nastaví politika, ktorou sa bude následný test riadiť. Nastavenie politiky:
Záložka Policies → New Policy → Host Discovery
Okno Settings → BASIC → Name (meno politiky)
→ DISCOVERY → Scan Type → Host enumeration
Táto politika je hotová a možno ju uložiť tlačidlom Save a použiť pri skenovaní siete. Ako typ skenu bolo zvolené „Host enumeration“, v preklade výpočet hostí. Tento test kontroluje prítomnosť hostí v sieti pomocou troch protokolov: TCP, ARP a ICMP.
Nasleduje priradenie politiky ku konkrétnemu testu. To je možné urobiť v záložke My Scans → New Scan → User Defined a tam vybrať vytvorenú politiku. Do novo otvoreného okna vyplniť Name (meno) a Targets (ciele). Ako cieľ môže užívateľ zvoliť sieť, v ktorej je práve pripojený, v tomto prípade `192.168.3.0/24`. Nakoniec uložiť a spustiť tlačidlom Save → Launch.

Po dokončení testu je možné vidieť výsledky, ktoré sú zobrazené na obrázku 6.10. Nessus správne určil dve zariadenia nachádzajúce sa v sieti. Počítač, na ktorom prebiehalo skenovanie a IP adresu východzej brány, ktorú má firewall Hillstone.

Obr. 6.10: Nájdený hostia pri skene siete.

Pri tomto teste bol vytvorený záznam o útoku vo firewalle zhodný so záznamom pri využití nástroju Nmap na obrázku 6.5. Dôvodom je rýchle skenovanie siete ktoré má firewall uložené ako signatúru útoku „Port Scan“.

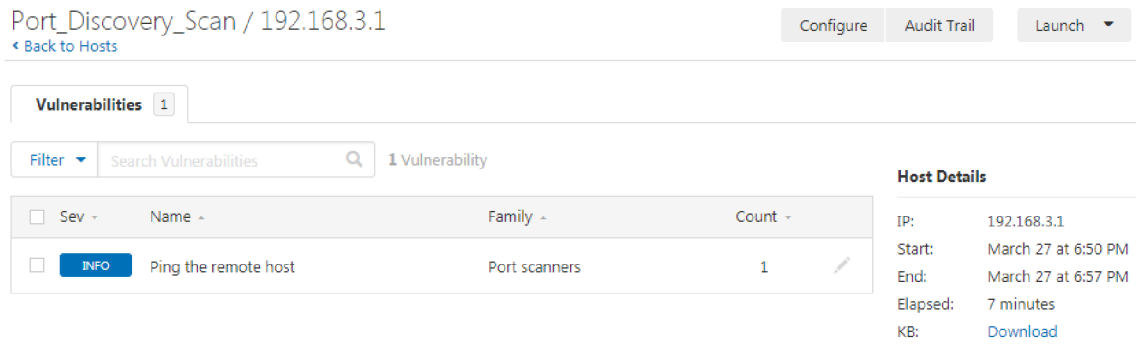
Skenovanie otvorených portov

Ako druhý test bude vykonaný sken otvorených portov, na ktoré by bolo možné zaútočiť. Nakoľko užívateľ je v sieti sám, bude skenovať len IP adresu východzej brány `192.168.3.1`. Ak by sa v sieti nachádzali aj iné zariadenia, mohol by skenovať aj ich porty zadaním ich IP adresy do rozsahu cieľov alebo adresu celej siete. Ako pri prvom teste je nutné znova nastaviť novú politiku. Nastavenie politiky:
Záložka Policies → New Policy → Host Discovery
Okno Settings → BASIC → Name (meno politiky)
→ DISCOVERY → Scan Type → Port scan (all ports)
Týmto bolo nastavené skenovanie všetkých portov (1-65535), ktoré zaberie viac času, ale je väčšia pravdepodobnosť nájdenia zraniteľného portu.
Opäť sa priradí politika k novému testu ako v predošlom prípade. Jediná zmena je v okne Targets, kde bude IP adresa východzej brány. Test je pripravený na spustenie.

Pri pohľade na výsledky testu na obrázku 6.11 je zreteľné, že Nessus nenašiel žiadny otvorený port. Ako jediný záznam je vidieť informačná hláška „Ping the remote host“ ktorá hlási, že hosť, ktorý je za IP adresou, odpovedal na ping a je aktívny. Neznamená to ale, že je akokoľvek zvýšené riziko útoku.

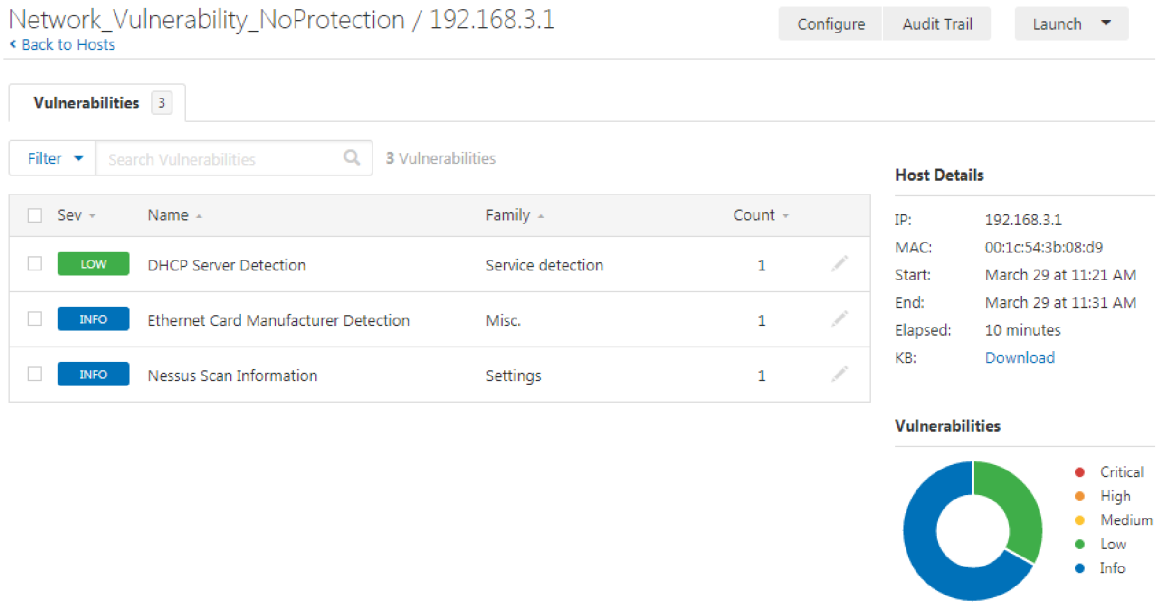
Skenovanie zraniteľností vo vnútornej sieti

Pri poslednom teste bude pomocou nástroja Nessus skenovaný firewall Hillstone za účelom nájdenia prípadných chýb a zraniteľností systému. Ako v predošlých testoch sa najprv vytvorí nová politika.



Obr. 6.11: Výsledky testu skenovania portov.

Nastavenie politiky:
Záložka Policies → New Policy → Basic Network Scan
Okno Settings → BASIC → Name (meno politiky)
→ DISCOVERY → Scan Type → Port scan (all ports)
→ ASSESSMENT → Scan Type → Default
→ ADVANCED → Scan Type → Default
Politika sa priradí k testu, cieľová adresa ostáva `192.168.3.1` a test sa môže spustiť. Znova sa skenujú všetky porty, takže test môže trvať dlhší čas. Výsledky sa zobrazia hneď po dokončení testu a sú vidieť na obrázku 6.12.



Obr. 6.12: Výsledky skenovania zranitelných miest firewallu.

V tomto prípade možno vidieť tri hlásenia, z ktorých sú dve informatívne a jedno hlásenie je označené nízkym stupňom nebezpečenstva. Prvé informačné hlásenie obsahuje informácie o skene ako dĺžku skenu, rozsah portov, počet skenovaných hostov a iné. Druhé hlásenie obsahuje výrobcu zariadenia, ktorého zistilo podľa MAC adresy firewallu Hillstone. Tretie hlásenie, ktoré už je považované za zraniteľnosť, upozorňuje na informácie poskytované DHCP serverom. V niektorých prípadoch môže DHCP server poskytovať informácie, ktoré by sa dali využiť pri útoku, ako napríklad list webových serverov nachádzajúcich sa v sieti.

Nástroj Nessus kontaktoval na UDP porte 67 DHCP server, ktorý je nastavený vo firewalle, a snažil sa zistiť informácie o sieti. Na obrázku 6.13 možno vidieť všetky informácie poskytované DHCP serverom. Patrí ku nim IP adresa s maskou siete pridelená hostovi, východzia brána a IP adresa DNS serveru. V tomto prípade sa nejedná o zraniteľnosť, ale Nessus aj napriek tomu vyhotovil toto hlásenie, aby upozornil administrátora siete na informácie ktoré poskytuje DHCP server v sieti.

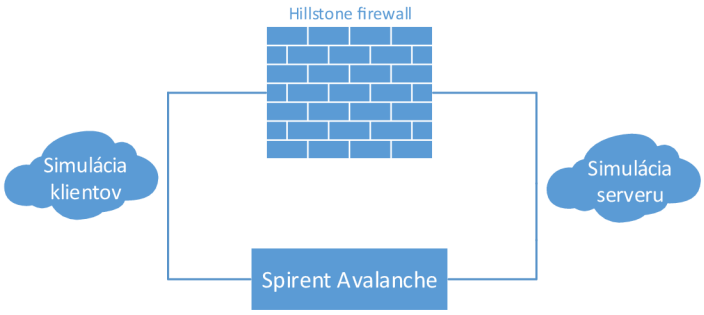
```
Nessus gathered the following information from the remote DHCP server :

  Master DHCP server of this network : 0.0.0.0
  IP address the DHCP server would attribute us : 192.168.3.200
  DHCP server(s) identifier : 192.168.3.1
  Netmask : 255.255.255.0
  Router : 192.168.3.1
  Domain name server(s) : 147.229.71.10
```

Obr. 6.13: Informácie získané od DHCP serveru.

6.3 Testovanie výkonu

Ako bolo opísané v metodike testovania výkonu v sekcii 5.3, tak sa bude postupovať pri záťažovom testovaní. Reálne zapojenie môžno vidieť na obrázku 6.14.



Obr. 6.14: Zapojenie výkonnostného testovania so zariadením Spirent Avalanche.

6.3.1 Testovanie výkonu pomocou HTTP serveru

Testovanie s malým počtom užívateľov

Najprv je nutné v programe Spirent TestCenter Layer 4-7 Application 4.43 založiť nový projekt a v ňom si vytvoriť Advanced Device Test na pokročilé testovanie zariadenia. Nasleduje nastavenie časti klienta:

1. V záložke Loads:
   Specification: SimUsers/second
   Label: Test
   Pattern: Flat
   Height: 50
   Ramp Time: 30
   Steady Time: 270
2. V záložke Actions vložiť do poľa príkaz:
   `1 get http://192.168.5.2/index.html`
3. Záložka Subnets:
   Add Subnet → IP Address Range: `192.168.4.2-192.168.4.254`
   Netmask: /24, Default Gateway: `192.168.4.1`
4. Záložka Ports:
   Priradíme Port 8.
5. Záložka Associations:
   Priradiť vytvorené profily k jednotlivým prvkom a klientská časť je nastavená.

Nastavenie časti Server:

1. Záložka Transactions:
   Body Content Type: Binary
   Size: 30200
2. Záložka Profiles:
   Type: HTTP
   Transaction Profile: Default
3. Záložka Subnets:
   Add Subnet → Network: `192.168.5.0`
   Netmask: /24, Default Gateway: `192.168.5.1`
4. Záložka Ports:
   Priradíme Port 9.
5. Záložka Associations:
   Priradiť vytvorené profily k jednotlivým prvkom a nastaviť IPv4 Address Range: `192.168.5.2`.

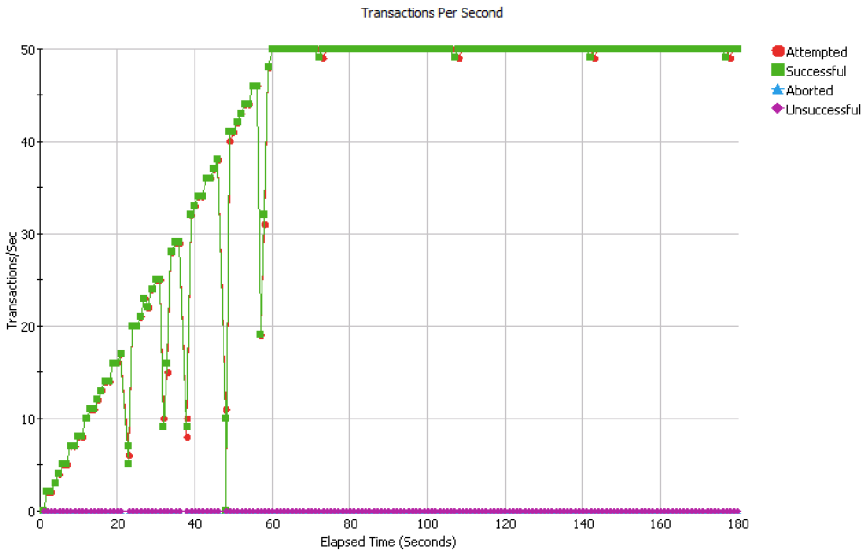
Teraz je všetko pripravené na spustenie testu. To sa vykoná tlačidlom „Run test now!“. Tento test bude trvať 5 minút.
Výsledky možno vidieť v záložke Results.

Tabuľka na obrázku 6.15 ukazuje úspešnosť transakcií, o ktoré sa klienti pokúšali. Celkový počet požiadaviek bol 7319 za dĺžku trvania 5 minút. Je vidieť že firewall s týmto nemal žiaden problém a vybavil 100% požiadaviek.

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	7319	40	Minimum	0.0	0.0	0.178	0.078	0.0	Attempted	7319
	Successful	7319	40	Maximum	0.0	0.0	1466.045	0.294	0.033	Established	7319
	Unsuccessful	0	0	Average	0.0	0.0	0.798	0.087	0.0		
	Aborted	0	0								

Obr. 6.15: Úspešnosť požiadaviek na strane klientov.

Druhý obrázok (6.16) znázorňuje graf závislosti počtu transakcií na čase. Počiatočných 60 sekúnd transakcie lineárne rastú až na hodnotu 50 transakcií za sekundu. Za týmito transakciami je možné predstaviť si jednotlivých študentov, odosielajúcich požiadavky na server. Je vidieť, že kým sa graf neustáli, transakcie majú tendenciu rapídne klesať. Toto môže byť spôsobené zariadením Spirent Avalanche, ktoré prestane na moment odosielať SYN-ACK odpovede klientom. Toto nenaruší výsledky testu, pretože je 100% úspešnosť vybavenia transakcií, ale oneskorí to prijatie odpovede SYN-ACK od serveru u niektorých klientov (maximálna hodnota časového oneskorenia je z obrázku 6.16 vidieť: 1466, 045 ms).



Obr. 6.16: Počet transakcií na strane klientov.

Testovanie s veľkým počtom užívateľov

Ako bolo vidieť pri testovaní s malou záťažou nemal firewall žiadny problém spracovávať všetky žiadosti. V ďalšom teste bude zvýšený počet klientov na 1000 za sekundu. Bude zmenená len konfigurácia klientskej časti, konkrétne tieto položky:

1. V záložke Loads sa zmení z predošlého testu:
   Height: 1000
   Ramp Time: 30
   Steady Time: 150

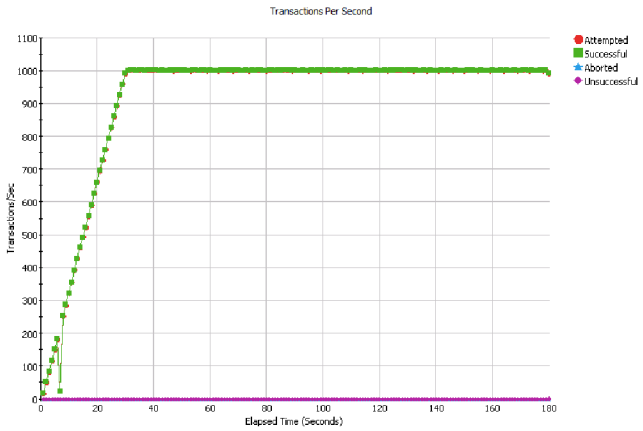
Test je pripravený na spustenie. Bude trvať 3 minúty, a počas prvých 30 sekúnd narastie počet transakcií na maximum, tj. 1000 za sekundu.

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	165086	917	Minimum	0.0	0.0	0.099	0.075	0.0	Attempted	165086
	Successful	165085	917	Maximum	0.0	0.0	995.214	0.348	0.247	Established	165086
	Unsuccessful	1	0	Average	0.0	0.0	0.112	0.079	0.0		
	Aborted	0	0								

Obr. 6.17: Úspešnosť požiadaviek na strane klientov pri 1000 používateľoch.

Ako je vidieť na obrázku 6.17, jedna požiadavka nebola úspešná. To je ale zanedbateľné množstvo pri celkovom počte 165086 transakcií. Priemerná hodnota neúspešných požiadaviek bola 2,4 pri desiatich opakovaniach, čo je úspešnosť viac ako 99,99 %. Najvyššie oneskorenie SYN-ACK odpovede od serveru je 995 ms, to možno vidieť znova na začiatku testu pri lineárnom raste transakcií na obrázku 6.18. Pri opakovaných testoch sa táto výchylka vyskytuje náhodne v lineárnej časti.

Obrázok 6.18 znázorňuje, ako rástol počet klientov za sekundu, firewall nemal ani s týmto problémy a zvládal tento nápor klientov.



Obr. 6.18: Počet transakcií pri 1000 klientoch za sekundu.

6.3.2 Testovanie výkonu pomocou FTP serveru

Ako prvý krok je nutné nakonfigurovať stranu klientov a následne stranu serveru. Táto konfigurácia sa bude meniť v priebehu všetkých testov len minimálne. Konkrétne sa bude meniť veľkosť sťahovaného súboru, ktorá bola určená v časti 5.3.2 podľa maximálnych priepustností.
Nastavenie klientskej časti:

1. V záložke Loads:
   Specification: SimUsers/second
   Label: Start
   Pattern: Flat
   Height: 100
   Ramp Time: 60
   Steady Time: 0
2. Add a Phase
   Label: Running
   Pattern: Flat
   Height: 100
   Ramp Time: 0
   Steady Time: 120
3. Add a Phase
   Label: End
   Pattern: Flat

Height: 0

Ramp Time: 50

Steady Time: 130

4. V záložke Actions vložiť do poľa príkaz[1]:
   `1 ftp://192.168.20.2/13m`
5. Záložka Subnets:
   Add Subnet → IP Address Range: `192.168.10.2-192.168.10.254`
   Netmask: /24, Default Gateway: `192.168.10.1`
6. Záložka Ports:
   Priradíme Port 12.
7. Záložka Associations:
   Priradiť vytvorené profily k jednotlivým prvkom a klientská časť je nastavená.

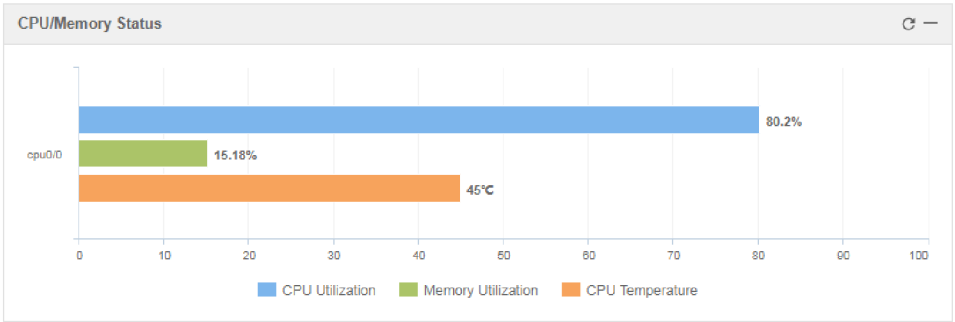
Nastavenie časti Server:

1. Záložka Profiles:
   Type: FTP
2. Záložka Subnets:
   Add Subnet → Network: `192.168.20.0`
   Netmask: /24, Default Gateway: `192.168.20.1`
3. Záložka Ports:
   Priradíme Port 13.
4. Záložka Associations:
   Priradiť vytvorené profily k jednotlivým prvkom a nastaviť IPv4 Address Range: `192.168.20.2`.

Konfigurácia FTP serveru je dokončená. Každý test bude trvať šesť minút.

Testovanie bez funkcií IPS a antivíru

Pri tomto teste nie je nutné konfigurovať funkcie na zariadení Hillstone, a je možné hneď spustiť test. Obrázok 6.19 zobrazuje informácie o CPU a RAM.

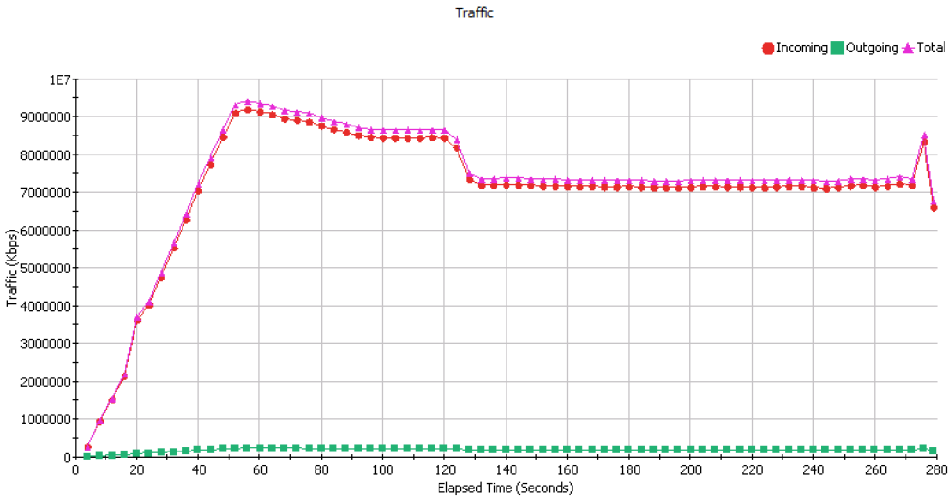


Obr. 6.19: Využitie procesora firewallu bez funkcií firewallu novej generácie.

[1]Číslo za poslednou lomkou udáva veľkosť sťahovaného súboru v MB.

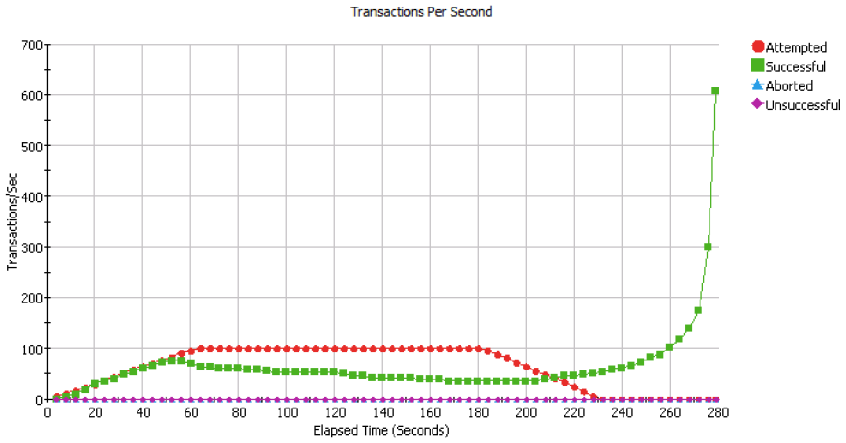
Možno na ňom vidieť percentuálne využitie RAM a CPU spolu s jeho teplotou. Využitie procesora sa v pokojnom stave pohybovalo okolo 1 %. Pri najvyššej záťaži sa pohybovalo v rozmedzí 65-75 %.

Na obrázku 6.20 možno vidieť premávku na klientskej strane. Najvyššia zaznamenaná rýchlosť bola 9,4 Gb/s, čo sa približuje maximálnej priepustnosti XFP modulov.



Obr. 6.20: Graf veľkosti prevádzky za sekundu bez funkcií firewallu novej generácie.

Pri pohľade na obrázok 6.21 je vidieť počet transakcií za sekundu na klientskej strane. Transakcie stúpajú až do hodnoty 75 transakcií za sekundu, kde pomaly začnú klesať. Na konci testu možno vidieť vysoký nárast transakcií. To je spôsobené ukončovaním všetkých FTP spojení. Úspešnosť transakcií je 100 %.



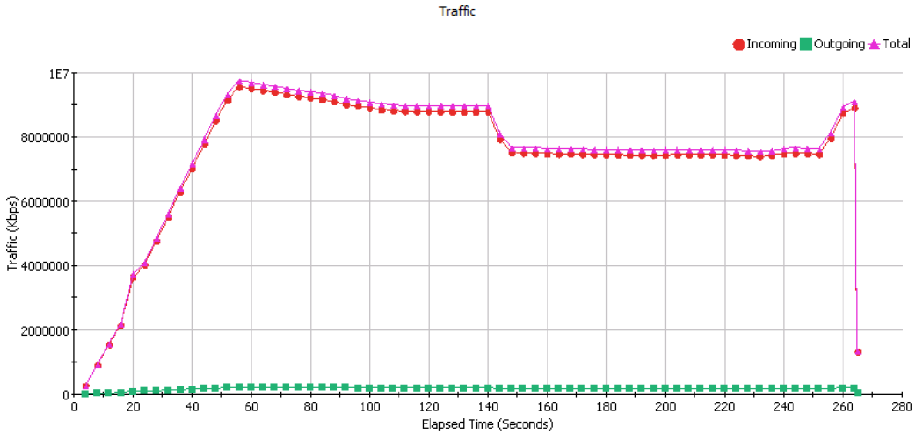
Obr. 6.21: Počet transakcií za sekundu bez funkcií firewallu novej generácie.

Testovanie s funkciou IPS

Najprv je nutné nakonfigurovať IPS na firewally a následne je test možné spustiť.

1. Záložka Policy → any → Protection → IPS: Enable
   → Profile: predef_default
2. Záložka Network → trust → Threat protection → IPS: Enable
   → Profile: predef_default

Výsledky sú veľmi podobné predošlému testu, z dôvodu maximálnej priepustnosti s funkciou IPS až 12 Gb/s. Využitie CPU sa pohybovalo vo vyšších hodnotách od 85 do 90 %. Na obrázku 6.22 možno vidieť graf prevádzky za sekundu, je takmer zhodný s predošlým prípadom.



Obr. 6.22: Graf veľkosti prevádzky za sekundu s funkciou IPS.

Graf počtu transakcií za sekundu nebude z dôvodu totožnosti s predchádzajúcim prípadom ukázaný. Zmena nastáva len v počte prerušených transakcií. Tých je v tomto prípade 7 z celkového počtu 17437. To znamená úspešnosť transakcií 99,95 %.

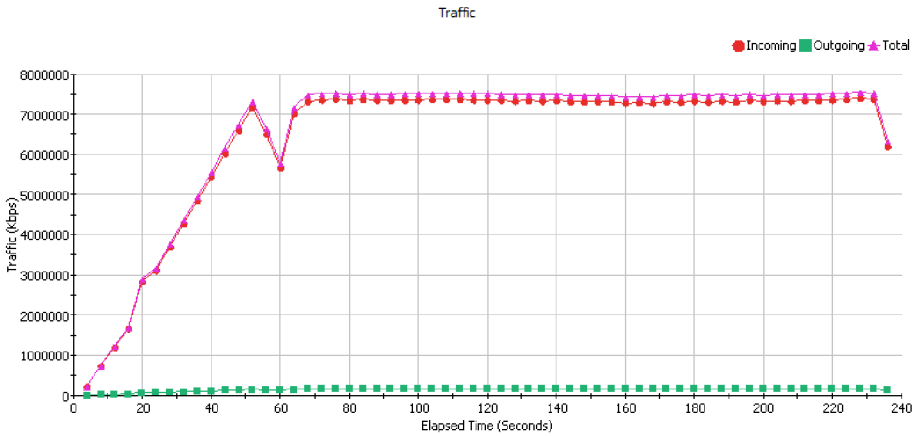
Testovanie s antivírom

Ako v predchádzajúcom prípade, je nutné nakonfigurovať funkciu antivíru:

1. Záložka Policy → any → Protection → Antivirus: Enable
   → Profile: predef_middle
2. Záložka Network → trust → Threat protection → Antivirus: Enable
   → Profile: predef_middle

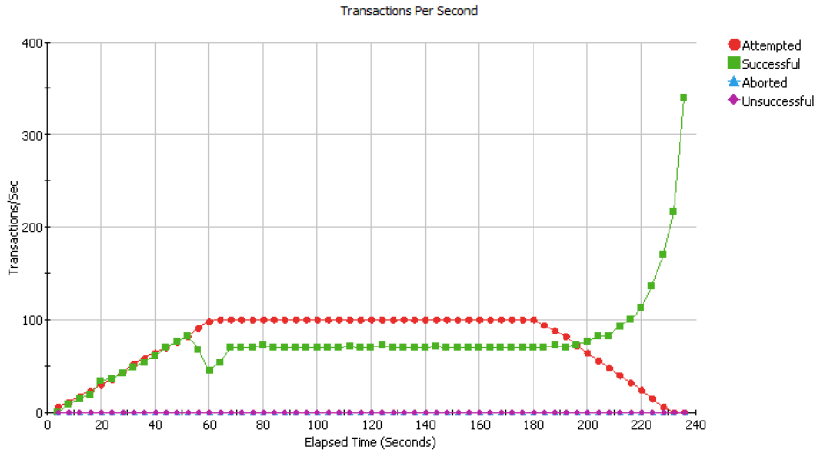
Po nakonfigurovaní firewallu je potreba zmeniť veľkosť sťahovaného súboru v klientskej časti zariadenia Spirent Avalanche. Veľkosť súboru bude 10 MB, ako bolo uvedené v časti 5.3.2.

Pri teste so zapnutým antivírom sa využitie CPU sa pohybovalo okolo 80 %. Pri pohľade na obrázok 6.23 je vidieť, že maximálna priepustnosť je o niečo vyššia ako udáva výrobca. Dostala sa až na hodnotu 7,5 Gb/s, čo je o 0,5 Gb/s viac ako v dokumentácií.



Obr. 6.23: Graf veľkosti prevádzky za sekundu s antivírom.

Počet transakcií možno vidieť na obrázku 6.24. Ich počet lineárne rastie až do hodnoty 82 za sekundu, neskôr sa ustáli okolo hodnoty 70 transakcií. Na konci testu je opäť rapídny vzrast transakcií.
Pri zapnutej funkcii antivíru bolo prerušených 10 transakcií z 17438, čo znova znamená vysokú úspešnosť až 99,94 % úspešných transakcií.

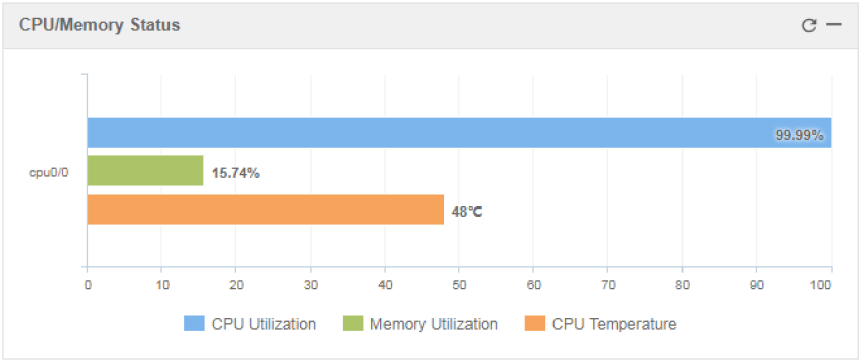


Obr. 6.24: Počet transakcií za sekundu s antivírom.

Testovanie s funkciou IPS a antivírom

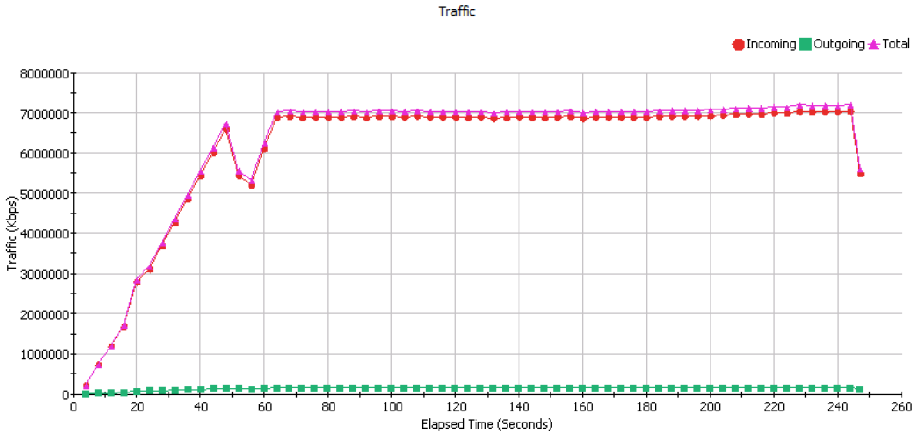
Posledný výkonnostný test bude prebiehať so zapnutými oboma funkciami firewallu novej generácie. To znamená že ich je nutné nakonfigurovať vo firewalle. Veľkosť sťahovaného súboru ostáva nezmenená z predošlého testu.

Najviac vyťažený bol firewall práve v tomto teste. Obrázok 6.25 ukazuje, ako stúplo využitie procesora. Počas testu sa pohybovalo od hodnoty 93 % vyššie, až na hraničnú hodnotu 99,99 %.



Obr. 6.25: Využitie procesora firewallu s funkciou IPS a antivírom.

Celková prevádzka prechádzajúca cez Hillstone bola v tomto prípade 8 Gb/s. Z pohľadu na obrázok 6.26 možno vidieť, že sa priepustnosť držala pri hodnote 7 Gb/s.



Obr. 6.26: Graf veľkosti prevádzky za sekundu s funkciou IPS a antivírom.

Graf počtu transakcií za sekundu je takmer zhodný s predošlým prípadom pri použití antivíru, preto nebude ukázaný. Počet prerušených transakcií bol 6 z celkového počtu 17435, tj. úspešnosť transakcií je 99,96 %.

6.3.3 Porovnanie záťažových testov s FTP serverom

Tabuľka 6.1 ukazuje porovnanie hodnôt pri všetkých štyroch výkonnostných testoch. Reálna priepustnosť je pri prvých dvoch testoch obmedzená na rýchlosť 10 Gb/s kvôli XFP modulom. Pri poslednom teste výrobca neudáva maximálnu priepustnosť pri kombinácii funkcií IPS a antivíru, preto bola zvolená teoretická hodnota 8 Gb/s pri testovaní.

Tab. 6.1: Porovnanie výsledkov jednotlivých výkonnostných testov.

Funkcia	**Udávaná priepustnosť**	**Reálna priepustnosť**	**Využitie CPU**
Žiadna	25 Gb/s	9,4 Gb/s	65-75 %
IPS	12 Gb/s	9,7 Gb/s	85-90 %
AV	7 Gb/s	7,5 Gb/s	80 %
IPS + AV	Neudávané	7 Gb/s	93-99,99 %

Firewall Hillstone zvládol všetky testy bez väčších odchýliek od výrobcom udávanej maximálnej priepustnosti. Testovanie s funkciou antivíru bolo schopné vyššej prevádzky, ako bola udávaná výrobcom.
Zariadenie bolo umiestnené v klimatizovanom priestore zo stálou teplotou 23 °C. Hodnota teploty procesora sa počas celého testovania pohybovala od 44 °C pri pokojnom stave, až do 48 °C pri najväčšej záťaži.

7 ZÁVER

Počas bakalárskej práce boli v teoretickej časti opísané typy firewallov a ukázané funkcie firewallov novej generácie. V praktickej časti bola zachytávaná sieťová premávka a následne boli vykonávané testy bezpečnosti a výkonu firewallu.

Pri skúmaní odchytenej premávky bolo ukázané, ako sa zariadenie pripája do siete a využíva sieťové protokoly na začatie komunikácie. Firewall Hillstone v pokojnom stave bez pripojených klientov komunikoval zo svojimi domovskými stránkami na získanie aktualizácií a kontrolu licencií.

Na bezpečnostné testovanie boli využité štyri nástroje z operačného systému Kali Linux, a to „Nmap“, „Hping3“, „Firewalk“ a „Nessus“.
Prvým spomenutým nástrojom bola skenovaná sieť zo snahou získať informácie o firewalle Hillstone a prvkoch v sieti. Podarilo sa zistiť výrobcu firewallu pomocou MAC adresy. Nástroj taktiež oskenoval logické porty v zariadení, pričom zistil, že boli všetky zatvorené. Druhý nástroj bol využitý na DoS útok cez firewall. Pri oboch testoch bol zapnutý systém IPS na detekciu nezvyčajných javov v sieti, takže bol útočník odhalený akonáhle sa začal útok. Pomocou nástroju Firewalk bolo ukázané, ako môže sieťový administrátor skontrolovať konfiguráciu prístupových zoznamov. Posledný bezpečnostný test bol vykonaný nástrojom Nessus, slúžiacim na celkové skenovanie zraniteľností v sieti. Bola nájdená zraniteľnosť označená nízkym stupňom nebezpečenstva, a to možnosť zneužitia informácií, ktoré poskytuje DHCP server. Tieto informácie sú nastavované administrátorom siete, takže záleží na konfigurácii či bude DHCP server poskytovať citlivé informácie, ktoré môžu byť zneužité.
Počas bezpečnostných testov neboli nájdené závažné zraniteľnosti a tak nemožno navrhnúť zlepšenie zabezpečenia.

Výkonnostné testovanie bolo vykonávané zariadením Spirent Avalanche 3100 ktoré simulovalo ako klientskú časť, tak časť serveru.
Prvé dva testy prebiehali simuláciou HTTP serveru, nasledujúce štyri testy využívali FTP server. Pri prvom teste bolo využitých 50 klientov dotazujúcich sa na simulovaný webový server VUT, z ktorého klienti získavali domovskú stránku VUT o veľkosti 30,2 kB. S týmto nemal firewall problém. Druhý test ukázal, ako si poradí s 1000 užívateľmi za sekundu. Úspešnosť požiadaviek sa pri tomto teste držala nad hranicou 99,99 % s priemerom 2,4 neúspešných transakcií na test.
Testy pomocou FTP severu prebiehali sťahovaním súboru o rôznej veľkosti 100 užívateľmi. Veľkosť súboru bola určená podľa maximálnej priepustnosti udanej výrobcom. Jednotlivé testy overovali priepustnosť pri rozličných funkciách firewallu novej generácie a následne boli výsledky zobrazené v grafoch a porovnané v tabuľke. Vo všetkých testoch bola priepustnosť blízka tabuľkovej hodnote, až na test s funkciou antivíru, kde bola priepustnosť o 0,5 Gb/s vyššia, ako udávaná výrobcom.

LITERATÚRA

[1] *Internet Users. Internet Live Stats.* [online] USA: Real Time Statistics Project, 2017 [cit. 2017-10-20]. Dostupné z URL: <http://www.internetlivestats.com/internet-users/>.

[2] THOMAS, Thomas M. *Zabezpečení počítačových sítí: bez předchozích znalostí.* Brno: CP Books, 2005. Cisco systems. ISBN 80-251-0417-6.

[3] About Us. *About Hillstone Networks* [online] USA: Hillstone, 2017 [cit. 2017-10-24]. Dostupné z URL: <http://www.hillstonenet.com/about-us/>.

[4] Hillstone E-Series Next-Generation Firewalls: Comprehensive network security and advanced firewall features. *Hillstone Networks* [online] USA: Hillstone, 2017 [cit. 2017-11-27]. Dostupné z URL: <http://www.hillstonenet.com/our-products/next-gen-firewalls-e-series/>.

[5] SolutionBase: Strengthen network defenses by using a DMZ. *TechRepublic*[online]. USA: TechRepublic, 2005 [cit. 2017-10-20]. Dostupné z: <https://www.techrepublic.com/article/solutionbase-strengthen\-network-defenses-by-using-a-dmz/>.

[6] Stavíme firewall (3). *Root*[online]. Česká Republika: Root, 2002 [cit. 2017-10-21]. Dostupné z: <https://www.root.cz/clanky/stavime-firewall-3/>.

[7] KUGLER, Zdeňek. *Proxy firewall.* Brno, 2009. Diplomová práce. Vysoké učení technické v Brně. Vedoucí práce Ing. Radim Pust.

[8] Intro to Next Generation Firewalls. *ESecurity Planet*[online]. USA: eSecurity Planet, 2011 [cit. 2017-11-28]. Dostupné z: <https://www.esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html>.

[9] ANDERSON, Ross. *Security engineering: a guide to building dependable distributed systems.* Second edition. New York: Wiley Computer Publishing, 2001. ISBN 04-713-8922-6.

[10] Sypware. *TechTarget*[online]. United States: TechTarget, 2016 [cit. 2017-11-13]. Dostupné z: <http://searchsecurity.techtarget.com/definition/spyware>.

[11] ESET Services: Bezpečnostní audit. *ESET*[online]. Slovensko: ESET, 2017 [cit. 2017-11-14]. Dostupné z:
<https://www.eset.com/cz/firmy/eset-services/#c134947>.

[12] WEIDMAN, Georgia. *Penetration testing: a hands-on introduction to hacking.* First edition. San Francisco: No Starch Press, 2014. ISBN 978-1-59327-564-8.

[13] What is Kali Linux? *KALI*[online]. United States: Kali Linux, 2013 [cit. 2017-11-14]. Dostupné z:
<https://docs.kali.org/introduction/what-is-kali-linux>.

[14] Firewalk *KALI TOOLS*[online]. United States: Kali Linux, 2014 [cit. 2018-04-28]. Dostupné z:
<https://tools.kali.org/information-gathering/firewalk>.

[15] Nessus Professional *Nessus*[online]. United States: Tenable, 2018 [cit. 2018-3-31]. Dostupné z:
<https://www.tenable.com/products/nessus/nessus-professional>.

[16] Spirent Avalanche *Avalanche*[online]. United States: Spirent, 2018 [cit. 2018-3-31]. Dostupné z:
<https://www.spirent.com/Products/Avalanche>.

[17] Stresstesting. *Ibis Instruments*[online]. United States: Ibis Instruments, 2017 [cit. 2017-11-18]. Dostupné z:
<http://www.ibis-instruments.com/en/test---measurement/meterology-and-lab/stresstesting.htm>.

[18] CIGÁNEK, Josef. *Bezpečnostní analýza firewallu.* Brno, 2016. Bakalárska práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačných technológií, Ústav telekomunikácií. Vedoucí práce Doc. Ing. Jan Hajný, Ph.D.

ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK

ACK	Acknowledgement
ACL	Access Control List
ARP	Address Resolution Protocol
AV	Antivírus
BGP	Border Gateway Protocol
CAM	Content Addressable Memory
CISA	Certified Information System Auditor
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMZ	demilitarizovaná zóna
DNS	Domain Name System
FTP	File Transfer Protocol
FW	Firewall
GUI	Graphical User Interface
HIDS	Host-based Intrusion Detection System
HTTP	Hypertext Transfer Protocol
HW	Hardware
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
LAN	Local Area Network
MAC	Media Access Control
MB	Megabajt
NIDS	Network-based Intrusion Detection System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
QoS	Quality of Service
RIPv2	Routing Information Protocol version 2
SSH	Secure Shell
SSL	Secure Sockets Layer
SW	Software
SYN	Synchronize
TCP	Transmission Control Protocol
TTL	Time To Live
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol

ZOZNAM PRÍLOH

A PRÍLOHA

A.1 Základná konfigurácia firewallu Hillstone

```
configure terminal
interface ethernet0/0
zone  "mgt"
ip address 192.168.1.105 255.255.255.0
exit

interface ethernet0/1
zone  "untrust"
ip address dhcp
description "ISP"
reverse-route prefer
exit

interface ethernet0/2
zone  "trust"
ip address 192.168.2.1 255.255.255.0
description "LAN_office"
dhcp-server enable pool "ethernet0/2_addrpool"
exit

interface ethernet0/3
zone  "dmz"
ip address 192.168.3.1 255.255.255.0
description "DMZ_Hostia"
dhcp-server enable pool "ethernet0/3_addrpool"
exit

interface ethernet0/4
zone  "trust"
ip address 192.168.4.1 255.255.255.0
description "Avalan_Client"
exit
```

```
interface ethernet0/5
zone  "untrust"
ip address 192.168.5.1 255.255.255.0
description "Avalan_Server"
exit

interface xethernet2/0
zone  "trust"
ip address 192.168.10.1 255.255.255.0
description "Avalan_Gb_Client"
exit

interface xethernet2/1
zone  "untrust"
ip address 192.168.20.1 255.255.255.0
description "Avalan_Gb_Server"
exit

address "snat_IP"
ip 192.168.2.0/24
exit

address "DMZ_IP"
ip 192.168.3.0/24
exit

dhcp-server pool "ethernet0/2_addrpool"
netmask 255.255.255.0
gateway 192.168.2.1
address  192.168.2.100 192.168.2.200
dns 147.229.71.10  147.229.71.13
exit

dhcp-server pool "ethernet0/3_addrpool"
netmask 255.255.255.0
gateway 192.168.3.1
address  192.168.3.100 192.168.3.200
dns 147.229.71.10
exit
```

```
rule id 1
action permit
src-zone "trust"
dst-zone "untrust"
src-addr "Any"
dst-addr "Any"
service "Any"
exit
```

A.2 Konfigurácia prepínaču Mikrotik

1. Pripojíme sa do interface ether1-master.
2. Zapneme WinBox a v Neighbors vyberieme MAC adresu E4:8D:8C:6C:BC:DD.
3. Connect – Login: Admin, bez hesla
4. Záložka Interface → ether19-in → master port → none
   → ether20-out → master port → ether19-in
   → ether21-tap → master port → ether19-in
5. Záložka Switch → Mirror → Infress Mirror 0 To Port: ether21-tap
   → Ingress Mirror 1 To Port: switch1-cpu
   → Egress Mirror 1 To Port: switch1-cpu
   → Egress Mirror 0 To Port: ether21-tap
   → Egress Mirror Format: modified

B OBSAH PRILOŽENÉHO CD

- `/` ..... koreňový adresár priloženého CD
  - `Bakalárska práca` ..... adresár obsahujúci bakalársku prácu
    - `Sasko_Dominik_bakalárska_práca.pdf`
  - `Konfigurácia Hillstone` ..... kompletná konfigurácia firewallu Hillstone
    - `Hillstone_config.DAT` ..... exportovaná konfigurácia s GUI
    - `Hillstone_config.txt` ..... konfigurácia v textovom dokumente
  - `Nessus skeny` ..... výsledky testovania pomocou Nessusu
    - `Host_Discovery_Scan.pdf`
    - `Network_Vulnerability_NoProtection.pdf`
    - `Port_Discovery_Scan.pdf`
  - `Odpočúvanie premávky` ... súbory s odchytenou premávkou pomocou Wiresharku
    - `premavka_hillstone_den.pcapng`
    - `premavka_hillstone_noc.pcapng`
  - `Testy Spirent Avalanche` ..... výsledky výkonnostného testovania
    - `FTP_1_no_protection.rar` ..... testovanie s FTP serverom bez IPS a antivíru
    - `FTP_2_IPS.rar` ..... testovanie s FTP serverom s IPS
    - `FTP_3_AV.rar` ..... testovanie s FTP serverom s antivírom
    - `FTP_4_AV_IPS.rar` ..... testovanie s FTP serverom s IPS a anitivírom
    - `HTTP_test_50.rar` ..... testovanie s HTTP serverom s 50 klientmi
    - `HTTP_test_1000.rar` ..... testovanie s HTTP serverom s 1000 klientmi