VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2017 Pavol Varmus

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

ZABEZPEČENÍ SÍTĚ POMOCÍ VIRTUÁLNÍCH FIREWALLŮ NOVÉ GENERACE
SECURE NETWORK BASED ON VIRTUAL NEXT-GENERATION FIREWALL

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Pavol Varmus**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Lukáš Malina, Ph.D.**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Pavol Varmus ***ID:*** 173775
Ročník: 3 ***Akademický rok:*** 2016/17

NÁZEV TÉMATU:

Zabezpečení sítě pomocí virtuálních firewallů nové generace

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s firewally nové generace a s funkčností virtuálního firewallu. Dílčím cílem práce je navrhnout zabezpečení malé až střední sítě pomocí firewallů nové generace (FWng). Dalším cílem bude návrh zabezpečení nakonfigurovat na FWng. Hlavním cílem práce je konfigurace a experimentální ověření řešení FWng a návrh laboratorní úlohy na základní konfiguraci FWng.

DOPORUČENÁ LITERATURA:

[1] Pfleeger, Charles P., and Shari Lawrence Pfleeger. Analyzing computer security: A threat/vulnerability/countermeasure approach. Prentice Hall Professional, 2012.

[2] Hogg, Scott and Vyncke, Eric. IPv6 Security, 2009.

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

Vedoucí práce: Ing. Lukáš Malina, Ph.D.
Konzultant:

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

ABSTRAKT

Cieľom bakalárskej práce je preštudovať problematiku zabezpečenia sietí pomocou firewallov, zhodnotiť vlastnosti jednotlivých typov firewallov a následne ich zdokumentovať. Ďalším z cieľov je návrh zabezpečenia malej až stredne veľkej siete, s následným popisom optimálneho zabezpečenie. Hlavným výstupom bakalárskej práce je návrh zapojenia laboratórnej úlohy, s popisom jednotlivých krokov a ich následným odskúšaním. V tejto úlohe má študent za cieľ pochopiť dôležitosť využitia ochranných sieťových prvkov v podobe firewallov a vyskúšať si rôzne druhy ochrán na danej sieti. Úloha je zakončená experimentálnym overením odolnosti firewallu voči sieťovému útoku.

KĽÚČOVÉ SLOVÁ

Firewall, Nová generácia, Sieť, Návrh, Laboratórna úloha, Bezpečnosť, Zabezpečenie, Ochrana, Filtrácia, Hillstone, VMWare, Sieťový Útok, Fortigate, DoS

ABSTRACT

The bachelors thesis aims to study the issue of security of the networks that use firewalls. The next goal is to evaluate the characteristics of a different types of firewalls and to summarize its results. The other object is to design a small or medium sized network with description of best practice. The main objective of the thesis is to design a lecture task for students to test with a step-by-step solution. This task is for students to undertand the importance of firewalls as a network protection service tools and to try out different types of filters for maintainin network security. The task ends with a practical stress test made by a network attack in order to see its resistance to the attack.

KEYWORDS

Firewall, Next generation, Network, Design, Lecture task, Security, Protection, Filtration, Network Attack, Hillstone, VMWare, Fortigate, DoS

VARMUS, Pavol *Zabezpečení sítě pomocí virtuálních firewallů nové generace.*: semestrálny projekt. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2017. 80 s. Vedúci práce bol Ing. Lukáš Malina, Ph.D.

VYHLÁSENIE

Vyhlasujem, že som svoj semestrálny projekt na tému „Zabezpečení sítě pomocí virtuálních firewallů nové generace.“ vypracoval(a) samostatne pod vedením vedúceho semestrálneho projektu, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor(ka) uvedeného semestrálneho projektu ďalej vyhlasujem, že v súvislosti s vytvorením tohoto semestrálneho projektu som neporušil(a) autorské práva tretích osôb, najmä som nezasiahol(-la) nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý(-á) 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(-ky)

POĎAKOVANIE

Rád by som sa poďakoval môjmu vedúcemu semestrálnej práce pánovi Ing. Lukášovi Malinovi, Ph.D. za odborné vedenie, konzultácie, trpezlivosť a cenné rady k práci, ako aj sprostredkovanie komunikácie s firmou Hillstone a zasielanie podkladov. Zároveň by som chcel poďakovať firme Hillstone, ktorá tieto materiály poskytla, spolu s vybavením pre túto prácu.

Brno . . . . . .

. . . . . .

podpis autora(-ky)

OBSAH

ZOZNAM OBRÁZKOV

ÚVOD

Bezpečnosť mala vždy jednu z najvyšších priorít pri sprostredkovaní pripojenia na infraštruktúru informačných sietí a je to tak aj v prípade tých virtuálnych.

Užívateľia aj firmy spoliehajú na diskrétnosť prenosu ich dát a nízku zraniteľnosť ich sieťových pripojení. Preto sa chránia rôznymi antivírovými programami, alebo sieťovými prvkami s možnosťou kontroly toku, zamädzenia útoku, prípadne jeho prevencii. Jedným z ochranných prvkov využívaným na pomyselnej bojovej línii je firewall, ktorý si našiel svoje miesto aj medzi virtuálnymi systémami.

Rýchlosť vývoja virtuálnych sietí a protokolu IPv6 spôsobila rozmach v oblasti ich zabezpečenia, kedy na scénu prichádzajú po fyzických firewalloch virtuálne a následne virtuálne firewally novej generácie.

Táto práca sa venuje zabezpečeniu virtuálnych a fyzických sietí pomocou firewallov novej generácie a popisom využitia virtuálnych firewallov novej generácie. Dôraz je kladený na firewally značky Hillstone, ktorých vlastnosti budú testované a porovnávané v jednotlivých častiach tejto práce.

Práca je rozdelená do siedmich kapitol. Prvá kapitola vyobrazuje využitie firewallov v oblasti bezpečnosti sietí. Ďalej popisuje jednotlivé spôsoby ochrany, ale aj typy útokov. Druhá kapitola je zameraná na porovnanie fyzických a virtuálnych firewallov. Tretia kapitola má za cieľ vysvetliť konkrétne funkcie a vlastnosti virtuálneho firewallu. V štvrtej kapitole je kladený dôraz na firewall Hillstone CloudEdge a jeho popis. V piatej kapitole je stručné predstavenie virtualizačného programu VMWare a otestovanie samotného zapojenia na virtuálnej sieti skonštruovanej pre účely predvedenia funkcií. V šiestej kapitole sa nachádza návrh zabezpečenia malej až strednej siete spolu s radami pre zabezpečenie siete. V poslednej kapitole je rozpísaný návrh laboratórnej úlohy, zameraný na zabezpečenie siete pomocou firewallu Hillstone a jeho nasledovné otestovanie.

1 FIREWALL A ZABEZPEČENIE SIETE

Prvá časť je zameraná na obecnú bezpečnosť sietí, jej vývoj a rôzne útoky, ktoré môžu nastať. Ďalej je vyobrazené, ako môže firewall zabrániť jednotlivým pokusom o pripojenie, prípadne útokom po sieti. Následne je uvedené vyobrazenie firewallov a predstavenie ich vlastností z hľadiska využitia jednotlivých firewallov ako aktívnych bezpečnostných prvkov, po implementácií do jednotlivých sietí.

1.1 Využitie firewallov

Firewall je zariadenie so špecifickou funkciou v oblasti bezpečnosti, využíva sa na kontrolu a riadenie sieťového toku. Vlastnosťou firewallu je zamedzenie alebo povolenie priechodu dátam s určitou vlastnosťou, stanovenou v podobe pravidiel. Tieto pravidlá si určuje správca na základe požiadaviek, pričom sú delené na rôzne úrovne. Využíva sa ako kontrolný prvok medzi internou sieťou a internetom, prípadne ako prvok na podsieti, filtrujúci danú komunikáciu na základe stanovenej ochrannej úrovne.

1.2 Druhy firewallov

Existujú rôzne druhy firewallov, ktorých základnými vlastnosťami sú:

- **paketový filter** – alebo aj premietací smerovač (screening router). Funguje na princípe Access Control List (ACL) a prepúšťa len pakety, ktoré majú v hlavičke informácie spĺňajúce pravidlá filtru.
- **stavový firewall** – obdoba paketového filtru. Prepúšťa len konkrétne pakety, povolené v rámci spojenia.
- **aplikačný proxy** – filtrácia je možná napríklad samotnými údajmi zo stránok, alebo aj na základe jej Uniform Resource Locator (URL).
- **circuit-level gateway**– voľným prekladom okružno-úrovňová brána. Jedná sa o firewall, ktorý povoľuje, aby bola jedna sieť rozšírením tej druhej.
- **ochranca (guard)** – podobne ako proxy povoľuje pripojenie na základe nadobudnutých informácií, o ich povolení však rozhoduje sám prepočtami a spoľahlivými znalosťami o identite vonkajšieho užívateľa spolu s predchádzajúcimi komunikáciami.
- **osobný firewall** – priamy kontakt s koncovou stanicou s najväčšou možnosťou filtrovania, príkladom je Windows Firewall a ďalšie.

1.2.1 Paketový filter

Najstarší a v minulosti najvyužívanejší firewall, ktorého využitie sa nájde aj v dnešnej dobe v praktickom sieťovom zapojení. Ochrana pred sieťovým útokom prebieha tak, že vďaka prednastaveným adresám a portom, ktoré sa nachádzajú na zozname s povoleným vstupom, povoľuje, alebo zakazuje priechod sieťového toku, čím aktívne pomáha k ochrane proti útokom.

Táto kontrola využíva formu takzvaného ACL, pričom porovnáva hlavičku paketu, ktorá je nositeľom informácií o prenose. V nej porovná informácie so zadaným listom hodnôt, ktoré majú povolenie na prechod týmto filtrom. Jedná sa o informácie podliehajúce danému pravidlu, na ktorý port a adresu má ktorá adresa a port povolené komunikovať. Táto kontrola prebieha na tretej a štvrtej vrstve. Nevýhodou je nedostatočná kontrola, presnosť a len povrchná analýza paketov, bez ďalších operácií. To znamená, že paketový filter dokáže zabrániť nežiadúcej komunikácií, avšak nedokáže zabrániť útoku, ktorý by mohol prejsť cez adresu spadajúcu do tých, ktoré sú v ACL vedené ako povolené. [1]

1.2.2 Stavový firewall

Niekedy nazývaný aj stavový paketový filter. Ich funkčnosť vychádza zo základných paketových filtrov, avšak s možnosťou ukladania logov predchádzajúcich spojení, ktoré boli povolené alebo zakázané. Z tejto vlastnosti neskôr vychádza, aby mohol pri opätovnej komunikácií z takejto adresy konať úkon zamietnutia, alebo povolenia komunikácie rýchlejšie. V prípade, že sa tak v minulosti nestalo, paket musí byť najskôr skontrolovaný, potom budú informácie o prenose ako zdrojová a cielová IP adresa a porty priradené do logu, vyhodnocujúcom jeho budúcu komunikáciu a následne poslaný v sieti ďalej, prípadne zamietnutý a potom zahodený. Ďalšou z výhod, okrem zvýšenej rýchlosti spracovania údajov, je aj úroveň zabezpečenia.

Najnovšie stavové paketové filtre umožňujú ukladanie stavov spojení spolu s možnosťou hĺbkovej kontroly, ktorá prináša funkciu Intrusion Detection System (IDS). Úlohou IDS je vyhľadávať a analyzovať útoky, alebo im preventívne zabrániť, vďaka online databáze, z ktorej čerpá najčastejšie vzory útokov. V prípade nesprávnej konfigurácie sa však môže stať, že správa môže byť chybne vyhodnotená ako hrozba. [1]

1.2.3 Aplikačný proxy

Nazývaný aj Aplikačná brána simuluje efekty aplikácií, čím preberá dočasne úlohu klienta a tým zabezpečuje komunikáciu medzi klientom a serverom. V tomto zapojení

sa proxy brána (proxy gateway) javí ako prostredník medzi klientom a serverom, ktorých komunikáciu sprostredkováva a posudzuje.

V prípade využitia aplikačnej brány ako proxy serveru, možno filtrovať dané pripojenia na základe zasielaných údajov. To znamená, že užívateľ má možnosť filtrovať konkrétny obsah stránky, ich prehliadanie, alebo úplné zakázanie prístupu na ne. Kontroly prebiehajú na aplikačnej vrstve, pričom výhodou je vysoká variabilita zabezpečenia. Nevýhodou sú nároky na výkon, s tým spojené aj vyššie náklady, znižovanie prenosovej rýchlosti kvôli oneskoreniam a náročnosť konfigurácie. [1]

1.2.4 Circuit-level gateway

Tento firewall, pracujúci na relačnej vrstve (layer 5), funguje ako virtuálna brána medzi dvoma sieťami, pričom jedna sieť býva rozšírením tej druhej. Okruh je dočasné logické pripojenie, ktoré je testované len pri jeho vytvorení, vtedy môžu byť stanovené limity na to, aké spojenie môže byť vytvorené. Využitie tejto brány je napríklad na implementáciu Virtual Private Network (VPN). Pre zabezpečenia privátnej komunikácie je v rámci sietí nainštalované šifrovacie zariadenie. Do neho táto brána presmeruje všetku komunikáciu, smerovanú na druhú sieť. Toto zariadenie zašifruje komunikáciu prichádzajúcu z jednej siete a v druhej sieti rovnako vybavené zariadenie vykoná dešifrovanie. [1]

1.2.5 Ochranca (guard)

Podobne ako proxy firewall aj tento dostáva dátové jednotky, vyhodnotí ich a pošle rovnaké, alebo odlišné protokolové dátové jednotky. Ochranca rozhodne, ktoré úkony môžu byť vykonané v mene užívateľa, vzhľadom na ním nabodubnuté informácie, s ohľadom na spoľahlivosť užívateľovej identity, predchádzajúcu komunikáciu a podobne. Stupeň kontroly sprostredkovaný ochrancom je limitovaný len na to, čo je prepočítateľné. Avšak rozdiel medzi proxy a ochrancom je častokrát minimálny, hlavným znakom je to, že bezpečnostné opatrenia (zásady) implementované ochrancom sú komplexnejšie, ako tie implementované pomocou proxy firewallu. To však znamená že kvôli komplexnejšiemu kódovaniu je ochranca zranitelnejší a viac vystavený chybám. [1]

1.2.6 Osobný firewall

Jedná sa o firewall, ktorého vlastnosti reprezentuje zväčša softwarový program, nainštalovaný na koncovej stanici. Jeho priamy kontakt umožňuje najviac možností kontroly a zabezpečenia, na vrstvách 2 až 7. Osobný firewall môže vykonávať činnosť bežného firewallu tým, že premieta dáta, ktoré jediná stanica prijíma. Rovnako ako klasický firewall kontroluje prichádzajúci a odchádzajúci tok na sieti, osobný firewall kotroluje tok na jedinej stanici. Užívateľ si môže sám nakonfigurovať, na ktoré stanice, prípadne stránky môže mať prístup a ktoré môžu mať prístup na neho. Napríklad Windows Firewall disponuje prednastavenými vlastnosťami a vlastným black listom stránok, na ktoré je už od inštalácie zakázané pristupovať. Zároveň si osobný firewall vedie záznamy, ktoré ukladá do logov. Najoptimálnejšou ochranou je kombinácia osobného firewallu s antivírovým programom. Niektoré antivírové programy disponujú niektorými vlastnosťami osobným firewallov a nesprávnou kombináciou firewallu a antivíru, prípadne dvoch antivírov vzájomne, môže nastať konflikt záujmov a tým pádom sa stane ochrana neefektívnou. [1]

1.2.7 Zhrnutie jednotlivých vlastností

V prílohe A.1, obsahujúcej tabuľku, je vyobrazené porovnanie vlastností a funkcií jednotlivých firewallov spomínaných v predchádzajúcich častiach prvej kapitoly. Jedná sa o vlastnosti firewallov typu – Paketový Filter, Stavový Firewall, Aplikaćný Proxy, Okružná Brána (Circuit Gateway), Ochranca (Guard) a Osobný Firewall.

1.3 Spôsob ochrany

Hlavnou činnosťou firewallu je kontrola prístupu a jeho následné riadenie z dôvodu zakázania prístupu nežiadúcich zdrojov. Túto činnosť firewall vykonáva filtráciou údajov na základe jednotlivých vlastností, ktorých niektoré príklady boli spomenuté v predchádzajúcej časti zahŕňajúcej využitie firewallov. Táto časť sa zaoberá podrobnejšie spôsobom, akým firewall zamedzuje prístup a pomáha k zabezpečeniu komunikácie po sieti, do ktorej je umiestnený.

Za účelmi kontroly prístupu majú firewally v rámci svojho aplikačného rozhrania možnosť zahrnúť takzvané bezpečnostné zásady (security policy). Zásady sú súborom pravidiel a obmedzení nastavených administrátorom, užívateľom alebo samotným firewallom. Ich funkciou je popis nežiadúcich prístupov, alebo útokov, ktoré by mohli nastať za účelom ich filtrovania. V prípade zásad záleží vždy na uvážení užívateľa/administrátora, pred akými útokmi sa chce brániť (prípadne aké útoky

možno očakávať) a aký typ datového toku, spolu s jeho smerom, by chcel zakázať. V rámci zásad prebieha okrem filtrácie aj možnosť sledovania dát a vyhodnocovania hrozieb, na ktoré môže byť neskôr aplikovaný filter. Takáto jednoduchá filtrácia môže byť nastolená napríklad zakázaním konkrétneho portu, čo by malo za následok úplné zamietnutie prístupu sieťového toku z alebo do daného portu.
Ďalším príkladom zásady je napríklad filtrácia paketov, ktorá je zároveň jednou z najbežnejších a najstarších. Pri nej dochádza ku kontrole hlavičky paketu, tá určí jeho zdroj a cieľ. Následne ho porovná s ACL, ten predstavuje list povolených prístupov, na základe ktorého je porovnávaná príchodzia komunikácia.

Zásady hrajú rolu aj v prípade uvažovania, ktorým sa komunita, ktorá sa zaoberá bezpečnosťou sietí, rozdeľuje na dve skupiny. Jedná sa o rozdielne názory v spôsobe nastavenia takzvaného prednastaveného prístupu (default access).
Jedna skupina zastáva názor *„čo nie je explicitne zakázané, to je povolené“*, čo znamená, že štandardne je prístup povolený (default permit).
Druhá skupina zastáva názor *„čo nie je explicitne povolené, to je zakázané“*, čo znamená že štandardne je prístup zakázaný (default deny) [1].

1.4 Najčastejšie útoky

Pri útokoch na zabezpečenú sieť, server, alebo koncovú stanicu možno rozlíšiť spôsoby útoku na rôzne kategórie, ako aj ich účel a pôvod útoku. Problémy pri ochrane pred danými útokmi sú, že firewall nie je schopný sám vyfiltrovať, prípadne zabrániť všetkým útokom, ktoré by sa mohli vyskytnúť. Jeho spoľahlivosť závisí na umiestnení, správnej konfigurácii a zároveň aj na výbere optimálneho typu firewallu. Čomu však väčšina firewallov nemôže zabrániť, to sú takzvané útoky z vnútra. A síce, ak by sa útok odohral v rámci siete, prípadne by bol smerovaný ako vírus prenesený cez prenosné médium priamo na prístroj (napríklad cez USB/CD). Na ochranu voči takýmto útokom sa špecializujú okrem firewallov spomínaných v kapitole 2.2 aj antivírové programy.

Vzhľadom na veľkú variabilitu útokov budú v nadchádzajúcom zozname spomenuté len tie najbežnejšie, so základným popisom ich konania:

Denial-of-Service (DoS) – najbežnejšia forma útoku po sieti, ktorej účel je zamedzenie prístupu, alebo vyradenie prístroja na určitý čas. Využíva zraniteľnosť siete, prípadne serveru/koncovej stanice z hľadiska ich maximálnych kapacít (pre sieť je príznačné jej zahltenie routru požiadavkami, ktoré základné Quality of Service (QOS) nedokáže odfiltrovať v dostatočnej miere), hardwarovej

predispozície a výkonu. Jedná sa o útok, spôsobený napríklad hromadným pripojením veľkého množstva počítačov na server. Server je následne preťažený nárazovo veľkým množstvom požiadaviek, čo znamená jeho neschopnosť ich vyplňovať. Obdobou tohoto útoku je distributed denial-of-service (DDoS). Táto forma útoku je častokrát vykonávaná po únose (hijack) počítača (pričom vlastník/obsluha tohto stroja, o tom často ani nemusí vedieť) a jeho následným využitím na distribuovaný útok (napríklad paket-flow na určitú destináciu).

Vírusy a škodlivé programy – formy softwarového napadnutia. V prípade, ak majú pôvod v programe, tak sú aj jednoducho prenositeľné. Softwarové firewally sú voči nim častokrát neúčinné a vyžadujú si byť kontrolované na to špecifikovanými antivírovými programami. Medzi najznámejšie škodlivé programy patria vírusy, červy (worms) a trójske kone (trojan horses).

Man-in-the-Middle (MITM) – v preklade človek medzi. Táto forma útoku prebieha narušením skutočného spojenia medzi dvoma počítačmi a jeho následným únosom. To znamená že užívateľ ktorý sa pripojí na server posiela dáta, ktoré spočiatku server prijíma, MITM však spôsobí to, že medzi toto pripojenie vstúpi tretia strana (prostredník), na ktorú užívateľ posiela dáta, ktoré by normálne smerovali na server. Útočník ich tým pádom môže zneužiť, upraviť, zmazať, alebo kompletne nahradiť, čo by malo za výsledok, že server by dáta, ktoré mu boli doručené, rozpoznal ako užívateľove, pritom by však boli útočníkove.

Napodobenie (impersonation) – touto formou si útočník získa údaje tak, že napríklad vytvorí web stránku, ktorá sa tvári ako cudzia legitímna stránka. Na ňu sa užívatelia pripoja a ponechajú tam svoje údaje. Tohoto sa dosiahne napríklad presmerovaním užívateľa vďaka zmene informácií na DNS servery, alebo priamym otvorením odkazu na túto stránku.

Odpočúvanie – narušenie dátového toku za účelom získania údajov. Sieťové protokoly, ktoré používajú prenos čistého textu, ako napríklad File Transfer Protocol (FTP), sú najjednoduchšie na odpočúvanie. Odpočúvať možno prakticky na každej verejnej sieti, ktorej komunikácia nie je šifrovaná, alebo iným spôsobom chránená. Odpočúvať v rámci siete možno však len interne, čo znamená, že útočník by musel mať fyzický prístup k sieti, alebo by musel na prístroj pripojený do takejto siete preniesť škodlivý software, ktorý by túto činnosť umožnil. V prípade pripojenia na internet však možno odpočúvať na celej

trase od užívateľa k cieľovej stanici.

Ostatné útoky – väčšinou sa jedná o útoky s pôvodom v bezpečnostných nedokonalostiach, za ktoré môže výrobca, alebo napadnutý vlastnou nepripravenosťou. Patria medzi ne:

1. Útoky, ktoré prebehnú vďaka nedostatočnému zabezpečeniu – útočník poznal heslo na prístup, ktoré sa buď nejakým spôsobom dozvedel, prípadne patrilo medzi štatisticky najvyužívanejšie heslá a teda jednoducho uhádnuteľné, alebo bolo absentujúce, prípadne bolo prelomené (vtedy je však na mieste zvážiť komplexnosť hesla a jeho šifrovania, alebo prejsť na vyšší stupeň ochrany).
2. Zraniteľnosť, kvôli ponechaniu pôvodnej konfigurácie systému. Mnohé systémy bývajú vystavené riziku len kvôli tomu, že neboli prekonfigurované z továrenských nastavení, prípadne z verejne známej pôvodnej konfigurácie (default configuration).
3. Prelomenie systému na základe chyby (bug). Chyby, ktoré vznikli pri vývoji softwaru alebo hardwaru a boli ponechané, či už zámerne, alebo nie, aj po jeho dodaní zákazníkovi. Môžu byť využité k priamemu pripojeniu na stroj obsahujúci túto chybu, alebo k prelomeniu zabezpečovacieho systému. Takéto chyby sa označujú ako bezpečnostné diery a v prípade softwarových firewallov sú pravideľne opravované a vylepšované pravideľnými aktualizáciami.
4. Útok za použitia programu využívajúceho funkciu prieniku Backdoor (zadné vrátka), prenášaného pomocou škodlivého softwaru (napr. trójskeho koňa), vďaka ktorému sa útočník pripojí do systému bez bezpečnostnej autorizácie. Takáto forma útoku býva často spojená aj s už definovanými pôvodnými konfiguráciami, alebo chybami. Jedná sa o útok využívajúci napríklad výrobcami skryté účty s vysokou úrovňou privilégií. V prípade ponechania pôvodnej konfigurácie sa môže jednať o pripojenie na administrátorský účet, definovaný výrobcom (prihlasovacie meno/heslo: admin/admin).

A mnoho ďalších využívajúcich nedokonalostí systémov, zabezpečenia, ale aj nedostatočného dosahu firewallov na zabezpečenie v rámci siete. [2]

1.5 Demilitarizovaná zóna

Demilitarizovaná zóna (DMZ) je zóna, ktorá vznikne, ak je firewall nakonfigurovaný tak, aby rozdelil sieť na viacero sieťových segmentov (zón). Tieto zóny sprostredkovávajú zabezpečenie systému, ktorý sa v nich nachádza, s rozdielnou úrovňou zabezpečenia a rozdielnymi zásadami mendzi nimi. Zo zariadení z internej a externej siete je možno komunikovať s tými, nachádzajúcimi sa v DMZ. Avšak zariadenia, ktoré sa nachádzajú v DMZ majú možnosť spojenia len s tými z externej siete. Z tohoto dôvodu sa využívajú napríklad ako miesto, kde sídli web server. V prípade spoločností je využitá DMZ na spôsob pripojenia zákazníka z externej siete, do DMZ (zamedzí sa tak priamemu konktaktu s tou internou).

Zo zapojenia s použitím DMZ vyplývajú aj bezpečnostné výhody, ktorých opodstatnenie vychádza z faktu, že v prípade útoku na systém, nachádzajúci sa v tejto zóne, prichádza útočník o možnosť rozvinúť svoj útok ďalej na tú internú. Tomuto útoku sa dá zamedziť vďaka tomu, že v prípade použitia DMZ ako ochrannej hranice pre privátnu sieť, je možné nakonfigurovať firewall, aby zakázal všetky pokusy o prístup na internú sieť. To znamená, že útočník je obmedzený len na útok na systémy, nachádzajúce sa v DMZ a nie sú dodatkovo chránené iným firewallom.

Častým spôsobom zvyšovania zabezpečenia siete pomocou DMZ býva doplnkový firewall, ktorý sa nachádza za firewallom oddeľujúcim DMZ od internej siete. Jeho umiestnenie je sporadicky DMZ, za ňou je zasadený DMZ firewall (ktorý vlastne samotné DMZ vytvára) a až za ním sa nachádza tento firewall. Tento firewall je potom predsadený pred internú sieť, ktorú chráni pred možným útokom zo strany DMZ firewallu, ktorý by útočník mohol prekonať. [3]

Medzi ďalšie výhody, ktoré pochádzajú z využitia zapojenia za pomoci DMZ patria:

- Zvýšená kontrola sieťového toku. To je zapríčinené tým, že všetky dáta, ktoré prichádzajú do DMZ sú skontrolované. Po kontrole firewall rozhodne, či môžu byť zaslané do DMZ, prípadne ju opustiť. Neobvyklým prípadom je aj možnosť, že ak to zásady filtrujúce dátový tok umožňujú, prejdú dáta z DMZ smerom na firewall chrániaci internú sieť. Tam podliehajú ďalšej kontrole.
- Samotné zabezpečenie systémov nachádzajúcich sa v DMZ. Jednotlivé zariadenia sú chránené pred útokmi tak, že DMZ kontroluje sieť pred potenciálnymi útočníkmi, ako aj zariadania ako také, ležiace v DMZ.

Využitia DMZ sú rôzne z hľadiska ich vlastností, spôsobov, zapojenia, ale aj samotnej ochrany. Ich využitie však často vyžaduje vynaloženie väčšieho množstva finančných prostriedkov, preto je dôležité dbať na to, či je ich využitie v rámci konkrétnej siete opodstatnené.

1.5.1 Druhy DMZ

DMZ s jedným firewallom: Jednou z požiadaviek na to, aby mohol byť tento firewall použitý je to, že firewall musí podporovať 3 a viac rozhraní. Výhodou je jednoduchšia konfigurovateľnosť, nižšie nároky na náklady a údržbu, ako aj jednoduchšia správa pre administrátorov. Jedná sa o DMZ s nižšou úrovňou zabezpečenia proti útokom v porovnaní s DMZ s viacerými firewallmi. Využíva sa väčšinou na riadenie toku z Internetu do DMZ, pričom jediným bodom ochrany je len jeden firewall.

DMZ s viacerými firewallmi: Možnosť použitia DMZ s viacerými firewallmi prináša aj lepšie zasadenie DMZ v rámci siete. Toto fyzické zasadenie viacerých firewallov vytvorí zónu medzi súkromnou sieťou a Internetom. Tým sa zvýšia možnosti zabezpečenia a kontroly, čo napomáha k zvýšeniu ochrany.

K zvýšeniu zabezpečenia možno ešte prispieť využitím odlišných firewallov od rôznych výrobcov. To spôsobí, že útočník bude musieť použiť odlišné metódy útoku. Ďalšou z výhod je odľahčenie toku prechádzajúceho firewallmi. Nevýhody tohto zapojenia sú zvýšené náklady, zložitosť konfigurácie a správy. [2]

2 POROVNANIE FIREWALLOV

Pomyselne možno rozdeliť firewally na dve skupiny v závislosti na ich naviazanosť na hardware. Z tohoto dôvodu možno predpokladať, že jedna skupina má hardware určený výhradne na účely slúžiace firewallu. Tá druhá skupina je charakteristická svojou nezávislosťou v rámci využitia daného stroja.

Výber firewallu závisí od viacerých faktorov, medzi tie najdôležitejšie patria:

- charakter siete – Či jedná sa o fyzické zapojenie alebo virtuálne.
- potenciál využitia – Ak sa jedná len o ochranu osobného zariadenia pre konkrétneho užívateľa, využíva sa softwarový firewall.
- veľkosť siete – Tá zväčšia priamo úmerne ovplyvňuje množstvo firewallov.
- architektúra siete – Čím vyššie nároky na filtráciu medzi vonkajšou a vnútornou sieťou, alebo len v rámci vnútornej siete, tým viac firewallov potreba.

2.1 Fyzický firewall

Firewall, ktorý je fyzicky vložený do sieťovej infraštruktúry. Spôsob ochrany nie je zameraný na zabezpečenie konkrétneho prístroja, ale na všetky prvky, ktoré sú v sieťovej infraštrukúre zapojené za firewallom. To zároveň zvyšuje dôležitosť umiestnenia daného prvku v sieti. Keďže firewall oddeľuje vnútornú zabezpečenú sieť od tej vonkajšej a nezabezpečenej, prikladá sa dôraz na sieťové usporiadanie a architektúru tej danej siete, ktorá má byť neskôr fyzickým firewallom zabezpečená.

Princíp ochrany fyzickým firewallom spočíva zväčša v tom, že na základe jednoducho nakonfigurovaných pravidiel a zásad rozhodujú, či paket zahodia, alebo pošlú ďalej, smerom k adresátovi. Tým sa usmerňuje daná komunikácia medzi užívateľom vo vnútri siete a vonkajším prostredím (napríklad iným užívateľom mimo tejto siete). Ak je však firewall zapojený tak, aby filtroval komunikáciu vo vnútri siete, môže tak robiť aj medzi jednotlivými stanicami do nej spadajúcej.

2.2 Softwarový firewall

Jedná sa o firewally, ktoré sú či už priamo inštalované v prístroji, naviazané na aplikačnú sféru konkrétneho operačného prístroja, alebo slúžia len ako dodatková sieťová ochrana.

Hlavným rozlišovacím znakom v porovnaní s fyzickými je, že stroj nezastáva jediný účel, ale môže slúžiť viacerým úkonom popri tom, ako je na ňom firewall spustený. Ďalšou charakteristickou vlastnosťou je spätosť so strojom. Možnosť priamej

kontroly je tým pádom oveľa jednoduchšia a forma administrátorských obmedzení vo firmách využívaných prípadným zakázaním prístupu na konkrétne webové portály, je možná hromadne a na diaľku, s nastavením konkrétnych zásad a právomocí len na určité skupiny ľudí, bez nutnosti zásahu do okolitých prvkov napojených na sieťovú infraštruktúru, ktorých sa dané obmedzenie netýka.

Jednoduchosť nastavenia často ocenia domáci užívatelia, pre ktorých je napríklad Windows Firewall, v rámci operačného programu Microsoft Windows, automatickou ochrannou pomôckou. Z tohoto hľadiska sa jedná zväčša o takzvané stand-alone aplikácie (samostatne pracujúce), s účelom ochrany na viacerých sieťových vrstách spolu s možnosťou vnútornej ochrany v rámci počítača – antivírové programy, ktoré prichádzajú s podobnými inováciami a prinášajú možnosť chrániť počítač, popri aktívnej sieťovej ochrane. Dôvod ich častého uprednostňovania je ten, že okrem ochrany voči prichádzajúcej a odchádzajúcej komunikácii v sieti, softwarový firewall môže ochraňovať aj voči vírusom ako je napríklad Trojan, Worm ...

Charakteristickou vlastnosťou spoľahlivého softwarového firewallu je, že beží na pozadí a podieľa sa len minimálne na využití výkonu počítača. Firewall software je často aktualizovaný, aby mal aktuálny prístup k databáze na porovnávanie najnovších možných útokov a mohol im efektívne zabrániť. [4]

Do skupiny softwarových firewallov patria napríklad už spomínané aplikačné, osobné a v dnešnej dobe čoraz viac využívané virtuálne firewally. Virtuálne firewally začali byť vo väčšom merítku používané kvôli smeru, akým sa začal vývoj sieťových infraštruktúr orientovať. Virtuálne servery, klienti a prepojenie na cloudy zvýšili atraktívnosť virtuálnych sietí pre útočníkov, zaujímajúcich sa o získanie dát, alebo spôsobenie škody.
Do virtuálnej siete sa dostávajú informácie z fyzicky napojenej dátovej siete, ktorá býva chránená vlastnými prvkami, preto je dobré chrániť aj prvky virtuálne. Spôsob aplikácie takéhoto firewallu býva zväčša sekundovaný fyzickým firewallom, pre zvýšenie zabezpečenia. Ten býva napojený buď na najbližšiu možnú fyzickú stanicu alebo pred samotné servery, ktoré takéto virtuálne procesy hostujú.

3 VIRTUÁLNY FIREWALL

Virtuálne firewally predstavovali bezpečnostnú záplatu, ktorá vznikla pri presadzovaní virtuálnych sietí. Avšak táto záplata sa zmenila v plnohodnotný ochranný sieťový prvok. Jedná sa o firewall, fungujúci na virtuálnom rozhraní (niekedy aj so špeciálne prispôsobeným užívateľským rozhraním), ktorý kontroluje komunikáciu medzi virtuálnymi strojmi, často na sieti, ktorá je tiež virtuálna. Funguje na rovnakom princípe ako obyčajný firewall, kontrola paketov za využitia bezpečnostných zásad so zámerom blokovania nepovolenej komunikácie medzi jednotlivými virtuálnymi strojmi.
Virtuálny firewall môže najčastejšie fungovať v dvoch možných režimoch a to:

- premosťovací režim (bridge-mode) – Správa sa ako fyzický firewall, zároveň musí byť rovnako umiestnený (napríklad medzi sieťovými rozhraniami). Negatívum môže byť, že keď sa firewall v tomto režime nainštaluje, stane sa sám o sebe virtuálnym strojom.
- hypervízny režim (hypervisor-mode) – V tomto režime firewall nie je súčasťou virtuálnej siete, ale je súčasťou takzvaného virtual machine monitor (VMM), ktorý kontroluje správanie virtuálneho stroja. To, že nie je priamou súčasťou virtuálnej siete, prináša nevýhodu v obmedzených možnostiach prístupu [5].

3.1 Výhody a nevýhody virtuálnych firewallov

Pri úvahách nad aplikáciou virtuálneho firewallu si často kladú záujemcovia otázku, či daný virtuálny stroj dokáže plnohodnotne nahradiť ten fyzický. Odpoveďou však je, že nedokáže nahradiť, dokáže ho však v dostatočnej miere zastúpiť a reprezentovať jeho funkciu ako zabezpečovacieho prvku. Toto tvrdenie sa odráža od vlastností virtuálneho firewallu, ktoré sa od toho fyzického líšia. Tieto vlastnosti sú rozpísané v následujúcich odsekoch. V oblasti sieťových zabezpečovacích technológií má fyzický firewall nezastupiteľné miesto, avšak na portfóliu virtuálnych sietí sa oplatí uplatniť aj ten virtuálny. To má za následok spoluprácu oboch firewallov, zvýšenie zabezpečenia a spoľahlivosti ochrany pred útokmi.

Jedným z rozlišovacích prvkov, patriacich k virtuálnym firewallom, je jeho viacúčelnosť. Medzi ďalšie **výhody virtuálnych firewallov** patria:

Nezávislosť na prenosovej technológií. To znamená možnosť pracovať s prenosovými technológiami, ktoré nie sú priamo závislé na fyzickom pripojení na dané stroje. Napríklad v prípade sprostredkovateľov cloudových úložísk (cloud provider), technológie, ktoré fyzický firewall umožňuje, nie sú schopné správne vyfiltrovať prevádzku

na sieti. V prípade pripojenia pomocou Virtual Local Area Network (VLAN), alebo Virutal Extensible LAN (VXLAN), sú fyzické firewally nedostačujúce.

Jednoduchý prenos virtuálnych strojov. Táto mobilita umožňuje jednoduchú migráciu dát medzi data centrami. V prípade vyradenia z prevádzky alebo jeho poruchy, je jeho prenositeľnosť priamo úmerná s jednoduchou zálohou a obnovou. Na disk sa ukladajú dáta, ktoré stačí len preniesť na iný hostujúci stroj a virtuálny firewall funguje okamžite.

Konfiguráciu a správu virtuálnych firewallov, spolu s ostatnými zariadeniami, je možné rozdeliť medzi ostatných site administrátorov, ktorý dostanú na správu vlastný firewall, čo dáva možnosť preneseniu právomoci a zodpovednosti za jednotlivé segmenty sietí. Pre administrátorov je jednoduchý prístup k vzdialenej správe zariadenia.

Nevýhody virtuálnych firewallov: Nedostatočný výkon. Tento problém prichádza do súvisu s hardwarovými požiadavkami na prevádzku virtuálnych strojov. Virtuálne stroje sú však nepriamo ovplyvnené hardwarovými nedostatkami a to z dôvodu zlej implementácie. Zlá implementácia v prípade útokov na hypervisor virtuálnej siete, prípadne útoku na firewall, ktorý je spustený na rovnakom fyzickom serveri, môže ovplyvniť výkon.

Nejednotnosť v smere prenosov dát. Napríklad v dátových centrách je po zapojení fyzickej sieťovej architektúry možné identifikovať trasu takzvaného traffic flow (tok premávky) dát. V prípade nesprávnej konfigurácie virtuálnej siete môže dôjsť k zlému smerovaniu toku.

3.2 Virtuálne firewally novej generácie

Z dôvodu dynamického rozvoja sietí a internetu sa stalo, že port-based firewally stratili svoju efektivitu. Problémom je zároveň aj to, že väčšina firewallov vidí len obecný tvar vecí, ale pre konkrétne zameranie problému by potrebovala podrobnejšiu definíciu, alebo jednoducho nemá prístup k takzvanému jadru veci (dnes zastúpené funkciou sandbox). Preto prichádzajú na trh rôzne typy firewallov, ktoré ponúkajú rôzne inovatívne možnosti ochrany siete, prípadne len vylepšujú tie staré. Medzi nimi sa nachádza aj takzvaná rada firewallov novej generácie, od ktorých vývoja sa odvíjajú aj tie virtuálne.

Typické vlastnosti firewallu, ako filtrácia paketov, Network Address Translation (NAT) a Port Address Translation (PAT), stavová kontrola, podpora VPN, spadajú do vlastností, ktoré prevzali a rozšírili firewally novej generácie, spolu so schopnosťami zabrániť útokom a podpismi pre čelenie hrozbám a zraniteľnostiam. Firewally

novej generácie sú obohatené aj o iné vlastnosti, podľa ktorých by malo byť možné rozoznať firewall novej generácie, ako napríklad:

1. Identifikácia aplikácie bez ohľadu na využívaný port, protokol, Secure Sockets Layer (SSL) šifrovanie, pred tým, než spraví čokoľvek iné.
2. Sprostredkovanie prehľadu a kontroly za pomoci zásad nad aplikáciami, zahŕňajúc jednotlivé funkcie.
3. Presná identifikácia užívateľov a zároveň využitie informácií o identite ako atribút na vytvorenie nového pravidla spadajúceho do kontroly pomocou zásad.
4. Sprostredkovanie aktuálnej ochrany proti veľkej škále hrozieb, týkajúcej sa aj tých, ktoré sa dejú na aplikačnej vrstve.
5. Podpora zapojenia multi-gigabit liniek s minimalizovaním strát na výkone.
6. Zahrnutie a vylepšenie vlastností, majúcich na starosti zamedzenie sieťových hrozieb, ktoré pripadajú klasickým firewallom.

Tento typ firewallu má vlastnosti a možnosti klasického firewallu, avšak dokáže vykonávať aj nové indentifikačné techniky s prídavnými funkciami a vyšším výkonom [6].

4 VIRTUÁLNY FIREWALL HILLSTONE

Virtuálny firewall Hillstone CloudEdge, patrí medzi firewally novej generácie, ktorých vlastnosti v porovnaní s predchádzajúcou generáciou napredujú. Tento firewall sprostredkováva zvýšené možnosti ochranných prostriedkov medzi vrstvami Layer 2-7, spolu s hlavnými funkciami firewallu. Firewall disponuje dvoma možnosťami vloženia do sieťovej infraštruktúry. Jedným je vloženie cez Cloud Management Platforms (CMPs) ako firewall služba. Druhým je vloženie ako security gateway (ochranná brána) pre Virtual Private Cloud (VPC) vo verejnom cloude.

CloudEdge indetifikuje a zabraňuje možným hrozbám spojeným s vysoko rizikovými aplikáciami, zatiaľ čo zabezpečuje policy-based kontrolu (kontrolu na základe stanovených zásadách) nad aplikáciami, užívateľmi a skupinami užívateľov. Smerovanie na základe zásad a správa šírky pásma môžu byť vytvorené pre priorizáciu jednej aplikácie a obmedzenie ďalších, alebo na základe časových a aplikačných vlastností.[8][9]

4.1 Vlastnosti a fukncie Hillstone CloudEdge.

Tento firewall prináša okrem funkcií klasického firewallu aj nové funkcie prislúchajúce do kategórie firewallov novej generácie, spolu s novými praktickými vlastnosťami. V následujúcich sekciách je zoznam niektorých funkcií, spolu so stručným popisom spôsobov, akými sa danej funkcie dosahuje.

4.1.1 Možnosti identifikácie

- **Identifikácia užívateľa** – podpora lokálnych užívateľských databáz na čerpanie informácií pre prístup a podpora AAA serverov. AAA predstavuje Autentizáciu, Autorizáciu, Accounting (správu účtov). AAA je zároveň vyššou úrovňou zabezpečenia a kontroly, ktorej špecifickými vlastnosťami v praxi sú, že pri pripájaní sa na server povolí prístup len už overeným alebo autorizovaným užívateľom.
  Podpora autentifikačných metód s použitím Remote Access Dial-In Service (RADIUS) a Terminal Access Controller Access-Control System (TACACS+) pre AAA.
  TACACS+ je protokol využívaný na správu zariadení AAA ale aj na sieťový prístup AAA. Využíva Transmission Control Protocol (TCP) s portom 49 na komunikáciu klient-server, pričom vždy šifruje celý paket. Narozdiel od funkcie RADIUS dokáže oddeliť AAA funkcie separátne.

RADIUS má podobné funkcie ako TACACS+, ale je využívaný aj ako transportný protokol, prípadne ako rozšírenie autentifikácie v Point-to-Point Protokole (PPP), v druhej vrstve, používanom medzi koncovými užívateľmi a sieťovými prístupovými serverami (NAS), na prenos autentifikácie z NAS na AAA server. Pri tejto komunikácií šifruje len heslo a využíva User Datagram Protocol (UDP).
Možnosť využitia Active Directory (AD), ktorý sprostredkúva autentifikáciu, zoznamy registrov a zásady. Možnosť využitia štandardy aplikačného protokolu Lightweight Directory Access Protocol (LDAP), ktorého funkciou je komunikácia s dátami v zoznamoch a samotná úprava položiek v zozname sprostredkovateľa služieb, ako napríklad AD.
Implementácia autentifikačného systému WebAuth na kontrolu sieťového prístupu. Pomáha zabraňovať neoprávneným vstupom a povoľuje prístup aj užívateľom, ktorí nepodporujú autentifikáciu s IEEE 802.1X (zabezpečovací mechanizmus pracujúci na vrstve 2 ISO/OSI modelu). [7] Single Sign-On (SSO) je spôsob kontroly prístupu k viacerým aplikáciám/systémom. Táto služba overuje, či má užívateľ práva na spustenie danej aplikácie, väčšinou s využitím LDAP a zaznamenáva údaje do logov.
A ďalšie funkcie, ako napríklad overenie pomocou 802.1x, vzdialený VPN prístup a užívateľsky/skupinovo zamerané zásady.

- **Identifikácia aplikácií** – podpora veľkého množstva aplikácií, ktoré môžu byť filtrované podľa rôznych údajov. Špeciálne funkcie predstavujú popisky každej aplikácie, kde sa nachádzajú informácie o aplikácií (používané porty, URL), bezpečnostné riziká predstavované aplikáciou. Vďaka tomu ich možno monitorovať, zablokovať, prípadne upraviť im prislúchajúci sieťový tok. Zároveň je podporovaná aj dešifrácia pomocou SSL. Tieto všetky funkcie sú prevedené do užívateľského rozhrania.

- **Geolokácia** – graficko analytická funkcia, ktorá vyobrazuje zdroj komunikácie na mape, pomocou ktorej môže užívateľ napríklad zakázať všetku komunikáciu z konkrétneho štátu. Analytická vlastnosť spočíva vo vyhodnotení počtu útokov z konkrétneho miesta, čím je možné zvýšiť bezpečnosť jednoduchými zákazovými pravidlami pre rizikové oblasti, z ktorých pochádza najviac útokov. Na konkrétne vyhľadávanie geografických pozícií zdrojov je využívaná funkcia GeoIP.

- **SSL Dešifrovanie** – Prezeranie zašifrovanej SSL komunikácie podporuje aj povolenia na šifrovanie SSL pre antivírus. Podpora URL filtrácie pre zašifrovanú komunikáciu pomocou HTTP Secure (https).[8][9]

4.1.2 Možnosti ochrany a filtrácie

- **URL Filter** – filtrácia založená na kontrole webového toku. Jednou z možností definovania filtru je manuálne, nastavením rôznych kategórií a podmienok, prípadne lokálnym čerpaním zo súborov cache. Ďalšou možnosťou je dynamicky, získavaním kategorizačných údajov v reálnom čase z rôznych databázových serverov. Ďalšou možnosťou je filtrovať konkrétne applety, cookies, zablokovať Hypertext Transfer Protocol (HTTP), logy vyhľadávaných slov a iné.
- **IP Reputácia** – je automatický systém, ktorý vďaka predchádzajúcej komunikácií vyhodnocuje a predpokladá výsledky tej nadchádzajúcej. To znamená, že v prípade pokusu o útok z nejakej IP adresy tento systém adresu zaznamená a v prípade nastavenia ju pre budúcu komunikáciu zakáže. Ďalším spôsobom ochrany je Botnet, ktorý komunikuje so serverom, v ktorom je vedená globálna databáza IP Reputácií, podľa ktorej následnú komunikáciu vyhodnocuje.
- **IPS** – Intrusion Prevention System, zabezpečuje ochranu proti pokročilým typom útokov (ako napríklad DoS, portscan, flooding a mnoho ďalších), vďaka hĺbkovej kontrole paketov, IP reputácií a analýze malware.
- **QoS** – prináša možnosť priradiť presne garantovanú, prípadne maximálnu šírku pásma. Priradenie tunelov na základe bezpečnostných domén, rozhraní, adries, užívateľov, skupín, serverov, aplikácií, VLAN . . . Priradenie šírky pásma na základe času, priority, prípadne zhodného zdieľania – Type of Service (TOS). Maximalizácia využitia pripojenia priradením zvyšnej šírky pásma.
- **Anti-Virus** – antivírus zameraný na dátový tok. Zahŕňa protokoly ako HTTP, FTP, Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol 4 (IMAP4), ale aj vyhľadávanie vírusov v .zip dokumentoch.[8][9]

4.1.3 Ďalšie možnosti

- **DLP** – Data Loss Prevention je software so zameraním na vyhľadávanie stratových miest v sieti, detekciu a blokáciu pred zneužitím citlivých dát, ako aj na zabránenie ich úniku. Zároveň ponúka možnosť filtrovania s ohľadom na veľkosť súboru, typ súboru a meno súboru.
- **IPv6** – správa prostredníctvom IPv6, využívanie IPv6 prihlasovania. Tunelovanie pomocou IPv6. Zároveň do úvahy prichádzajú rôzne druhy smerovaní (Statické, RIPng, OSPFv3. . .). Využitie NAT64 ako prekladač medzi IPv4 a IPv6 protokolmi.

A ďalšie iné, ako napríklad funkcia monitorovania, Anti-DDOS ochranný systém, ako aj podpora Virtuálnych Systémov a cloudových pripojení. [8][9]

5 OVERENIE PRAKTICKÉHO ZAPOJENIA

V tejto kapitole je popísané zapojenie siete malého rozsahu s použitím virtuálneych firewallov a klienta Windows 7, napojených navzájom vo virtuálnej sieti. V prvej časti úlohy je použitý firewall Fortigate a druhej znázornené využitie firewallu Hillstone CloudEdge. Úloha vychádza z predpokladu, že fyzický počítač, na ktorom je úloha konfigurovaná, má prístup na externú sieť WAN s prístupom na internet.

5.1 Sieťové zapojenie programu VMWare

Na účel praktického zapojenia je využitý program VMWare Workstation, slúžiaci na prácu s virtuálnymi stanicami, virtuálnymi sieťovými prvkami. Jeho funkciami je okrem inštalácie staníc do už zostavenej fyzickej siete, aj zostavenie virtuálneho zapojenia siete. K tomuto účelu si software sám vytvorí na fyzickom rozhraní stroja sieťový adaptér, ktorý neskôr využije na pripojenie na externú sieť. Pred samotným predstavením postupu pre danú úlohu je potreba uviesť základné pojmy pomenúvajúce jednotlivé možnosti napojenia danej virtuálnej siete na fyzickú sieť. Tieto potenciálne najvýhodnejšie možnosti sú 2 a síce:

Bridge – ako bolo už popísané v kapitole 3, zaoberajúcej sa vrituálnym firewallom a jeho funkčnými režimami, tak podobne aj bridged networking, preložené aj ako premostenie sietí, je spôsob zapojenia virtuálnej siete na fyzickú (za predpokladu že je ethernet sieť napojená na hostujúcom stroji). V tomto prípade dostane virtuálna sieť vlastnú IP adresu, na ktorú môže fyzická sieť referovať. Táto vlastnosť robí z virtuálneho stroja plnohodnotného účastníka v rámci sieťového pripojenia, čo znamená prístup k ostatným užívateľom (koncovým staniciam a sieťovým prvkom), ale aj vyššie možnosti konfdigurácie. [10]

NAT – network address translation je možnosť prepojenia s využitím funkcie takzvaného prekladu adries. Dôvodom využitia tohto pripojenia je jednoduchosť v rámci pripojenia na TCP/IP sieť bez priraďovania IP adresy pre externú sieť virtuálnemu stroju. Na sieť sa zväčša pripája pomocou dail-up, prípadne iným pripojením (napríklad broadband connection). Použitím pripojenia pomocou NAT sa vytvorí privátna sieť, pre ktorú dostane virtuálny stroj adresu z virtuálneho DHCP serveru. Toto riešenie je využívané na fyzických sieťach najmä z dôvodu šetrienia využitia ip adries, obzvlášť v protokole IPv4. [11]

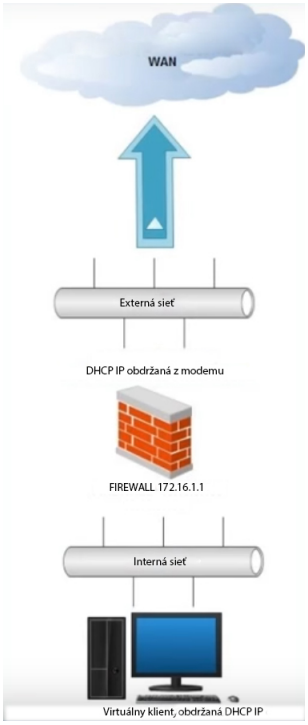
V rámci vypracovania danej úlohy bude kladený dôraz na zapojenie pomocou bridge módu, v spojistosti s ďalšími sieťovými prepojeniami.

5.2 Postup zapojenia siete

V tejto praktickej časti je venovaná pozornosť zapojeniu malej virtuálnej siete obsahujúcej základné prvky, jej nasledovnému zabezpečeniu a vyhodnoteniu výsledkov, z toho vyplývajúcich. Pre zapojenie virtuálnej siete bol použitý program na prácu s virtuálnymi prostrediami VWMare. Ďalšou súčasťou bola virtuálna stanica, ktorú predstavoval Windows 7 klient.

Z dôvodu desynchronizácie sériových čísel pri neštandardnej inštalácií virtuálneho firewallu Hillstone je pre túto časť úlohy použitý virtuálny firewall Fortigate. Obdobné nastavenie zapojenia je pre väčšinu virtuálnych firewallov, líšia sa až pri spôsoboch a možnostiach filtrovania. Pre ne bude vyobrazený popis základného nastavenia filtrácie vo webovom rozhraní už pre firewall Hillstone.

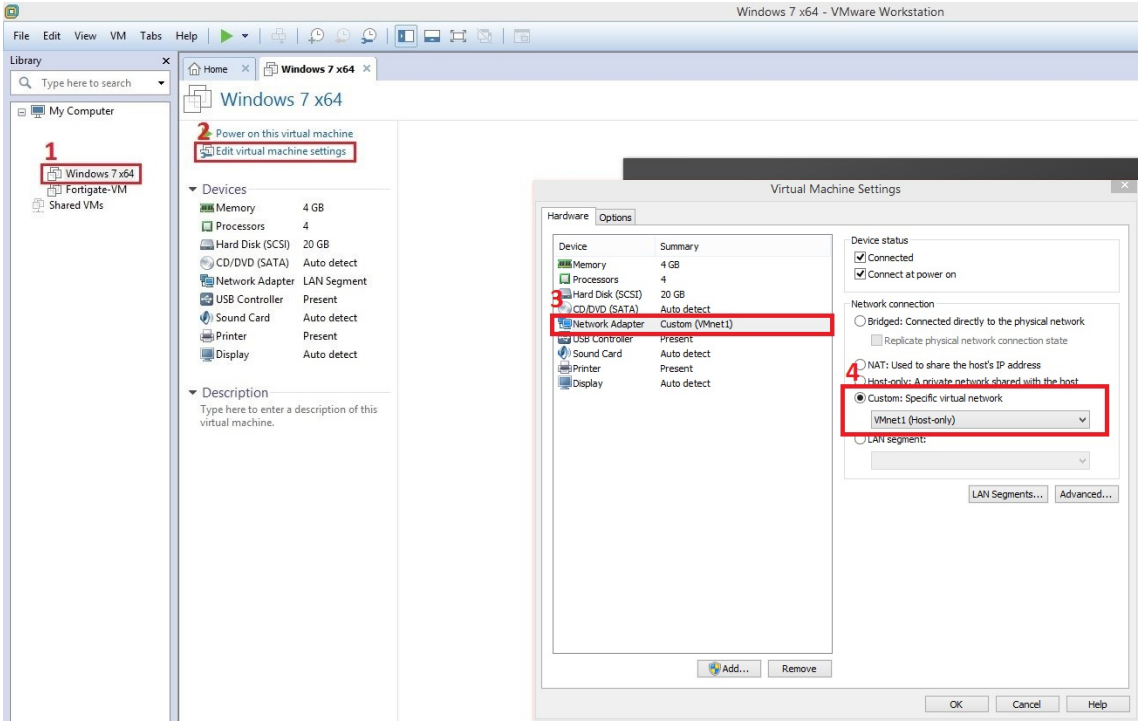
Zapojenie príslušnej virtuálnej siete je uskutočnené podľa obrázku 5.1.



Obr. 5.1: Zapojenie vytváranej siete.

5.2.1 Nastavenie sieťových adaptérov a konfigurácia portu

Po inštalácií príslušného firewallu do programu VMware je potreba nastaviť príslušné sieťové adaptéry. Nasledovný postup je naznačený na obrázku 5.2.

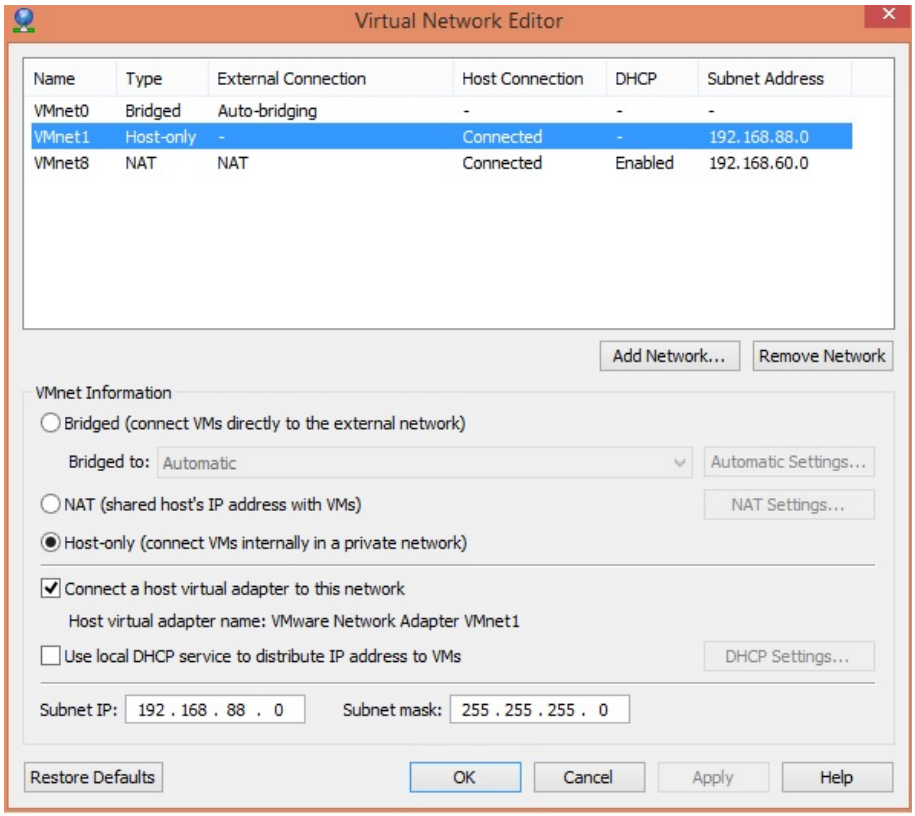


Obr. 5.2: Nastavenie sieťového adaptéru v prostredí VMWare.

Po rozkliknutí konkrétneho virtuálneho stroja (bod 1), konkrétne klient Windows 7, kliknite na možnosť editovať nastavenia (bod 2), po zobrazení nastavenia treba upraviť sieťový adaptér (bod 3), aby bol zapojený do siete cez Custom: Specific viurtal network (bod 4) a vybrať možnosť VMnet1 (Host-only). V prípade že sa v nastaveniach daný adaptér nenachádza, možno ho pridať tlačítkom Add, následne vybrať sieťový adaptér a potvrdiť. Väčšina virtuálnych strojov má prednastavený adapter na možnosť Bridged. Preto treba overiť, či je virtuálny sieťový adaptér na fyzickom počítači správne nastavený. Vo VMWare kliknite na Edit a záložku Virtual Network Editor. V nej treba nastaviť adaptér VMnet1 podľa obrázku 5.3.

Obdobne prebieha nastavenie aj pre Fortigate-VM firewall. Ten má však od pôvodného nastavenia viacero adaptérov. My budeme používať prvé 2. Defaultne nastavený adaptér 1 ponecháme na možnosti Bridged a adaptér 2 prepneme na rovnaké nastavenie ako adaptér pre Windows 7 virtuálneho klienta. A síce na editovanú verziu Custom: Specific Virtual Network – VMnet1 (host–only). Prvý adaptér bude slúžiť ako WAN na komunikáciu firewall-internet a druhý ako LAN na komunikáciu firewall-client. Všetky nastavenia následne potvrdíme a oba stroje zapneme.

Po zapnutí sa dostaneme do CLI konfigurovateľného režimu zadaním login: admin a heslo prázdne. Následnými príkazmi nastavíme na port 2 (nami zvolený pre LAN prepojenie medzi klientom a firewallom) nami zvolenú IP adresu (pre tento prípad



Obr. 5.3: Editor virtuálnych sietí VMWare.

172.16.1.1 s maskou 255.255.255.0) a možnosť pripojenia cez webové rozhranie (aj zabezpečené webové rozhranie), ssh, telnet a ping. Viď príkazy na obrázku 5.4.

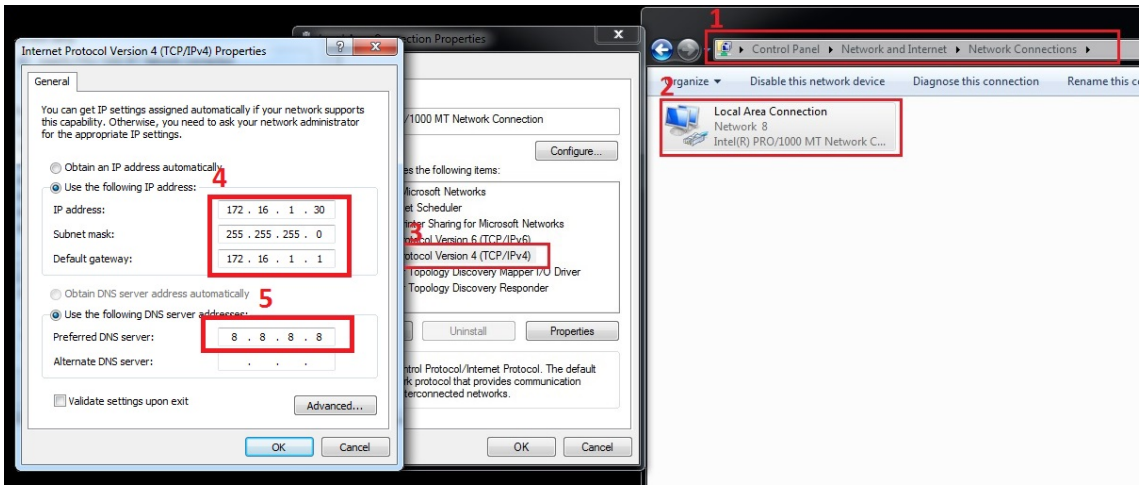
```
Fortigate-VM login: admin
Password:
Welcome !

Fortigate-VM # config system interface

Fortigate-VM (interface) # edit port2

Fortigate-VM (port2) # set ip 172.16.1.1 255.255.255.0

Fortigate-VM (port2) # set allowaccess https http ssh telnet ping

Fortigate-VM (port2) # end
```

Obr. 5.4: Prihlásenie na firewall a konfigurácia prístupu na port 2.

5.2.2 Overenie spojenia

Po vykonaní predchádzajúcich nastavení je možné overiť schopnosť pripojenia z virtuálneho klienta Windows 7 na webové rozhranie firewallu. To docielime nastavením

adaptéru priamo v systéme virtuálneho klienta Windows 7 otvorením cesty Control Panel>Network and Internet>Network Connections (bod 1), pravým klikom na adaptér a výberom vlastnosti (bod 2). Vo vlastnostiach rozkliknutím možnosti konfigurácie protokolu TCP/IPv4 (bod 3). Po jeho otvorení je potrebné kliknúť na možnosť Use the folowing IP address a nastavením ip adresy a masky (nami zvolená IP a maska klienta – 172.16.1.30 255.255.255.0) a nastavením Default gateway na nami nastavenú IP firewallu 172.16.1.1 (bod 4), DNS server použijeme 8.8.8.8 spoločnosti Google (bod 5). Toto nastavenie je vyobrazená na obrázku 5.5. Po potvrdení



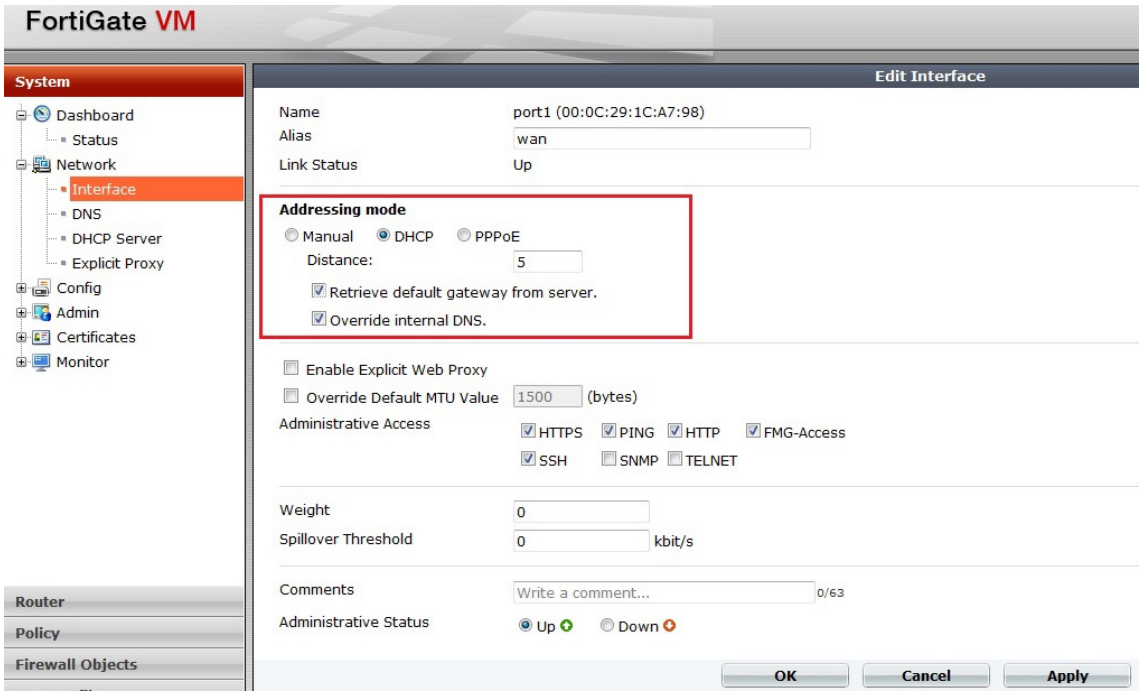
Obr. 5.5: Nastavenie sieťového adaptéru na virtuálnom klientovi Windows 7.

je možné sa z virtuálneho stroja Windows 7, pomocou webového rozhrania, pripojiť na firewall zadaním adresy 172.16.1.1 do prehliadača a následným prihlásením do rozhrania login:admin a heslo prázdne. Tým sme si overili funkčnosť spojenia medzi firewallom a Windows 7 klientom. Ďalej však bude prebiehať konfigurácia na fyzickom stroji, preto prehliadač zavrieme.

5.2.3 Nastavenie sieťových rozhraní

Pre možnosť konfigurácie virtuálneho firewallu z fyzického počítača, ktorý hostuje virtuálne stroje, je potrebná konfigurácia sieťového adaptéru. Do nastavenia sa dostaneme rovnakým postupom ako pri nastavovaní adaptéru pre virtuálny systém windows. Avšak v sieťových pripojeniach vyberieme adaptér – VMWare Network Adapter VMnet1, otvoríme vlastnosti>IPv4 protocol a nastavíme IP adresu ako 172.16.1.20, ostatné údaje rovnaké ako v obrázku 5.5. Tým sme docielili možnosť pripojenia na webové rozhranie priamo z fyzického stroja a môžme tak začať s nastavovaním firewallu. Pripojíme sa cez prehliadač na webové rozhranie zadaním IP adresy 172.16.1.1 .

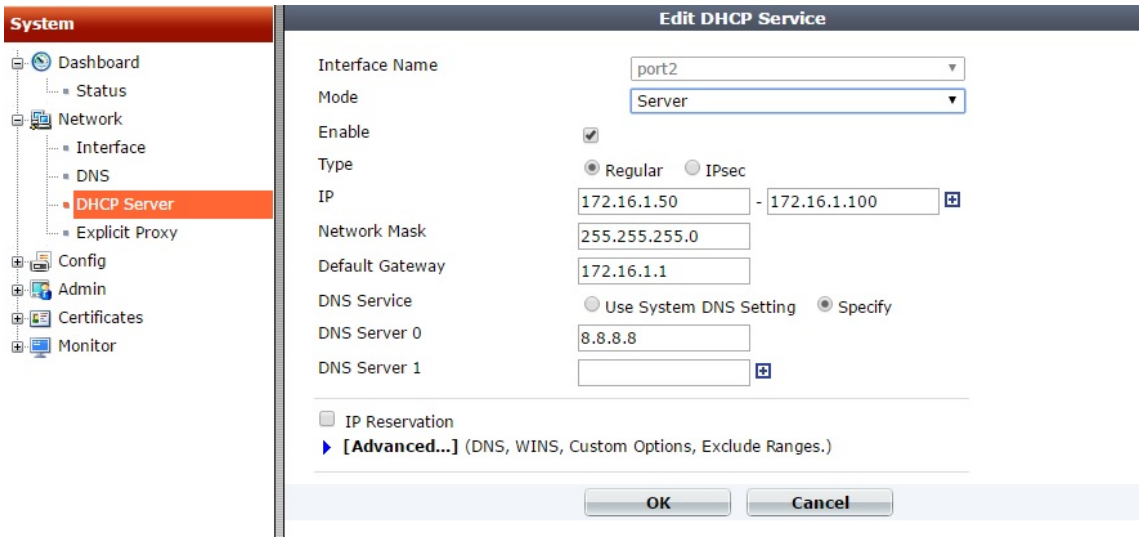
Po kliknutí na možnosť System>Network>Interface, nachádzajúcej sa v ľavom rohu, sa zobrazia všetky porty. Nás zaujímajú porty 1 a 2, pričom port 2, ktorý je „náš LAN“ už nekonfigurujeme, lebo sme ho už nastavili pomocou CLI commands. Preto otvoríme konfiguráciu portu 1 („náš WAN“) a nastavíme ho tak, aby addressing mode bol DHCP a zároveň bola povolená možnosť Retrieve default gateway from server, zároveň zaškrtneme možnosť HTTP pre administratívny prístup. Toto nastavenie spôsobí, že rozhraniu bude pridelená adresa od fyzického routru pomocou DHCP. Funkčnosť priradenej DHCP adresy možno overiť pomocou príkazu, zadaného do CLI firewallu, *execute ping www.google.com*. Táto priradená adresa bude verejnou adresou pre firewall. Zároveň môžme nastaviť Alias na ľubovoľné pomenovanie daného portu. Nastavenie možno vidieť na obrázku 5.6.



Obr. 5.6: Nastavenie rozhrania na porte 1.

5.2.4 Nastavenie DHCP serveru

Pre vytvorenie DHCP serveru kliknite v záložke System>DHCP Server a kliknite na Create New. Otvorí sa *nastavenie DHCP služby*, kde vyberieme názov interface port2 (lan) a zvolíme rozsah pridelovaných adries (napr. 172.16.1.50 - 172.16.1.100), ako Default Gateway nastavíme 172.16.1.1 čo znamená že brána bude smerovať na firewall a DNS Server nastavíme 8.8.8.8 (Google). Nastavenie možno vidieť na obrázku 5.7.



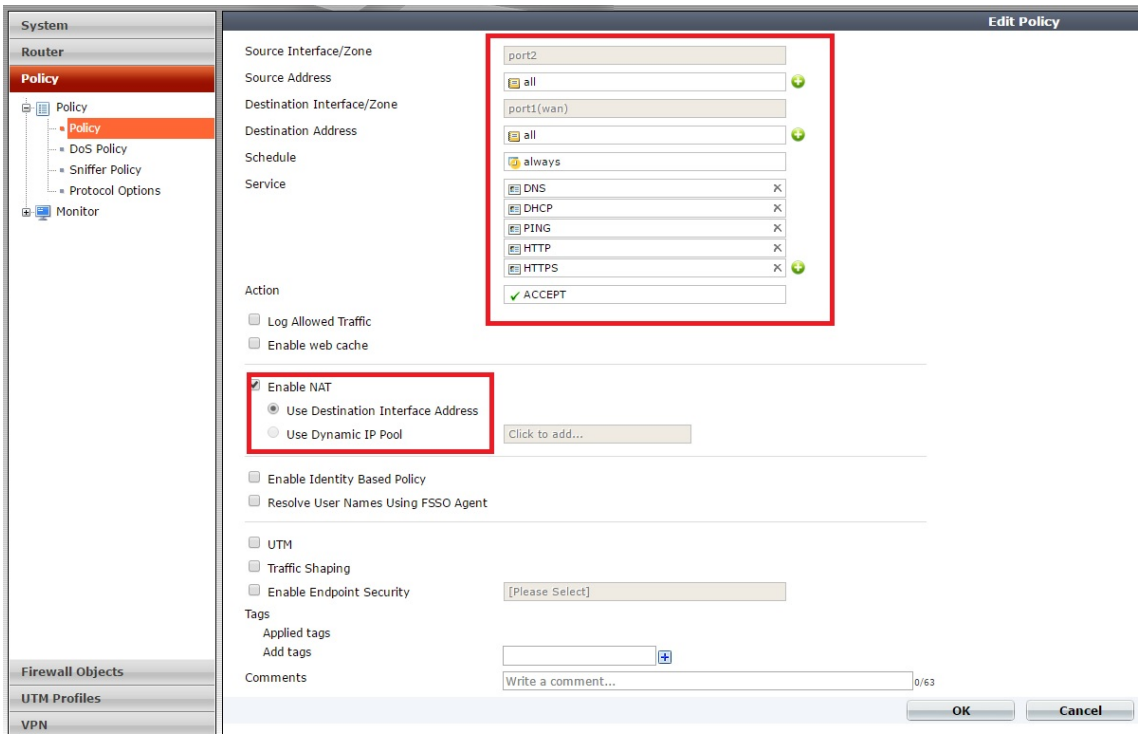
Obr. 5.7: Nastavenie DHCP serveru pre port 2.

5.3 Určenie zabezpečovacích pravidiel

V tejto časti je definovaná kompletizácia DHCP pripojenia pre port 2, na ktorý je pripojený klient Windows 7. Zároveň je tu sumarizované povolenie pripojenia na internet aktivovaním prístupových zásad pre protokol HTTP a HTTPS.

5.3.1 Nastavenie zásad

Pre dokončenie nastavenia DHCP serveru a povolenie prístupu na internet je potrebné nastaviť príslušnú zásadu smerovania. Otvoríme záložku, nachádzajúcu sa v ľavom rohu užívateľského rozhrania, Policy>Policy>Policy a klikneme na Create New. Nastavíme zdrojové a cieľové adresy a rozhrania podľa obrázku 5.8 a povolíme možnosť NAT. Služby, ktoré budú mať povolenie na spustenie zvolíme DNS, DHCP, PING, HTTP,HTTPS. Ostatné služby sú nastavené ako Default Deny, čo znamená, že pre dodatočné povolenie inej služby, ako jednej z tých vymenovaných by bolo potreba vytvoriť novú zásadu, prípadne editovať už existujúcu. Potvrdením vytvorenia tejto zásady sa prístup na internet povolí pre virtuálneho klienta Windows 7. Po sprístupnení internetového pripojenia možno konštatovať, že firewall funguje aj ako smerovač pre internetové pripojenie a prechádza cez neho celá komunikácia medzi klientskou koncovou stanicou a externými Internetovými servrami. Zároveň aj služba DHCP patrí medzi povolené a aktívne na rozhraní portu 2 (viz. funkčné pripojenie na internet), čo bolo možné overiť aj spustením príkazového riadku na klientskom virtuálnom Windows 7 a zadaním príkazu ipconfig, pričom vypísaná adresa bude pripadať do nami určeného rozmedzia.



Obr. 5.8: Nastavenie zásady smerovania.

5.3.2 Iné možnosti zabezpečenia

V prípade nastavenia firewallu Fortigate je možné nastaviť zabezpečenie pomocou zásad, ako bolo možné vidieť pri nastavovaní zásady smerovania tak, že po vytvorení skupiny, prípadne využití už vytvorených skupín, možno zakázať ich funkciu.

Pre príklad je možné zakázať služby programu Outlook, ktoré sa zakážu obdobne ako pri vytváraní smerovania (source a destination ostávajú rovnaké, ako aj schedule), service vyberieme Outlook (prípadne akýkoľvek preddefinovaný, alebo nami vytvorený) a zadáme Action Deny. Skupiny adries, služieb a podobne sa nachádzajú v záložke Firewall Objects, kde ich možno pridať. Zároveň pri vytváraní policy je možnosť povolenia UTM, kde je na výber napríklad možnosť použiť AntiVirus, Web Filter, Application Control a iné možnosti filtrovania.

5.4 Zhrnutie výsledkov

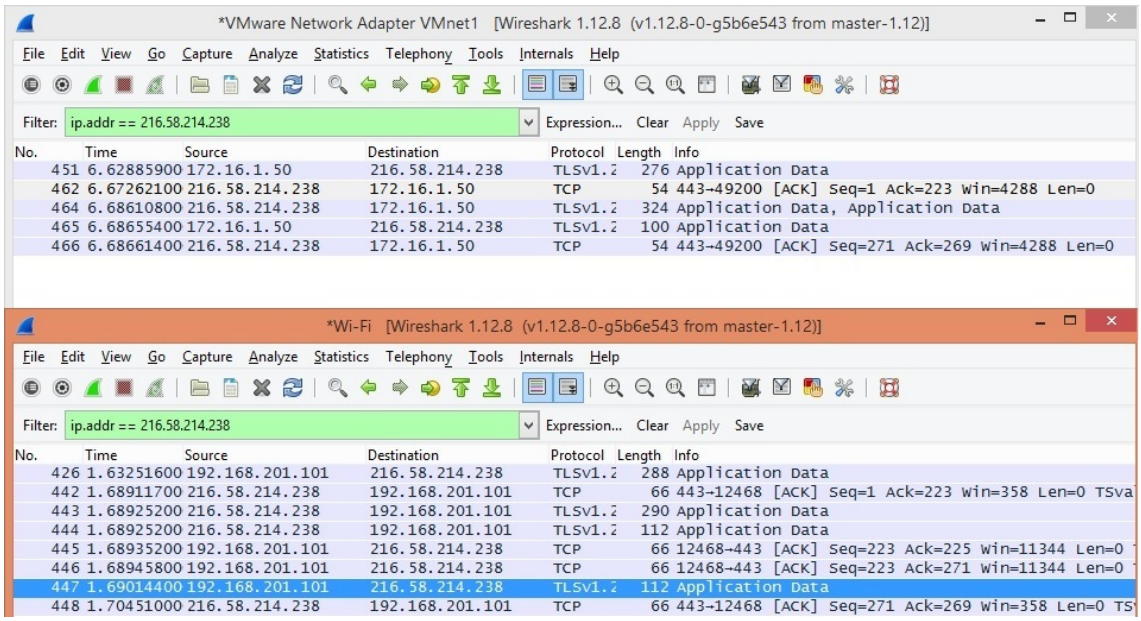
V zapojení malej virtuálnej siete sme vytvorili komunikujúcu sieť medzi vonkajšou sieťou – internetom (WAN) a internou sieťou (LAN). V zapojení sme vytvorili DHCP server na prideľovanie adries jednotlivým prístrojom pripájajúcim sa na rozhranie firewallu. V prípade, že by DHCP nebolo vytvorené, bolo by možné vytvoriť

ACL pre pripojenia pevne definovaných adries. Zároveň sme uskutočnili jednoduchú filtráciu pomocou firewallu Fortigate, ktorý povolil komunikáciu po sieti len v rámci povolených funkcii HTTP, HTTPS, PING... nastavených ako zásady pre smerovanie na rozhraní medzi firewallom a Windows 7 virtuálnym klientom.

Wireshark – po zachytení komunikácie pomocou programu wireshark môžme podrobnejšie preskúmať priebeh zapojenia. Prvé na radu na interface VMnet 1 príde registrácia samotného fyzického stroja a ako druhé po spustení oboch virtálnych strojov registrácia DHCP spolu s kontaktom a overením funkčnosti DNS doménového serveru.

Priebeh komunikácie – klient Windows 7 komunikuje s externým internetovým serverom následovne. Klient pošle žiadosť na Firewall, ktorý po ich kontrole posiela všetky žiadosti klienta na router, z ktorého odchádza komunikácia na externú sieť, odkiaľ môže byť splnená požiadavka pre komunikáciu s ním. Avšak po zobrazení komunikácie je možné vidieť, že klient posiela žiadosti z IP adresy 172.16.1.50 (pridelenej z DHCP) na firewall, ktorý ďalej posiela túto žiadosť po prekontrolovaní na router (s IP 192.168.201.101 – ktorá je pridelenou adresou pre firewall z routru pomocou DHCP). Ten následne prepošle túto žiadosť pod vlastnou externou IP adresou na externú sieť. Na obrázku 5.9 možno vidieť komunikáciu medzi klientom a externým serverom (obrázok v hore), pričom komunikácia je sprostredkovávaná firewallom, ktorý ju ďalej preposiela na router. Preposielanie komunikácie medzi firewallom a routrom (žiadosť o spojenie pochádza od klienta) je viditeľné na obrázku dole. Z prvého pohľadu je badateľný samotný rozdiel vo veľkosti paketov, čo je spôsobené prepisom hlavičky pre cieľové adresy, ako aj samotnou kontrolou firewallu. Keďže na firewalle nie je nastavené špecifické pravidlo na filtrovanie konkrétnych URL (táto funkcia je k dispozícií len so zakúpením licencie Fortiguard), tak firewall nezanecháva na komunikácií klient-server žiadnu „stopu“. Zároveň filtrovaná komunikácia nie je preposielaná na externý server, čo znamená že sa údaje, ktoré cez tento firewall prešli, nikam ďalej neposielajú. Z toho môžme vyvodiť, že firewall je bepečný na používanie z hľadiska „odpočúvania“ externou firmou, ktorou by mohol byť napríklad výrobca firewallu, ale zároveň to môže byť spôsobené používaním voľnej licencie. Táto licencia totiž neponúka možnosti využitia cloud externých kontrôl adries a ani iné ochranné prvky, vyžadujúce spojenie s centrálnymi servermi Fortigate.

V prípade, že je funkcia ping na rozhraní medzi komunikačným portom 2 a WAN zakázaná, žiadosť o ping (request) ostane bez odpovede a je firewallom ignorovaná. Ak by však bol na firewalle nastavený URL filter, príde k oznámeniu, že na konkrétnu adresu firewall zamietol prístup a môže prísť k prípadnému presmerovaniu na inú stránku.

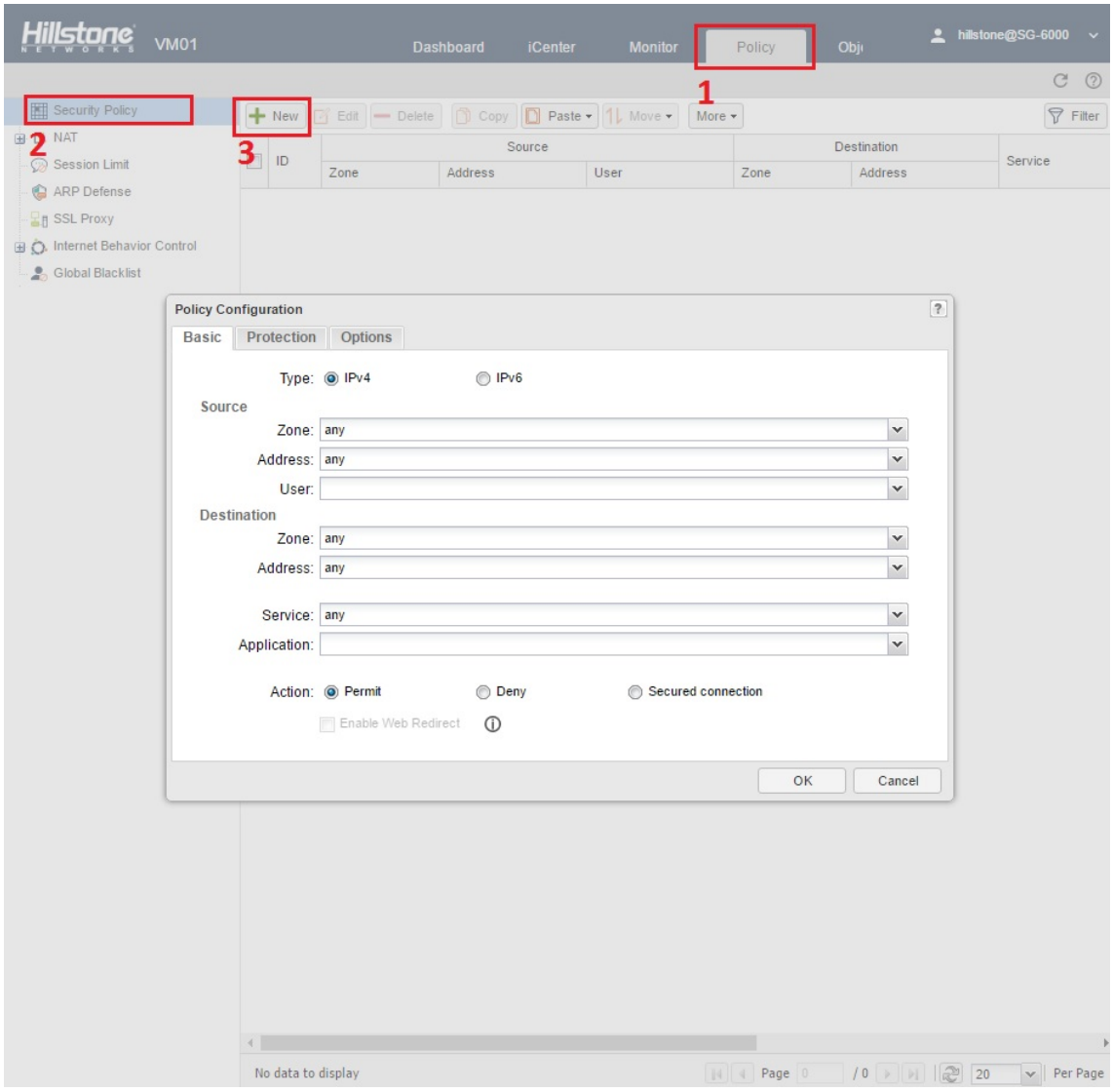


Obr. 5.9: Wireshark – zachytenie komunikácie na interface firewallu pre LAN (Hore) a WAN (Dole).

5.5 Filtrácia použitím firewallu Hillstone

Po obdobnom zriadení sieťového spojenia na virtuálnom rozhraní ako bolo spomenuté v predchádzajúcej kapitole, je možné na webovom užívateľskom rozhraní (WebUI), pracujúcom na StoneOS systéme, zriadiť možnosti filtrovania a zabezpečenia siete. Pokusy o porušenie nastavených pravidiel možno pozorovať na úvodnej obrazovke rozhrania, prípadne v záložke iCenter, v ktorom je grafické vyobrazenie Geolocation technológie spolu s informáciami o útokoch. V záložke monitor je stredisko informácií o prebiehajúcich spojeniach s výpisom podrobností o aplikáciách používajúcich sieťové pripojenie.

Na vytvorenie zásady, podľa ktorej bude firewall filtrovať sieťový tok je potrebne kliknúť na záložku Policy (bod 1), kliknúť na Security Policy (bod 2) a zvoliť možnosť New (bod 3), podľa obrázku 5.10. Po potvrdení tejto možnosti nastáva samotná konfigurácia zásady. V časti Type zvolíme, o aký druh IP sa jedná. V informáciách o zdroji uvedieme zónu, ktorá môže byť rôznych druhov (v závislosti na vrstve môže byť napríklad dôveryhodná, nedôveryhodná, prípadne DMZ). V prípade záujmu je možné nakonfigurovať, aby sa zásada kontroly vzťahovala na konkrétneho užívateľa, prípadne ich skupinu. V skupine nastavenia cieľa je potrebné taktiež zvoliť zónu a adresu. Konečným nastavením je výber konkrétnej služby, prípadne aplikácie, ktorá má byť zakázaná/povolená/kontrolovaná. Dodatková možnosť ochrany je navolenie URL kontroly, ďalšou možnosťou je ukladanie logov prípadne zapnutie QoS služby.



Obr. 5.10: Nastavenie zásady smerovania, Hillstone rozhranie.

6 ZABEZPEČENIE SIETE STREDNÉHO ROZSAHU

Táto časť je zameraná na zabezpečenie sietí stredných veľkostí, bežne využívaných vo väčších multimediálnych domácnostiach, prípadne na pracoviskách, ktoré neobsahujú veľa sieťových prvkov na to, aby boli klasifikované ako siete veľkých rozsahov. Sieť veľkého rozsahu býva v praxi využívaná nadnárodnými spločnosťami s prepojením medzi jednotlivými pobočkami, prípadne data centrami, alebo sa jedná o stanice sprostredkovateľov internetového pripojenia. V prípade týchto sietí počítame s nedokonalým spojením čo sa týka bezpečnosti, čo znamená že sieť nie je izolovaná od WAN, prípadne iných sieťových prvkov z takzvaných „vonkajších sietí“.

Cieľom tejto kapitoly je predstaviť zabezpečenie prislúchajúce veľkosti siete, ktorá počíta s bežnou prevádzkou bez zložitých cielených útokov. Zabezpečenie siete je mierené prevažne na kontrolu vnútornej sieťovej infraštruktúry a pridelenie prislúchajúcich sieťových protokolov k danej časti siete.

Pri práci na tejto časti boli použité poskytnutné materiály od firmy hillstone, na preštudovanie a rozvinutie danej problematiky [12],[13], ako aj presný postup práce so StoneOS systémom [14].

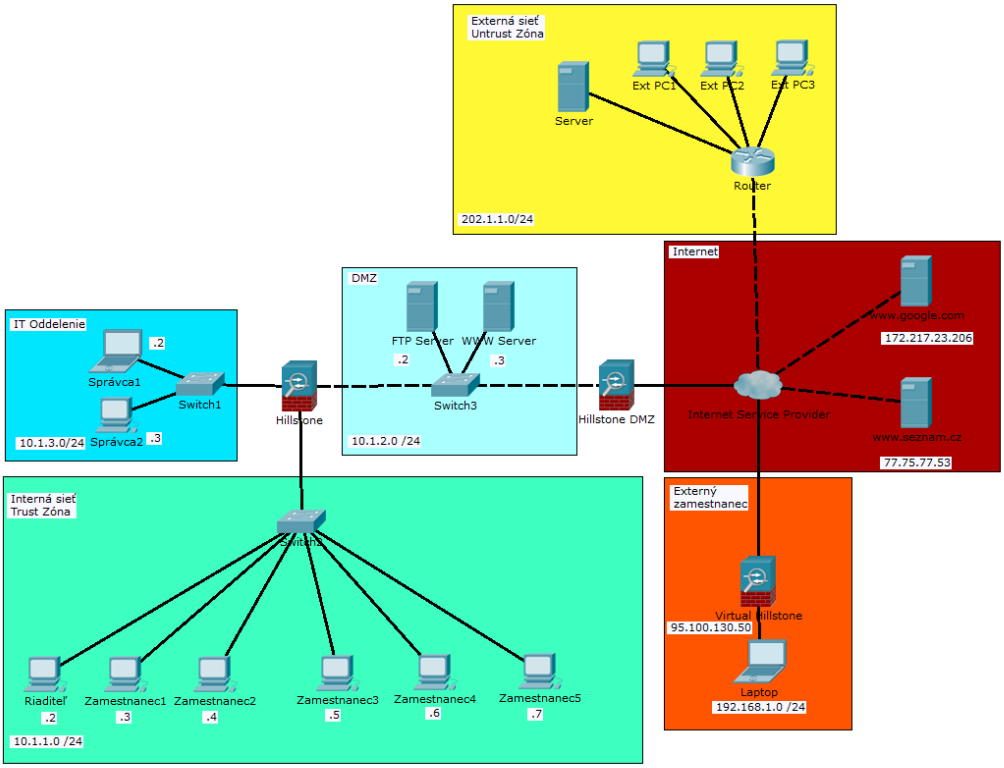
6.1 Návrh zabezpečenia siete

K návrhu zapojenia bol použitý program Cisco Packet Tracer verzia 7, avšak jednalo sa len o návrh topológie fiktívnej siete, nie o jej otestovanie. Dôvodom nevyužitia všetkých funkcií k otestovaniu sieťového zapojenia, ktoré tento program ponúka, bol fakt, že sieťové prvky, nachádzajúce sa v palete výberu, boli len obecného charakteru a zastupovali konkrétne sieťové prvky iných značiek, ktoré na výber neboli. A síce neponúkali možnosti konkrétneho firewallu novej generácie Hillstone.

Sieťová topológia, ktorá bola navrhnutá a vyobrazená na obrázku 6.1, pozostáva z jednotlivých sieťových segmentov a zón dôvery (trust zón). Zóna dôvery je vyjadrenie pre stupeň zabezpečenia sieťového segmentu v závislosti na predpoklade potencionálnych hrozieb, ktoré by mohli pochádzať z týchto alokovaných sieťových segmentov pripojených na konkrétny port firewallu. Pre príklad internetu, pripojenému na eth0/3 rozhranie Hillstone firewallu, priraďujeme zónu untrust. Sieťové segmenty vyobrazené v topológii sú – Externá sieť (untrust zóna), IT oddelenie, Interná sieť (trust zóna), Demilitarizovaná zóna (DMZ), Internet a sieť externe pripojeného zamestnanca. Zamestnanci sú pripojený v segmente Internej siete (trust zóne) a majú alokované IP adresy v podsieti 10.1.1.0/24. Zároveň majú najvyššiu pri-

oritu zabezpečenia spolu so segmentom IT oddelenia, ktorého IP pool je 10.1.3.0/24. Segment DMZ, obsahuje WWW server a FTP server, ktoré sú prístupné užívateľmi z internej siete, ale aj vonkajšími užívateľmi. Adresy v DMZ sú pridelené v podsieti 10.1.2.0/24. Externá sieť (untrust zóna) predstavuje vonkajšiu sieť a je názorným vyjadrením prístupu na internú sieť, pričom jej adresy sú zvolené ako 202.1.1.0/24 IP pool. Táto sieť je takmer totožná so segmentom siete pomenovaným Internet, ktorý pre názorné vyobrazenie obsahuje server www.google.com (172.217.23.206) a server www.seznam.cz (77.75.77.53). Pomocou tejto časti siete je pripojený aj externý zamestnanec, ktorý má na svojom súkromnom počítači nainštalovaný Virtuálny firewall Hillstone CloudEdge, ktorý je pripojený cez bridge na tento počítač.

Každý zo sieťových segmentov predstavuje inú úroveň zabezpečenia a obsahuje iné pravidlá prístupu a filtrovania komunikácie na sieti. Na tieto úkony je využívaný firewall Hillstone SG-6000-G2120, predstavujúci fyzický firewall a Hillstone ClodEdge, predstavujúci virtuálny firewall.



Obr. 6.1: Štruktúra navrhnutej fiktívnej topológie siete.

Spôsob smerovania a pravidlá zabezpečenia v sieti:

- Interná sieť – zamestnanci v tejto sieti majú prístup na internet, zároveň môžu pristupovať k serverom v DMZ. Internetový prenos je však obmedzený na servery www.seznam.cz (ktorý je pomocou URL filtra blokovaný) a na server www.google.com je nastavené ukladanie logov.
- Externá sieť – Jedná sa o sieťový segment, obsahujúci počítače a sieťové prvky, ktoré sú potencionálnym záujemcom o naviazanie spojenia s internou sieťou, prípadne DMZ.
- DMZ – Dva servery sú dostupné pre užívateľov a je k nim umožnený prístup aj zo siete Internet (ako aj z Externej siete). Jedná sa o servery FTP (10.2.2.2, port 21) a WWW server (10.1.2.3, port 80). Zároveň disponujú externou IP adresou, z poolu predstavujúci Externú sieť (202.1.1.10)
- Internet – Predstavuje zónu, ktorá má v logickom usporiadaní sieťovej infraštruktúry vyjadrenie v podobe 2 serverov pre lepšiu vizualizáciu v rámci udeľovania filtračných pravidiel na túto zónu. Inak sa jedná o rovnakého predstaviteľa, akým je Externá zóna.
- Externý zamestnanec – Sieťový segment, v ktorom figuruje na lokálnej sieti laptop zamestnanca a cez bridge prepojený virtuálny firewall, ktorý chráni a smeruje sieťovú komunikáciu z laptopu smerom na WAN pripojenie (segment Internet).

6.2 Spôsob zabezpečenia siete

Prvotným krokom pri návrhu siete je rozdelenie sieťových rozhraní v rámci prideľovania IP adries. Z topológie vyplýva, že prístup na konzolový port má len IT oddelenie, ktoré má však aj osobitne vyčlenený ethernet port v rámci pripojenia na firewall. Z dôvodu zvýšenia bezpečnosti siete je optimálne prideľovať IP adresy staticky. Pre hostí je možné, v prípade alokovania portu pre router, prideliť DHCP pool na prerozdelenie IP adries, avšak táto varianta počíta s nižšou úrovňou zabezpečenia a kontroly. Preto sú všetky pridelené adresy na konkrétne porty pridelené staticky, ako aj IP adresa pre VPN pripojenie.

IT Oddelenie – práva pre správu siete v rámci trust zóny spadajú len do ich eth. rozhrania. Prístup ku konfigurácií je umožnený pomocou protokolu SSH a zároveň protokolu https na webové rozhranie firewallu. Majú neobmedzený prístup na celú sieť, ako aj žiadnu filtráciu a blokovanie služieb.

Interná sieť – táto sieť má nastavené obmedzenie na využívanie internetových služieb. Prihlasovanie sa na sieť je vedené cez AAA a prihlasovanie užívateľa do siete.

Každý užívateľ má jedinečné prihlasovacie údaje pre zvýšenie kontroly a bezpečnosti. Zároveň je prístup na internet obmedzený časovo na pracovný čas od 6:00 do 20:00. V nastaveniach URL filtrácie je blokovaná a zaznamenaná komunikácia so serverami facebook.com a seznam.cz. Špeciálny dôraz pri vytváraní záznamov je kladený na adresu google.com, kde je vytvorený filter na zaznamenávanie a upozorňovanie na „ilegálnu aktivitu“, ktorý je prevzatý ako preddefinovaný od spoločnosti hillstone.
V sieti je implementovaný aj vlastný DNS server, čím je znížené riziko útokov a výpadkov, ktoré by mohli nastať v prípade využitia externého DNS.
Zároveň, pre zvýšenie bezpečnosti majú zamestnanci nastavený zákaz sťahovania .exe súborov, HTTP binárnych súbor a JAVA appletov.
Vďaka aktívnej kontrole aplikácií je možné vyhodnotiť správanie sa siete a prideliť konkrétnu šírku pásma tej, ktorá to potrebuje najviac. Príkladom je nastavenie QoS, preferujúce aplikácie využívajúce protokoly https a http (pripojenie na web stránky), ako aj využitie aplikácií Skype a Outlook. Aplikácie ako BitTorrent je možné, vďaka monitoringu sieťových aplikácií, zakázať a monitorovať pokusy o ich využitie.
Na sieti je zároveň nastavené pravidlo pre obmedzenie prispievania na Web, pričom blokovanie je nastavená na konkrétne slová (prevažne vulgarizmy), pre zachovanie dobrého mena spoločnosti.
Pre kontrolu nad zasielanými a prijatými mailami, je nastavená zásada filtrovania emailov. Tá umožňuje kontrolu nad SMTP a web mailami. V tomto prípade je nastavený filter na zákaz komunikácie s mailami @post.cz, z dôvodu častého výskytu nelegitímnych adries, zasielajúcich nežiadúci obsah.

Riaditeľ – užívateĺ, pripojený na internú sieť, bez obmedzení v podobe URL filtra, prípadne bez časových obmedzení. Kontrola v podobe zaznamenávania logov je však aktívna aj pre tohoto užívateľa.

Externá sieť – reprezentuje užívateľov v externej sieti, naväzujúcich pripojenie na WWW a FTP server. Prístup do tejto demilitarizovanej zóny je pre nich povolený, avšak všetka komunikácia, ktorá je smerovaná na DMZ a trust zónu, je dodatočne kontrolovaná cez ďalší firewall, zapojený v Tap Móde. Dôvodom tohto zapojenia je využitie funkcií firewallu novej generácie pre zvýšenie zabezpečenia siete. Jedná sa o funkcie ako Intrusion Prevention System, Advanced Threat Detection(ATD), Application Identification a Abnormal Behavior Detection (ABD). Zapojenie firewallu v Tap Móde sa vyznačuje spôsobom mirror – zrkadlením komunikácie medzi rozhraniami. Tento firewall následne porovnáva všetku komunikáciu s databázou hrozieb na serveroch a vyhodnocuje ju.
Nastavenie funkcie ATD znamená zároveň aj povolenie kontroly pred hrozbami typu Malware a inými druhmi vírusov. Funkcia ABD má na starosti ochranu proti útokom ako DoS, alebo Scan.

Internet – je sieťou, ktorá vyjadruje webové servery, na ktoré má užívateľ z internej siete buď povolený, alebo zamietnutý prístup. Nachádza sa v untrust zóne a bezpečnostné pravidlá spadajúce pre túto časť siete sú rovnaké, ako pre Externú sieť.

Externý zamestnanec – je pripojený na sieť pomocou tunelu SSL VPN, pričom virtuálny firewall, nainštalovaný na jeho laptope, plní funkciu antivírového software a chráni pred nežiadúcimi prístupmi. Pre nastavenie SSL VPN je potrebné zvoliť prihlasovacie údaje, prostredníctvom ktorých sa bude užívateľ prihlasovať a zároveň prideliť IP adresu. Prihlásenie užívateľa prebieha v Hillstone Secure Connect klientovi, ku ktorého stiahnutiu je užívateľ, ktorý sa chce pomocou tejto služby pripojiť vyzvaný. V neposlednej rade je potrebné pridať tunel, ktorý reprezentuje toto spojenie, do zóny untrust. Celá komunikácia prostredníctvom VPN je potom monitorovaná na strane fyzického firewallu.
Druhá možnosť nastavenia vzdialeného pripojenia je prostredníctvom IPSec VPN, táto funkcia nevyžaduje žiadneho prihlasovacieho klienta, pretože prístup na sieť je pevne nakonfigurovaný v možnostiach smerovania. Pri výbere tohto druhu vzdialeného prístupu je potrebné, okrem vytvorenia tunelu, vybrať hashovací a dešifrovací protokol. Zároveň je potrebné vytvoriť overovací kľúč a pevne prideliť adresy, ktoré budú smerované a naviazané na tunel.
Špeciálnou variantou VPN je nastavenie vzdialeného prístupu pre zariadenia využívajúce systémy Android a iOS. Prevažne sa jedná o mobilné zariadenia, ktoré je možné napojiť na iné prostredníctvom NAT, preto neboli v tomto prípade použité. Princíp je však obdobný ako pri SSL VPN. Najskôr je potrebné prevziať aplikáciu, prispôsobenú operačnému systému, cez ktorú je sa možné, po nastavení prihlasovacích pravidiel, pripojiť na vzdialenú sieť. Pre optimálne zabezpečenie je zapnutá možnosť IP reputácie s pripojením na servery. Zároveň, z dôvodu nežiadúcich útokov je nastavené pravidlo na filtráciu komunikácie s Čínou, využívajúc funkciu geolokácie.

Postup, ako nastaviť niektoré z týchto krokov je uvedený v časti 7.3, zaoberajúcej sa topológiou, vytvorenou pre experimentálne overenie funkcií v laboratórnom prostredí.

6.3 Tipy pre zabezpečenie siete

V prípade zabezpečenia siete existuje množstvo Best Practice tipov, ktorými je možné sa riadiť. Avšak vždy je cieľom eliminovať úroveň ohrozenia pred útokmi, za cenu čo najnižšieho vplyvu na využiteľnosť a plynulosť sieťového toku. Základom je vždy minimalizovať neovplyvniteľné scenáre, ktoré nemožno kontrolovať, ani nijak

usmerňovať.

Doporúčané kroky pre zabezpečenie siete:

- Pri zapájaní topológie je potrebné klásť dôraz na minimalizáciu slabých (zraniteľných) sieťových prvkov. Jedná sa hlavne o malé switche, ktoré v prípade, že zhlukujú niekoľko staníc a sú napadnuté, prípadne inak ovplyvnené, sú schopné pripraviť o sieťové spojenie množstvo ďalších prvkov, zapojených do siete. Najvhodnejší, avšak nereálny, scenár je, aby bol každý prvok zapojený do osobnitného portu vo firewalle. Toto nie je možné dosiahnuť, preto je však optimálne zredukovať počet ostatných sieťových prvkov a vytvoriť záložnú cestu, ktorú by v prípade výpadku táto sieť mohla použiť.

- Prerozdeliť IP adresy. Za predpokladu, že pri návrhu siete sa počíta s tým, že budú pevne umiestnené počítače na konkrétnych miestach v sieti, je ideálne využiť statické pridelenie IP adries. V prípade, že sa využije protokol DHCP a IP adresy sú automaticky prideľované, vzrastá riziko využitia voľných adries, ako prostriedku k útoku. Rovnako podstatné je využiť faktu, že ak sú niektoré porty nepoužívané, je potrebné ich zakázať.

- Pred započatím nastavovania pravidiel je vhodné najskôr začať zákazom všetkých funkcií. Následná konfigurácia by potom pozostávala z povolenia potrebných funkcií. Jedná sa o spôsob nastavenia firewallu na default deny, spomínanom v časti 1.3.

- Pri stanovení pravidiel smerovania a filtrácie je dôležité, aby boli všetky prehľadne zdokumentované a vhodne popísané. Ak sa vo firewalle vyskytujú nastavené pravidlá, ktoré sú nepoužívané, je ich vhodné odstrániť.

- Dôležitým, avšak často opomínaným faktorom je informovanie a zaškolenie užívateľov ohľadom sieťovej bezpečnosti. Jedná sa hlavne o vysvetlenie možných scenárov, ktorými môžu byť napadnutí a zhrnutie základných spôsobov, akým im môžu predísť. Príkladom je ostražitosť voči podozrivým prílohám.

6.3.1 Best Practice NGFW Hillstone

Pri zabezpečení siete je dobré dbať na to, že množstvo pravidiel, ktoré boli vytvorené pre zabezpečenie siete, sa môžu navzájom prelínať. Avšak optimálnym riešením je vyhnúť sa globálnym pravidlám (príklad je smerovanie zdroj Any – cieľ Any) a vždy smerovanie upresňovať.

Overenie užívateľov – jednoduchý spôsob, akým obmedziť prístup na internet, okrem nastavenia adries, je vytvorenie užívateľských účtov, cez ktoré sa budú prihlasovať. Zjednodušuje to spôsob monitorovania činnosti a možnosti administrácie. Firewall Hillstone podporuje overovanie užívateľov lokálne a vzdialene. Vzdialené overenie využívajú RADIUS, AD, LDAP a TACACS+ protokoly. Preto je možné nakonfigurovať pre konkrétne služby server, na ktorom sa budú prístupy overovať. Postup nastavenia AAA serveru je vyobrazený v časti 6.3.2 a obdoba prihlasovania pomocou WebAuth je v popísaná v laboratórnej úlohe v záložke 7.3.6.

URL filter – pre kontrolu nad prehliadaním internetového obsahu je bežné použiť zaznamenávanie logov. V prípade záujmu o zrušenie prístupu na konkrétny server je možné nastaviť blokovanie na konkrétnu adresu, prípadne kľúčové slovo. Postup je možné nájsť v časti 7.3.3.

Email filter – ideálne využitie na zamedzenie prijímania správ z pochybných mailových účtov. Zároveň je možné kontrolovať a zaznamenávať údaje v emaili ako – zasielateľ, prijímateľ, obsah a prílohy. Postup nastavenia tohoto filtru je v časti 6.3.2.

Špecifický Web filter – prvou alternatívou je *Web Content* filter, zameraný na filtrovanie stránok s konkrétnym obsahom (napríklad nevhodné stránky obsahujúce násilie, hazard, alebo iné). Postup na vytvorenie takéhoto filtra je v časti 6.3.2. Druhou alternatívou je *Web Posting* filter, ktorý kontroluje, aké príspevky je možné pridať na web, na základe kľúčových slov (forma cenzúry).Postup je vyobrazený v časti 6.3.2.

QoS – konkrétne funkcia iQoS predstavuje možnosť pridelenia konkrétneho výkonu siete a šírky pásma pre špecifikovanú službu. Napríklad je možné nastaviť obmedzenie datového toku na sťahovanie súborov prostredníctvom ftp a maximalizovať UDP prenos pre aplikáciu Skype. Pre optimálne použitie tejto funkcie je dobré poznať priepustné vlastnosti vedenia. Postup je možné vidieť v sekcii 6.3.2.

DNS – výhodnou možnosťou je konfigurácia vlastného DNS serveru, čím sa zníži riziko útokov typu MITM, ktoré by mohli nastať pri pripájaní na vzdialený DNS server.

Antivírus – za predpokladu, že nie je nastavený na inej platforme, prípadne že by sa jeho funkcie neprekrývali s funkciami antivírového systému „druhej strany“, je vhodné nastaviť túto možnosť ako prevenciu pred rôznymi škodlivými súbormi. Spôsob nastavenia pravidiel pre antivírus je vyobrazený v časti 6.3.2.

Geolokácia – jedná sa o informačnú databázu, predstavujúcu rozpis útokov a ich zdrojový štát. Na základe toho možno určiť, s ktorou krajinou je dobré zakázať komunikáciu. Táto databáza je aktívna a jediný údaj, ktorý treba nastaviť je

aktualizovanie.

IP reputácia – databáza, zhromažďujúca údaje o konkrétnom správaní IP adries, na základe ktorých k nej bude v budúcnosti pristupovať. Príkladom je, že ak by prebiehal častokrát z konkrétnej IP adresy útok, tak do budúcnosti akákoľvek komunikácia je už predom zahadzovaná a stavia sa k nej ako k útočníkovi. Rovnako ako u geolokácie je potrebné pravideľne túto databázu aktualizovať.

Vzdialený prístup – ideálnym scénárom je, keď pre sieť nie je povolený žiaden vzdialený prístup. Avšak ak je potrebné tento prístup vytvoriť, tak je výhodou ho prideľovať pevne pre užívateľov, nad ktorých zariadením má správca siete plnú kontrolu. Nastavenie SSL VPN je možné uskutočniť podľa postupu v záložke 6.3.2.

Systém blokovania narušení – cieľom IPS je monitorovať sieťové útoky a zabrániť im. Jedná sa o formu ochrany pred rôznymi typmi útokov. Výrobcom odporúčané nastavenie je, mať túto funkciu neustále zapnutú. Dôvodom je aj neustále udržiavanie aktuálnej verzie databázy útokov. Nastavenie IPS je popísané v časti 6.3.2.

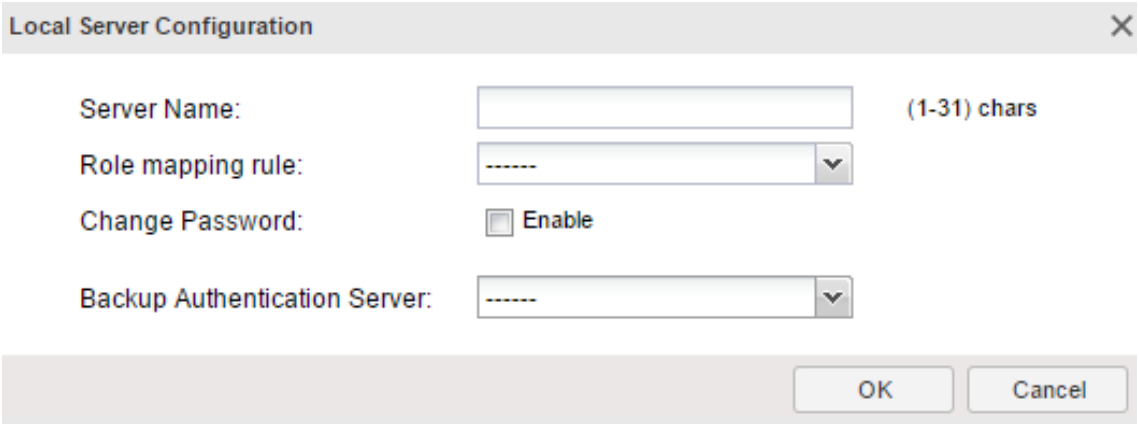
Attack Defense – jedná sa o systém ochrany pred najbežnejšími typmi útokov, ako je napríklad ICMP, UDP Flood, ARP Spoofing, SYN Flood ... Spustením tejto možnosti na ochranu siete sa automaticky stáva vytvorený profil aktívny a chráni sieť pred nežiadúcimi útokmi. Ochrana tejto kategórie spočíva v zabraňovaní vzorových a známych útokov, na základe už predom známej štruktúry. Nastavenie Attack Defense je možné vidieť v časti 6.3.2.

Firewall ponúka množstvo ďalších funkcií, avšak tieto sú spolu so základnou konfiguráciou hlavnými bezpečnostnými funkciami firewallu v sieti.

6.3.2 Nastavenie jednotlivých funkcií

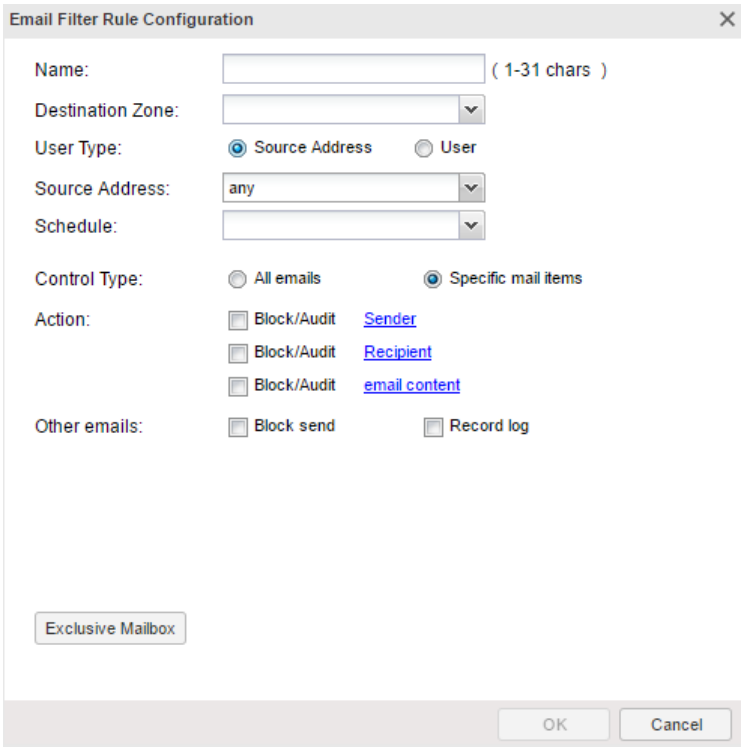
V tejto sekcii sú vyobrazené vzorové postupy pre nastavenie konkrétnych funkcií, spomínaných v predchádzajúcej časti.

Local AAA server. Vo WebUI je tento server možné nastaviť v záložke *Object/AAA Server>NEW>Local Server*. V záložke Role Mapping Rule je možné vybrať, aké pravidlo bude uplatnené pre ľudí, ktorý sa prostredníctvom tohoto serveru prihlásia. V prípade povolenia možnosti Change Password si môžu užívatelia zmeniť svoje prihlasovacie heslá. Možnosť Backup Authentication Server zasa predstavuje server, na ktorý sa presmeruje celá žiadosť o overovanie totožnosti, ak primárny server zlyhá. Na obrázku 6.2 je možné vidieť nastavenie jednotlivých funkcií.



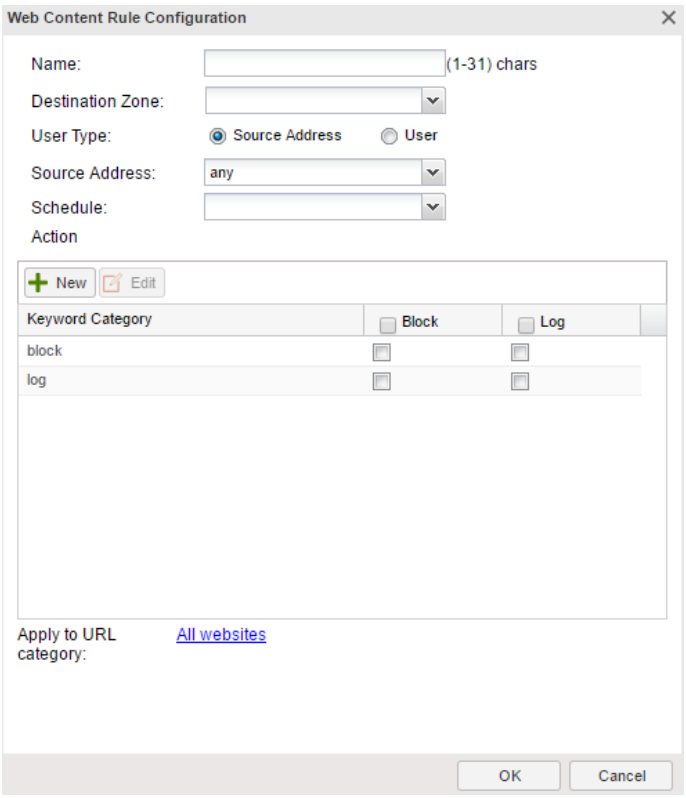
Obr. 6.2: Možnosti nastavenia lokálneho AAA serveru.

Email filter. V záložke *Policy/Internet Behavior Control/Email Filter>NEW* je možné vybrať, na aké zóny sa bude toto pravidlo vzťahovať, o aký časový úsek sa jedná, v možnosti Control Type je možné upresniť zasielateľa, prijímateľa a obsah mailu. V možnosti Exclusive Mailbox je možné nastaviť, o ktorý druh adresy sa bude jednať, prípadne o celú doménu, napríklad @gmail.com, ktorý je aj napriek zabezpečenej komunikácií možné kontrolovať. Tieto možnosti sú zobrazená na obrázku 6.3.



Obr. 6.3: Možnosti nastavenia filtru emailov.

Web Content. Kliknutím na *Policy/Internet Behavior Control/Web Content>Add* je možné vybrať, o aký druh filtrovania sa bude jednať. Princíp a forma nastavovania je rovnaká, ako pri URL filtry. Pričom čerpajú zo rovnakého zdroja informácií pri blokovaní, ako je vidieť na obrázku 6.4. Pre toto pravidlo je možné špecifikovať zdrojovú adresu, prípadne užívateľa, ako aj cieľovú zónu. V záložke schedule je možné vybrať, pre ktorý časový interval bude táto funkcia platiť. Kliknutím na položku NEW sa otvorí okno, v ktorom možno pridávať novú kategóriu slov s ich hodnotou dôveryhodnosti, na základe ktorej filtrácia prebieha. Zároveň je možné vybrať, aby firewall detekoval nielen doslovnú verziu daného nežiadúceho príspevku, ale aj slovné obmeny, ktoré by mohli byť použité. Po vytvorení tejto kategórie je následne možné vybrať, či komunikáciu blokovať, zaznamenávať, prípadne obe. V dolnej časti je možné vybrať, pre akú kategóriu stránok bude tento filter aktivovaný.

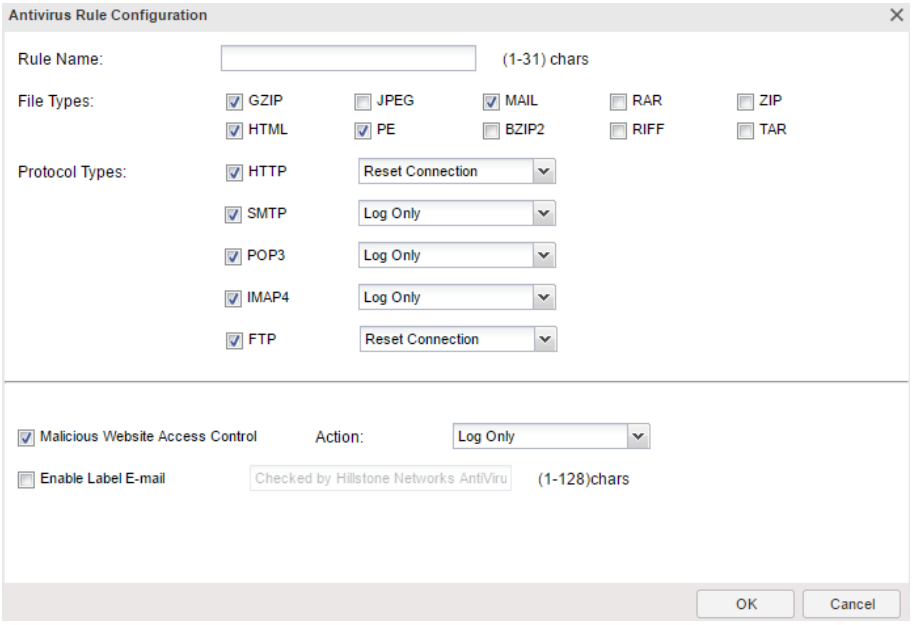


Obr. 6.4: Možnosti nastavenia filtru webového obsahu.

Web Posting. V záložke *Policy/Internet Behavior Control/Web Posting>NEW* je možné pridať filter rovnakým spôsobom, ako to bolo u Web Content filtru. Rozdiel medzi nimi je v tom, že jeden kontroluje obsah prezeraných stránok a druhý pridávanie príspevkov.

iQoS. Po preskúmaní sieťových možností je možné nastaviť iQoS zvolením *Policy/iQoS/Configuration*, v tejto položke je potrebné zvoliť *Enable iQoS*. Po tomto úkone je možné nastaviť jednotlivé „rúry“ (pipes), ako napríklad nastavením White Listu aplikácií, osobitné filtre na konkrétne rúry a podobne. Ďalej je možné vybrať, akým štýlom budú tieto rúry využívané. Jedná sa o obdobné nastavovanie pravidiel, ako pri iných filtráciách, pričom novou premennou je prenosová rýchlosť a množstvo povolených aplikácií.

Anti virus. Vo vytvorenej zóne (trust/untrust. . .) je po kliknutí na edit a zvolení kategórie *Threat Protection*, možnosť vybrať ochranu Antivirus. Po tomto úkone je v záložke *Object/Antivirus/Profile>NEW* možné pridať, o aký druh ochrany sa bude jednať a ako má s danými protokolmi a súbormi zaobchádzať. Tieto možnosti sú ukázané na obrázku 6.5. Konfigurácia obecného nastavenia antivíru je v záložke *Object/Antivirus/Configuration*, kde je možné definovať obecné správanie firewallu.

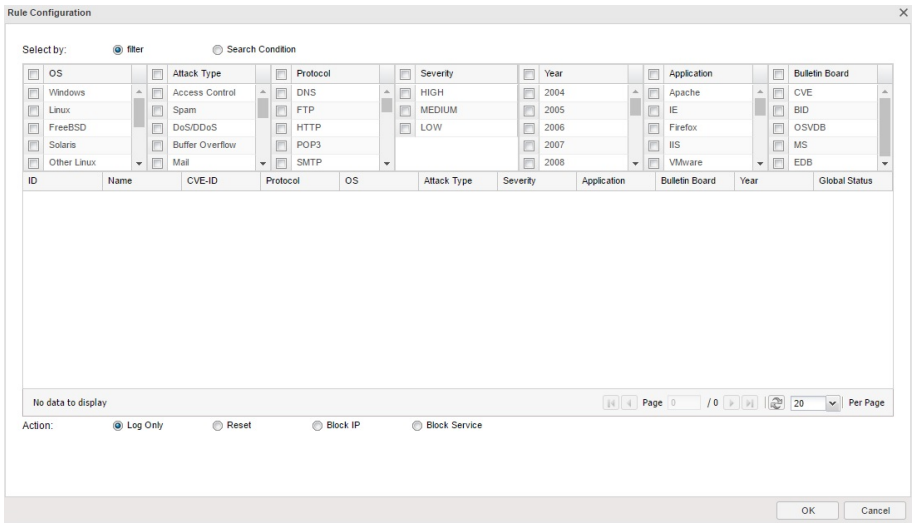


Obr. 6.5: Vytvorenie profilu pre antivírový systém.

SSL VPN. Po vytvorení užívateľa v záložke *Object/User*, je potrebné určiť VPN adresový priestor. To je možné urobiť v záložke *Network/VPN/SSL VPN> Address Pool*. Po určení konkrétnej IP adresy a vytvorení novej zóny je na rade spraviť tunel, ktorý sa pridáva v záložke *Network/Interface>NEW>Tunnel Interface*. Následne je potrebné vybrať profil užívateľa, ktorý sa prostredníctvom zabezpečeného programu bude prihlasovať do tejto siete. V záložke *Network/VPN/SSL VPN>NEW*. Tam je potrebné nastaviť AAA lokálny server, vybrať rozhranie a vytvorený tunel spolu s adresovým priestorom. V tunnel route je možné určiť IP adresu, ktorá musí byť z rovnakej podsiete, ako IP adresa na druhom interface. Následne je nutné, aby si vzdialený užívateľ prevzal program na prihlasovanie cez VPN Hillstone Secure Connect, ktorý je možno vidieť na obrázku 6.6, do ktorého sa prihlásil zadaním údajov z vytvoreného profilu.

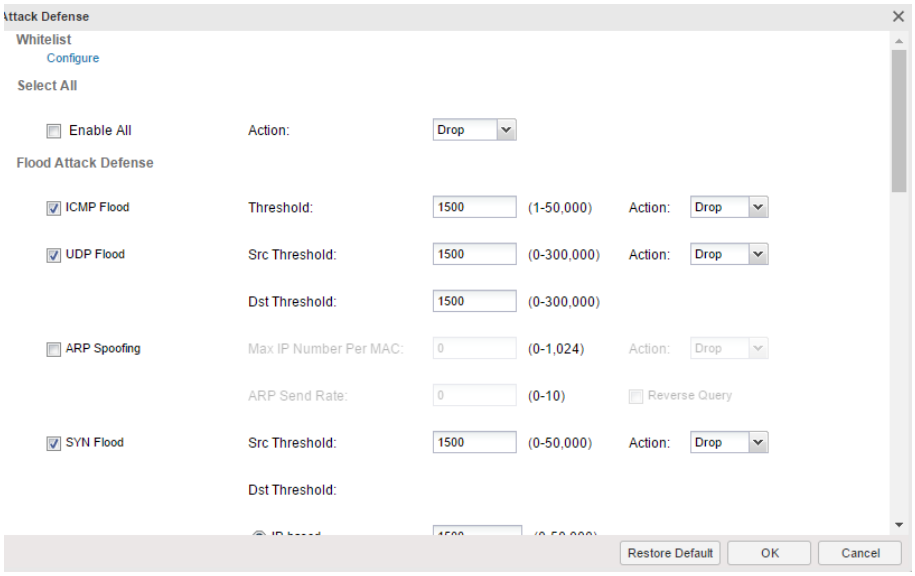
Obr. 6.6: Program Hillstone Secure Connect.

IPS. Pre nastavenie pravidiel IPS je nutné najskôr vytvoriť v záložke *Object/Intrusion Prevention System/Profile>NEW* profil, v ktorom budú tieto pravidlá definované. Opätovným kliknutím na tlačítko NEW sa naskytne možnosť pridať rozsiahly filter pravidiel, ako je ukázané na obrázku 6.7. Následne je možné vybrať, na aký typ útoku a od ktorej aplikácie/operačného systému/protokolu. . . sa pri kontrole sústrediť a ako ho vyhodnocovať. Najoptimálnejšie je prevziať IPS profil od prednastaveného Hillstone firewallu.



Obr. 6.7: Vytvorenie pravidla pre IPS profil.

Attack Defense. Zapnutie možnosti Attack Defense prebieha v rovnakej záložke ako nastavenie Antivírového programu. V konkrétnej zóne je potrebné v *Threat Protection* aktivovať Attack Defense, avšak pre zmenu nastavenia je potrebné kliknúť na Configure. V tomto zozname, viditeľnom na obrázku 6.8, je možné nastaviť, voči ktorým útokom sa má firewall brániť a po akom časovom intervale ich zahadzovať a podobne. Najvhodnejšie je nastaviť akciu drop na všetky nežiadúce útoky, bez ohľadu na ich vážnosť.



Obr. 6.8: Nastavenie Attack Defense ochrany.

6.3.3 Zhrnutie

Jednotlivé nastavenia zabezpečení majú aj pokročilé funkcie, na ktoré je však potrebná znalosť konkrétnych útokov a rozšírený prehľad o toku v sieti. Medzi ďalšie spôsoby ochrany je optimálne zaradiť aj monitoring, ktorý spočíva v kontrole toku a uchovávaní záznamov. Práve vďaka týmto záznamom je možné aplikovať nové pravidlá pre zabezpečenie siete.

7 NÁVRH LABORATÓRNEJ ÚLOHY

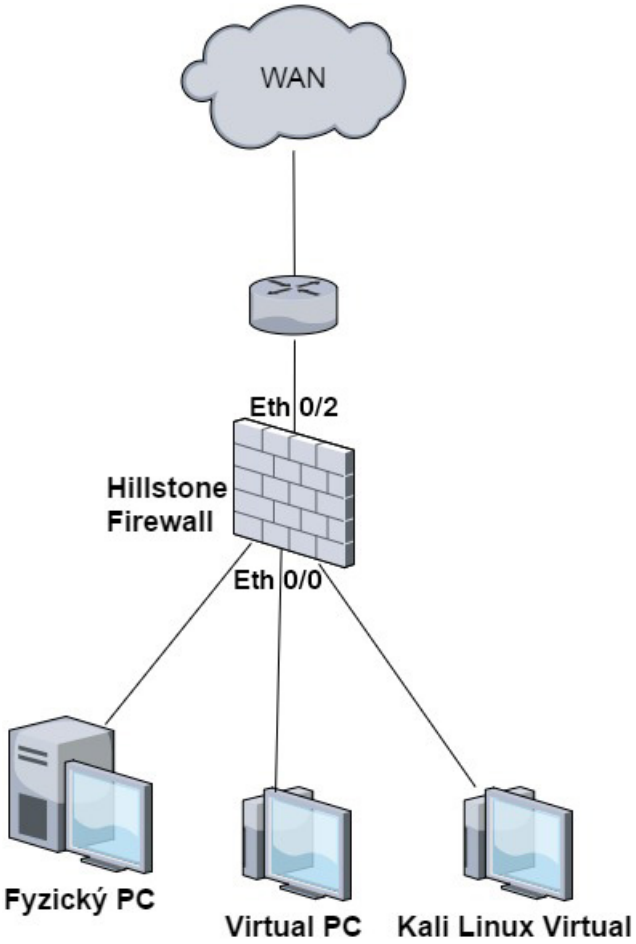
7.1 Úvod

V tejto laboratórnej úlohe bude cieľom predstaviť a overiť základné funkcie firewallu novej generácie od spoločnosti Hillstone. Hlavnou myšlienkou je vysvetliť dôležitosť bezpečnostného prvku firewall a popísať jeho využitie v sieťovej infraštruktúre v praxi. Študenti si vyskúšajú nastaviť a otestovať jednoduché pravidlá pre kontrolu a filtráciu v sieťovej infraštruktúre, využívajúcej zapojenie firewallu Hillstone (typ výrobku SG-6000-2120) ako ochranného prvku, medzi študentským stanoviskom PC a sieťou VUT, pripojenou pomocou služby poskytovanou ISP (Internet Service Provider) na internet.

7.2 Popis sieťovej topológie

V laboratórnej úlohe bude použitá sieťová topológia, zakreslená na obrázku 7.1. V sieti sa budú nachádzať prvky ako – Hillstone firewall, fyzický počítač, virtuálny počítač a virtuálny Kali Linux.

Firewall je na rozhraní eth 0/2 pripojený na WAN sieť VUT. Router na obrázku predstavuje sieťový prvok, ktorý prideľuje danému rozhraniu IP adresu s použitím DHCP. Na eth 0/0, ktorého IP adresa je 192.168.1.1, je pripojený fyzický počítač. Na tento fyzický počítač sú pomocou bridge módu programu VMWare pripojené oba virtuálne stroje. Na úlohu bude využitý rozsah IP adries pre rozhranie eth 0/0 od 192.168.1.2 až 192.168.1.4. Tieto adresy budú automaticky pridelené protokolom DHCP. V rámci pripojenia na WAN bude kladený dôraz na 3 webové servery, ktoré sú www.seznam.cz, www.zoznam.sk a www.facebook.com. Každý z nich bude mať v úlohe nastavené rozdielne filtračné pravidlá. Konfigurácia bude prebiehať na fyzickom počítači, virtuálny bude slúžiť ako počítač, predstavujúci zamestnanca vo firme, ktorého prístup na internet bude overovaný pomocou užívateľského konta. Virtuálny stroj Kali Linux bude použitý na DoS útok v rámci internej siete. Pri zapájaní kabeláže je vhodné, v prípade výskytu viacerých sieťových kariet na PC, odpojiť ostatné sieťové káble a ponechať len tie, potrebné na danú topológiu.



Obr. 7.1: Schéma zapojenia laboratórnej úlohy

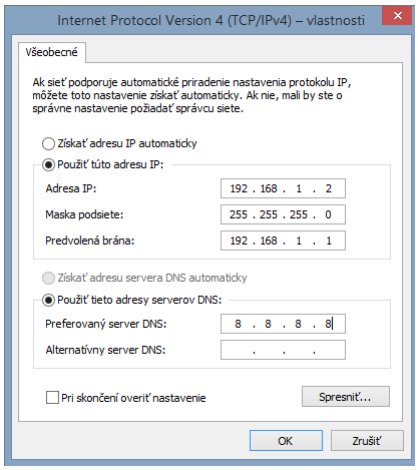
7.3 Pracovný postup

Po prepojení sieťových rozhraní podľa popisu zapojenia na obrázku 7.1, možno začať so samotnou konfiguráciou laboratórnej úlohy. Konfiguráciu vždy začíname na firewalle, ktorý bol uvedený do stavu továrenského nastavenia konfigurácie (default configuration). V tomto stave je možné sa na rozhraní eth 0/0 pripojiť a začať s nastavovaním. Na eth 0/0 je nastavená IP adresa 192.168.1.1, pričom rovnaká adresa je aj url pre užívateľské rozhranie v internetovom prehliadači.

7.3.1 Nastavenie spojenia pre administráciu

Pred úpravou sieťových adaptérov overíme, či na firewalle indikujú LED diódy na prípojených ethernet moduloch, že prebieha komunikácia. V prípade, že tomu tak nie je a diódy neblikajú, je potreba firewall reštartovať. Nasledovné nastavenie prebieha na fyzickom počítači a vyžaduje práva na úpravu týchto rozhraní. Po úspešnom

zapojení je možné prejsť na konfiguráciu IP adresy pre sieťový adaptér počítača, pripojeného na rozhraní eth 0/0. Otvoríme *Ovládacie panely>Sieť a internet>Centrum sietí>Zmeniť nastavenie adaptéra*, vyberieme príslušný Ethernet adapter, klikneme pravým a zvolíme *Vlastnosti>TCP/IPv4* a nastavíme adresu, ktorá zodpovedá adrese podsiete preddefinovanej na rozhraní eth 0/0. Pre tento prípad zvolíme napríkad 192.168.1.2/24, bránu nastavíme na 192.168.1.1 a využijeme DNS server 8.8.8.8 od spoločnosti Google. Nastavenie podľa obrázku 7.2.



Obr. 7.2: Nastavenie sieťového adaptéra.

Po nastavení adaptéru sa pripojíme na užívateľské rozhranie firewallu pomocou internetového prehliadača (odporúčané je použiť Google Chrome) zadaním adresy *https://192.168.1.1* (dôležité je použiť protokol https!). Po načítaní sa môže zobraziť stránka, informujúca o nezabezpečenom pripojení. Tú v rozšírených nastaveniach odklikneme a zvolíme pokračovať napriek riziku, pričom sa následne načíta stránka na prihlásenie.

Prihlasovacie údaje:
Login – **hillstone**
Password – **hillstone**

Po prihlásení si prezrite obsah úvodnej obrazovky spolu s vrchným menu.
Pre pripojenie cez telnet, využívajúc programu Putty, je potrebné túto možnosť nastaviť v otvorenom webovom rozhraní v záložke *Network/Interface/Ethernet 0/0*, kliknutím na edit a zaškrtnutím *Management>Telnet* je táto možnosť aktivovaná.

7.3.2 Zriadenie internetového pripojenia

Nastavenie rozhraní firewallu

Pre správne fungovanie internetového spojenia je potrebné najskôr zvoliť rozhranie, na ktorom sa bude nachádzať WAN. Tento krok prebieha po pripojení sa z fyzického počítača, prostredníctvom internetového prehliadača, na užívateľské rozhranie. Vo WebUI firewallu, v položke *Network/Interface/Ethernet 0/2*, je po kliknutí na Edit možné zvoliť:
Description: WAN (dobrovoľný údaj, nie je potrebné uvádzať)
Binding Zone: Layer 3 Zone
Zone: untrust
IP Configuration: DHCP
A možnosť Set gateway information from DHCP server as the default gateway route

Nastavenie zásad

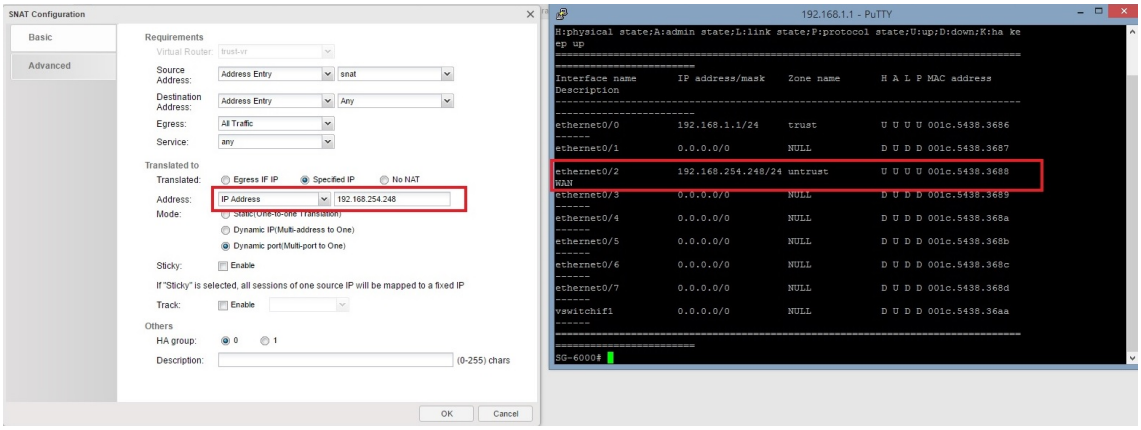
Následne je potrebné nastavenie „bezpečnostnej zásady“ (security policy), ktorá je využívaná, ako pravidlo a spôsob smerovania toku v sieti. V záložke *Policy/Security policy>NEW*, zdrojovou zónou je dôveryhodná LAN sieť (*source – zone/trust*) a cieľovou je nedôveryhodná WAN sieť (*destination – zone/untrust*), ostatné možnosti ostávajú na „Any“ a Action je zakliknutá voľba Permit. To znamená, že všetky služby, ktoré sú smerované z internej siete na internet sú povolené.

Nastavenie SNAT

Ďalším krokom je nastavenie prekladania adries, za ktorého účelom bude použitý SNAT (Static Network Address Translation). Preto treba najskôr vytvoriť adresu v záložke *Object/Address entry>NEW*.
Meno: snat
Member: IP/Netmask – 192.168.1.0 / 24

A v záložke *Policy/NAT/SNAT>NEW* je potrebné túto adresu zadať ako zdrojovú – Source Address - Address Entry – snat (názov vytvorenej adresy). *Translate to* je potrebné nastaviť na preklad adresy, ktorú pridelilo DHCP pre port eth 0/2 napojený na WAN. Túto adresu možno zistiť pripojením na telnet pomocou Putty (prihlasovacie údaje aj IP adresa sú rovnaké ako na WebUI) a zadaním príkazu v exec móde *show interface*, prípadne v karte *Network/Interface*. Postup je vyobrazený na obrázku 7.3. Po zadaní IP adresy je potrebné nastaviť možnosť Dynamic port (Multi-port to One). V záložke Advanced zároveň potvrdiť možnosť NAT Log, aby bolo možné prezerať záznamy o prekladoch adries.

Zároveň v *Monitor/Log/Log Management* je potrebné zvoliť u všetkých záložiek (Event až Threat) možnosť Enable.



Obr. 7.3: Postup nastavenia SNAT.

Nastavenie DNS

Tento krok je skôr overením správnosti prevzatia DNS serveru cez DHCP klienta na rozhraní. V záložke *Network/DNS* by mali byť viditeľné prevzaté DNS servery cez DHCP pre ethernet 0/2. Jedným z nich je DNS server 8.8.8.8 . Avšak ak sa tam tento server nenachádza, je nutné ho manuálne pridať.

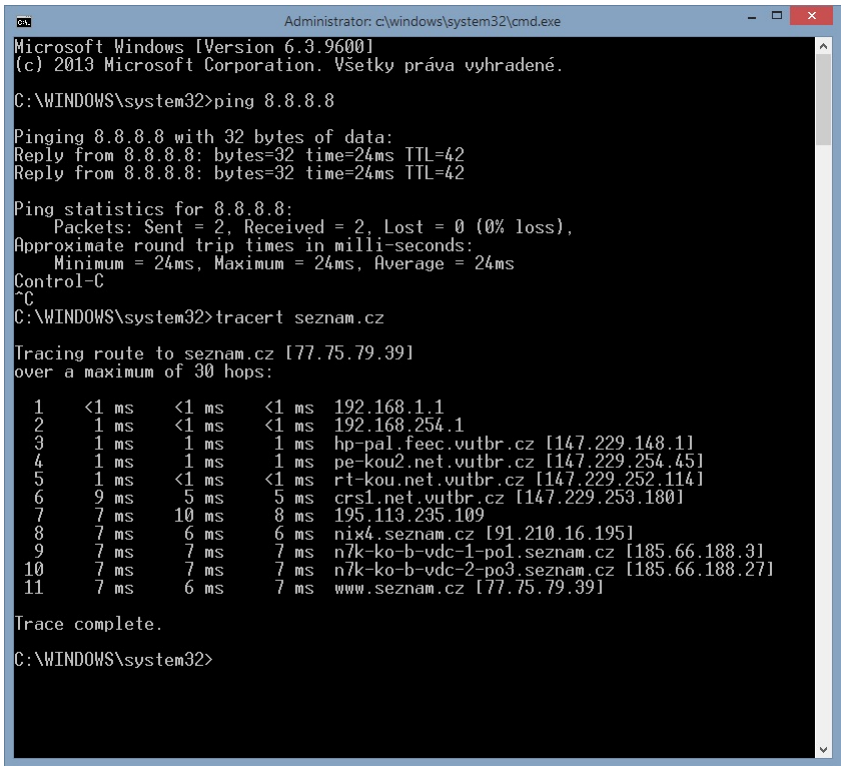
Nastavenie smerovania

Ďalšie overenie prevzatých údajov zo serveru DHCP, kde v záložke *Network/Routing/Destination Route* sa nachádza možnosť, kde je zo zdroja 0.0.0.0/0 smerovaný tok na podsieť DHCP (jedná sa o školskú podsieť 192.168.254.1). V prípade, že nebola automaticky pridelená z DHCP, je potrebné túto možnosť smerovania pridať manuálne.

Overenie pripojenia

Po správnom prevedení týchto krokov, je pripojenie na internet pre fyzický počítač spojazdnené. To možno overiť otvorením príkazového riadku (CMD) a pingom na adresu napríklad 8.8.8.8. Príkazový riadok na danom fyzickom počítači je možné spustiť stlačením kombinácie kláves *Win+R* a následným napísaním cmd. Po potvrdení sa táto funkcia spustí a je možné ping otestovať. Druhou možnosťou je otvorenie webového prehliadača a pripojenie sa na ľubovoľné stránky, využívajúcej protokol http://. URL využívajúce zabezpečený protokol https, využívajúci hsts bezpečnostný prvok, ktorý vyhodnocuje zraniteľnosť pripojenia, nie je v aktuálnom stave možné otvoriť. V CMD je zároveň možné, pomocou príkazu *tracert*, sledovať

nastavené smerovanie. Na obrázku 7.4 je možné vidieť, že najskôr je zaslaná požia-



Obr. 7.4: Zachytenie priebehu smerovania príkazom tracert.

davka na bránu, potom na nastavenú podsieť z predchádzajúceho bodu, následne už na sieť VUT, až cez ISP na WAN a k serveru stránky.

Prezeranie záznamov

Povolené Logy z prekladu adries je možné následne skontrolovať v *Monitor/Log/NAT*. V zaznamenaných logoch je možné vidieť prekladanie adries pomocou SNAT z lokálnej (Source IP) na nastavenú adresu pre WAN port (Transated IP). Zároveň je možné si prezrieť aj destination IP, na ktorú bol tento preklad smerovaný. Tieto záznamy možno porovnať so vzorovými, na obrázku 7.12, v sekcii s výsledkami.

Nastavenie DHCP

Pre nastavenie DHCP, ktoré bude prideľovať adresy aj lokálnemu, aj virtuálnemu PC, je potrebné zvoliť v záložke *Network/DHCP>NEW DHCP server*:

Basic

interface: eth0/0

Gateway: 192.168.1.1

Netmask: 24

DNS 1: 8.8.8.8

DNS 2: 8.8.4.4
Address Pool
Start IP: 192.168.1.2
End IP 192.168.1.4

Následne je možné v nastaveniach adaptéru vo fyzickom PC prepnúť z možnosti statickej IP na prevzatie dynamickej pomocou už nastaveného DHCP. Pre overenie, že táto zmena prebehla, je vhodné v CMD zadať príkaz *ipconfig /release* a následne *ipconfig /renew*. Overenie tejto zmeny sa uskutoční príkazom *ipconfig*.

7.3.3 Určenie filtrovacích pravidiel

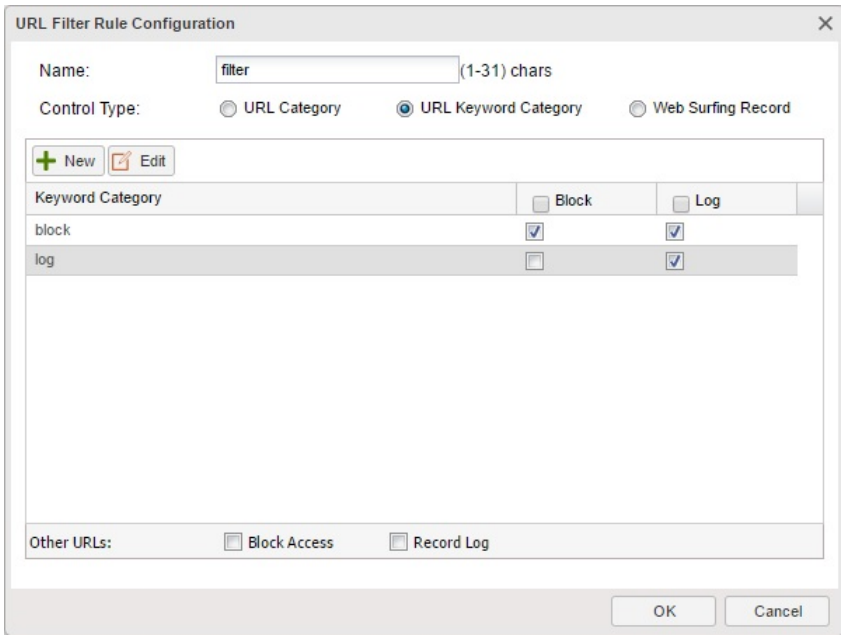
Na tieto účely bude použitý URL filter. Jeho úlohou je kontrola a filtrácia komunikácie, ako aj vedenie záznamov o uskutočnení danej činnosti na základe zadanej URL adresy.

Nastavenie filtrácie

V tomto bode je predstaviteľom pripojenia na internet server www.seznam.cz. Druhú kategóriu internetového pripojenia tvoria servery www.zoznam.sk a www.facebook.com. Pričom server facebook.com využíva pripojenie pomocou protokolu https. Pre obe kategórie budú nastavené iné pravidlá.

Nastavenie prebieha v záložke *Object/URL Filter>NEW*. Po zvolení možnosti *URL Keyword Category* sa otvorí panel na vytvorenie vlastného zoznamu stránok. Kliknutím na NEW sa otvorí možnosť, v ktorej prvý názov je Category: block a kliknutím na NEW sa otvorí možnosť pridať keyword, do ktorého príde postupne zoznam.sk (potvrdí sa tlačítkom Add) a opätovným stlačením NEW aj stránka facebook.com. Po potvrdení všetkého, je možné vo výslednom menu zvoliť, či z tejto kategórie chce administrátor komunikáciu blokovať, alebo zaznamenať. Opätovným kliknutím na new a vytvorením novej kategórie s názvom Category: log, je posledným krokom pridaná adresa seznam.cz. Po potvrdení je v konfiguračnom menu URL filtra možné určiť, ktorej kategórií prináleží ktorá činnosť. Podľa obrázku 7.5 je vhodné zvoliť pre kategóriu block (obsahujúcu domény zoznam.sk a facebook.com) block a log, pre kategóriu log (obsahujúcu doménu seznam.cz), zasa možnosť log.

Pre aktivovanie filtra je potrebné upraviť nastavenú security policy, zvoliť v nej možnosť *Protection/URL Filter* a vybrať vytvorený profil.



Obr. 7.5: Kategórie v URL filtri.

Prezeranie logov

Záznamy, ktoré sme zvolili, sa po pokuse o pripojenie na dané adresy vedú v *Monitor/Log/URL*. Je možné nastaviť aj možnosť monitorovania všetkých URL adries upravením nastavenia už vytvoreného URL filtra a v dolnej časti potvrdením možnosti Other URLs: Record Log.

7.3.4 Povolenie protokolu HTTPS

Pre pripojenie internetového prehliadača na stránky, ktoré využívajú protokol https, je potrebné vygenerovať certifikát, ktorý túto činnosť povolí. V tejto časti je ukázané, ako povoliť toto pripojenie, ale aj ako ho dešifrovať.

Nastavenie SSL profilu a zásad

Prvým krokom je vytvoriť nové pravidlo, ktoré bude predstavovať konfiguráciu pre šifrovanie a dešifrovanie. To sa nastaví v *Policy/SSL Proxy>NEW*, Name: profil, ostatné položky ostávajú rovnaké, ostáva len potvrdiť. Následne je potrebné SSL Proxy aktivovať v už existujúcej zásade. Upravením už vytvorenej bezpečnostnej zásady (security policy) v záložke Options je potrebné povoliť *SSL Proxy* a vybrať vytvorený profil.

Vloženie certifikátu

Aby bolo možné uskutočniť pripojenie na stránky, využívajúce protokol https, je potrebné vložiť do prehliadača certifikát, ktorým sa táto zabezpečená komunikácia umožní. Vygenerovanie certifikátu sa dosiahne cez *System/PKI/Management*, doména – trust_domain_ssl_proxy_2048 (ak bol v nastavení profilu použitý modulus 2048) a Action – export. Po potvrdení sa stiahne daný certifikát do zložky v počítači.

V prehliadači Google Chrome je potom potrebné otvoriť Nastavenia>Rozšírené nastavenia a v časti HTTPS/SSL vybrať *Spravovať certifikáty...*. Následne v položke Dôveryhodné koreňové certifikačné autority Importovať tento prevzatý certifikát. Je potrebné ho importovať do danej zložky a potvrdiť. Úspešnosť tohoto importu je možné overiť znovuotvorením zoznamu certifikátov a rozkliknutím SG-6000, nesmie tam byť žiadna chybová hláška, ani upozornenie.

V zóne untrust, v záložke *Network/Zone* je potrebné povoliť Application Identification, zároveň je vhodné skontrolovať, či je zvolená aj položka WAN Zone. Ukončením týchto krokov je možné pripojiť sa na stránky využívajúce protokol https, pričom by sa mal aj spätne aktivovať vytvorený URL filter na už prístupnú (avšak blokovanú) stránku facebook.com.

Prezeranie logov

Možnosť preskúmania logov, ktoré boli v tejto časti vedené na základe povoleného dešifrovania komunikácie, sa aktivuje v *Monitor/Monitor Configuration* a povoliť možnosť Application monitor. V prípade záujmu je možné povoliť aj ostatné možnosti monitoringu a prezrieť si ich. Získané záznamy sa zobrazia v *Monitor/Application/Application Details*, pod záložkou HTTPS.

7.3.5 Zamedzenie sťahovania exe súborov

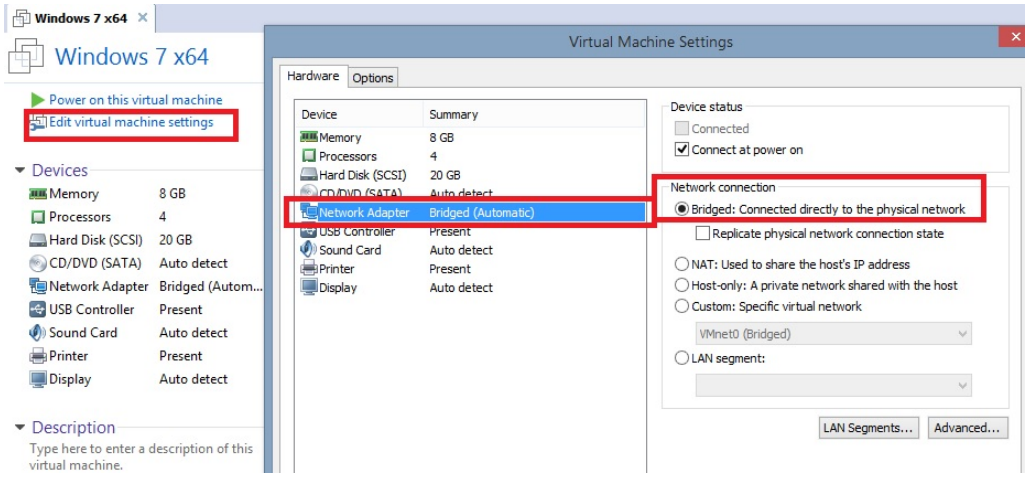
Jednou z možností, ako zabezpečiť sieť pred bežným šírením vírusov, je jednoduchý zákaz prevzatia toho konkrétneho formátu, ktorý nám príde nebezpečný.

Samotný postup k vytvoreniu tohoto zákazu je vytvorenie kontroly nad preberaním v záložke *Policy/Internet Behavior Control/HTTP/FTP Control>NEW*. Tu je možné meniť pravidlá pre prijímanie a odosielanie súborov pomocou FTP protokolu, ako aj kontrolu nad HTTP protokolom. Avšak v tejto časti je dôležitá práve položka Block HTTP downloads a prípona .exe. Destination Zone je potrebné zvoliť ako untrust a názov: zákaz.

Teraz je možné skúsiť v prehliadači na internete vyhľadať ľubovoľný .exe súbor a presvedčiť sa o funkcii tohoto pravidla.

7.3.6 Pripojenie viacerých užívateľov

Táto časť využíva zapojenie virtuálneho počítača formou bridge pripojenia cez program VMWare. Preto je potrebné pred spustením virtuálneho stroja overiť, že jeho sieťový adaptér je nastavený na možnosť bridge. Postup nastavenia, ako je znázornené na obrázku 7.6, je nasledovný. Po spustení programu VMWare je nutné vybrať virtuálny stroj a kliknúť možnosť editovať. Následne medzi možnosťami vybrať Network Adapter a ako formu pripojenia zvoliť Bridged Connection. Táto forma napojenia spôsobí, že hillstone detekuje tento počítač ako osobitne pripojený, čo znamená, že mu DHCP pridelí vlastnú IP adresu, s ktorou je možné pracovať.



Obr. 7.6: Nastavenie sieťového adaptéra VMWare, bridge-mode.

Cieľom tejto časti je dosiahnuť zabezpečenia siete, v ktorej topológii reprezentuje fyzický počítač administrátora s pevným prístupom na internet. Virtuálny počítač reprezentuje užívateľa, ktorý má prístup obmedzený časovo a návšteva stránok je podmienená autentifikáciou užívateľa (prihlásením s jedinečným menom a heslom).

Vytvorenie konta Prvým krokom je vytvorenie konta pre užívateľa, pod ktorým sa potom neskôr bude prihlasovať. Tento krok sa robí v záložke *Object/User>NEW>User*:
Name: **uzivatel**
Password: **heslo**
Následne je potrebné heslo opätovne potvrdiť.

Ďalším krokom je spustenie virtuálneho stroja a zistenie jeho IP adresy (overenie správneho premostenia sietí a funkcie DHCP). Táto adresa bude použitá pri vytváraní pravidiel pripájania. Najskôr je však potrebné túto adresu vytvoriť v zozname *Object/Address Entry>NEW*:

Name: virtual
IP/Netmask: jeho IP adresa/32
Description: DHCP adresa virtuálneho PC (nepovinné, len informačné)

Zároveň je potrebné ostatné adresy z DHCP poolu dať do druhého adresára. To znamená kliknúť na NEW a adresy z DHCP poolu, okrem tej pridelenej virtuálemu stroju, pridať do novej podmnienky s názvom adresy-permit. Napríklad ak by mal virtuálny stroj IP adresu 192.168.1.2, tak by v prvej adrese s názvom virtual figuroval len on s maskou 32 a v druhom novom adresári s názvom adresy-permit by boli v tomto prípade 192.168.1.3/32 a 192.168.1.4/32. Príklad tohoto nastavenia je znázornený na obrázku 7.7.

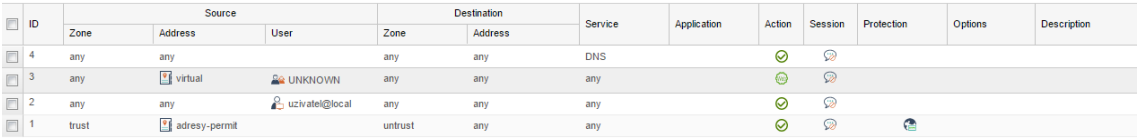
Obr. 7.7: Vytvorenie adries v poli adresových vstupov.

Nastavenie overenia prístupu

V záložke *Network/Authentication Management* je po kliknutí na WebAuth Wizard potrebné odkliknúť všetky možnosti, čím sa vytvoria nové zásady v security policy. Tie je potrebné upraviť a síce:

- pôvodnú zásadu smerovania, označenú číslom 1 upraviť, aby zdrojová(source) adresa bola Address: adresy-permit (zoznam DHCP adries okrem adresy virtuálneho stroja)
- v novovytvorenej zásade s číslom 2 pridať do Source/User:uzivatel
- v zásade číslo 3 vybrať Source address: virtual

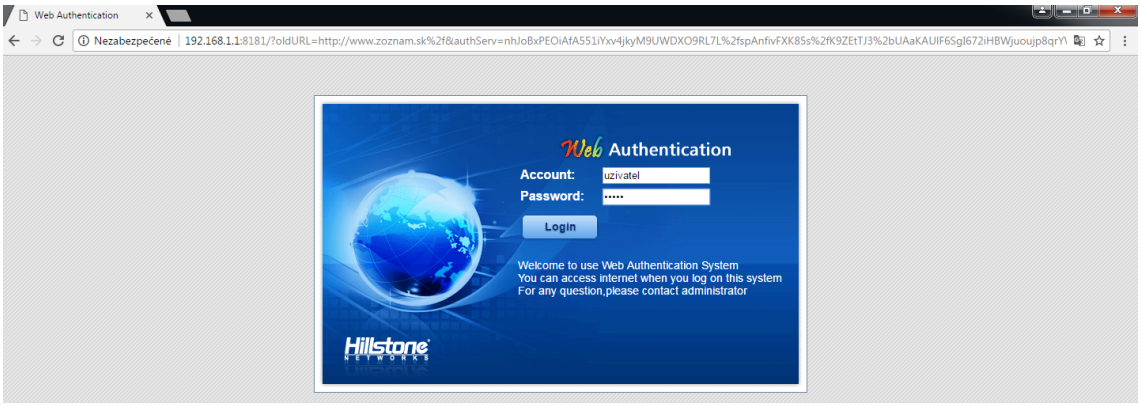
Výsledok by mal zodpovedať obrázku 7.8, pričom je potrebné správne nastaviť adresy, ktoré boli pomocou DHCP pridelené. Aktivovanie tejto funckie možno overiť



Obr. 7.8: Zásady overenia užívateľa.

zapnutím prehliadača na virtuálnom počítači. Po pokuse o pripojenie, napríklad na stránku seznam.cz, si firewall zažiada overenie identity daného užívateľa prostredníctvom prihlasovacích údajov. Po ich zadaní (uzivatel/heslo) sa povolí prístup na internetové stránky. Zároveň sa „práca“ tohto užívateľa zaznamenáva osobitne v

logoch a monitoroch prostriedkov. Napríklad v záložke *Dashboard* je možné v štatistikách užívateľov vidieť, že sa tento účet zaradil medzi užívateľov, akými sú ostatné IP adresy. Prihlasovanie sa spustí cez WebAuth funkciu vo webovom prehliadači, ako je vypísané na obrázku 7.9.



Obr. 7.9: Overenie užívateľa vo webovom rozhraní.

7.3.7 Časový harmonogram

Ďalšou z možností, ktorá je k dispozícii na obmedzenie prístupu pre interných užívateľov, je možnosť nastavenia takzvaného rozvrhu. Tento rozvrh je časovým rozpisom, ktorý povoľuje danú funkciu v daný moment. To znamená, že užívateľom možno povoliť prístup na internet napríklad len v pracovných hodinách.

Táto funkcia sa nastaví v záložke *Object/Schedule>NEW* a kliknutím na Add pridať nové možnosti:
Name: pracovny cas
Type: Days , v tejto možnosti je optimálne vybrať pracovné dni
Start Time: 8:00 End Time: 18:00

Zároveň je potrebné túto možnosť pridať aj v Security Policy, zabezpečujúcej prístup na Internet pre užívateľov (ID 1). Pri editovaní v záložke Options vybrať Schedule: pracovny cas. Je možné tento čas upraviť ľubovoľne a otestovať, či toto pravidlo funguje, aj keď je tento čas nastavený na nočné hodiny (v tom prípade by prístup na internet nemal fungovať).

7.3.8 DoS útok

Na overenie detekcie útokov bude v tejto časti použitý virtuálny PC, obsahujúci OS Kali Linux, spustený ceze VMWare. Tento počítač bude pripojený na firewall cez

Bridge mód adaptéru. Využitý bude fakt, že IP adresa, ktorá mu bude priradená cez DHCP, je už po predchádzajúcich krokoch zaznamenaná v zozname povolených adries. Po zapnutí virtuálneho stroja a následnom prihlásení (Login: *root*; Pass: *toor*), je potrebné overiť, či si túto IP adresu naozaj prevzal. Po otvorením terminálu (pravý klik na plochu>Open Terminal) stačí zadať príkaz *ifconfig*. Keď sa adresa zhoduje, je možné prejsť na samotnú prípravu útoku.

Inštalácia programu

V spustenom termináli je potrebné zadať príkaz *ls*, ktorý zobrazí obsah súborov v danom adresári. Dôležitý je výskyt priečinku **pentmenu**, ktorý je potrebné pridať, ak sa tam nenachádza. Na obrázku 7.10 je ukázaný výpis súborov, obsahujúci súbor pentmenu.

Obr. 7.10: Výpis súborov príkazom ls.

Pridanie sa uskutoční zadaním príkazu do terminálu:
git clone https://github.com/GinjaChris/pentmenu.git
Tento príkaz prevezme súbory z danej adresy a uloží ich do aktuálne otvoreného adresára. Po ukončení preberania je tento súbor už vo výpise (overenie príkazom ls).

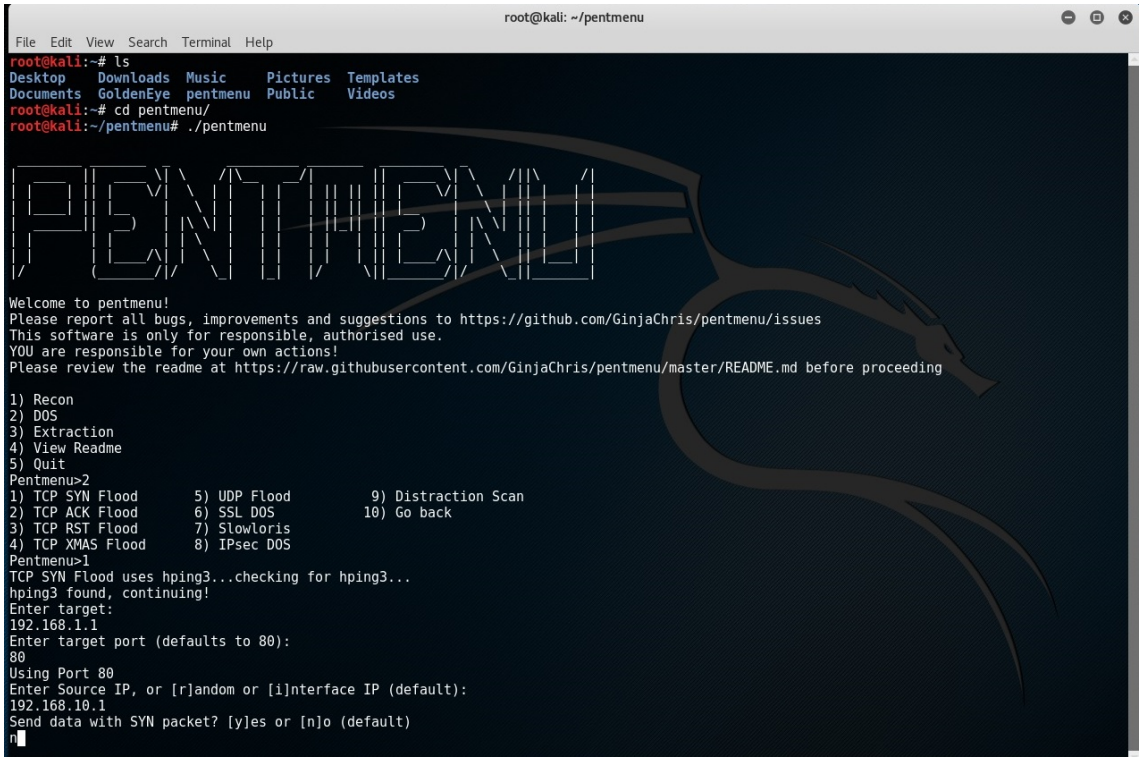
Nastavenie detekcie hrozieb

Pred spustením útoku je potrebné nastaviť možnosť detekovania hrozieb na konkrétnej zóne. V hillstone záložke *Network/Zone>trust* je potrebné pridať v *Threat Protection> Itrusion Prevention System a Attack Defense*. Následne je vhodné otvoriť iCenter, prípadne Dashboard a počkať na výsledky z útokov.

Spustenie útoku

Program, nainštalovaný na Kali Linux, spúšťajúci útok sa otvorí v termináli príkazmi:
cd pentmenu/
./pentmenu
Po vypísaní menu je na položke 2 DOS útok. Toto číslo je zvolené zápisom 2 a potvrdením v termináli. Následne zvolíme možnosť 1, predstavujúcu TCP SYN Flood. Po tomto úkone si program vypýta údaje ako:

Enter target: **192.168.1.1**
Enter target port: **80**
Enter Source IP :**192.168.10.1**
Send data with SYN packet: **n**
Na obrázku 7.11 je vyobrazený spôsob zadávania údajov.



Obr. 7.11: Nastavenie DOS útoku.

Význam údajov je, že útočník 192.168.10.1, za ktorého sa aktuálne vydáva, útočí na adresu 192.168.1.1 s portom 80. Jedná sa o útok zahltenia požiadavkami TCP SYN. Útok sa ukončí klávesou *Ctrl+c*.

Zhrnutie útoku

Výsledky zachovania sa firewallu voči útoku je možné prezrieť v záložke Dashboard, kde je vypísaná úroveň hrozby spolu s množstvom útokov a na pravej strane je TOP 10 útokov (zoradené podľa úrovne ohrozenia), kde destination IP je zadaná 192.168.1.1 . V záložke iCenter je podrobnejší popis útoku spolu so zdrojovou adresou útočníka. Táto adresa je v programe nastavená, aby sa predstavila ako 192.168.10.1. Najpodrobnejší popis správania firewallu je možné nájsť v logoch *Monitor/Log/Threat*, kde je po rozkliknutí konkrétneho útoku vypísané ako dlho prebiehal, čo upozornilo firewall na toto nebezpečie a ako sa zachoval (drop).

Zároveň bolo možné si počas uskutočňovania útoku všimnúť vyťaženie rozhrania eth 0/0.
Sumarizáciu útokov je možné nájsť v sekcii 7.4.1 obsahúcujej výsledky.

7.3.9 Uvedenie firewallu do stavu pôvodnej konfigurácie

Po dokončení úlohy je potrebné sa prihlásiť prostredníctvom programu Putty cez Telnet na ip adresu 192.168.1.1. Po zadaní hillstone prihlasovacích údajov, v exec móde zadať príkaz **unset all**, ktorý resetuje konfiguráciu firewallu, ktorý tak môže byť pripravený na ďalšiu úlohu. Zároveň je po vyzvaní potrebné odsúhlasiť zmazanie konfigurácie a povoliť reštart.

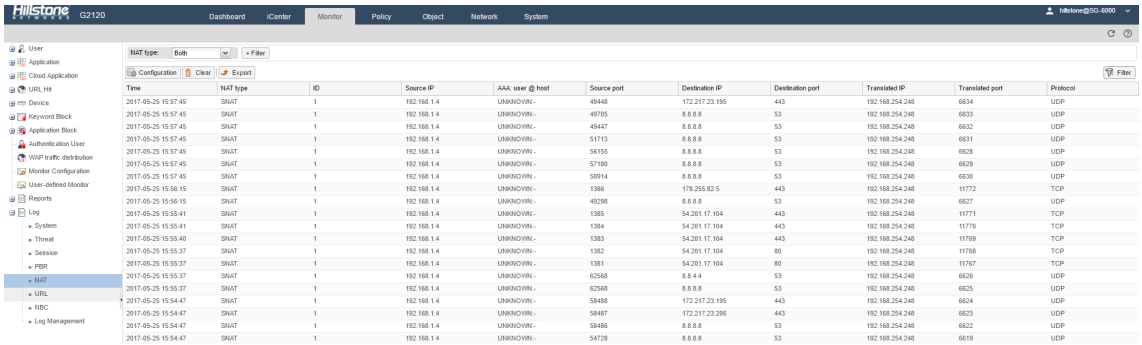
Následne je potrebné **odstrániť pridaný certifikát** v prehliadači Google Chrome. Jeho umiestnenie bolo zvolené v postupe úlohy a názov je SG-6000.

7.4 Záver

V tejto laboratórnej úlohe mal študent za úlohu vyskúšať a overiť základné a pokročilé funkcie firewallu Hillstone. Zároveň mal prakticky overiť správanie firewallu pod útokom zo strany užívateľa (DOS). Cieľom bolo študentovi priblížiť dôležitosť firewallu a spôsob jeho využitia v praxi.

7.4.1 Výsledky

- V prvej časti s názvom Nastavenie SNAT, mal študent za úlohu zhotoviť funkčný preklad adries, jeho funkciu si je možné prezrieť v záznamoch o činnosti NAT. Tu by mali výsledné logy vyzerať ako na obrázku 7.12.



Obr. 7.12: Záznam statického prekladu adries.

- V druhej časti, zaoberajúcej sa nastavením filtrovacích pravidiel je možné pozorovať v logoch správanie URL filtra, ako v prílohe na obrázku B.1. Zo záznamov možno vidieť, kto sa pokúšal pristúpiť na danú stránku a akou zásadou bolo k tejto žiadosti pristúpené.
- V tretej časti, v ktorej úlohou bolo povolenie protokolu HTTPS, sa po pripojení na stránku, využívajúc protokol HTTPS, uloží dešifrovaný záznam do logov aplikácií, ktorý je možné si prezrieť.
- V poslednej časti, kde cieľom bolo vyskúšať DoS útok, je podľa štatistického zhrnutia útokov v prílohách na obrázku B.2, ako aj logov na obrázku B.3 a B.4, možné spätne zistiť správanie firewallu, voči takýmto útokom. Zo záznamov je zrejmé, že po detekovaní hrozby automaticky komunikáciu dropuje. V prípade, že by bol firewall napojený na server IP reputácie, tak by sa po častom opakovaní týchto útokov každá komunikácia z tejto IP adresy zablokovala.

7.4.2 Zaujímavosti

Počas návrhu tejto laboratórnej úlohy, sa firewall Hillstone stal terčom útokov formou napríklad UDP Flood, ako aj IP spoofingu z IP adresy s pôvodom v Amerike. To len dokazuje, že zabezpečenie sietí nie je dokonalé a aj napriek viacerým firewallom školskej siete, ktoré sa nachádzajú medzi firewallom Hillstone a WAN sieťou, prešli aj takéto útoky až k užívateľovi. Útok IP spoofing bol z lokálne adresy prostredníctvom DNS serverov spoločnosti Google distribuovaný na cieľovú adresu. Vzhľadom na rozšírenosť vírusu WannaCry v dnešnej dobe je pravdepodobné, že nosičom tohto nového vírusu mohol byť akýkoľvek útok z externej siete. Avšak inteligentné firewally Hillstone využívajúce aj Cloudové funkcie udržujúce kontakty s externým serverom sú schopné túto hrozbu detekovať a zabrániť jej. Priebehy útokov sú zobrazené na obrázkoch C.1 a C.2 obsiahnutých v prílohách.

8 ZÁVER

V teoretickej časti bakalárskej práce bol všeobecne popísaný princíp zabezpečenia sietí, ochrana pred nežiadúcimi útokmi, spolu s ich popisom. Špeciálny dôraz bol kladený na problematiku zabezpečenia sietí pomocou virtuálnych firewallov a síce ich využitie, funkcie a ďalšie výhody v porovnaní s fyzickými.

Poznatky nadobudnuté pri študovaní teórie o virtuálnych firewallov som využil pri zhodnotení jeho využitia v praxi. Po skúsenosti s takýmto druhom ochrany som dospel k subjektívnemu názoru, že tieto firewally sú zamerané na špecifických záujemcov o túto službu, na rozdiel od širokospektrálne zameraných fyzických firewallov. Preto je možné tvrdiť, že tieto firewally sú koncipované pre data centrá a iné cloudové služby, ktoré preferujú minimalizáciu hardwarových strojov, prípadne sú vhodným využitím pri doplnkovom zapojení bezpečnostného prvku ako sekundujúci firewall tomu fyzickému.

Pri používaní softwaru VMWare, určeného na prácu s virtuálnymi zariadeniami, vznikli v praktickej časti problémy s preťažením hardwaru u fyzického počítača, ktoré mali často za následok kompletné resetovanie virtuálnych prístrojov. Z tohto dôvodu po pokuse o prechod z verzie VMWare Player na VMWare Workstation Pro prišlo k zmene sériových čísiel vo firewalle Hillstone CloudEdge, čo bolo spôsobené neštandardnou inštaláciou. Preto je časť z piatej kapitoly demonštrovaná na firewalle Fortigate VM a následný návrh laboratórnej úlohy je dokončený na fyzickom firewalle Hillstone. V šiestej kapitole práce bol vyobrazený návrh malej až strednej siete s jeho zabezpečením, pričom poznatky z tejto časti boli prenesené do praktického návrhu v poslednej časti.

V poslednej kapitole tejto práce, venovanej návrhu laboratórnej úlohy, je popísaný postup na nastavenie rôznych funkcií a zabezpečovacích zásad. Tieto funkcie sú porozdeľované do kategórií, z ktorých každá časť je ukončená prezretím výsledkov v záznamoch. Zakončenie laboratórnej úlohy je testovaním DoS útoku na firewall prostredníctvom virtuálneho stroja Kali Linux. Práve v tejto časti je možné vidieť, ako firewallu hillstone nerobí problém väčšia záťaž vyvíjaná na jeho interface.

Pri práci s firewallom Hillstone z užívateľského pohľadu hodnotím kladne prehľadnosť jeho WebUI, v ktorom sa po bližšom preskúmaní dá intuitívne orientovať. Výhodnou vlastnosťou je aj množstvo preddefinovaných funkcií ochrany, ktoré boli použité v laboratórnej úlohe na zabránenie DoS útoku. Z hardwarového hľadiska sa jednalo o verziu obsahujúcu 4 ethernet rozhrania, čo je pre využitie vo väčšej sieti nedostatočné. Pre malé až stredné siete a laboratórne účely je však tento firewall dostačujúcou voľbou.

LITERATÚRA

[1] PFLEEGER, Charles P. a Shari Lawrence. PFLEEGER. *Analyzing computer security: a threat/vulnerability/countermeasure approach.* Upper Saddle River, NJ: Prentice Hall, c2012. ISBN 0132789469.

[2] KOMAR, Brian, Ronald BEEKELAAR a Wettern JOERN. *Firewalls For Dummies.* 2nd Edition, Wiley Publishing, Inc. NY: 10022, c2003. ISBN: 0-7645-4048-3.

[3] FRAHIM, Jazib; SANTOS, Omar; OSSIPOV, Andrew. Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services. 3rd Edition. Indianapolis: Cisco Press, 2014 , s7, ch1. ISBN-13: 978-1-58714-307-6

[4] BullGuard Security Center *How does firewall work*[online], BullGuard, [cit. 6. 11. 2016]. Dostupné z URL: <http://www.bullguard.com/bullguard-security-center/pc-security/computer-security-resources/how-does-a-firewall-work.aspx>.

[5] BERTHELOT, Clement. *Evaluation of a Virtual Firewall in a Cloud Environment* [online], School of Computing, 2011, s. 21.[cit. 6. 11. 2016]. Dostupné z URL: <http://buchananweb.co.uk/09014406_MSc_VirtualFirewall.pdf>

[6] MILLER, Lawrence C.. *Next-Generation Firewalls For Dummies.* Wiley Publishing, Inc. NY:10022, 2011, ISBN: 978-0-470-93955-0.

[7] Cisco Systems, Inc, *Local WebAuth Deployment Guide* [online], 170 West Tasman Dr., Cisco Systems, Inc, posledná akutalizácia 1. 9. 2011. [cit. 10. 11. 2016]. Dostupné z URL: <http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/WebAuth/WebAuth_Dep_Guide.html#wp392180>

[8] Hillstone Networks Inc., *Hillstone CloudEdge Virtual Next-Generation Firewall* [online], Hillstone Networks [cit. 10. 11. 2016]. Dostupné z URL: <http://www.hillstonenet.com/our-products/hillstone-cloudedge/>

[9] Hillstone Networks Inc., *Hillstone Features Overview* [online], Hillstone Networks [cit. 10. 11. 2016]. Dostupné z URL: <http://www.hillstonenet.com/wp-content/uploads/Hillstone_CloudEdge_V5.5R3_EN.pdf>

[10] VMware Inc., *VMware Workstation 5.0 Bridged Networking* [online], Palo Alto, CA 94304, USA, VMWare [cit. 13. 11. 2016]. Dostupné z URL: <https://www.vmware.com/support/ws5/doc/ws_net_configurations_bridged.html>

[11] VMware Inc., *VMware Workstation 5.0 Network Address Translation (NAT)* [online], Palo Alto, CA 94304, USA, VMWare [cit. 13. 11. 2016]. Dostupné z URL: <https://www.vmware.com/support/ws5/doc/ws_net_configurations_nat.html>

[12] Hillstone Networks Inc., *Hillstone Product Overview*, Sunnyvale: Hillstone Networks, 2015

[13] Hillstone Networks Inc., *Hillstone Features Overview*, Sunnyvale: Hillstone Networks, 2016

[14] Hillstone Networks Inc., *StoneOS 5.5R3 CLI User Guide* [online], Hillstone Networks [cit. 10. 5. 2016]. Dostupné z URL: <http://docs.hillstonenet.com/en/Content/PDF%20Downloads_5.5R3.htm>

ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK

ABD	Abnormal Behavior Detection – detekcia nezvyčajného správania
ACL	Access Control List – zoznam na kontrolu prístupov
AD	Active Directory – aktívny zoznam
ATD	Advanced Threat Detection – pokročilá identifikácia ohrozenia
CD	Compact Disc – kompaktný disk
CMP	Cloud Management Platforms – menežment cloudových platforiem
DDoS	Distributed Denial of Service – distribuované zamietnutie prístupu
DLP	Data Loss Prevention – Zamädzenie straty dát
DMZ	Demilitarized Zone – demilitarizovaná zóna
FTP	File Transfer Protocol – protokol prenosu súborov
HTTP	Hypertext Transfer Protocol – protokol na prenos hypertextu
IDS	Intrusion Detection System – detekčný systém narušiteľa
IMAP4	Internet Message Access Protocol 4 – prístupový protokol pre internetové správy
ip	Internet Protocol – internetový protokol
LDAP	Lightweight Directory Access Protocol – prístupový protokol pre ľahké zoznamy
MITM	Man in the Middle – človek medzi
NAT	Network Address Translation – preklad sieťových adries
NGFW	Next Generation Firewall – firewall novej generácie
PAT	Port Address Translation – preklad adries portov
POP3	Post Office Protocol 3 – protokol poštových služieb
PPP	Point-to-Point Protocol – protokolo z bodu na bod
QoS	Quality of Service – kvalita služby

RADIUS	Remote Access Dial-In Service – slúžba vzdialeného prístupu vytáčania
SMTP	Simple Mail Transfer Protocol – protokol na prenos jednoduchých správ
SSL	Secure Sockets Layer – vrstva zabezpečených soketov
SSO	Single Sign-on – jedno prihlasovanie
TACACS	Terminal Access Controller Access-Control System – terminálová kontrola prístupu ovládací prístup-ovládací systém
TCP	Transmission Control Protocol – protokol na kontrolu prenosu
ToS	Types of Service – typy služieb
UDP	User Datagram Protocol – protokol užívateľských datagramov
URL	Uniform Resource Locator – jednotné označenie zdrojov
USB	Universal Serial Bus – univerzálna sériová zbernica
VLAN	Virtual Local Area Network – virtuálna lokálna sieť
VMM	Virtual Machine Monitor – monitor virtuálnych strojov
VPC	Virtual Private Cloud – virtuálny súkromný cloud
VPN	Virtual Private Network – virtuálna súkromná sieť
VXLAN	Virtual Extensible Local Area Network – rozšíriteľná virtuálna lokálna sieť

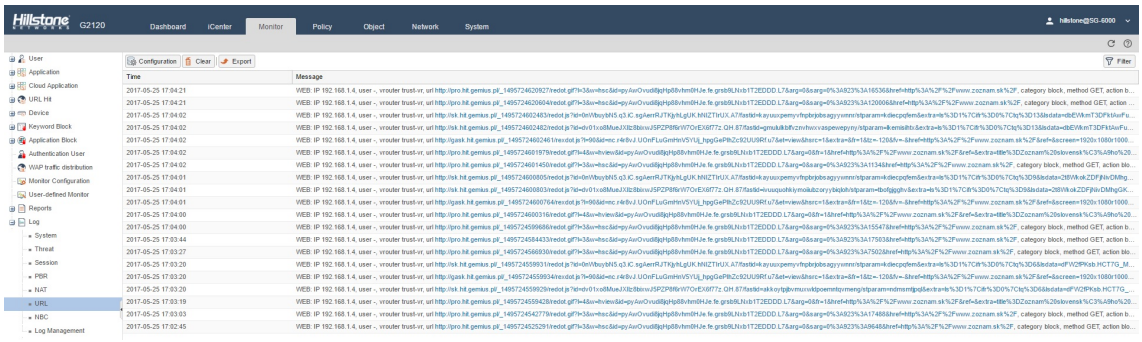
ZOZNAM PRÍLOH

A PRÍLOHY K BAKALÁRSKEJ PRÁCI

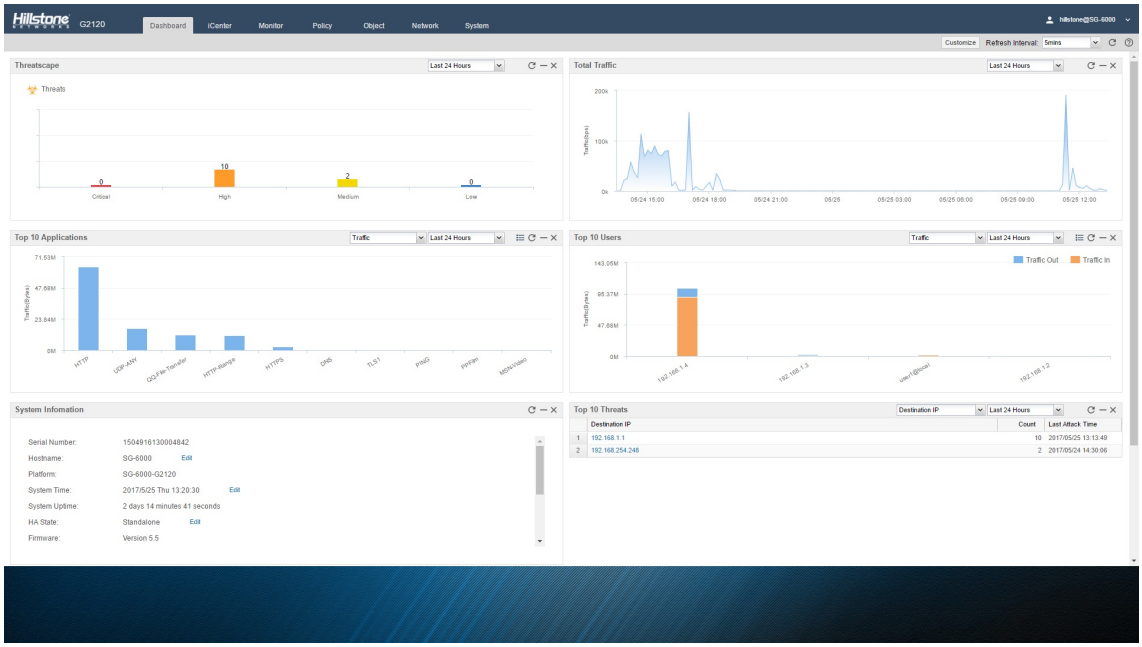
	Paketový Filter	Stavový Firewall	Aplikačný Proxy	Circuit Gateway	Ochranca (GUARD)	Osobný Firewall
Zložitosť rozhodovania	Najjednoduchšie rozhodovacie pravidlá	Jednoduché rozhodovacia pravidlá	Stredná zložitosť rozhodovania	Zložitosť na rozmedzí Paketového Filtru a Stavového Firewallu	Najkomplexnejší	Nízka zložitosť, ktorá sa ale začína stupňovať
Hĺbka analýzy dát	Vidí len adresy a služby protokolu	Vidí adresy a dáta	Vidí a analyzuje všetky dáta v balíku	Vidí adresy a dáta	Vidí a analyzuje celý súbor dát	Vidí všetky dáta
Možnosť zvolenia auditu	Audit obmedzený kvôli rýchlosti	Audit možný	Audit pravdepodobný	Audit pravdepodobný	Audit pravdepodobný	Audit pravdepodobný
Spôsob kontroly toku	Kontrola na základe pravidiel pripojenia	Kontrola na základe informácií naprieč viacerými paketmi (v hlavičkách alebo dátach)	Kontrola na základe správania aplikácií	Kontrola na základe adries	Kontrola na základe interpretácie obsahu	Bežne kontroluje na základe obsahu každého paketu individuálne, v závislosti na adresách alebo obsahu
Komplexnosť zabezpečovacích funkcií	Komplexné adresačné pravidlá môžu zapríčiniť zložitejšiu konfiguráciu	Bežne predkonfigurované na detekciu konkrétnych podpisov útokov	Jednoduché proxy môžu nahradiť komplexné rozhodovacie pravidlá, ale musia poznať správanie aplikácií	Relatívne jednoduché adresačné pravidlá robia konfiguráciu jednoduchou	Komplexné ochranné fukcie môžu byť zložité na presnú definíciu	Zvyčajne začína v móde zamietať všetok príchodzí tok, pridáva adresy a funkcie do dôveryhodných

Obr. A.1: Tabuľka vlastností jednotlivých firewallov.[1]

B PRÍLOHY K LABORATÓRNEJ ÚLOHE

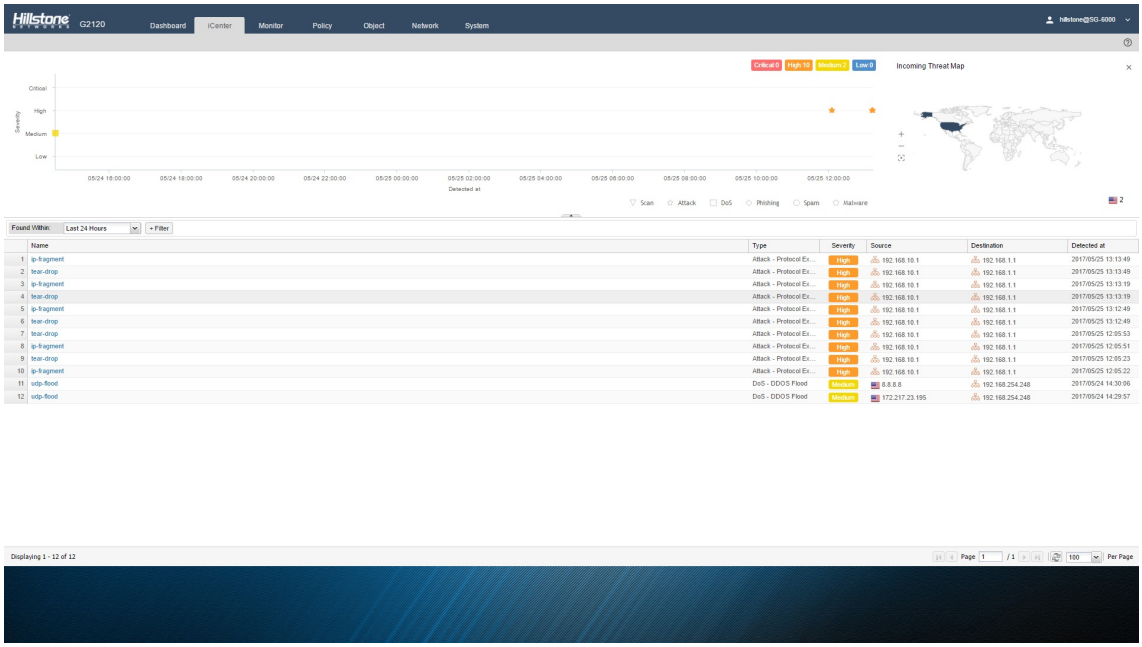


Obr. B.1: Záznamy prístupov na filtrované stránky.

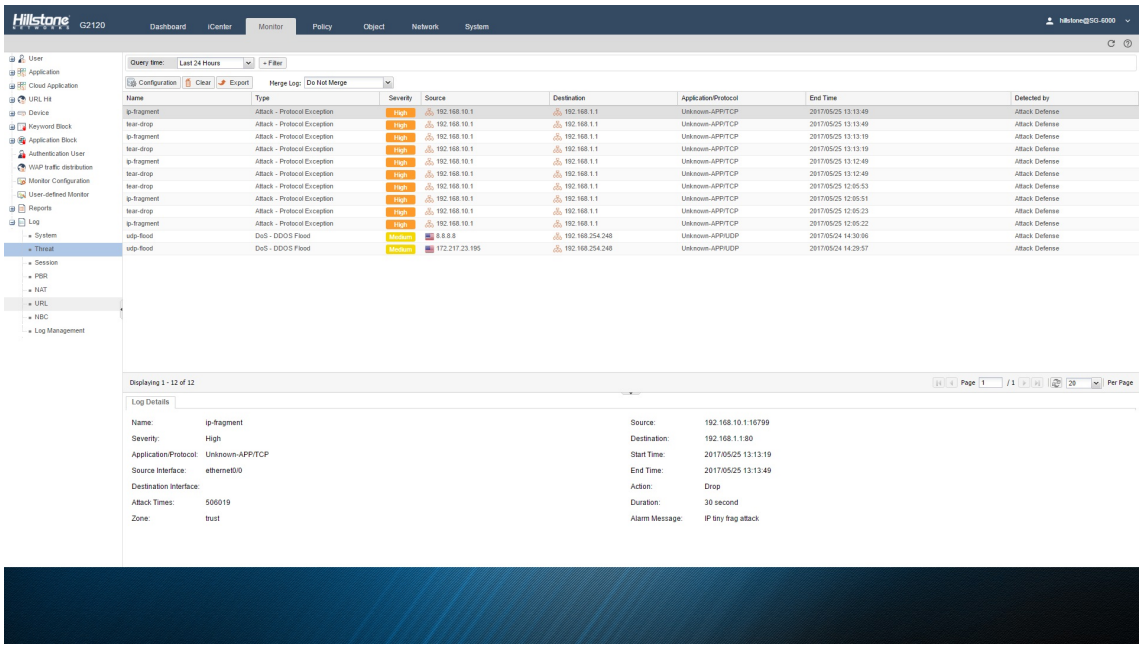


Obr. B.2: Úvodná stránka WebUI, obsahujúca štatistiky.

Na obrázku B.2 je možné v ľavom hornom rohu vidieť množstvo hrozieb, v pravo vyťaženie siete. Zároveň je možné vidieť grafy vyjadrujúce využitie siete danými užívateľmi a protokolmi. V pravom dolnom rohu je vyobrazenie najnebezpečnejších útokov na firewall.

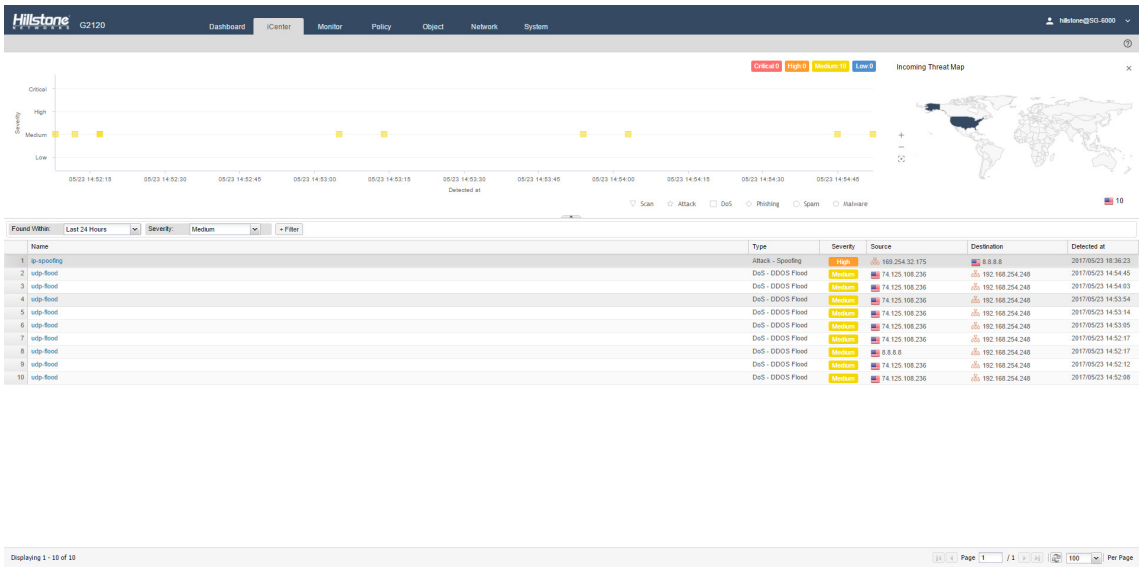


Obr. B.3: Útoky vyobrazené v záložke iCenter.

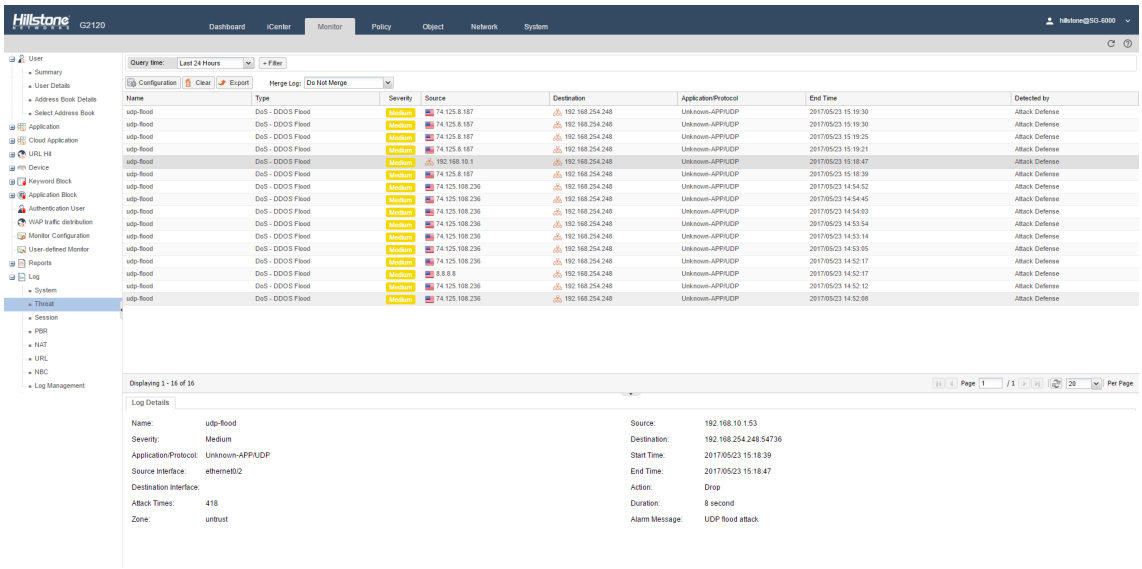


Obr. B.4: Záznamy útokov vyvolaných pomocov DoS.

C ZHRNUTIE ÚTOKOV NA FIREWALL HILLSTONE



Obr. C.1: Vyobrazenie útokov v záložke iCenter.



Obr. C.2: Logy útokov v záložke Threat.

D OBSAH PRILOŽENÉHO CD

V priloženom médiu je možné nájsť elektronickú verziu bakalárskej práce vo formáte pdf. V zložke obrázky sú umiestnené obrázky a prílohy, použité v práci, v ich pôvodnom rozlíšení.

V zložke pentmenu-master sa nachádza inštalačný program vo formáte .zip, využitý na penetračné testy pomocou operačného systému Kali Linux. Jeho voľná verzia sa však nachádza na internete k stiahnutiu.

D.1 Stromová štruktúra obsahu adresára

- `BC Praca` ..... koreňový adresár priloženého CD
  - `xvarmu05` ..... Elektronická verzia bakalárskej práce vo formáte PDF
  - `obrazky` ..... Obrázky a prílohy v pôvodnom rozlíšení
    - `Obr 5.2 VMWare adapter.jpg`
    - `Obr 5.5 Windows adapter.jpg`
    - `Obr 5.6 Fortigate interface.jpg`
    - `Obr 5.7 Fortigate DHCP.jpg .3 Obr 5.8 Fortigate policy.jpg`
    - `Obr 5.9 Wireshark.jpg`
    - `Obr 6.1 Schema.png`
    - `Obr 6.3 Email filter.png`
    - `Obr 6.4 Webcontent filter.png`
    - `Obr 6.5 Antivir configuration.png`
    - `Obr 6.6 HSC.jpg`
    - `Obr 6.7 IPS.jpg`
    - `Obr 6.8 Attack Defense.png`
    - `Obr 7.2 Sietovy adapter.png`
    - `Obr 7.3 SNAT.jpg`
    - `Obr 7.4 Tracert.jpg`
    - `Obr 7.5 URL filter.jpg`
    - `Obr 7.6 Bridge-mode.png`
    - `Obr 7.7 Nastavenie adries.png`
    - `Obr 7.8 User authentication.png`
    - `Obr 7.9 Web authentication.png`
    - `Obr 7.11 Pentmenu DoS.jpg`
    - `Obr 7.12 Log SNAT.png`
    - `Priloha B.1.jpg`
    - `Priloha B.2.jpg`
    - `Priloha B.3.jpg`
    - `Priloha B.4.jpg`
    - `Priloha C.1.jpg`
    - `Priloha C.2.png`
  - `pentmenu-master` ..... Inštalačná zložka programu pre Kali Linux