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

HIGH AVAILABILITY FIREWALLY

HIGH-AVAILABITY FIREWALLS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — Bc. Tibor Frátrik

AUTHOR

VEDOUCÍ PRÁCE — doc. Mgr. Karel Slavíček, Ph.D.

SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Bc. Tibor Frátrik ***ID:*** 211787
Ročník: 2 ***Akademický rok:*** 2022/23
NÁZEV TÉMATU:

High availability firewally

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je prozkoumat možná řešení redundance stavových firewallů a to jak komerčních, tak zejmén opensource řešení. Firewall bude provozován na dvou či více hardwarových instancí v režimu active - standb Mezi těmito instancemi je nutné synchronizovat minimálně stav dynamického překladu adres (NAT), sta sestavených a částečně sestavených TCP spojení a stav VPN spojení terminovaných na daném firewallu. Úkole práce je implementovat redundantní řešení firewallu na některé z dostupných open-source platforem (např. Lin nebo BSD Unix) a porovnat vlastnosti opensource řešení s vybranými komerčními produkty.

DOPORUČENÁ LITERATURA:

Podle pokynů vedoucího práce.

Termín zadání: 6.2.2023 ***Termín odevzdání:*** 19.5.2023

Vedoucí práce: doc. Mgr. Karel Slavíček, Ph.D.

doc. Ing. Jan Hajný, Ph.D.

předseda rady studijního programu

ABSTRAKT

Táto diplomová práca je venovaná výskumu možnosťam redundancie firewallov a to špeciálne komerčným, softvérovým alebo hardvérovým. V teoretickej časti sú popísane jednotlivé firewally a ich možnosti redundancie. Diplomová práca bola viac zameraná na dva konkrétne firewally: ASA a Pfsense. V rámci praktickej časti boli navrhnuté a implementované topógie pre otestovanie redundancie u týchto firewallov. Pre testovanie boli vybrané dynamické preklady adries (NAT), stav VPN spojení, či už VPN spojenie typu site-to-site alebo remote-access a tiež spojenia TCP. Na záver boli porovnané výsledky pre jednotlivé firewally. Kde bolo skúmané a porovnané prevažne to, ako počítačová sieť u jednotlivých typov firewallov reaguje na redundanciu.

KĽÚČOVÉ SLOVÁ

Firewall, ASA, Pfsense, VPN, NAT, TCP

ABSTRACT

This diploma thesis is dedicated to researching the possibility redundancy of firewalls, especially commercial, software or hardware firewalls. The theoretical part describes individual firewalls and their redundancy options. The diploma thesis was more focused on two specific firewalls: ASA and Pfsense. As part of the practical part, topologies were designed and implemented for testing the redundancy of these firewalls. Dynamic address translations (NAT), VPN connection status, either site-to-site or remote-access VPN connections, and TCP connections were selected for testing. Finally, the results for individual firewalls were compared. Where it was mainly researched and compared, how the computer network reacts to redundancy in individual types of firewalls.

KEYWORDS

Firewall, ASA, Pfsense, VPN, NAT, TCP

Bibliografická citácia

FRÁTRIK, Tibor. *High availability firewally* [online]. Brno, 2023 [cit. 2023-04-23]. Dostupné z: https://www.vut.cz/studenti/zav-prace/detail/151244. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Karel Slavíček.

Vyhlásenie autora o pôvodnosti diela

Meno a priezvisko autora:	Bc. Tibor Frátrik
VUT ID autora:	211787
Typ práce:	Diplomová práca
Akademický rok:	2022/23
Téma záverečnej práce:	High availability firewally

Vyhlasujem, že svoju diplomovú prácu na tému „High-availability firewally“ som vypracoval samostatne pod vedením vedúceho diplomovej práce a s použitím odbornej literatúry a dalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej diplomovej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto diplomovej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následku porušenia ustanovenia § 11 a nasledujúcich autorského zákona 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 č. 40/2009 Sb.

V Brne dňa . . . .

podpis autora

Poďakovanie

Chcel by som sa veľmi rád poďakovať doc. Mgr Karolovi Slavíčkovi, Ph.D za konzultácie, odborné vedenie a pripomienky pri vypracovaní mojej diplomovej práce.

V Brne dňa . . . .

podpis autora

Obsah

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ÚVOD

Internet je dnes používaný miliónmi ľuďmi po celom svete. Následne sú medzi týmito ľudmi vo veľkom množstve vymieňaňé informácie. Cieľom komunikácie je, aby táto informácia bola doručená v čas a bezpečí. Kvôli tomu netreba podceňovať bezpečnosť počítačových systémov. Hrozby, ktoré dnes existujú sú veľmi rôznorodé. Aby bol ochránený internet, bezpečnostný systém alebo aby bola ochránená nejaká počítačová sieť je potrebné inštalovať rôzne bezpečnostné prvky: od antivírusových programov, firewally až po programy pre šifrovanie.

Práve firewally sú z jedných základných pilierov na zabezpečenie počítačových sietí. Najčastejšie sú používané na oddelenie sietí s rôznymi prístupovými právami a tiež na kontrolu toku dát medzi týmito sieťami. Taktiež sa prostredníctvom firewallov dajú nastaviť rôzne pravidlá na povolenie alebo obmedzenie prístupu.

V samotnej diplomovej práci sú detailnejšie popísané firewally. Diplomová práca sa skladá zo siedmich kapitol: počítačové siete, firewall, high availability, high availability firewally, ASA firewally, praktická časť a záver. Samotným cieľom diplomovej práce bolo správne nakonfigurovať a overiť funkčnosť HA (High Availability) pri jednotlivých firewallov. Ďalším cieľom bolo porovnať dopad HA na tieto firewally.

V kapitole počítačové siete sú popísané útoky na počítačové siete. Tiež sú tu popísané rôzne techniky zabezpečenia počítačových sietí.

V kapitole firewall sú detailnejšie rozobrané vlastnosti a funkcie firewallu. Taktiež je tu spomenuté aj plánovanie firewallov.

Tretia a štvrtá kapitola je zameraná na problematiku HA Kde je riešený problém s konfiguráciou klastrov u firewallov. Ďalej je tu spomínaná náhrada HA u prepínačov a smerovačov, ako sú napríklad smerovacie protokoly alebo STP (Spanning Tree Protocol). V štvrtej kapitole je popísaná problematika HA u firewallov. Sú tu popísané rôzne techniky nasadenia HA u softvérových a hardvérových firewallov. Piata kapitola je zameraná na ASA firewally. V tejto kapitole sú tiež teoretický popísané problematiky NAT a VPN spojenia. V neposlednom rade je tu tiež riešený režim HA pre ASA firewally.

V diplomovej práci bola problematika HA implementovaná na softvérový ASA a Pfsense firewall. Boli implementované jednotlivé VPN spojenia, či už IPsec alebo Anyconnect VPN spojenie. Problematika HA bola tiež rozšírená a skúmaná aj pre režim NAT alebo pre TCP spojenia ako sú: Telnet, SSH alebo BGP.

V závere sú zhrnuté výsledky praktickej časti. Kde sú porovnané výsledky pre ASA a Pfsense firewall.

1. POČÍTAČOVÉ SIETE

Na začiatku je potreba zobrať do úvahy, že ľudstvo sa nachádza v prepojenom svete. To znamená, že informácia sa vyrába a neustále vymieňa. V digitálnom svete slúži na vymieňanie informácií počítačová sieť. Počítačová sieť je systém vzájomne prepojených počítačov za účelom výmeny dát medzi nimi. Najčastejším dôvodom prepojenia počítačov je zdielanie informácií. A tieto informácie je nutné uchovať v bezpečí.

1.1 Typy počítačových sieti

Existujú rôzne tipy počítačových sietí. Na základe geografickej oblasti sú počítačové siete kategorizované ako:

- PAN (Personal Area Network) – Je to počítačová sieť, ktorá je vytvorená z niekoľkých osobných zariadení ako notebooky, počítače, mobilné telefóny alebo tlačiarne. Všetky tieto zariadenia sa nachádzajú v dosahu do desiatich metrov. Na prenos údajov sa väčšinou používa bezdrôtové pripojenie ako napr. Bluetooth.
- LAN (Local Area Network) – Je to počítačová sieť, ktorá je vytvorená z niekoľkých osobných zariadení ako notebooky, počítače, mobilné telefóny alebo tlačiarne. Všetky tieto zariadenia sa nachádzajú v jednej miestnosti alebo v jednej budove. Konektivita zariadení je zaistená pomocou ethernetových káblov, optických káblov alebo cez Wi-fi (Wireless Fidelity). Dáta v sieti LAN sú väčšinou prenášané rýchlosťou od 100 Mbps (Megabits per second) do 10 Gbps (Gigabits per second), kde Gbps znamená gigabity za sekundu. Rýchlosť 10 Gbps je podporovaná u Gigabit Ethernetu.
- MAN (Metropolitan Area Network) – Je rozšírená forma LAN, ktorá pokrýva väčšiu geografickú oblasť ako napr. mesto. Rýchlosť prenosu dát v MAN sa tiež pohybuje v Mbps. Káblová TV sieť alebo káblové širokopásmové internetové služby sú príklady MAN. Tento druh siete môže byť rozšírený až na 30-40 km. Sieť MAN sa väčšinou skladá z viacerých sieti LAN.
- WAN (Wide Area Network) – Táto sieť predstavuje počítače a ďalšie siete LAN a MAN, ktoré sú rozmiestnené v rôznych krajinách či kontinentoch. Využíva sa u veľkých obchodných, vzdelávacích a vládnych organizáciách.

1.2 Sieťové Zariadenia

Na komunikáciu a výmenov údajov prostredníctvom rôznych prenosových médií sú vyžadované rôzne zariadenia. Ide o zariadenia ako:

- Smerovač – Je aktívne sieťové zariadenie v počítačových sieťach. Úlohou smerovača je prenášať údaje do iných počítačových sietí. Najčastejšie je kvôli smerovaču prepojená lokálna sieť spolu so sieťou internet. Smerovačom sú poskytované pokročilé možnosti, ako analyzovať dáta, rozhodnúť a zmeniť spôsob ich zabalenia.
- Prepínač – Je aktívne sieťové zariadenie. Prepínač je najčastejšie používaný v sieťach typu LAN. Je používaný na prepojenie viacerých počítačov alebo komunikujúcich zariadení. Prepínač je považovaný za inteligentné zariadenie, lebo dáta sú odoslané len jedným portom a nie všetkými ako je to u sieťového zariadenia Hub.
- Modem – Alebo modulátor-demodulátor sa vzťahuje na zariadenie používané na konverziu medzi analógovými signálmi a digitálnymi bitmi.
- Firewall – Je bližšie popísaný v kapitole číslo 2 [1].

1.3 Útoky na počítačovú sieť

Prostredníctvom počítačových sieti je realizovaný dnešný moderný svet. Vyhľadávanie informácií, platenie účtov alebo videokonferencia je schopná fungovania len na základe počítačových sietí. Z toho je potrebné zobrať do úvahy samotnú bezpečnosť počítačových sietí. Útoky na počítačovú sieť sú vykonateľné na všetkých sieťových zariadeniach, počítačových systémov, sieťových tlačiarňach alebo na mobilných zariadeniach. Pri týchto sieťových zariadeniach je používaný TCP/IP (Transmission Control Protocol/Internet Protocol) alebo akýkoľvek iný sieťový protokol [2].

1.3.1 Pasívne útoky

Pri pasívných útokov je monitorovaná nešifrovaná komunikácia. Hlavným cieľom je zachytiť heslá alebo citlivé informácie. Výsledkom pasívných útokov je spristupnenie informácií útočníkovi bez súhlasu alebo vedomia používateľov. Medzi pasívne útoky patria:

- Snooping – Je to typ pasívného útoku. Cieľom útočníkov je predovšetkým získanie dôležitých informácií o používateľoch siete, ako sú prihlasovacie údaje alebo informácie o kreditnej karte. Celkovo ide o neoprávenený prístup k údajom. IP adresy hostiteľov sú zvyčajne sledované útočníkom.
- Traffic analysis – Cieľom tohto útoku je zachytenie komunikačnej cesty medzi príjemcom a odosielateľom. Tým je umožnené aby táto zachytená komunikácia bola analyzovaná útočníkom.

1.3.2 Aktívne útoky

Pri aktívnych útokov je cieľom útočníka preniknutie do zabezpečených systémov. V týchto zabezpečených systémov je následne zavedený škodlivý kód s cieľom upraviť alebo ukradnút citlivú informáciu [3]. Medzi aktívne útoky patria:

- Červ – Je to typ aktívného útoku. Je to program so škodlivým kódom, pri ktorom sú napádané hostiteľské počítače. Šírenie červa je aktívne cez rozosielanie svojich kópií cez LAN alebo internet.
- Vírus – Je to typ škodlivého programu. Na vytváranie vlastných kópií sú potrebné spustiteľné súbory. Šírenie je prostredníctvom dátových nosičov ako CD, DVD alebo USB (Universal Serial Bus). Vírusy je možno rozdeliť na štyri skupiny: súborové, skriptové, boot a makro vírusy.
- Trójsky kôň – Je to taktiež typ škodlivého program. Trojský kôň je zvyčajne vyskytovaný vo forme spustiteľných súborov (.exe, .com). Škodlivý kód je ukrývaný v týchto súboroch. Jediným riešením je vymazať tento kód [4].

1.4 Zabezpečenie počítačových sietí

Počítačová sieť môže byť ohrozená jendnotlivými útokmi. Počítačové siete majú otvorenosť, vzájomnú prepojenosť, zdieľanie online informačnej bezpečnosti a ďalšie vlastnosti, ktorými je spôsobená existencia nedostatkov. Preto je potrebné prijať opatrenia na zabezpečenie siete vo všetkých smeroch pre rôzne hrozby. Veľmi dôležité je chrániť dôvernosť, integritu a dostupnosť sieťových informácií. Najčastejšími chybami pre slabo zapezpečené počítačové siete sú chybajúce ľudské, finančné a materiálne zdroje na posilnenie bezpečnosti siete. Ďalšími chybami sú nesprávne nakonfigurovateľné bezpečnostné politiky, nesprávne nakonfigurovateľné bezpečnostné mechanizmy, nedostatok pokročilých technológií, nástrojov a produktov na zabezpečenie siete.

Na druhej strane je dôležité uplatniť politiku bezpečnosti informácií v počítačovej sieti. Pod týmto pojmom sa rozumie:

- Kontrola prístupu – Je to bezpečnostná politika založená na kontrole identity užívateľa a overenie heslom. Cieľom je získať skutočnú identitu užívateľa a uľahčiť sledovanie správania počítačovej siete.
- Posilnenie detekcie narušenia – Hlavným cieľom je, aby monitorovací systém bol schopný detekovať v reálnom čase útoky, a aby včas bolo týmto monitorovacím systémom poskytnuté bezpečnostné upozornenie.
- Zašifrovanie informácií – Na zašifrovanie informácií sú poskytnuté šifrovacie algoritmy, ktorým sú šifrované surové dáta.
- Zatvorenie nepoužitých portov a služieb – Je možné nainštalovať program monitorovania portov. Cieľom je detekovať tie porty, ktoré sa nepoužívajú.
- Skrytie IP (Internet Protocol) adresy – Na skrytie IP adresy sa najčastejšie používa proxy server. Kde útočníkom môže byť detekovaná len IP adresa proxy servera a nie reálna IP adresa používateľa.

- Autentifikačná technológia – U veľmi veľa počítačových systémov je potrebné potvrdiť legitimitu cez autentifikáciu a následne potvrdiť určité povolenie. To je predpokladom, že autentifikácia je základ kontroly autentizácie. Len cez overenie platnej identity bude zaistená implementácia kontroly prístupu alebo systém prevencie.
- Včasná oprava zraniteľnosti – Je potrebné nainštalovať program na opravu zraniteľností, aby boli vyriešené bezpečnostné problémy, ktoré predstavuje zraniteľný program. Na skenovanie zraniteľnosti sa používajú špecializované skenery zraniteľnosti, ako je napr. COPS (Computer Oracle and Password Systém) alebo Tripwire.
- Technológia šifrovania súborov, alebo technológia digitálneho podpisu – Pri tejto technológií je posilnená ochrana dát proti krádeži alebo zničeniu.
- Nastavenie firewallu – Bezpečný prístup z vonkajšej siete do vnútornej [5].

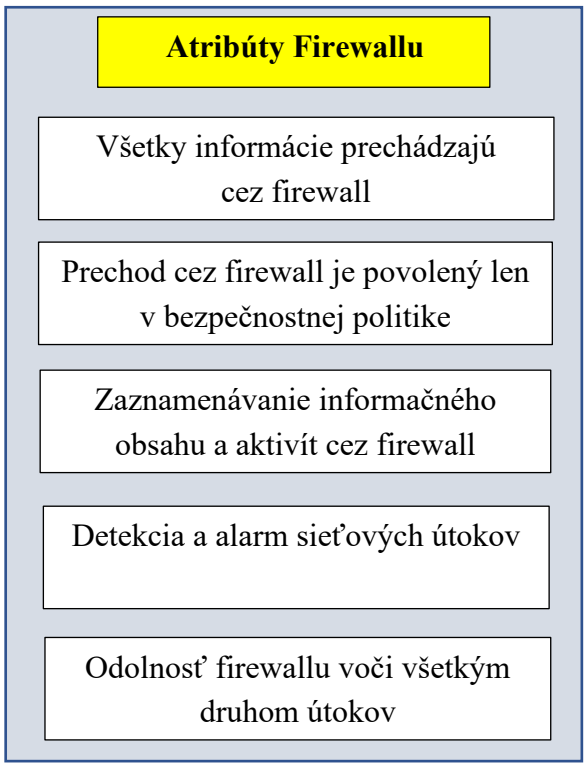
2. FIREWALL

Firewall je v počítačových sieťach chápaný ako aktívne sieťové zariadenie, prostredníctvom ktorého je blokovaná alebo povolená komunikácia na základe preddefinovaných pravidiel a politik. Je používaný medzi vnútornou sieťou a sieťou internet. Vďaka firewallu je zaistená konektivita medzi vnútornou sieťou a sieťou internet. Firewall je základným prostriedkom na zaručenie bezpečnosti sieťových informácií. Bez firewallu je súčasne tok informácií do a zo siete riadený na základe kontroly bezpečnostnej politiky, ako je povolenie, odmietnutie a monitorovanie.

Firewall je taktiež aj analyzátor. To znamená, že cez funkčný firewall je možné analyzovať tok informácií. Vo výsledku to znamená, že počítačová sieť alebo sieťové údaje sú výborne chránené [6].

2.1 Vlastnosti firewallu

Vo všeobecnosti existuje päť atribútov, ktorými sú popísané vlastnosti firewallu. Tieto atribúty sú zobrazené na obrázku č.2.1 [6].



Obr. č.2.1 Atribúty firewallu

2.2 Funkcie firewallu

Hlavnou funkciou firewallu je technológia dynamického filtrovania paketov. Je to schopnosť zachytávať pakety cez firewall. Je tu popísané rozhodnutie o odmietnutí alebo prijatí v závislosti od bezpečnostnej informácie. Cez firewally je možné dynamický riadiť toky informácií cez ich porty.

Ďalšou funkciou je ovládanie nebezpečnej služby. Táto nebezpečná služba je efektívne kontrolovaná firewallom. Cieľom je odmietnuť nebezpečné služby zo siete internet. Je tu vyžadovaná vopred nastavená politika bezpečnosti medzi dôvernou a nedôvernou doménou.

Treťou funkciou je bezpečnostná centralizovaná ochrana. Prostredníctvom firewallu je umožnené centralizovať všetok softvér potrebný na ochranu vnútornej siete. Centralizované riadenie bezpečnosti pomocou firewallov je efektívnejšie a hospodárnejšie [6].

2.3 Evolúcia firewallov

Technologické prostredie je neustále vyvíjané. No na druhej strane sú taktiež vyvíjané aj nové inovatívne hrozby. Tým sú zvýšené nároky na ochránenie rôznych aktív. Kvôli tomu bol potrebný neustály vývoj firewallov [7].

Prvá generácia firewallov bola navrhnutá na obranu proti necieleným útokom. Druhá generácia bola navrhnutá na obranu proti cieleným útokom. Neskôr bola vyvinutá aj tretia generácia firewallov. Tá bola navrhnutá tak, aby bol najskôr určený zámer útoku a potom aby boli využité vhodné bezpečnostné opatrenia. S neustálym vývojom hrozieb a kybernetických útokov bola vyvíjaná aj inteligencia a bezpečnosť, ktorým sú ponúkané riešenia firewallov novej generácie [8].

Packet filtering firewally

Jedna z najjednoduchších a najlacnejších foriem firewallovej ochrany je známa ako statické filtrovanie paketov. Hlavnou myšlienkou je, že každý paket je kontrolovaný na základe súboru pravidiel definovaných používateľom. Tým sa definuje, ktorý paket je za potreba zakázať a ktorý povoliť. Pakety sú skúmané na základe nasledujúcich kritérií [9]:

- Cieľová IP adresa
- Zdrojová IP adresa
- Zdrojový port TCP/UDP (User Datagram Protocol)
- Cieľový port TCP/UDP

Proxy firewally

U proxy friewallov je umožnené filtrovať prevádzku v sieti na aplikačnej úrovni. Je tu skúmaná prevádzka pre protokoly aplikačnej vrstvy, ako je HTTP (HyperText Transfer Protocol) a FTP (File Transfer Protocol). Taktiež je tu využívaná stavová a hĺbková kontrola paketov na identifikáciu škodlivej prevádzky.

SMLI (Stateful multiplayer inspection firewalls)

Pri firewallov pre stavovú viacvrstvovú inšpekciu sú filtrované pakety na sieťových, transportných a aplikačných vrstvách. Tieto pakety sú následne porovnávané so známymi dôveryhodnými paketami. Jednotlivé pakety môžu opustiť firewall ak sú prechádzané každou vrstvou samostatne.

NAT (Network address translation) firewalls

Cez firewally s prekladom sieťových adries je umožnené niekoľkým zariadeniam so sieťovými adresami pripojiť sa k internetu prostredníctvom jedinej IP adresy, čím sú chránené skryté jednotlivé IP adresy. Dôsledkom bude znížená schopnosť útočníkov zachytiť hľadané IP adresy, čo ponúka väčšiu bezpečnosť proti útokom.

NGFW (Next-generation firewalls)

Firewally novej generácie sú súčasťou tretej generácie technológie firewall. Sú to tradičné firewally spolu s ďalšími funkciami filtrovania sieťových zariadení, ako je napríklad systém prevencie vniknutia alebo aj hĺbková kontrola paketov. Cez hĺbkovú kontrolu paketov sú analyzované dáta v samotnom pakete, čo používateľom umožňuje efektívnejšie zisťovať, klasifikovať alebo zastaviť pakety so škodlivými údajmi.

U tradičných firewallov bolo na 3. a 4. vrstve povolovanie alebo blokovanie prevádzky na základe portu a protokolu s využitím stavovej kontroly, ďalej sa robili rozhodnutia založené na definovaných politikách. Ale u firewallov novej generácie sa začali poskytovať všetky možnosti tradičného firewallu ako aj ďalšie možnosti kontroly aplikácií alebo integrovaná prevencia narušenia.

WAF (Web Aplication Firewall)

Webový aplikačný firewall je špecializovaný firewall určený na filtrovanie a riadenie HTTP prevádzky cez internetovú komunikáciu medzi webovými klientmi a aplikačnými servermi. Tieto tipy firewallu sú dôležitým komponentom pre silné zabezpečenie aplikácií. Hlavnou úlohou WAF je chrániť konkrétne aplikácie pred webovými útokmi na aplikačnej úrovni. V tabuľke č.1 sú zobrazené základné rozdiely medzi NGFW a WAF [7].

	NGFW	WAF
Model ISO/OSI	3-7 vrstva	7 vrstva
Ochrana pred sieťovými hrozbami	ÁNO	ÁNO, ale len s HTTPS
IDS/IPS	ÁNO	ÁNO
DDos ochrana	3-4 vrstva	3-7 vrstva
Ochrana webových aplikácií	Základná	Plne podporovaná
Pravidlá webovej aplikácie	NIE	Podporovaná

Tab. č.1 základné rozdiely medzi NGFW a WAF

Hybrid firewall

Je to firewall, ktorý je kombináciou vyššie uvedených typov firewallov. Vo väčšine aplikácií je hybrid firewallom ponúkané simultánne filtrovanie paketov, proxy služby alebo je umožnené sledovať sieťovú prevádzku [10].

2.4 Plánovanie firewallov

Ako pri každom nasadení novej technológie, plánovanie firewallu by sa mala riešiť postupne. Úspešné nasadenie firewallu možno dosiahnuť dodržiavaním jasného plánovania krok za krokom. Samotné plánovanie firewallov sa skladá z piatich fáz: plán, konfigurácia, testovanie, nasadenie a spravovanie. Plánovanie firewallov je zobrazené graficky na obrázku č.2.2.

Obr. č.2.2 Plánovanie firewallov

Plán

Prvá fáza procesu je identifikácia všetkých požiadaviek, ktoré by mali byť organizáciou zvážené pri určovaní, ktorý firewall je nutné implementovať aby bola presadená bezpečnostná politika organizácie. Medzi základné princípy, ktoré by organizácie mali dodržiavať pri plánovaní nasadenia firewallu patria:

- Používať zariadenia tak, ako boli určené – To znamená, že firewally by nemali byť postavené zo zariadení, ktoré nie sú určené ako firewall. Napr. smerovače by mali byť určené na smerovanie a nie na filtrovanie ako firewally, čo by nadmerne zaťažilo procesor smerovača. Na druhej strane sa očakáva, že firewally by mali byť určené na poskytovanie služieb, ktoré súvisia so zabezpečením a nie so službami ako napr. webový server alebo e-mailový server.
- Vytvorenie hĺbkovej ochrany – Hĺbková ochrana by mala zahŕňať vytvorenie viacerých vrstiev bezpečnosti. V prípade brán firewall je možno hĺbkovú ochranu dosiahnuť použitím viacerých brán firewall v rámci organizácie. Aby bola hĺbková ochrana skutočne efektívna, firewally by mali byť súčasťou celkového bezpečnostného programu, v ktorom by boli zahrnuté aj produkty ako antimalware a softvér na detekciu narušenia.
- Venovanie pozornosti vnútorným hrozbám – Tu platí pravidlo, že všetky dôležité interné systémy by mali byť umiestnené za internými firewallmi.
- Dokumentácia firewallu – Každý model brány firewall má iné možnosti a obmedzenia. Tým sú ovplyvnené plánovania bezpečnostnej politiky organizácie a stratégie nasadenia brány firewall.

Každá sieť a organizácia má jedinečné požiadavky, ktoré vyžadujú jedinečné riešenia. Pri nákupe a implementácii riešenia brány firewall by organizácie mali zvážiť nasledovné:

- Bezpečnostné schopnosti – Ktoré oblasti organizácie je potrebné chrániť (interné oddelenia, vzdialené kancelárie, špecifické služby alebo klientov)? Ktoré typy technológií firewallu sú potrebné, aby jednotlivé druhy prevádzky boli chránené (filtrovanie paketov, stavová kontrola, aplikačný firewall, alebo proxy firewall)? Ďalej si treba určiť či sú nutné ďalšie funkcie zabezpečenia ako napr. detekcia narušenia alebo VPN (Virtual Private Network).
- Riadenie – Si treba určiť, ktoré protokoly firewall podporuje pre vzdialenú správu ako napr. SSH (Secure Shell Protocol), alebo sériový kábel.
- Výkon – Definovať si pri jednotlivých firewallov aké majú množstvo priepustnosti, požiadavky na latenciu a taktiež na high availability.
- Integrácia – Bude firewall vyžadovať špecifický hardvér, aby sa správne integroval do sieťovej infraštruktúry? Musí byť firewall kompatibilný s inými

zariadeniami v sieti, ktoré poskytujú bezpečnosť? Bude pri inštalácií firewallu vyžadovaná zmena v iných oblastiach počítačovej siete?

- Fyzické prostredie – Kde bude firewall fyzicky umiestnený, aby sa zabezpečila fyzická bezpečnosť? Je na fyzickom mieste, kde bude firewall umiestnený, dostatočný priestor? Bude na fyzickom mieste potrebné dodatočné napájanie alebo záložné napájanie?
- Personál – Je nutné si určiť, že kto bude zodpovedný za správu firewallu a tiež, či sa bude vyžadovať školenie pred nastavením firewallu.

Konfigurácia

Pri druhej fáze plánovania firewallu sú zahrnuté všetky aspekty konfigurácie brány firewall. To zahŕňa inštaláciu hardvéru a softvéru ako aj nastavenie pravidiel a bezpečnostných politík pre systém. Podrobnosti o vytváraní sady pravidiel sa líšia podľa typu firewallu.

Počas inštalácie a konfigurácie by mal byť firewall schopný spravovať iba správca, ktorý túto prácu vykonáva. Po nainštalovaní a zabezpečení firewallu môžu byt správcom vytvorené zásady brány firewall. U niektorých firewallov sú implementované politiky prostredníctvom explicitných pravidiel. U niektorých firewallov sú vyžadované konfigurácie nastavení brány firewall, ktorými sú potom vytvárané interné pravidlá. U niektorých firewallov sú vytvárané politiky a pravidlá automaticky, a poslednou štvrtou skupinou sú firewally, pri ktorých sa používa kombinácia týchto troch typov konfigurácie. Konečným výsledkom je súbor pravidiel, v ktorom je popísaný firewall, ako funguje.

Ďalším krokom v procese konfigurácie je nastavenie logov. Nastavenie logov je kritickým krokom pri prevencii a obnove zlyhaní, ako aj pri zaistení správnej konfigurácie zabezpečenia na bráne firewall. Správne nastavenie logov môže tiež poskytnúť dôležité informácie pre reakciu na bezpečnostné incidenty. Okrem konfigurácie logov by mali byť nastavené aj upozornenia v reálnom čase, ktoré upozornia administrátorov, keď sa na firewalle vyskytnú dôležité udalosti.

Testovanie

Ďalšia fáza je testovanie. Táto fáza zahŕňa implementáciu a testovanie prototypu navrhnutého riešenia v testovaciom prostredí. Primárnymi cieľmi testovania je zhodnotiť:

- Konektivitu
- Kompatibilitu aplikácií
- Logy
- Výkon
- Bezpečnosť implementácie
- Synchronizáciu

Nasadenie

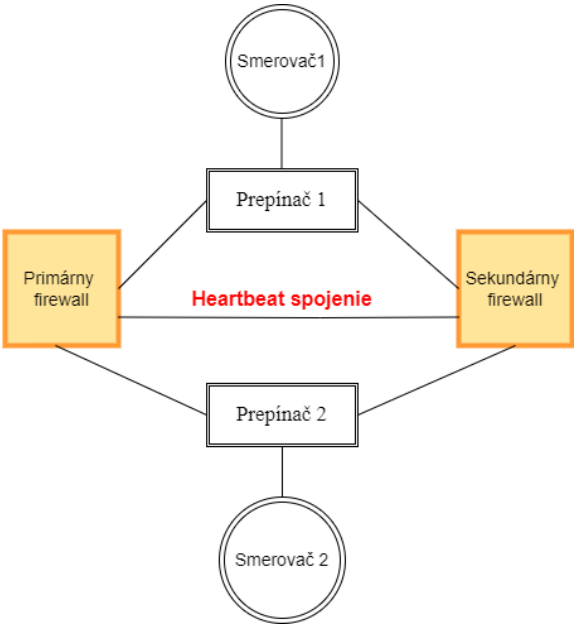
Nasadenie je fáza plánovania, ktorá predstavuje nasadenie firewallu v podniku. Musí nasledovať po dokončení fáze testovania a po vyriešení všetkých problémov. Pred nasadením brány firewall by správcovia mali upozorniť používateľov koho majú oznámiť ak sa vyskytnú nejaké problémy.

Spravovanie

Poslednou fázou plánovania firewallov je spravovanie. Počas celého životného cyklu musí byť firewall spravovaný tak, aby zahŕňal údržbu komponentov a podporu pri prevádzkových problémoch. Jedným z príkladov typickej údržby je testovanie a aplikácia opráv na firewallové zariadenia. S novými hrozbami môže byť potrebné aktualizovať pravidlá politiky. Logy by mali byť tiež nepretržite monitorované aby sa identifikovali hrozby, ktoré môžu ohroziť systém. Ďalšou dôležitou úlohou je vykonávať pravidelné testovanie na overenie či pravidlá brány firewall fungujú podľa očakávania. Pravidlá a sady pravidiel brány firewall by sa tiež mali pravidelne zálohovať. Je dôležité často kontrolovať politiku brány firewall. Kontrolou sa môžu odhaliť pravidlá, ktoré už nie sú potrebné ako aj nové požiadavky na politiku, ktoré je potrebné pridať do brány firewall. Najlepšie je kontrolovať politiku brány firewall v pravidelných intervaloch. Každá kontrola by mala zahŕňať podrobné preskúmanie všetkých zmien od poslednej pravidelnej kontroly, najmä kto a za akých okolností zmeny vykonal. Na vykonanie bezpečnosti firewallu môže byť použité penetračné testovanie. Toto testovanie možno použiť na overenie či sada pravidiel brány firewall funguje tak, ako by mala [11].

3. HIGH AVAILABILITY

HA je schopnosť systému pracovať nepretržite bez zlyhania sieťovej infraštruktúry počas určeného časového obdobia. Namiesto použitia jedného firewallu na ochranu siete sú dva alebo viac firewallov nasadených v skupine nazývanej klaster. Tieto brány firewall sa navzájom synchronizujú pomocou tzv. heartbeat spojenia, ktorým je informovaný jeden firewall, ak druhý zlyhal. Následne je redundantným firewallom bezproblémovo poskytnuté existujúce pripojenie a aj poskytnutá nepretržitá ochrana bez prerušenia. Vzorová počítačová sieť s HA je na obrázku č.3.1. Tu sa črtá otázka, že prečo je potrebné nakonfigurovať HA u firewallov. U HA je vždy potrebné nakonfigurovať synchonizáciu. Firewall sa oproti smerovaču odlišuje tým, že smerovač má smerovacie tabuľky a firewall má TCP spojenia otvorené. Synchronizácia je potrebná napr. pre nastavenie služby NAT. Redundancia u prepínačov sa robí pomocou STP a redundancia u smerovačov sa robí pomocou smerovacích protokolov [12].



Obr. č.3.1 HA

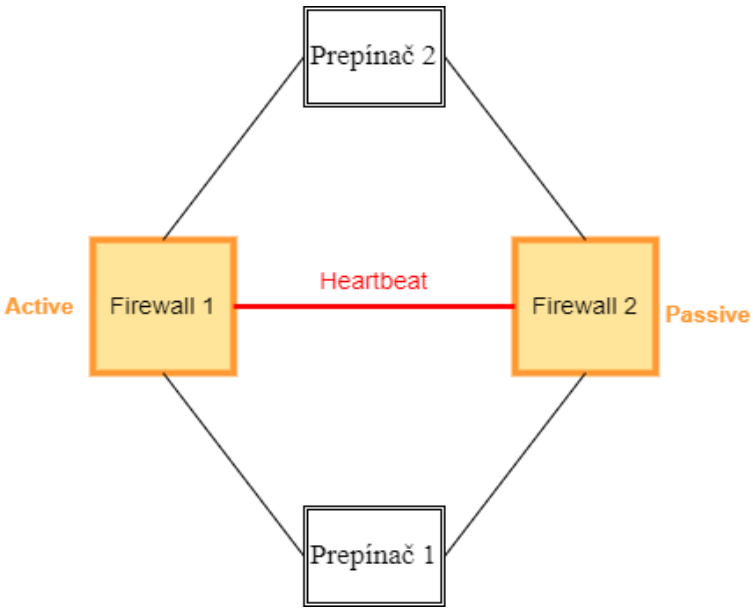
Aktívny a pasívny firewall

Aktívny firewall je firewall, ktorý je aktuálne aktívny. Pasívny firewall je firewall, ktorý je aktuálne neaktívny, cez ktorého neprechádza žiadna sieťová prevádzka. Taktiež je označovaný aj ako náhradný, sekundárny alebo záložný firewall [12].

3.1 Konfigúracia firewallov klastra

Samotné firewally je možné nasadiť pomocou rôznych konfigurácií firewallov v klastri. Existuje päť základných typov [13]:

- Aktívny/Pasívny– V Aktívnej/Pasívnej konfigurácií je cez jeden firewall aktívne riadená prevádzka, zatiaľ, čo druhý friewall je synchronizovaný a pripravený na prechod do aktívneho stavu v prípade zlyhania. V tomto režime sú cez oba firewally zdieľané rovnaké konfiguračné nastavenia a cez jeden firewall je aktívne riadená prevádzka, kým nedôjde k zlyhaniu cesty, spojenia, systému alebo siete. Keď aktívny firewall zlyhá, následne je pasívny firewall prejdený do aktívneho stavu a plynule je ním prevezmutá kontrola a sú zároveň presadené rovnaké zásady na udržanie bezpečnosti siete. Aktívna/Pasívna konfigurácia je zobrazená na obrázku č.3.2.



Obr. č.3.2 Aktívny/Pasívny klaster

- Aktívny/Aktívny – V konfigurácií Aktívny/Aktívny je viac aktívnych firewallov. Ak dôjde k výpadku jedného firewallu, premávka, ktorá je preň určená, sa pridelí inému, aktívnemu firewallu. Zároveň sa vyrovná záťaž medzi zostávajúcimi uzlami.
- N+1 – V konfigurácií N+1 existuje aspoň jeden záložný firewall pre skupinu N aktívnych firewallov. Ak niektorý aktívny firewall vypadne, záložný firewall by mal byť schopný prevziať svoje povinnosti.
- N+M – Konfigurácia N+M má viac ako jeden záložný firewall, čo poskytuje väčšiu redundanciu ako nastavenie N+1.
- N to N – Je to kombinácia Aktívny/Aktívny a N+M konfigurácie [13].

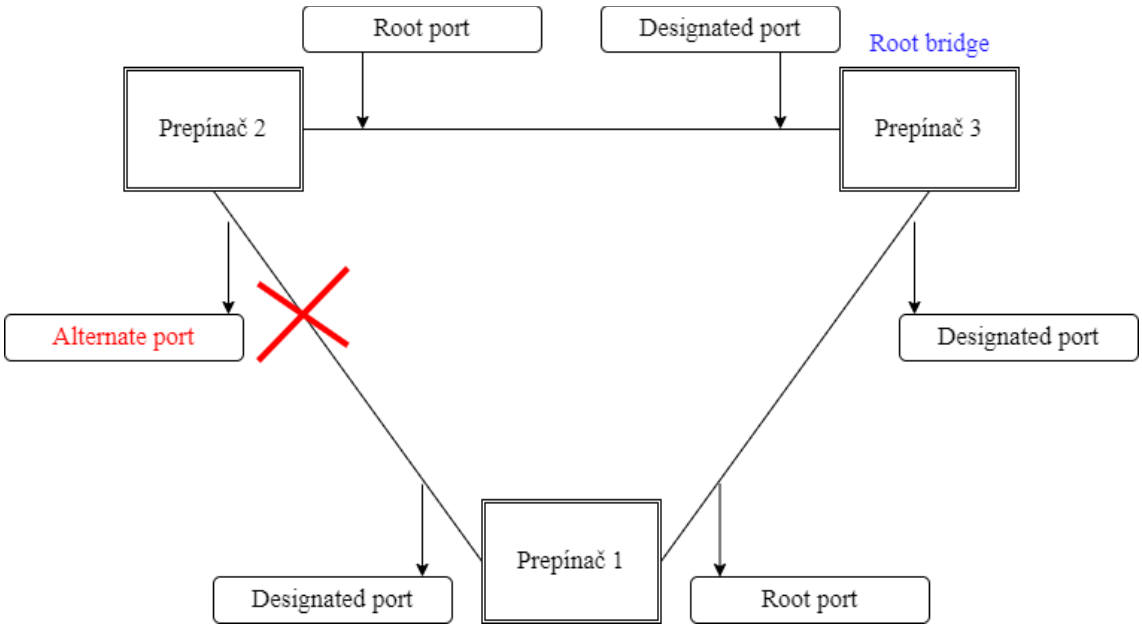
Prepínač

Pojem HA je známejší skôr u firewallov. U prepínačov môže byť problém s HA riešený napr. prostredníctvom STP.

U prepínačov je veľmi dôležité, že rámce nemajú na rozdiel od paketov TTL (Time To Live). Ak sú prepínače zapojené do slučky, dochádza k „rozmnožovaniu rámcov“ a následne je zahltená celá počítačová sieť – Broadcast storm. Z tohto dôvodu existuje STP, ktorým je zhodená linka tak, aby zostala iba kostra siete a boli odstránené slučky. Aby sa tak stalo, tak sú medzi všetkými prepínačmi v sieti vymieňané správy BPDU (Bridge protocol data Unit), aby bolo všetkými prepínačmi dohodnuté na tzv. Root bridge. Po výbere Root bridge musí byť každým prepínačom určené, ktorý z jeho portov bude Root port. To je určené na základe najnižšej ceny. Toto nastavenie sa dá zmeniť. Cieľom je vytvoriť logickú topológiu bez smyčiek tak, že bude blokovaný provoz na vybraných portov [14]. Rozdelenie portov a ich popis je zobrazený v tabuľke č.2. Počítačová sieť so STP je zobrazená na obrázku č.3.3.

Port	Popis
Root port	Porty najbližšie k Root bridge
Designated port	Ostatné fungujúce porty
Alternate port	Blokujúce porty, blokovaná prevádzka

Tab. č.2 Rozdelenie portov a ich popis



Obr. č.3.3 Počítačová sieť so STP

Smerovač

U smerovačov môže byť problém s HA riešený cez smerovacie protokoly. Smerovacie protokoly sa delia na:

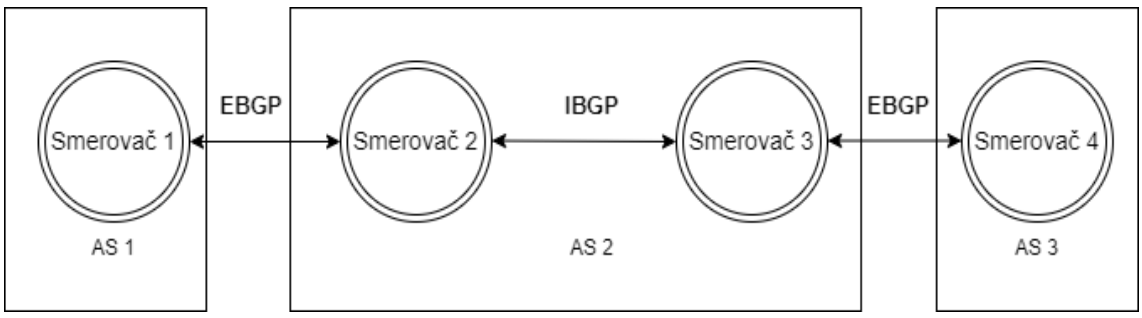
- Distance vector protokoly – Predstavujú typ smerovacích protokolov založených na distribuovanom výpočte v rámci ktorého je každým smerovačom spočítaná najlepšia cesta k dostupným sieťam. Táto najlepšia cesta je vektorovými protokolmi odmeraná a nazýva sa počet skokov. Počet skokov sa vzťahuje na konkrétny počet smerovačov, cez ktoré môžu dáta prechádzať pred dosiahnutím konečného cieľa. Následne sú tieto informácie cez distance vector protokoly odoslané do iných blízkych smerovačov. Odoslaním týchto informácií sú distance vector protokolmi určené najefektívnejšie smerovacie cesty.
- Link state protokoly – Je to typ smerovacích protokolov, ktorý predstavuje pokročilejší spôsob hľadanie najlepšej cesty. Namiesto počítania skokov sú priradené k linkám váhové koeficienty, tzv. metriky. Cieľom je nájsť cestu s najmenšou celkovou metrikou. Informácie o priradených metrikách sa vymieňajú medzi susednými smerovačmi pomocou správ LSA (Link State Agreement). V správe LSA je uvedené, ktorá časť informácie od ktorého smerovača pochádza. Následne je v týchto prijatých správach pridaná každým smerovačom informácia o sieťach a metrikách. Vo výsledku to znamená, že všetky smerovače poznajú celú topológiu počítačovej siete a majú rovnaké informácie k rozhodovaniu [15].

Medzi hlavné smerovacie protokoly patrí:

- OSPF (Open shortest path first) – Smerovací protokol OSPF je predstavitel link state protokolov. Patrí medzi protokoly IGP (Interior Gateway Protocol), čo znamená, že informácie sú vymieňané smerovačmi v rámci jednotlivých autonómnych systémov. Tieto systémy môžu zahŕňať jednu smerovaciu sieť alebo skupinu sietí fungujúcich pod rovnakou kontrolou. OSPF protokol podporuje delenie siete na podsiete, pričom používa masky. Pre prenos paketov sú používané linky, ktoré majú najmenšiu celkovú metriku. V prípade výpadku linky sa OSPF dokáže prispôsobiť zmenám v počítačovej sieti a nájsť alternatívnu cestu prostredníctvom záložných trás. Metrika jednotlivých liniek je odvodená od fyzickej vzdialenosti, zabezpečenia alebo od prenosovej rýchlosti. Hodnota metriky sa dá nastaviť administrátorom a pohybuje sa v intervalu 1-65535. V súčasnosti je veľmi požadovaná podpora alternatívnych ciest a aj podpora rozloženia záťaže [16].
- RIP (Routing Information Protocol) – Je to typ distance vector protokolov. Jeho využitie je možné nájsť predovšetkým v lokálnych sieťach. Maximálny počet skokov, ktoré môže RIP obsahovať, je 15 skokov. Smerovacie informácie sú na smerovači odosielané každých 30 sekúnd. Ak nie je smerovačom zachytená

informácia po dobu 180 sekúnd, tak je cesta označená ako nepoužitelná. Ak to bude 240 sekúnd, tak budú odstránené zo smerovacej tabuľky všetky informácie, ktoré sa vzťahujú k sieti. Vyvažovanie záťaže môže byť riešené prostredníctvom dvoch ciest s rovnakým počtom skokov. Ďalšia možnosť môže byť v riešení alternatívnej cesty. To znamená, že ak dôjde k výpadku primárnej cesty s najmenším počtom skokov, tak bude následne vybraná alternatívna cesta, ktorá mala pred výpadkom viac skokov ako primárna cesta. No po výpadku primárnej cesty sa stane táto alternatívna cesta primárnou cestou a bude mať ona v sieti najmenší počet skokov k cieľu [17] .

- BGP (Border Gateway Protocol) – Je to smerovací protokol, pri ktorom je cieľom nájsť najlepšiu cestu pre sieťový provoz prostredníctvom autonómného systému. Autonómný systém je skupina smerovačov a IP prefixov so spoločnou smerovaciou politikou a pod spoločnou politikou. Vlastné autonómné systémy majú napr. datacentra alebo poskytovateľa internetových služieb. Tieto autonómné systémy majú jedinečné číslo nazývané ASN (Autonomus System Number). Číslo autonómného systému predstavuje 16-bitového pole, takže môže mať až 65536 hodnôt. Prostredníctvom BGP je určená najlepšia cesta k ASN v závislosti od topológie sieťových uzlov a aktuálnych podmienok siete [18]. Pre prenos sa používa protokol TCP s portom 179. Smerovačom, ktoré medzi sebou komunikujú prostredníctvom protokolu BGP sa hovorí „peer“. Výmena smerovacích informácií medzi týmito smerovačmi sa nazýva „peering“. Pre prenos medzi autonómnymi systémami sa pužíva eBGP (Exterior Border Gateway Protocol). Ak sa prenášajú smerovacie informácie v rámci jedného autonómného systému, tak sa pužije iBGP (Interior Border Gateway Protocol). Vzorová počítačová sieť s iBGP a eBGP je zobrazená na obrázku č.3.4 [19].



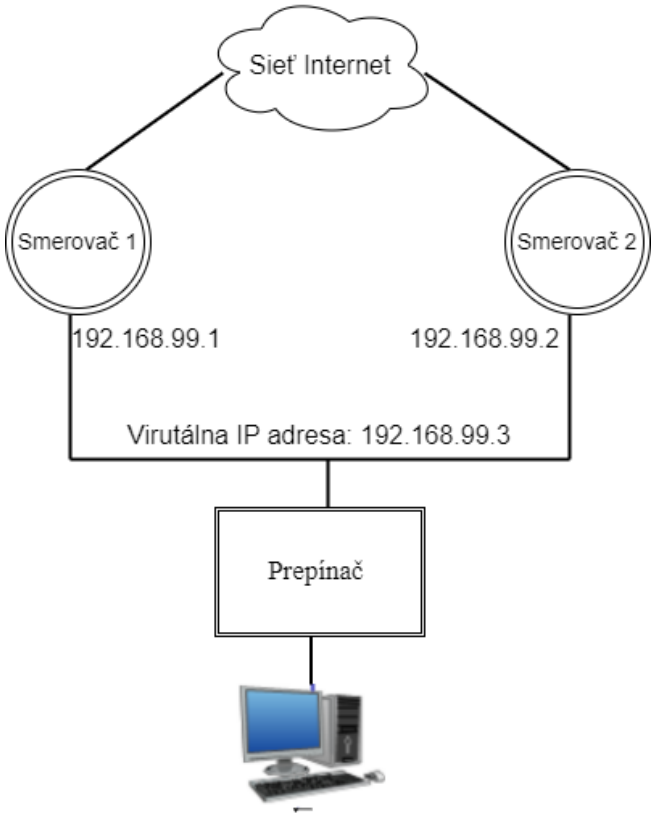
Obr. č.3.4 Počítačová sieť s BGP

HSRP

HSRP (Hot Standby Router Protocol) je protokol, ktorým je umožnené zálohovať zdroje dostupnosti východzej brány. Je to protokol od firmy Cisco. U HSRP je používaný UDP port 1985 a u prenosu je používaný multicast. Pakety HSRP majú nastavené TTL na 1. To znamená, že HSRP môže byť použitý len v rámci jednej siete. Hlavným cieľom tohto protokolu je združovanie minimálne dvoch smerovačov do skupiny za účelom zálohovania východzej brány pre koncové stanice, ktoré sa nachádzajú iba v jednej sieti. Taktiež sa veľmi často používa na rozdeľovanie záťaže medzi viacerými smerovačmi.

Princíp HSRP spočíva v tom, že každý smerovač ma svoju vlastnú IP adresu, ale skupina smerovačov má jednu virtuálnu IP adresu. Následne je jeden smerovač zvolený za aktívny (active), ktorým bude plnená funkcia východzej brány. Tento smerovač bude obsahovať virtuálnu IP adresu. V ďalšej skupine bude jeden smerovač zvolený ako záložný (standby) smerovač. Ak aktívny smerovač zlyhá, tak bude prebraná funkcia východzej brány práve týmto záložným smerovačom.

Medzi aktívnym a záložným smerovačom sú vymieňané správy. Tieto správy sú posielané každé tri sekundy (hello interval). Smerovač je považovaný za nedostupný ak nepríde odpoveď od druhého smerovača po viac ako desiatich sekundách (hold interval). Na obrázku č.3.5 je zobrazená počítačová sieť s HSRP protokolom [20].



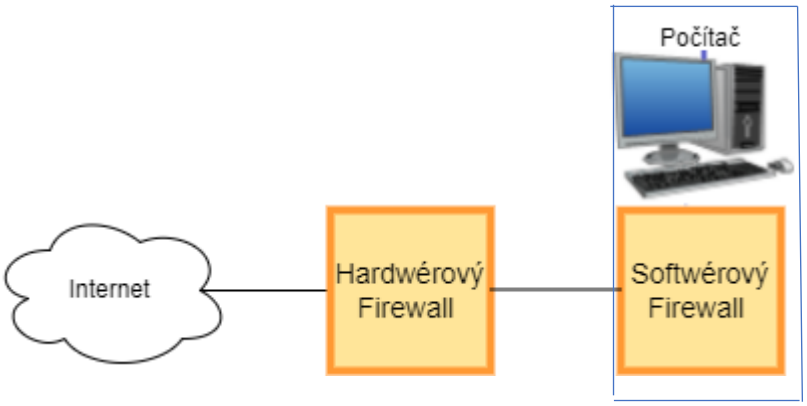
Obr. č.3.5 Počítačová sieť s HSRP protokolom

VRRP

VRRP (Virtual Router Redundancy Protocol) je tiež protokol, ktorým je umožnené zálohovať zdroje dostupnosti východzej brány. Je to otvorený štandard IETF (Internet Engineering Task Force) v RFC (Request For Comments) 3768. Čo znamená, že tento protokol je ideálne použiť v sieti vtedy, ak sa v sieti nachádzajú zariadenia od rôzných výrobcov [21].

4. HIGH AVAILABILITY FIREWALLY

Firewally sú rozdelené na tri druhy skupín. Sú to softvérové, hardvérové a virtuálne firewally. Na obrázku č.4.1 je počítačová sieť s hardvérovým a aj so softvérovým firewallom.



Obr. č.4.1 Počítačová sieť s hardvérovým a aj so softvérovým firewallom

4.1 Softvérové firewally

Hlavnou myšlienkou je, že počítač používáme ako firewall. Zástupcom osobných počítačov môže byť napr. domáci počitač [22].

Softvérový firewall je typicky reprezentovaný serverom s dvoma sieťovými rozhraniami a špeciálnou aplikáciou, ktorá je zodpovedná za také funkcie, ako filtrovanie paketov alebo NAT. Všetky pakety prechádzajúce z jednej podsiete do druhej sú filtrované podľa pravidiel napísaným administrátorom. Softvérové firewally majú vyhradené prostriedky operačného systému, na ktorom sú nainštalované a nemôžu fungovať automaticky. Pre správnu činnosť je ich možné rozšíriť o ďalšie prídavné moduly. Výhodou softvérového firewallu je, že na internete je dostupných veľa bezplatných verzií [23].

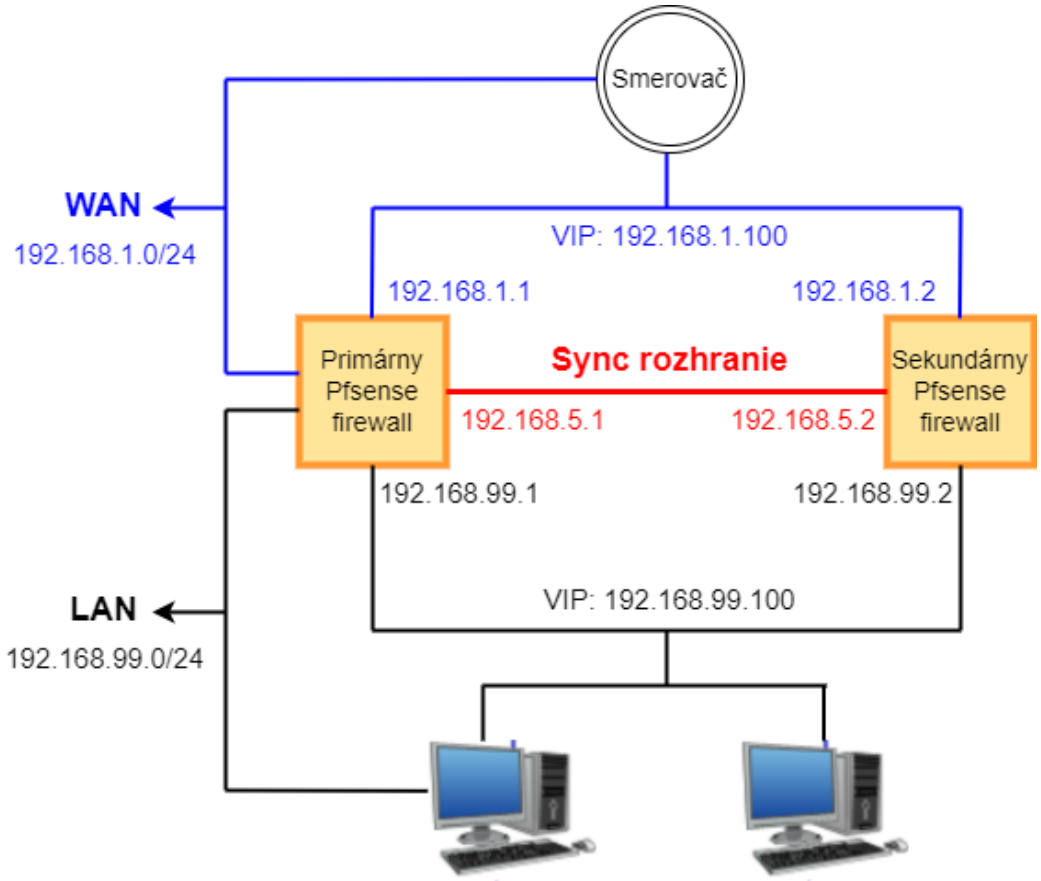
4.1.1 Pfsense

Pfsense je bezplatný open source firewall. Môže byť nainštalovaný na rôznom hardvéri. Tento firewall má pre konfiguráciu užívateľský prívetivé webové rozhranie, ktorým je uľahčená správa aj pre používateľov s obmedzenými sieťovými znalosťami. Samotné aktualizácie softvéru je možné spustiť z webového používateľského rozhrania. Tiež je tu umožnená inštalácia balíkov tretích strán s otvoreným zdrojovým kódom, ako napr. Snort [23].

Pfsense je jedným z mála riešení s otvoreným zdrojovým kódom, kde funguje high availability. Vzorová počítačová sieť s Pfsesne firewallami je zobrazená na obrázku č.4.2.

Na dosiahnutie čo najlepšej high availability slúžia tieto tri funkcie:

- CARP (Common Address Redundancy Protocol) pre redudanciu IP adries
- XMLRPC na synchronizáciu konfigurácie a replikáciu údajov z jedného servera na druhý
- pfsync na synchronizáciu tabuľky stavov medzi uzlami klastra



Obr. č.4.2 Počítačová sieť s Pfsense firewallami

S Pfsense firewallami je vytvorený aktívny/pasívny klaster, pričom primárny uzol je hlavný uzol a sekundárny uzol je v úlohe zálohovania. V prípade zlyhania primárného uzla sú funkcie primárného uzla prebrané sekundárnym uzlom. Dva alebo viac sekundárnych firewallov sa často nazývajú „HA klaster“. Jedno rozhranie na každom uzle klastra je vyhradené pre úlohy synchronizácie. Toto sa zvyčajne označuje ako rozhranie Sync a používa sa na synchronizáciu konfigurácie a synchronizáciu stavu pfsync. Taktiež aj zmeny v tabuľke stavu na primárných uzlov sú odosielané do sekundárnych uzlov cez rozhranie Sync a naopak. Je možné použiť akékoľvek dostupné rozhranie na firewalle. Na druhej strane toto rozhranie nie je určené na prenos CARP. Najbežnejšia a najideálnejšia konfigurácia klastra High Availability obsahuje iba dva uzly. V klastri je možné mať viac uzlov, ale neposkytujú výraznú výhodu. Konfigurácie s viac ako dvoma uzlami nie sú oficiálne podporované.

CARP bol vytvorený vývojármi OpenBSD ako bezplatné, otvorené redundantné riešenie na zdieľanie IP adries medzi skupinou sieťových zariadení. CARP bol vytvorený v októbri 2003. CARP má podobnú funkciu ako HSRP.

Virtuálna IP adresa (VIP) typu CARP je zdieľaná medzi uzlami klastra. Jeden uzol je hlavný a je určený na prijímanie IP adresy a ostatné uzly sú určené na udržiavanie stavu zálohovania a tiež na monitorovanie prevzatia role hlavného firewallu ak predchádzajúci hlavný uzol zlyhá. Keďže IP adresa je používaná súčasne iba jedným členom klastra, nedochádza ku konfliktu IP adries pre CARP VIP. Aby prepnutie medzi firewallami pri zlyhaní fungovalo správne, je dôležité, aby prichádzajúca prevádzka do klastra bola posielaná na CARP VIP a odoslaná prevádzka bola posielaná z CARP VIP. Ak by bola prevádzka adresovaná priamo uzlu a nie CARP VIP, potom túto prevádzku nepríjmú iné uzly [24].

4.2 Hardvérové firewally

Sa používajú pre väčšie počítačové siete. Tieto firewally majú vyhradené komponenty a zdroje, ktoré sú optimálne prispôsobené pre správnu a rýchlu prácu. Pri výbere konkrétneho modelu hardvérového firewallu by sa mala starostlivo analyzovať technická dokumentácia výrobcu. Dôležitou vlastnosťou hardvérových firewallov je, že nie sú závislé od softvéru tretej strany. Medzi hardvérové firewally patria: Palo Alto, Juniper, Fortigate alebo ASA firewall [10].

4.2.1 FortiGate

FortiGate je vysokovýkonné zariadenie NGFW pre veľké podniky a poskytovateľov služieb so vstavanými schopnosťami SD-WAN, šifrovanými tunelmi IPSEC (Internet Protocol Security) a rôznymi možnosťami nasadenia.

Na vytvorenie high availability režimu je potrebné, aby záložný Fortigate firewall mal rovnakú verziu firmwaru FortiOS a rozhrania aby neboli nakonfigurované na získavanie adries z DHCP (Dynamic Host Configuration Protocol). Predtým nainštalovaný FortiGate bude naďalej fungovať ako primárna jednotka a nový FortiGate bude fungovať ako záložný FortiGate. Pre HA je tu používaný FGCP (FortiGate Clustering Protocol), ktorý poskytuje ochranu pred zlyhaním. Toto nastavenie sa volá FortiGate High Availability [25].

4.2.2 Palo Alto

Sú to firewally od spoločnosti Palo Alto Networks. Tiež je to vysokovýkonné zariadenie NGFW. Cez tieto firewally je poskytnutá viditeľnosť a kontrola nad aplikáciami, používateľmi a obsahom.

V jednom klastri môže byť maximálne 16 firewallov. Tieto firewally môžu byť v klastri vytvorené ako pár alebo môžu byť vytvorené samostatne. Ak nastane zlyhanie na firewalle v HA páre alebo samostatne v klastri, tak záložný firewall prevezme úlohu

zabezpečenia prevádzky. Tento záložný firewall sa v Palo Alto firewalloch často označuje aj ako peer firewall.

Existuje tu high availability režim aktívny/aktívny, kde je výkon distribuovaný do dvoch rovnakých konfigurovateľných zariadení, alebo je tu tiež režim aktívny/pasívny, kde prebieha synchonizácia z primárného firewallu. V režime aktívny/pasívny, keď aktívny firewall zlyhá, tak pasívny firewall sa stane aktívným. Tento režim má jednoduchší dizajn. V režime aktívny/aktívny je synchrónne spracovanie firewallov. Smerovacie tabuľky obi dvoma firewallami sú udržované a navzájom synchronizované. V režime aktívny/aktívny nie je podporovaný klient DHCP. Taktiež môže ako DHCP relay fungovať iba primárny firewall. V tomto režime pri konfigurácií nedochádza k vyvažovaniu záťaže. Oproti režimu aktívny/pasívny má režim aktívny/aktívny zložitejší dizajn, kde je nutné replikovať NAT rozsahy. Aktívny/aktívny režim sa odporúča, ak je potrebné u každého firewallu nakonfigurovať vlastné inštancie smerovania. Avšak existujú aj výnimky, kde HA má väčšie obmedzenia, sú to firewally série VM na Azure a firewally série VM na AWS, kde u týchto firewallov existuje len aktívny/pasívny HA. Ak na firewall AWS sa nasadí služba Amazon Elasc Load, tak HA nefunguje vôbec. Taktiež HA nefunguje aj u firewallu série VM na platfome Google Cloud. Požiadavky na aktívny/pasívny a aktívny/aktívny HA sú zobrazené na v tabuľke č.3.

Požiadavky na Aktívny/Pasívny a Aktívny/Aktívny HA u Palo Alto firewallov
Obi dva firewally musia mať rovnaký model
Obi dva firewally musia mať rovnakú verziu
Obi dva firewally musia mať rovnakú schopnosť multivirtuálného systému
Obi dva firewally musia mať rovnaký typ rozhraní
Obi dva firewally musia mať rovnaký druh licencií
Obi dva firewally musia mať povolený HA

Tab. 3 Požiadavky na Aktívny/Aktívny a Aktívny/Pasívny HA (Palo Alto)

Niektoré modely firewallu Palo Alto majú vyhradené porty HA: radiace prepojenie (HA1) a dátove prepojenie (HA2). U členov klastra HA je používané HA4 záložné prepojenie na vykonanie synchronizácie stavu relácie. HA1, HA2 a preposielanie paketov (HA3) nie sú podporované medzi členmi klastra, ktoré nie sú pármi v HA. HA1 sa používa na výmenu pozdravov, heartbeat a na informácie o stave HA. Na výmenu heartbeat je používaný ICMP (Internet Control Message Protocol) protokol. HA1 je prepojenie tretej vrstvy a je tu vyžadovaná IP adresa. Pre HA1 je používaný TCP port 28260 na komunikáciu. Dátove prepojenie HA2 sa používa na synchronizáciu relácií, preposielanie tabuliek, IPsec asociácií a na preposielanie ARP (Address Resolution Protocol) tabuliek. Dátový tok na linke HA2 je vždy jednosmerný. To znamená, že dátovy tok je nastavený tak, aby mohol ísť z aktívného firewallu do pasívného firewallu. Prepojenie HA2 je spojenie druhej vrstvy. U HA2 sú využívané na prenos porty 99 alebo 29281. Prepojenie H4 je určené na synchronizáciu vyrovnávajúcej pamäte medzi všetkými členmi klastra HA s rovnakým ID (Identification Number) klastra [26].

4.2.3 Juniper

Sú to taktiež NGFW. Sú ideálnym riešením pre viditeľnosť, kontrolu a prevenciu na okraji siete. Ochrana pred hrozbami začína úplným prehľadom o tom, kto a čo prechádza sieťou. U Juniper firewallov je výborná schopnost detekovať hrozby v reálnom čase [27].

4.3 Virtuálne firewally

Je to firewall implementovaný ako virtuálny stroj, najčastejšie používaný na filtrovanie paketov v SDN (Software Defined Networks) a na ochranu dát v cloudových službách. Funkčnosť virtuálnych počítačov je v prostredí monitorové hypervízorom. Hypervízor je technika virtualizácie, pri ktorej je umožnené spúšťať viac operačných systémov na hostiteľovi. Keď v rámci jedného virtuálneho prostredia funguje viacero strojov, tak potom je vytvorená virtuálna sieť zahŕňajúca všetky fyzické sieťové prvky. Vďaka virtualizačnej vrstve je možné meniť hardvérové prostriedky priradené stroju. Virtuálny firewall je zodpovedný za bezpečnosť komunikácie virtuálneho hostiteľa, ale aj za komunikáciu medzi fyzickou a virtuálnou sieťou. Výhodou virtuálnych firewallov je flexibilita pri zmene hardvérových parametrov každého stroja [10].

5. ASA FIREWALLY

ASA (Adaptive Security Appliance) firewally sú firewally od spoločnosti Cisco. Je to bezpečnostné zariadenie, ktoré kombinuje firewall, antivírus a VPN (Virtual Private Network). Prostredníctvom ASA firewallov sú poskytované služby, ktorými je chránená sieť pred hrozbami, ako je DoS (Denial of Service) útok alebo iné typy útokov. Tieto firewally môžu byť použité ako bezpečnostné riešenie pre malé aj veľké siete [28]. Existujú ako hardvérové a softvérové firewally. Tieto softvérové firewally majú označenie ASAv (Adaptive Security Virtual Appliance) [29].

Pri konfigurácií ASA firewallov existuje všeobecný postup ako nakonfigurovať ASA firewally. Tento postup sa skladá z piatich krokov, pričom každý krok je síce dobrovoľný, no pre ideálnu bezpečnú sieť je doporučovaný. Jednotlivé kroky pre ideálne zabezpečenie počítačovej siete ASA firewallom sú:

- Prístupové pravidlá – Tieto pravidlá môžu byť aplikované buď na rozhranie alebo globálne, a predstavujú prvú ochrannú líniu. V predvolenom nastavení majú ASA firewally nastavený voľný tok prevádzky z vnútornej siete do vonkajšej siete. Na obmedzenie premávky do vnútornej alebo vonkajšej siete sa používájú prístupové pravidlá. Existujú základné pravidlá prístupu riadenia prevádzky na základe portu, protokolu a cieľovej adresy. Pravidlá môžu byť kontrolované aj na základe identity. Tým je umožnené konfigurovať pravidlá na základe identity používateľa. Je potrebné si nainštalovať Cisco CDA (Context Directory Agent), tiež známy ako AD agent, na samostatný server, aby by mohli byť na ňom zhromaždené informácie o používateľovi. Pravidlá na základe identity užívateľa tiež môžu byť konfigurované cez modul ASA FirePOWER.
- Filtrovanie aplikácií – Dnes sú vo veľkom množstve po celom svete používané webové aplikácie. A práve u týchto webových aplikácií sú používané protokoly aplikačnej vrstvy HTTP a HTTPS (HyperText Transfer Protocol Secure). Na základe základných pravidel prístupu je možné tieto protokoly zakázať alebo povoliť. Na ASA je možné nainštalovať modul, ktorým sa zabezpečí filtrovanie aplikácií cez protokoly aplikačnej vrstvy. Následne môže byť zabranené aplikáciám, ktoré sú pre sieť neprijateľné. Zástupcom takéhoto modulu je napr. ASA FirePOWER.
- Filtrovanie URL (Uniform Resource Locator) – Filtrovanie adries URL sa používa na zablokovanie alebo povolenie prístupu na webovú stránku. Tým sa môžu definovať služby, ktoré sú nežiadúce, ako sú napr. hazardné hry. Na aplikovanie filtrovania URL adries je taktiež ideálny ASA FirePOWER.
- Ochrana pred hrozbami – Je umožnená implementácia opatrení na ochranu pred skenovaním, DoS útokmi alebo inými útokmi. U ASA firewallov je umožnená fragmentácia IP paketov. Čo znamená, že budú zahodené pakety, ktoré neboli schválené bezpečnostnou kontrolou. Na túto možnosť ochrany

nie je potrebná žiadna konfigurácia. Ďalšia ochrana pred hrozbami spočíva v limitoch pripojení TCP a UDP pripojenia. Tieto limity pripojenia sú predovšetkým určené na ochranu pred DoS útokmi, ako je napr. TCP SYN flood útok.

- NAT – Je bližšie popísaný v kapitole 5.1 [30].

5.1 NAT

Jednou z hlavných funkcií prekladu sieťových adries NAT je umožniť privátnym IP sieťam pripojiť sa k internetu. NAT predstavuje preklad súkromnej IP adresy na verejnú IP adresu, pričom tieto IP adresy je možné použiť v sieti internet. Týmto spôsobom je prostredníctvom NAT umožnené šetrenie verejných IP adries, lebo jedna verejná IP adresa môže predstavovať celú sieť. Medzi ďalšie funkcie NAT patria:

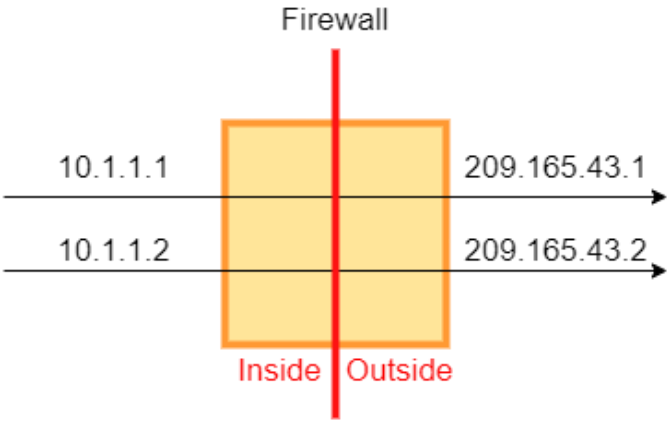
- Bezpečnosť – Pod pojmom bezpečnosť sa rozumie udržiavanie skrytých súkromných IP adries, čo odrádza od priamych útokov.
- Flexibilita – Možnosť meniť podľa vlastnej potreby súkromné IP adresy bez ovplyvnenia verejných IP adries.
- Preklad medzi IPv4 (Internet Protocol version 4) a IPv6 (Internet Protocol version 6) – Pri NAT je umožnené preklad týchto dvoch adries.

Súkromné IP adresy sú pevné definované. V RFC 1918 je definované, ktoré IP adresy môžu byť ako súkromné IP adresy. Sú to:

- 10.0.0.0 až 10.255.255.255
- 172.16.0.0 až 172.31.255.255
- 192.168.0.0 až 192.168.255.255

Dynamický NAT

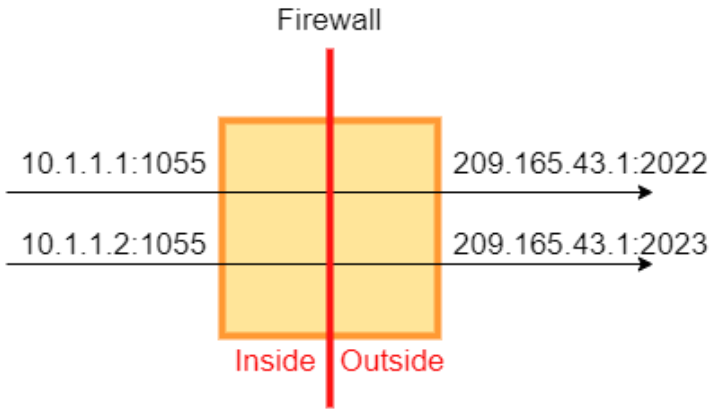
Pri dynamickom preklade adries je skupina súkromných IP adries mapovaná na skupinu mapovaných verejných IP adries. To znamená, že sú dynamicky vyberané adresy z globálného fondu adries, ktoré aktuálne nie sú nikde priradené. Preklad sa vytvorí len vtedy, keď je hostiteľom inicializované spojenie. Dynamický NAT je vykreslený na obrázku č.5.1.



Obr. č.5.1 Dynamický NAT

PAT (Dynamic Port Address Translation)

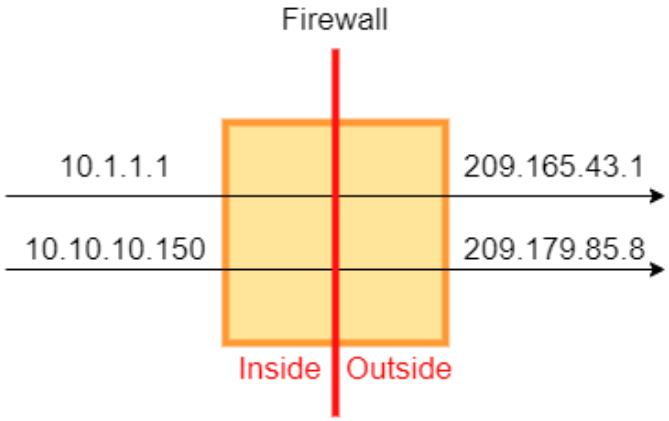
Tu je skupina IP adries mapovaná na jednu IP adresu pomocou jedinečného zdrojového portu tejto IP adresy. Preklad adries prostredníctvom PAT je vykreslený na obrázku č.5.2.



Obr. č.5.2 PAT

Statický NAT

Statický NAT je mapovanie medzi jednou súkromnou a jednou verejnou IP adresou. Tým je umožnené spustenie obojsmernej inicializácie pripojenia k hostiteľovi a aj od neho. Na obrázku č.5.3 je zobrazený typický scénar statického NAT [31].



Obr. č.5.3 Statický NAT

5.2 VPN

VPN je jednoduchý softvér, ktorý bol vytvorený s cieľom chrániť súkromie užívateľov a sťažiť život útočníkom tým, že bude anonymizovaná premávka a poloha. Ide o vytvorenie súkromného tunela pre dáta a komunikáciu, keď sa v komunikácií používajú verejné siete. Je vytvorené bezpečné a šifrované spojenie medzi počítačom a internetom.

U VPN je presmerovaná komunikácia cez iné servery. To znamená, že aktuálna fyzická poloha bude skrytá. Zdroj pripojenia bude zobrazený ako jeden z mnohých smerovačov VPN – nazývaných proxy server. Existujú dva základné typy VPN: site-to-site VPN a remote-access VPN [32].

Šifrovanie a tunelovanie u VPN

Šifrovanie znamená zmenu otvoreného textu na nečitateľnú časť. Existujú tri hlavné typy šifrovania: hašovanie, symetrická kryptografia a asymetrická kryptografia.

Je tu proces tunelovania, ktorým je umožnené použiť verejnú sieť, ako je internet, na vytváranie bezpečných spojení medzi vzdialenými používateľmi a privátnou podnikovou sieťou. Každé zabezpečené pripojenie sa nazýva tunel. U ASA firewallov sú používané na budovanie a správu tunelov štandardy tunelovania ISAKMP (Internet Security Association and Key Management Protocol) a IPsec ((Internet Protocol Security). Pri ASA firewalloch sú prijímané pakety zo súkromnej siete, následné sú zapuzdrené, potom sa vytvorí tunel a na koniec sú poslané na druhý koniec tunela, kde sú nezapuzdrené a odoslané do svojho konečného cieľa. Samotný proces pozostáva z následovných krokov:

- 1. Dohodnutie parametrov tunela
- 2. Vytvorenie tunela
- 3. Overenie užívateľov
- 4. Spravovania bezpečnostného kľúča
- 5. Šifrovanie a dešifrovanie údajov
- 6. Spravovanie prenosu údajov cez tunel [33]

IPsec

IPsec je skupina protokolov, ktoré sú používané na nastavenie šifrovaných spojení medzi zariadeniami. Tým sú dáta odosielané cez verejnú sieť v bezpečí. Veľmi často sa používa na nastavenie sietí VPN, kde sú z overeného zdroja šifrované pakety. IPsec je bezpečný, pretože predstavuje proces šifrovania a autentizácie [32].

IPsec je pri HA u ASA firewallov povolený iba pri aktívnej/pasívnej konfigurácií [33]. IPsec nie je iba jeden protokol, ale súbor protokolov. Balík IPsec je vytvorený z týchto protokolov:

- AH (Authentication Header) – U tohto protokolu je zaistené, že pakety majú pôvod z dôveryhodného zdroja a, že neboli modofikované. U AH nie je poskytnuté šifrovanie.
- ESP (Encapsulating Security Protocol) – Pri tomto protokole je poskytnuté šifrovanie IP hlavičky.
- SA (Security Association) – Predstavuje protokoly, ktoré sú používané na vyjednávanie šifrovacích kľúčov a algortimov. Jeden z najbežnejších protokolov SA je IKE (Internet Key Exchange).

Balík IPsec je možné použiť v dvoch režimoch, ako je tunelový režim a transportný režim. V tunelovom režime je okrem paketu šifrovaná aj pôvodná hlavička IP paketu. V transportnom režime je obsah paketu zašifrovaný, ale pôvodná IP hlavička nie je šifrovaná [32].

ISAKMP

Je vyjednávací protokol, ktorým je možné dohodnúť sa na vytvorení priradenia zabezpečenia IPsec (SA). IKE používa ISAKMP na nastavenie SA pre IPsec. Prostredníctvom IKE sú vytvárané kryptografické kľúče, ktoré sú následne používané na autentizáciu. U ASA sú podporované verzie EKEv1 a EKEv2. Vytvorenie politiky IKE zahŕňa:

- Typ autentizácie – Väčšinou ide o podpis RSA (Rivest-Shamir-Adleman) pomocou certifikátov alebo o predzdieľaný kľúč.
- HMAC (Hashed Message Authentication) – Na zabezpečenie identity odosielateľa a na zabezpečenie toho, že správa nebude pri prenose zmenená.
- Diffie-Hellman – Na určenie sily algoritmu pre šifrovací kľúč. U ASA je používaný tento algoritmus na odvodenie šifrovacích a hash kľúčov.
- Obmedzenie času – Je to čas, počas ktorého ASA používa šifrovací kľúč pred jeho výmenou [33].

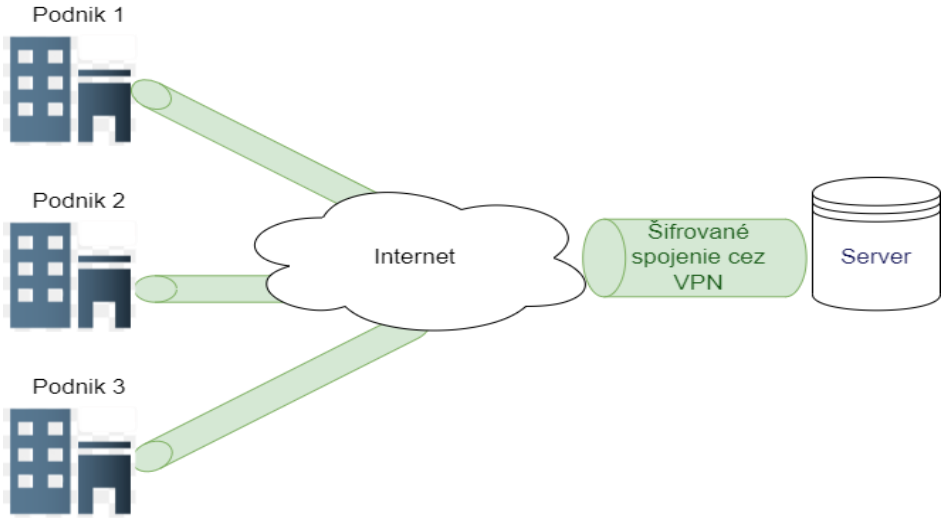
Remote-access VPN

U tohto druhu VPN je umožnené pripojiť užívateľov k inej sieti cez súkromný šifrovaný tunel. Pri tomto type VPN je umožnené organizáciam zdielať súbory so svojími zamestnancami. Je to ideálna možnosť ako sa pripojiť bezpečným spôsobom k spoločnosti. Je tu využitý model klient/server. Klient je aplikácia nainštalovaná na zariadený ako je napr. telefón alebo notebook, ktorou sú smerované aktivity cez server a aj šifrované údaje. Pri ASA firewalloch sa tento druh VPN nazýva Annyconect VPN. Pri Pfsense firewalloch sa tento druh VPN nazýva OpenVPN. Vzorový obrázok remote-access VPN je na obrázku č.5.4 [34].

Obr. č.5.4 Remote-access VPN

Site-to-site VPN

Tento druh VPN je použitý predovšetkým v podnikových prostrediach. Väčšinou vtedy ak má podnik sídla na rôzných miestach ako je napr. vládna agentura s viacerými kanceláriami. Inými slovami ide o spôsob prepojenia LAN sieti na rôzných miestach prostredníctvom verejného internetu. Užívateľ nemusí mať na svojom zariadený nainštalovaného klienta ako je to pri remote-access VPN. Šifrovací tunel existuje medzi bránami na každej lokalite. Pri ASA a Pfsense firewallov sa tento druh VPN nazýva IPsec VPN. Vzorový obrázok site-to-site VPN je na obrázku č.5.5 [35].



Obr. č.5.5 Site-to-Site VPN

5.3 HA

Na vytvorenie HA u ASA firewallov sú potrebné aspoň dva ASA firewally. U ASA firewallov je použitý termín failover. Je to možnosť automatického a bezproblémového prechodu na spoľahlivý zálohovací systém. U ASA sú podporované dva režimi failover: aktívny/aktívny a aktívny/pasívny. Existujú jednotlivé požiadavky na failover:

- Hardvérové požiadavky – Rovnaký model, rovnaký počet a typy rozhraní, nainštalované rovnaké moduly, rovnaká pamäť RAM (Random Access Memory).
- Softvérové požiadavky –Rovnaká verzia softvéru.
- Licencové požiadavky – Nemusia mať rovnaké licencie.

Ak sú splnené tieto podmienky, tak u ASA firewallov môže existovať failover. Cez failover sa medzi ASA firewallami oznamujú následovné informácie:

- Aktuálny stav jednotky
- Stav sieťového spojenia
- Správy keep-alive
- Replikácia konfigurácie a synchronizácia

Rozhranie failover pri zlyhaní nie je nakonfigurované ako bežné sieťové rozhranie, ale existuje len pre núdzovú komunikáciu. Toto rozhranie môže byť použité aj pre stavové prepojenie. Avšak ak existuje veľká konfigurácia, tak je potrebné zvážiť zvlášť rozhranie pre prepojenie stavu – statefull link a prepojenie pri zlyhaní – failover link. Pre prepojenie stavu sa môže použiť dátové rozhranie, ethernetové rozhranie alebo LAN. Stav aktívnych rozhraní a jednotiek je monitorovaný, aby sa určilo či sú splnené špecifické podmienky pre failover. Ak sú tieto podmienky splnené, dôjde k prepnutiu medzi ASA. Pri optimálnom výkone by latencia pre stavové pripojenia mala byť menšia ako 10 milisekúnd a nie väčšia ako 250 milisekúnd. V praxi sa odporúča aby failover linky

a dátové rozhrania existovali na rôznych cestách, aby sa znížila pravdepodobnosť, že všetky rozhrania zlyhajú súčasne. U stavového prepojenia je podporované:

- Tabuľka NAT
- Pripojenia a stavy TCP a UDP
- Tabuľka pripojenia HTTP
- Stavy pripojenia SCTP (Stream Control Transmission Protocol)
- Tabuľka ARP
- Tabuľka ISAKMP a IPsec SA
- Signalizačná relácia SIP (Session Initiation Protocol)
- Stav pripojenia ICMP
- Statické a dynamické smerovacie tabuľky
- Server DHCP (Dynamic Host Configuration Protocol)

No na druhej strane má stavové prepojenie aj svoje nevýhody. U stavového prepojenia nie je podporované:

- Tabuľka overenia používateľa
- Multicast smerovanie
- Presmerovanie portov
- Pluginy [36]

6. PRAKTICKÁ ČASŤ

V praktickej časti diplomovej práci boli vybrané dva firewally: Pfsense a ASA firewall. V diplomovej práci bola prakticky spracovaná problematika HA v režime NAT a vo VPN spojení. Tiež bolo otestované aj TCP spojenie, a to konkrétne pre protokol Telnet, SSH a BGP. Na praktickú realizáciu u ASA firewallu boli použité dva softvérové programy: GNS3 a Packet Tracert. Na praktickú realizáciu u Pfsense firewallu bol použitý program GNS3. Ako softvérové ASA firewally boli vybrané ASAv firewally s verziou 9.8.1. Tieto ASAv firewally predstavovali virtuálne sieťové zariadenia. Na druhej strane Pfsense firewally boli použité ako virtuálne stroje. Čo vo výsledku mohlo viesť ku skresleniu výsledkov, keďže virtuálne stroje majú väčšie nároky na procesor a operačnú pamäť. Cieľom praktickej časti bolo nakonfigurovať, overiť a porovnať správnosť nastavenia HA v režime VPN, NAT a TCP spojení pri jednotlivých firewalloch.

6.1 Realizácia ASAv firewallu v programe Packet Tracert

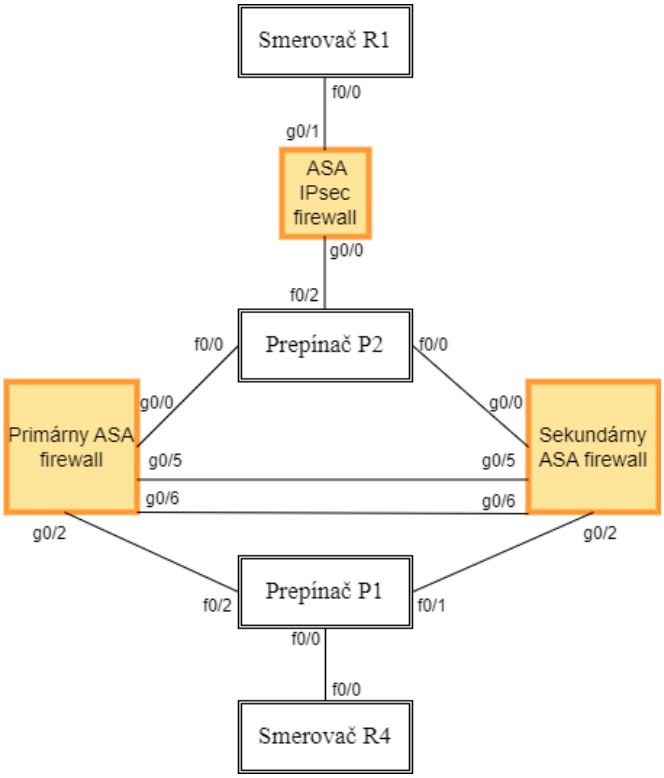
Na praktickú realizáciu u ASA firewallu bol ako prvý použitý softvérový program Packet Tracert. Cieľom bolo vyskúšať funkčnosť HA v softvérovej podobe u ASA firewallu. V programe bol použitý ASA firewall 5505 a ASA firewall 5506-X. Ako je vidieť z obrázka č.6.1, tak program Packet Tracert nepodporuje failover u týchto ASA firewallov.

```
ASA5506-X(config)#failover
                  ^
% Invalid input detected at '^' marker.

ASA5506-X(config)#show fail
ASA5506-X(config)#show failover
                    ^
% Invalid input detected at '^' marker.

ASA5506-X(config)#
```

Obr. č.6.1 ASA – Packet Tracert

6.2 Realizácia ASAv firewallu v programe GNS3 – IPsec VPN

Ako druhý softvér bol použitý program GNS3. Pre ASAv firewally bolo použitých päť topológií. Prvá bola určené pre IPsec VPN spojenie, druhá bola určená pre otestovanie správnosti dynamického NAT, tretia bola použitá pre Anyconnect VPN spojenie, a posledné dve boli určené pre overenie správnosti TCP spojenia. Boli použité softvérové ASAv firewally s verziou 9.8.1. Na obrázku č.6.2 je zobrazený grafický návrh počítačovej siete pre IPsec VPN spojenie a v tabuľke č.4. sú popísané rozhrania a k ním určené jednotlivé IP adresy.



Obr. č.6.2 IPsec VPN – GNS3

Názov	Port + IP adresa + zóna	Port + IP adresa + zóna	Port + IP adresa	Port + IP adresa
Primárny ASA firewall	G0/0 200.0.0.1 Outside zóna	G0/2 192.168.1.1 Inside zóna	G0/5 1.1.1.1	G0/6 2.2.2.1
	200.0.0.3 (Standby)	192.168.1.2 (Standby)	1.1.1.2 (Standby)	2.2.2.2 (Standby)
ASA IPsec firewall	G0/0 200.0.0.2 Outside zóna	G0/1 192.168.2.1 Inside zóna		

Tab. 4 IP adresy a rozhrania – IPsec VPN GNS3

Ako prvé boli nastavené IP adresy na daných rozhraniach ako je vidieť v tabuľke č.4. Smerovač s označením R4 mal iba jednu IP adresu: 192.168.1.20 a smerovač s označením R1 mal tiež len jednu IP adresu: 200.0.0.20. Tieto IP adresy mali obi dva smerovače na rozhraní f0/0. Ako smerovací protokol bol použitý protokol OSPF. Na obrázku č.6.3 je vidieť smerovaciu tabuľku smerovača R1 a taktiež aj neúspešný ping zo smerovača R1 na smerovač R4. Je zreteľné, že smerovač R1 mal smerovacie informácie vo svojej smerovacej tabuľke, no ping nefungoval, lebo nebolo nastavenie IPsec VPN spojenie medzi primárným ASAv firewallom a ASAv IPsec firewallom.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

O   IA 200.0.0.0/24 [110/11] via 192.168.2.1, 00:00:10, FastEthernet0/0
O   IA 192.168.1.0/24 [110/21] via 192.168.2.1, 00:00:10, FastEthernet0/0
C        192.168.2.0/24 is directly connected, FastEthernet0/0
R1#ping 192.168.1.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.20, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Obr. č.6.3 Neúspešný ping z R1 na R4

Následne boli nastavené pravidlá na vytvorenie zapezpečeného IPsec VPN spojenia. Na obrázku č.6.4 sú znázornené príkazy na vytvorenie predzdielaného kľúča. Toto nastavenie bolo rovnaké pre primárny ASAv firewall a aj pre ASAv IPsec firewall.

```
crypto ikev1 policy 10          # Vytvorenie ikev1
authentication pre-share        # Predzdielaný kľúč
encryption aes-256              # Zvolenie šifri
hash sha                        # Zvolenie typu hash
group 5                         # Použitie Diffie-Hellman
lifetime 84600                  # Koľko sekúnd má linka tvrať
```

Obr. č.6.4 Nastavenie predzdielaného kľúča

V druhom kroku bola nakonfigurovaná konfigurácia IPsec balíčka. Táto konfigurácia bola tiež rovnaká na obi dvoch ASAv firewalloch a je zobrazená na obrázku č.6.5

```
crypto ipsec ikev1 transform-set IPsecVPN esp-aes-256 esp-sha-hmac
```

Obr. č.6.5 Konfigurácia IPsec balíčka

Rozdielná konfigurácia bola pri konfigurácií ACL (Access Control List), kde boli povolené jednotlivé rozhrania IP adries ako je vidieť z obrázka č.6.6.

```
access-list IPsecVPN extended permit ip 192.168.1.0 255.255.255.0 192.168.2.0
255.255.255.0          # Nastavenie pre Primárny ASAv firewall
access-list IPsecVPN extended permit ip 192.168.2.0 255.255.255.0 192.168.1.0
255.255.255.0          # Nastavenie pre IPsec ASAv firewall
```

Obr. č.6.6 Konfigurácia – ACL

Po vytvorení ACL následovalo vytvorenie tunela a predzdielaného kľúča. Toto nastavenie bolo rozdielné pre obi dva firewally. Toto nastavenie je zobrazené na obrázku č.6.7 pre primárny ASAv firewall a na obrázku č.6.8. pre IPsec ASAv firewall.

```
tunnel-group 200.0.0.2 type ipsec-l2l
tunnel-group 200.0.0.2 ipsec-attributes
ikev1 pre-shared-key SHAREDKEY
```

Obr. č.6.7 Vytvorenie tunela – Primárny firewall

```
tunnel-group 200.0.0.1 type ipsec-l2l
tunnel-group 200.0.0.1 ipsec-attributes
ikev1 pre-shared-key SHAREDKEY
```

Obr. č.6.8 Vytvorenie tunela – IPsec firewall

Ako posledný krok bolo nastavenie crypto mapy a priradenie ju k rozhraniu outside. Toto nastavenie bolo taktiež odlišné pre obi dva firewally. Nastavenie crypto mapy a jej priradenie pre primárny ASAv firewall je nastavené na obrázku č.6.9 a pre IPsec ASAv firewall je zobrazené na obrázku č.6.10.

```
crypto map IPsecMAP 10 match address IPsecVPN
crypto map IPsecMAP 10 set ikev1 transform-set IPsecVPN
crypto map IPsecMAP 10 set peer 200.0.0.2
crypto map IPsecMAP 10 set security-association lifetime seconds 3600
crypto map IPsecMAP interface outside
```

Obr. č.6.9 Vytvorenie crypto mapy – Primárny firewall

```
crypto map IPsecMAP 10 match address IPsecVPN
crypto map IPsecMAP 10 set ikev1 transform-set IPsecVPN
crypto map IPsecMAP 10 set peer 200.0.0.1
crypto map IPsecMAP 10 set security-association lifetime seconds 3600
crypto map IPsecMAP interface outside
```

Obr. č.6.10 Vytvorenie crypto mapy – IPsec firewall

Po týchto nastaveniach bolo vytvorené IPsec VPN spojenie. Bol vyskúšaný ping zo smerovača R4 s IP adresou 192.168.1.20 na smerovač R1 s IP adresou 192.168.2.20. Ako je vidieť z obrázku č.6.11, tak ping bol v tomto prípade už úspešný.

```
R4#ping 192.168.2.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/48/64 ms
R4#
```

Obr. č.6.11 Úspešný ping z R4 na R1 – úspešné IPsec spojenie

Po úspešnom pingu zo smerovača R4 na smerovač R1 nasledovalo nastavenie High Availability. Nastavenie HA sa nastavovalo na primárnom ASAv firewalle a aj na sekundárnom ASAv firewalle. Nastavenie pre primárny firewall je zobrazené na obrázku č.6.12.

```
failover
failover lan unit primary
failover lan interface FAILOVER gigabitethernet0/5
failover link STATEFULL gigabitethernet0/6
failover interface ip FAILOVER 1.1.1.1 255.255.255.0 standby 1.1.1.2
failover interface ip STATEFULL 2.2.2.1 255.255.255.0 standby 2.2.2.2
```

Obr. č.6.12 Nastavenie HA – primárny ASA firewall

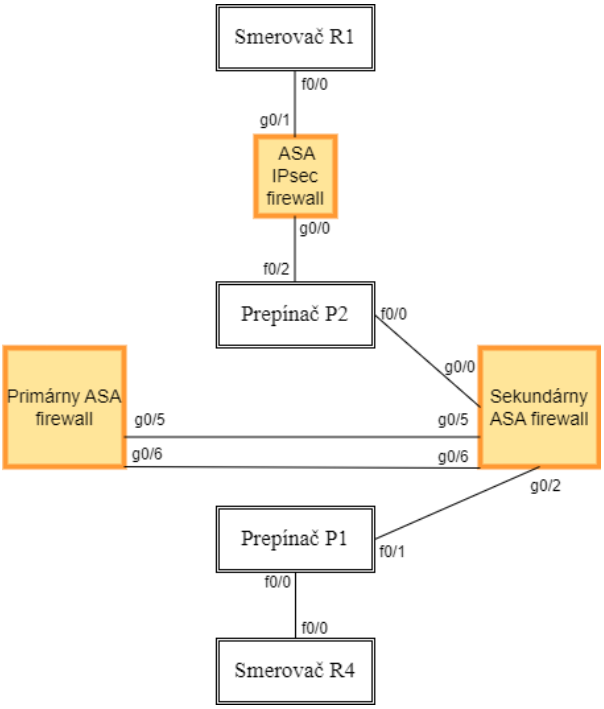
Ako je vidieť z obrázka č.6.12, tak daný ASAv firewall bol nastavený ako primárny cez príkaz *failover lan unit primary*. Rozhranie gigabitethernet0/5 bolo nastavené ako failover linka a rozhranie gigrabitethernet0/6 bolo nastavené ako statefull linka. Súčasne boli pre tieto rozhrania určené IP adresy a aj sekundárne tzv. standby adresy. Toto nastavenie bolo aj na sekundárnom ASAv firewalle, len s jednou výnimkou, že príkaz

failover lan unit primary bol nahradený príkazom *failover lan unit secondary*. Tým bol nastavený HA režim na obi dvoch firewalloch. Na obrázku číslo 6.13. je zobrazená kontrola nastavenia HA cez príkaz *show failover* na sekundárnom firewalle. Z tohto obrázka je vidieť, že na sekundárnom ASAv firewalle bol detekovaný primárny ASAv firewall.

```
Failover On
Failover unit Secondary
Failover LAN Interface: Failoverlink GigabitEthernet0/5 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 61 maximum
MAC Address Move Notification Interval not set
Version: Ours 9.8(1), Mate 9.8(1)
Serial Number: Ours 9A36BBFBB8F, Mate 9AHN7V6UJ8T
Last Failover at: 16:49:45 UTC Mar 12 2023
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: empty
                  Interface outside (200.0.0.3): Normal (Monitored)
                  Interface inside (192.168.1.2): Normal (Monitored)
        Other host: Primary - Active
                Active time: 1547 (sec)
                  Interface outside (200.0.0.1): Normal (Monitored)
                  Interface inside (192.168.1.1): Normal (Monitored)

Stateful Failover Logical Update Statistics
        Link : STATEFULL GigabitEthernet0/6 (up)
```

Obr. č.6.13 Kontrola nastavenia HA

Po zadaní príkazu *failover* na obi dvoch firewalloch bol súčasne zapnutý režim HA na obi dvoch firewalloch. Následne bola vypojená linka medzi primárnym ASAv firewallom a prepínačom P1 a taktiež aj linka medzi primárnym ASAv firewallom a prepínačom P2. Nová topológia počítačovej siete po vypojení daných liniek je zobrazená na obrázku č.6.14.



Obr. č.6.14 Zmenená topológia so sekundárnym ASAv firewallom

Z obrázka č.6.15 je vidieť, že sekundárny ASA firewall prešiel do aktívného módu a stal sa primárnym firewallom. Na obrázku č.6.15 nie je vidieť názov firewallu "ASASecundary", ale "ASAPrimary", lebo primárny firewall mal cez príkaz *hostname* nastavený názov "ASAPrimary". Následne po prepnutý sekundárneho firewallu do aktívného módu získal sekundárny firewall názov primarného firewallu – "ASAPrimary".

```
ASAPrimary(config)#
        Switching to Active
```

Obr. č.6.15 Sukundárny firewall v aktívnom móde

Z obrázka č.6.16 si je možné všimnúť, že sekundárny firewall bol v aktívnom móde a prevzial IP adresy primarného firewallu. Taktiež si je možné všimnúť, že primárny firewall mal nastavené a používané standby IP adresy.

```
Last Failover at: 21:45:42 UTC Mar 12 2023
        This host: Secondary - Active
                Active time: 67 (sec)
                slot 0: empty
                  Interface outside (200.0.0.1): Normal (Waiting)
                  Interface inside (192.168.1.1): Normal (Monitored)
        Other host: Primary - Failed
                Active time: 2809 (sec)
                  Interface outside (200.0.0.3): No Link (Waiting)
                  Interface inside (192.168.1.2): Normal (Monitored)
```

Obr. č.6.16 Výpis failover – sekundárny ASAv firewall

Po prepnutí sekundárného firewallu do aktívného módu bol otestovaný ping zo smerovača R4 na smerovač R1. Cieľom bolo otestovať funkčnosť nastavenia HA medzi dvoma softvérovými ASAv firewallami. Ako prvý bol zapnutý ping, neskôr boli prepojené linky podľa obrázka č.6.14. Z obrázka č.6.17 je vidieť funkčný ping medzi smerovačom R4 a smerovačom R1 aj po nastavení záložnej trasy cez IPsec firewall. Z tohto obrázku je vidieť aj chvíľkové prerušenie spojenia, no toto prerušenie spojenia nemalo vo výsledku veľký výpadok na sieťovú prevádzku. Vo výsledku to znamenalo, že bol na sekundárnom firewalle rýchlo načítaný OSPF proces a rýchlo sa vytvorilo susedstvo cez OSPF protokol. Tým bola overená správnosť nastavenia HA medzi softvérovými ASAv firewallami v IPsec VPN spojení.

```
R4#ping
Protocol [ip]:
Target IP address: 192.168.2.20
Repeat count [5]: 500
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 500, 100-byte ICMP Echos to 192.168.2.20, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!
*Mar 1 00:23:52.975 %OSPF-5-ADJCHG: Process 123, Nbr 200.0.0.1 on
FastEthernet0/0 from LOADING to FULL, Loading Done..
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (498/500), round-trip min/avg/max = 8/35/108 ms
```

Obr. č.6.17 Funkčný ping z R4 na R1

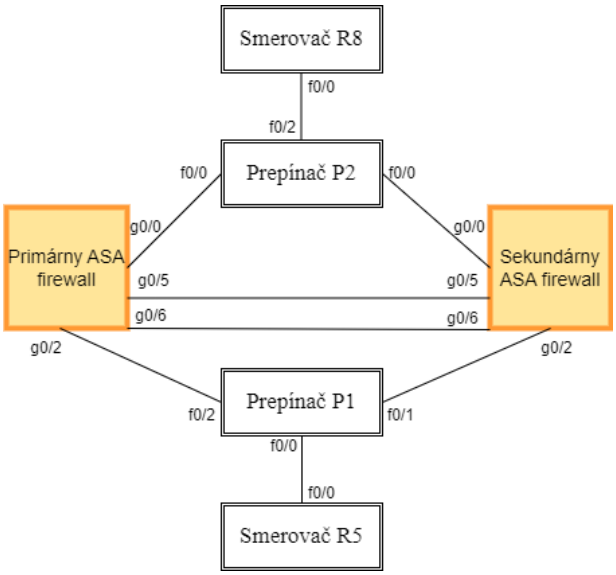
Nakoniec bola zobrazená na primárnom firewalle cez príkaz *show interface ip brief* tabuľka rozhraní a IP adries, tak ako je na obrázku č.6.18. Z tohto obrázka je vidieť, že na rozhraní g0/0 a g0/1 boli u primárného ASAv firewallu použité IP standby adresy a tiež, že tieto rohzrania sú vypnuté, čiže sú v režime down.

```
GigabitEthernet0/0         200.0.0.3       YES manual down                  down
GigabitEthernet0/1         unassigned      YES unset  administratively down down
GigabitEthernet0/2         192.168.1.2     YES manual down                  down
GigabitEthernet0/3         unassigned      YES unset  administratively down down
GigabitEthernet0/4         unassigned      YES unset  administratively down down
GigabitEthernet0/5         1.1.1.1         YES unset  up                    up
GigabitEthernet0/6         2.2.2.1         YES unset  up                    up
```

Obr. č.6.18 Standby adresy – primárny firewall

6.3 Realizácia ASAv firewallu v programe GNS3 – NAT

V druhej úlohe bolo za cieľ otestovať a overiť možnosť nastavenia HA pri konfigurácií dynamického NAT prostredníctvom softvérových ASAv firewallov v programe GNS3. Na obrázku č.6.19 je zobrazený grafický návrh počítačovej siete pre NAT a v tabuľke č.5. sú popísané rozhrania a k ním určené jednotlivé IP adresy pre primárny ASAv firewall. Smerovač s označením R8 mal IP adresu 200.200.200.20 na rozhraní f0/0. Smerovač s označením R5 mal IP adresu 192.168.1.20 na rozhraní f0/0.



Obr. č.6.19 NAT – GNS3

Názov	Port + IP adresa + zóna	Port + IP adresa + zóna	Port + IP adresa	Port + IP adresa
Primárny ASA firewall	G0/0 200.200.200.1 Outside zóna	G0/2 192.168.1.1 Inside zóna	G0/5 1.1.1.1	G0/6 2.2.2.1
	200.200.200.3 (Standby)	192.168.1.2 (Standby)	1.1.1.2 (Standby)	2.2.2.2 (Standby)

Tab. 5 IP adresy a rozhrania – NAT VPN GNS3

Po nakonfigurovaní IP adries na jednotlivých portov a OSPF protokolu bol nakonfigurovaný na primárnom ASAv firewalle dynamický NAT. Táto konfigurácia je zobrazená na obrázku č.6.20.

```
object network insideNAT
subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic interface
```

Obr. č.6.20 Konfigurácia NAT

Ešte pred samotnou konfiguráciou dynamického NAT bol zapnutý ping zo smerovača R5 na smerovač R8. Taktiež aj po konfigurácií dynamického NAT bol spustení ping zo smerovača R5 na smerovač R8. Na smerovači R8 bolo zapnutie debugovanie ICMP paketov pred a aj po nastavení dynamického NAT na primárnom ASAv firewalle. Na obrázku č.6.21 je možné vidieť odpoveď smerovača R8 paketom echo reply na smerovač R5. Tiež je možné vidieť pri odpovedi smerovača R8 paketom ICMP echo reply aj zmenu cieľovej IP adresy. Po nakonfigurovaní dynamického NAT už nie je vo výpise debugovania vidieť cieľová IP adresa smerovača R5, ale IP adresa rozhrania g0/0 na primárnom ASAv firewalle, to je 200.200.200.1.

```
R8#
*Mar  1 00:09:48.651: ICMP: echo reply sent, src 200.200.200.20, dst 192.168.1.20
*Mar  1 00:09:48.675: ICMP: echo reply sent, src 200.200.200.20, dst 192.168.1.20
*Mar  1 00:09:48.687: ICMP: echo reply sent, src 200.200.200.20, dst 192.168.1.20
*Mar  1 00:09:48.739: ICMP: echo reply sent, src 200.200.200.20, dst 192.168.1.20
*Mar  1 00:09:48.751: ICMP: echo reply sent, src 200.200.200.20, dst 192.168.1.20
R8#
*Mar  1 00:11:05.395: ICMP: echo reply sent, src 200.200.200.20, dst 200.200.200.1
*Mar  1 00:11:05.435: ICMP: echo reply sent, src 200.200.200.20, dst 200.200.200.1
*Mar  1 00:11:05.463: ICMP: echo reply sent, src 200.200.200.20, dst 200.200.200.1
*Mar  1 00:11:05.491: ICMP: echo reply sent, src 200.200.200.20, dst 200.200.200.1
*Mar  1 00:11:05.543: ICMP: echo reply sent, src 200.200.200.20, dst 200.200.200.1
```

Obr. č.6.21 Ping pred a po nakonfigurovaní NAT

Kontrola nastavenia NAT bola zobrazená aj na primárnom ASAv firewalle. Bol použitý príkaz *show xlate* – obrázok č.6.22. a tiež príkaz *show nat* – obrázok č.6.23.

```
ASAPrimary(config)# show xlate
0 in use, 0 most used

ASAPrimary(config)# show xlate
1 in use, 1 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net

ICMP PAT from inside:192.168.1.20/9 to outside:200.200.200.1/9 flags ri idle 0:0
0:08 timeout 0:00:30
```

Obr. č.6.22 Kontrola NAT – show xlate

```
ASAPrimary(config)# show nat

Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic insideNAT interface
    translate_hits = 1, untranslate_hits = 0
```

Obr. č.6.23 Kontrola NAT – show NAT

Po úspešnom nastavení a otestovaní NAT bol nastavený režim HA. HA bol nastavený na primárnom firewalle tak isto ako je na obrázku č.6.12, len na sekundárnom firewalle bol namiesto príkazu *failover lan unit primary* nastavený príkaz *failover lan unit secondary*. Neskôr bola prerušená linka medzi primárnym ASAv firewallom a prepínačom P1 a tiež medzi primárnym ASAv firewallom a prepínačom P2. Tým sa stal sekundárny ASAv firewall primárným, čiže bol v stave aktívny a primárny ASAv firewall sa stal sekundárnym a mal nastavené standby IP adresy na svojích rozhraniach. Potom bol otestovaný ping zo smerovača R5 na smerovač R8 a tiež bolo zapnuté debugovanie ICMP paketov na smerovači R8. Z obrázka č.6.24 je vidieť, že pri použití sekundárneho ASAv firewallu, ktorý bol v stave aktívny bol ping úspešný a tiež, že úspešnosť prijatých ICMP echo reply paketov bola na úrovni 100%. To znamenalo, že prepnutie sieťovej prevádzky na sekundárny ASAv firewall v režime NAT nemalo zásadný vplyv na sieťovú prevádzku.

```
R5#ping
Protocol [ip]:
Target IP address: 200.200.200.20
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 500, 100-byte ICMP Echos to 200.200.200.20, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
*Mar 1 01:24:06.939 %OSPF-5-ADJCHG: Process 123, Nbr 200.0.0.1 on
FastEthernet0/0 from LOADING to FULL, Loading Done..
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 3/33/95 ms
```

Obr. č.6.24 Úspešnosť prijatých ICMP echo reply paketov

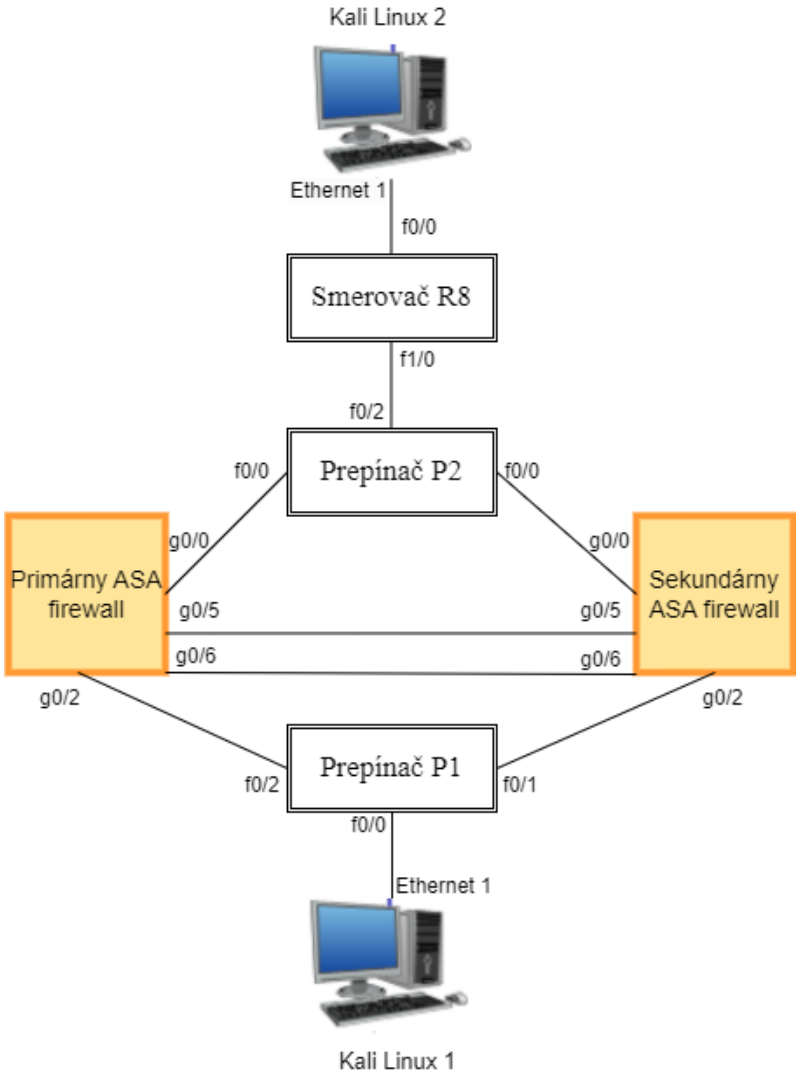
Z debugovania paketov na smerovači R8 si je možné všimnúť, že ICMP echo reply pakety zo smerovača R8 boli presmerované z primárného ASAv firewallu na sekundárny ASA firewall – obrázok č.6.25. Keďže IP standby adresa 200.200.200.3 bola určená pre primárny ASA firewall a IP adresa 200.200.200.1 bola určená pre sekundárny firewall. Vo výsledku to znamenalo, že bola úspešne nakonfigurovaná a overená metóda HA u softvérových ASAv firewallov pre dynamický NAT.

```
R8#
*Mar 1 01:24:35.171:  ICMP: redirect sent to 200.200.200.1 for dest 200.200.200.3,
use gw 200.200.200.3
R8#
*Mar 1 01:24:40.158:  ICMP: redirect sent to 200.200.200.1 for dest 200.200.200.3,
use gw 200.200.200.3
```

Obr. č.6.25 Presmerovanie paketov

6.4 Realizácia ASAv firewallu v programe GNS3 – Anyconnect VPN

Ako tretia metóda otestovanie HA pre softvérové ASAv firewally bola v programe GNS3 nakonfigurovaná počítačová sieť pre otestovanie anyconnect VPN. V počítačovej sieti bol použitý jeden ASAv firewall s verziou 9.8.1, dva prepínače a jeden smerovač. Ďalej tu boli použité dva počítače s operačným systémom Kali Linux. Grafický návrh experimentálnej počítačovej siete je zobrazený na obrázku č.6.26. Rozdelenie IP adries pre primárny ASAv firewall a smerovač R8 je zobrazené v tabuľke č.6.



Obr. č.6.26 Anyconnect VPN – GNS3

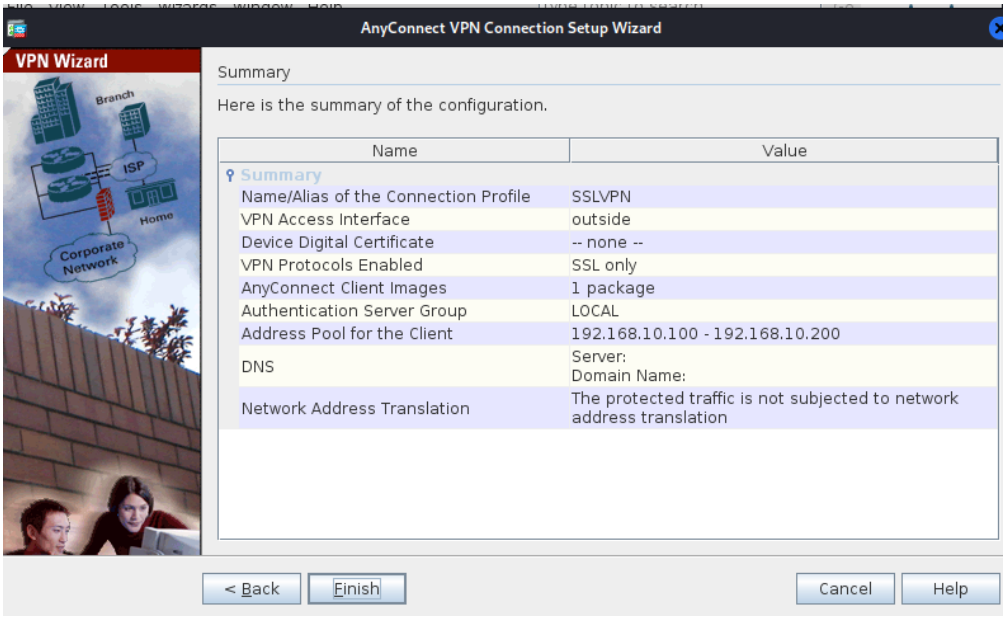
Názov	Port + IP adresa + zóna	Port + IP adresa + zóna	Port + IP adresa	Port + IP adresa
Primárny ASA firewall	G0/0 200.200.200.1 Outside zóna	G0/2 192.168.10.1 Inside zóna	G0/5 1.1.1.1	G0/6 2.2.2.1
	200.200.200.3 (Standby)	192.168.10.10 (Standby)	1.1.1.2 (Standby)	2.2.2.2 (Standby)
Smerovač R8	F1/0 200.200.200.2	F0/0 192.168.2.1		
Kali Linux 1	Etthernet 1 192.168.10.2			
Kali Linux 2	Ethernet 1 192.168.2.2			

Tab. 6 IP adresy a rozhrania – Anyconnect VPN GNS3

Základná konfigurácia bola veľmi podobná ako v minulých konfiguráciach. Základná konfigurácia zahrňovala: OSPF, priradenie IP adries rozhraniam a nastavenie HA. Nastavenie anyconnect VPN bolo potrebné konfigurovať cez Cisco ASDM-IDM Launcher. Kvôli tomu bol nakonfigurovaný na primárnom ASAv firewalle prístup k HTTP serveru. Táto konfigurácia je zobrazená na obrázku č.6.27. Samotný výsledok konfigurácie anyconnect VPN je na obrázku č.6.28.

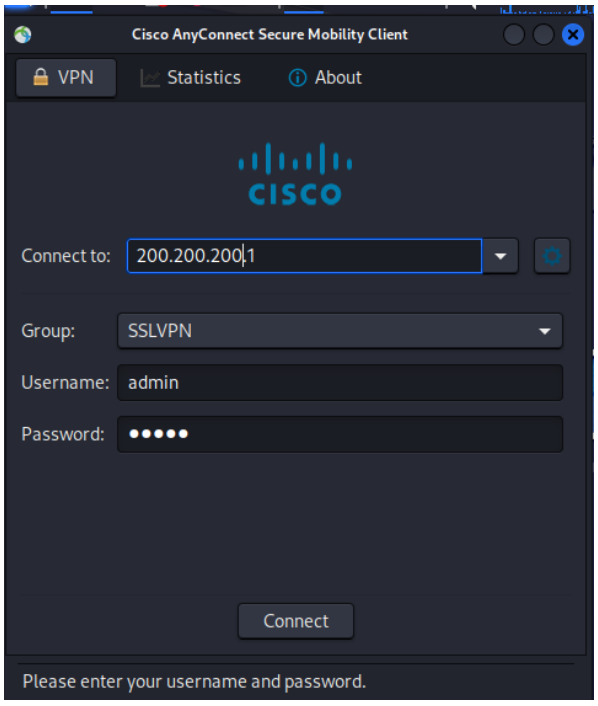
```
username admin password cisco
http server enable
http 192.168.10.0 255.255.255.0 inside
domain-name security.com
```

Obr. č.6.27 Konfigurácia HTTP servera

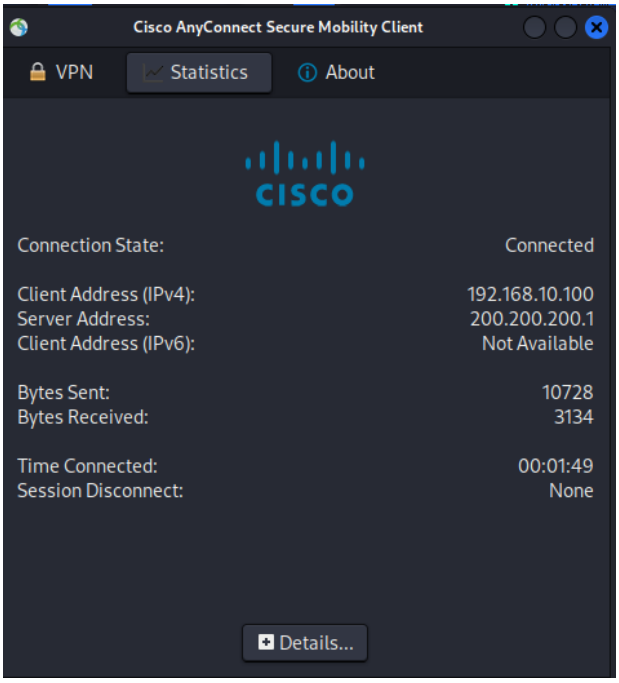


Obr. č.6.28 Konfigurácia anyconnect VPN

Z obrázka č.6.28 je detailne vidieť konfiguráciu anyconnect VPN. Ako profil bol nastavený názov SSLVPN, ako protokol bol povolený SSL (Secure Sockets Layer) protokol, ďalej bol nahraný obraz klienta a nakoniec bol určený rozsah súkromných IP adries 192.168.10.100 – 192.168.10.200. U klienta Kali Linux 2 bolo nutné zadať potrebné údaje na pripojenie k anyconnect VPN. Tieto údaje sú zobrazené na obrázku č.6.29. Bolo nutné zadať IP adresu primárného ASAv firewallu, názov profilu a tiež meno a heslo. Ako dôkaz úspešeného pripojenia existuje obrázok č.6.30.

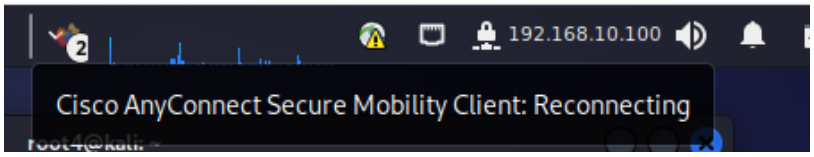


Obr. č.6.29 Prihlasovacie údaje



Obr. č.6.30 Úspešné pripojenie

Následovalo testovanie funkčnosti HA. Ako v minulých konfiguráciach, tak aj v tejto konfigurácií boli vypnuté nepotrebné rozhrania na primárnom ASAv firewalle. Na obrázku č.6.31 je vidieť, že nejaký čas trvalo kým bola sprovoznená konfigurácia sekundárneho ASAv firewallu. Na tomto obrázku je vidieť slovo “Reconnecting”, čo znamenalo, že klient Kali Linux 2 sa znova snažil o anyconnect VPN pripojenie počas zmeny sieťovej prevádzky cez sekundárny ASAv firewall.



Obr. č.6.31 Prerušenie spojenia

Po nejakom časovom úseku sa podarilo klientovi Kali Linux 2 pripojiť k VPN. Toto úspešné pripojenie je zobrazené na obrázku č.6.32, kde je v podobe pingu z klienta Kali Linux 2 na počítač Kali Linux 1. Ako prvý bol zapnutý ping z klienta Kali Linux 2 na klienta Kali Linux 1. Tento ping predstavoval v obrázku č.6.32 sekvenčné čísla paketov od 1 do 6. Ako je vidieť, tak časová odozva bola malá a pohybovala sa približne v normálnych hodnotách, čo je približne okolo 20 ms. Potom bola vypojená linka medzi primárným ASAv firewalllom a prepínačom P1 a tiež medzi primárnym ASAv firewallom a prepínačom P2. Z tohto obrázka sa dá vyčítať, že naozaj došlo nachvíľku

k prerušeniu spojenia, a to kontrétne medzi paketom so sekvenčným číslom 7 a 35. Toto prerušenie bolo v obrázku č.6.31 slovo “Reconnecting”. Čo zanemnalo, že sa klient Kali Linux 2 snažil o znovu pripojenie k VPN. Po pakete so sekvenčným číslom 35 bolo obnovené spojenie. Tiež je vidieť, že krátko po obnovení spojenia došlo k väčšej časovej odozve, ktorá začína od paketu so sekvenčným číslom 36. Krátko po tom ako sa klientovi Kali Linux 2 podarilo úspešené znovu pripojenie bola časová odozva paketu so sekvenčným číslo 36 až 47829 ms. To bolo spôsobené prevažne tým, že klient Kali Linux 2 sa znova snažil o pripojenie k VPN. Táto veľká časová odozva netrvala dlho a po určitom časovom úseku sa vrátila do normálu. Do normálných hodnôt sa časová odozva vrátila až približne pri pakete so sekvenčným číslo 83. Toto vrátenie do normálných hodnôt je vidieť na obrázku č.6.33. Už vo výsledku je známe, že prepojenie sieťovej prevádzky na sekundárny firewall malo horšie výsledky pre anyconnect VPN u softvérových ASAv firewallov ako u IPsec VPN spojenia.

```
┌──(root4㉿kali)-[~]
└─$ └─$ ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
64 bytes from 192.168.10.2: icmp_seq=1 ttl=64 time=65.2 ms
64 bytes from 192.168.10.2: icmp_seq=2 ttl=64 time=26.5 ms
64 bytes from 192.168.10.2: icmp_seq=3 ttl=64 time=23.7 ms
64 bytes from 192.168.10.2: icmp_seq=4 ttl=64 time=29.2 ms
64 bytes from 192.168.10.2: icmp_seq=5 ttl=64 time=14.7 ms
64 bytes from 192.168.10.2: icmp_seq=6 ttl=64 time=26.5 ms
64 bytes from 192.168.10.2: icmp_seq=36 ttl=64 time=47829 ms
64 bytes from 192.168.10.2: icmp_seq=37 ttl=64 time=46811 ms
64 bytes from 192.168.10.2: icmp_seq=38 ttl=64 time=45788 ms
64 bytes from 192.168.10.2: icmp_seq=39 ttl=64 time=44764 ms
```

Obr. č.6.32 Prerušenie spojenia + obnovenie spojenia, časť 1

```
64 bytes from 192.168.10.2: icmp_seq=73 ttl=64 time=9973 ms
64 bytes from 192.168.10.2: icmp_seq=74 ttl=64 time=8950 ms
64 bytes from 192.168.10.2: icmp_seq=75 ttl=64 time=7926 ms
64 bytes from 192.168.10.2: icmp_seq=76 ttl=64 time=6805 ms
64 bytes from 192.168.10.2: icmp_seq=83 ttl=64 time=13.1 ms
64 bytes from 192.168.10.2: icmp_seq=84 ttl=64 time=24.0 ms
64 bytes from 192.168.10.2: icmp_seq=85 ttl=64 time=14.6 ms
64 bytes from 192.168.10.2: icmp_seq=86 ttl=64 time=16.1 ms
64 bytes from 192.168.10.2: icmp_seq=87 ttl=64 time=13.5 ms
```

Obr. č.6.33 Prerušenie spojenia + obnovenie spojenia, časť 2

Tiež bolo vyskúšané aj spätné prepojenie sieťovej prevádzky na primárny ASAv firewall. Toto spätné prepojenie je vidieť na obrázku č.6.34. V tomto obrázku je vidieť, že prvé tri pakety, to je sekvenčné číslo 1, 2 a 3 boli odoslané cez icmp echo request a prijaté cez icmp echo reply v topológií, kde bol ešte stále použitý sekundárny firewall. Čiže sieťová prevádzka prehádzala ešte stále cez sekundárny ASAv firewall. Časová odozva bola v normálných hodnotách. Následne bola vypnutá linka medzi sekundárnym firewallom a prepínačom P1 a tiež aj medzi sekundárnym firewallom a prepínačom P2. Následne prebiehalo opätovné prepojenie klienta Kali Linux 2 prostredníctvom anyconnect VPN cez primárny firewall. Čiže sieťová prevádzka bola spätne prepnutá na primárny ASAv firewall. Pri tomto opätovnom prepojení vzniklo prerušenie spojenia, a to presne medzi paketami so sekvenčnými číslami 4 a 32. Toto spojenie sa podarilo úspešne zrealizovať a bolo ukázané v pingu až v pri pakete so sekvenčným číslom 33. Pri tomto sekvenčnom čísle bola vysoká časová odozva, a to až 41367 ms. Aj pri tomto prepojení sa vrátila časová odozva do normálných hodnôt a to približne pri pakete so sekvenčným číslom 75. Vrátenie časovej odozvy do normálných hodnôt si je možné pozrieť na obrázku č.6.35.

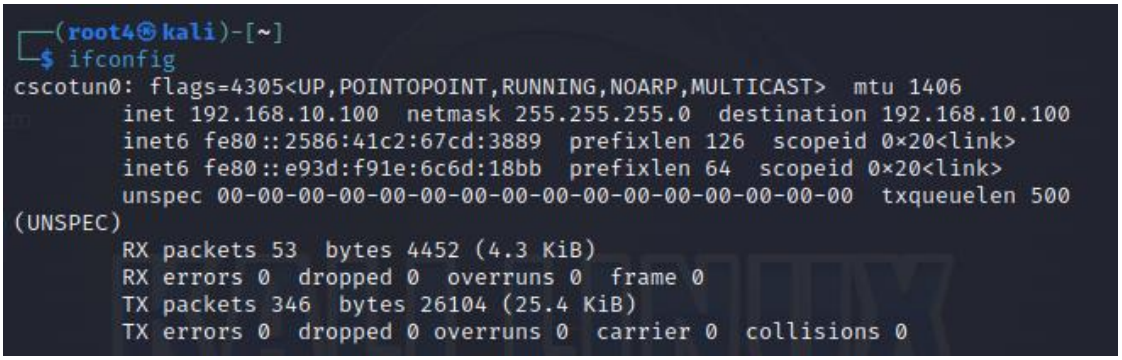
```
64 bytes from 192.168.10.2: icmp_seq=1 ttl=64 time=17.2 ms
64 bytes from 192.168.10.2: icmp_seq=2 ttl=64 time=15.9 ms
64 bytes from 192.168.10.2: icmp_seq=3 ttl=64 time=12.0 ms
64 bytes from 192.168.10.2: icmp_seq=33 ttl=64 time=41367 ms
64 bytes from 192.168.10.2: icmp_seq=34 ttl=64 time=40343 ms
64 bytes from 192.168.10.2: icmp_seq=35 ttl=64 time=38291 ms
```

Obr. č.6.34 Prerušenie spojenia + obnovenie spojenia, časť 3

```
64 bytes from 192.168.10.2: icmp_seq=69 ttl=64 time=4526 ms
64 bytes from 192.168.10.2: icmp_seq=70 ttl=64 time=3502 ms
64 bytes from 192.168.10.2: icmp_seq=71 ttl=64 time=2477 ms
64 bytes from 192.168.10.2: icmp_seq=72 ttl=64 time=1454 ms
64 bytes from 192.168.10.2: icmp_seq=74 ttl=64 time=13.3 ms
64 bytes from 192.168.10.2: icmp_seq=75 ttl=64 time=12.5 ms
64 bytes from 192.168.10.2: icmp_seq=76 ttl=64 time=18.8 ms
64 bytes from 192.168.10.2: icmp_seq=77 ttl=64 time=18.9 ms
```

Obr. č.6.35 Prerušenie spojenia + obnovenie spojenia, časť 4

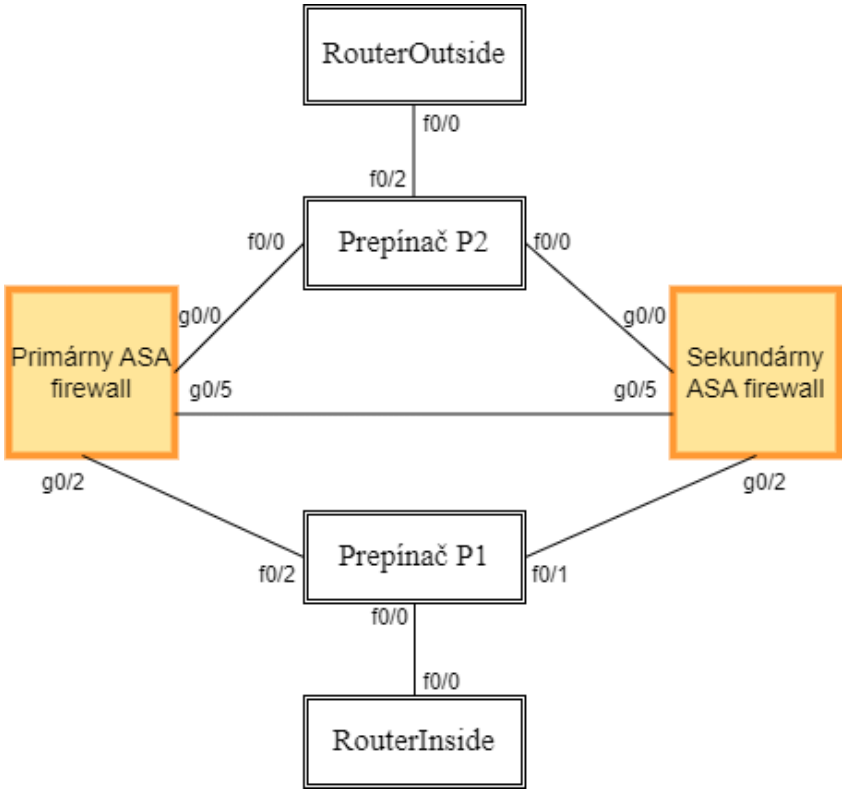
Na ďalšie overenie správnosti bol použitý výpis rozhraní cez príkaz *ifconfig*. Tento výpis je na obrázku č.6.36, kde je vidieť, že klient Kali Linux 2 aj po vypojení rozhraní na primárnom ASAv firewalle mal získané IP adresy so súkromého rozsahu 192.168.10.100 – 192.168.10.200. V tomto prípade získal klient Kali Linux 2 IP adresu 192.168.10.100.



Obr. č.6.36 Získaná súkromná IP adresa

6.5 Realizácia ASAv firewallu v programe GNS3 – TCP spojenie

Ako štvrtá topológia ASAv firewallu v programe GNS3 bola vybraná topológia na otestovanie TCP spojenia. Bolo použité Telnet spojenie a následne aj SSH spojenie spolu s NAT. Cieľom bolo navrhnúť a nakonfigurovať topológiu tak, aby pre technológiu failover nedošlo k zlyhaniu aktuálného TCP spojenia a aby sieťová prevádzka bola stále funkčná aj po vypnutí rozhraní na primárnom firewalle. Pre túto experimentálnu počítačovú sieť bolo pre technológiu HA použité len jedno ethernetové rozhranie. Znamenalo to, že pre linku failover a statefull bolo spoločné jedno ethernetové rozhranie. V predchadzajúcich topológiach bol nakonfigurovaný smerovací protokol OSPF, no v tejto úlohe bol nakonfigurovaný pre testovanie smerovací protokol EIGRP (Enhanced Interior Gateway Routing Protocol). Experimentálna počítačová sieť je na obrázku č.6.37. Návrh jednotlivých IP adries pre primárny ASAv firewall je v tabuľke č.7. Smerovač RouterInside mal na rozhraní f0/0 IP adresu 192.168.1.2 a smerovač RouterOutside mal na rozraní f0/0 IP adresu 192.168.2.2.



Obr. č.6.37 Experimentálna sieť – ASAv TCP

Názov	Port + IP adresa + zóna	Port + IP adresa + zóna	Port + IP adresa
Primárny ASA firewall	G0/0 192.168.2.1 Outside zóna	G0/2 192.168.1.1 Inside zóna	G0/5 1.1.1.1
	192.168.2.3 (Standby)	192.168.1.3 (Standby)	1.1.1.2 (Standby)

Tab. 7 IP adresy a rozhrania – ASAv TCP

Po základnej konfigurácií, ktorá zahrňovala nastavenie IP adries na jednotlivých rozhraniach a EIGRP smerovacieho protokolu bol nastavený režim failover. V tejto experimentálnej sieti bol nakonfigurovaný režim failover pre jedno spoločné rozhranie určené pre prepojenie stavu – statefull link, a prepojenie pri zlyhaní – failover link. Cieľom bolo overiť správnosť takéhoto nastavenia. Nastavenie na primárnom ASAv firewalle je na obrázku č.6.38. Následne nasledovalo nastavenie Telnetu na smerovači RouterOutside. Cieľom bolo aby sa smerovač RouterInside pripojil na cez Telnet na smerovač RouterOutside. Úspešné pripojenie cez Telnet je na obrázku č.6.39.

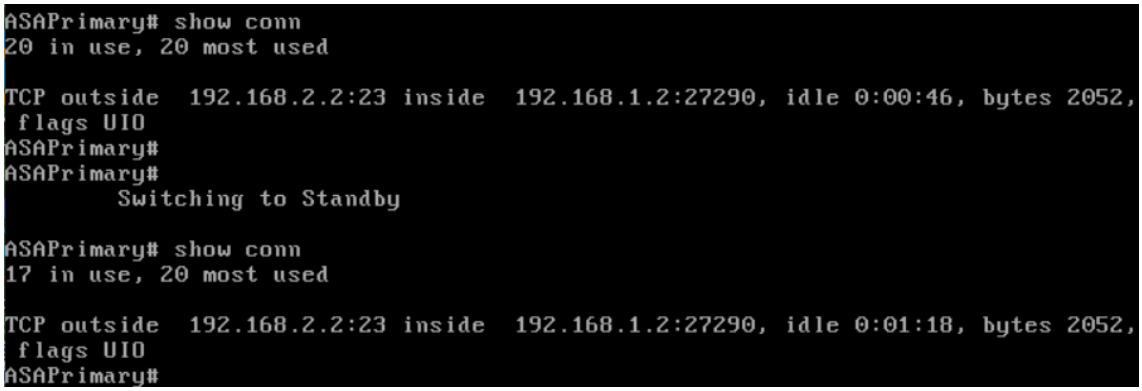
```
failover
failover lan unit primary
failover lan interface FAILOVER GigabitEthernet0/5
failover link FAILOVER GigabitEthernet0/5
failover key cisco
failover interface ip FAILOVER 1.1.1.1 255.255.255.0 standby 1.1.1.2
```

Obr. č.6.38 Nastavenie režimu HA pre jedno rozhranie – ASAv

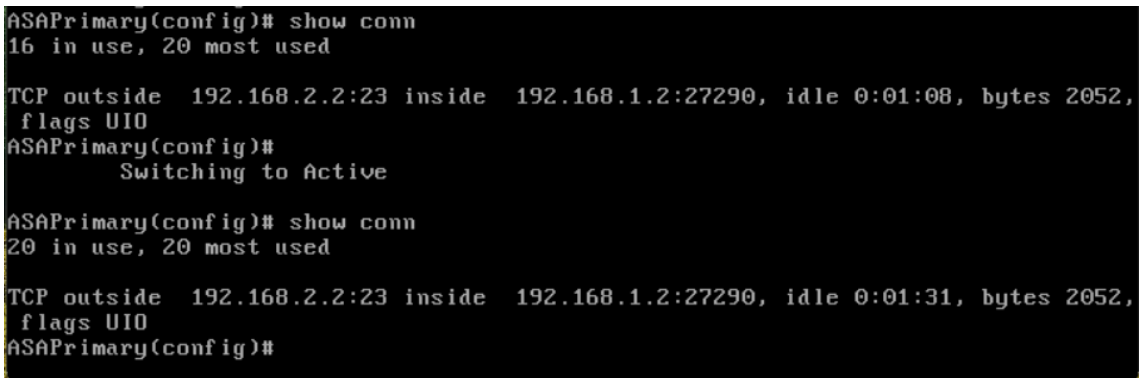
```
RouterInside#telnet 192.168.2.2
Trying 192.168.2.2 ... Open
User Access Verification
Username: admin
Password:
RouterOutside>
```

Obr. č.6.39 Úspešné pripojenie cez Telnet

Toto úspešné pripojenie cez Telnet zo smerovača RouterInside na RouterOutside je aj vidieť na primárnom ASAv firewalle – obr č.6.40, a aj na sekundárnom ASAv firewalle – obr č.6.41. Je vidieť, že IP adresa 192.168.1.2 bola pripojená na IP adresu 192.168.2.2 cez Telnet s portom 23. Tiež je vidieť, že TCP spojenie medzi primárnym a sekundárnym ASAv firewallom je to isté, čiže používajú sa tie isté porty, či už port 23 alebo port 27290. Cieľom bolo aby tieto porty neboli počas prepnutia sieťovej prevádzky na sekundárny ASAv firewall zmenené a tiež aby nezačalo nové TCP spojenie. Z týchto obrázkov je možné pozorovať, že pri prepnutí sieťovej prevádzky na sekundárny ASAv firewall naozaj nedošlo k zlyhaniu aktuálného TCP spojenia. Napr. v obrázku č.6.41 je vidieť prepnutie sekundárného ASAv firewallu do stavu aktívny cez výpis „Switching to Active“. To znamená, že jednotlivé porty zostali po prepnutí na sekundárny firewall úplne rovnaké, či už na primárnom alebo na sekundárnom ASAv firewalle. Toto úspešné spojenie bolo overené aj na smerovači RouterOutside, kde cez príkaz *show tcp brief* bolo zistené, že pri prepnutí na sekundárny firewall zostal ten istý port, a aj to isté TCP spojenie – obr č.6.42. Zaujímavosťou môže byť aj to, že pri tejto konfigurácií bol nakonfigurovaný smerovací protokol EIGRP.



Obr. č.6.40 Nezmenené TCP spojenie – primárny ASAv firewall



Obr. č.6.41 Nezmenené TCP spojenie – sekundárny ASAv firewall

```
RouterOutside#show tcp brief
TCB         Local Address         Foreign Address       (state)
655AF6AC    192.168.2.2.23        192.168.1.2.27290     ESTAB
RouterOutside#
*Apr 29 22:39:44.483: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor
192.168.2.1 (FastEthernet0/0) is down: peer restarted
*Apr 29 22:39:44.515: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor
192.168.2.1 (FastEthernet0/0) is up: new adjacency
RouterOutside#
RouterOutside#show tcp brief
TCB         Local Address         Foreign Address       (state)
655AF6AC    192.168.2.2.23        192.168.1.2.27290     ESTAB
RouterOutside#
```

Obr. č.6.42 Nezmenené TCP spojenie – smerovač RouterOutside

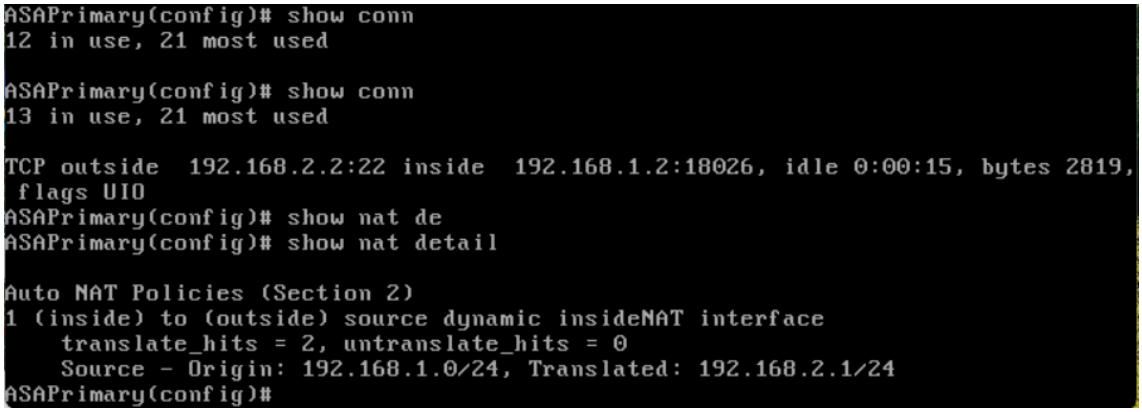
Po úspešnom nakonfigurovaní a overení TCP spojenia cez Telnet bola vyskúšaná možnosť konfigurácie SSH spojenia s použitím NAT. Cieľom bolo správne nakonfigurovať SSH spojenie spolu s NAT, tak aby sa zachovalo počas prepnutia sieťovej prevádzky na sekundárny firewall aktuálne TCP spojenie a skúmať dopad spolu s NAT. Konfigurácia SSH na smerovači RouterOutside je na obrázku č.6.43. Potom nasledovalo úspešené pripojenie cez SSH zo smerovača RouterInside na smerovač RouterOutside. Toto úspešné TCP pripojenie spolu s prekladom NAT bolo zobrazené aj na primárnom a sekundárnom ASAv firewalle.

```
ip domain-name security.com
crypto key generate rsa modulus 1024
ip ssh version 2
username admin  password cisco
line vty 0 15
trasnport input ssh
login local
```

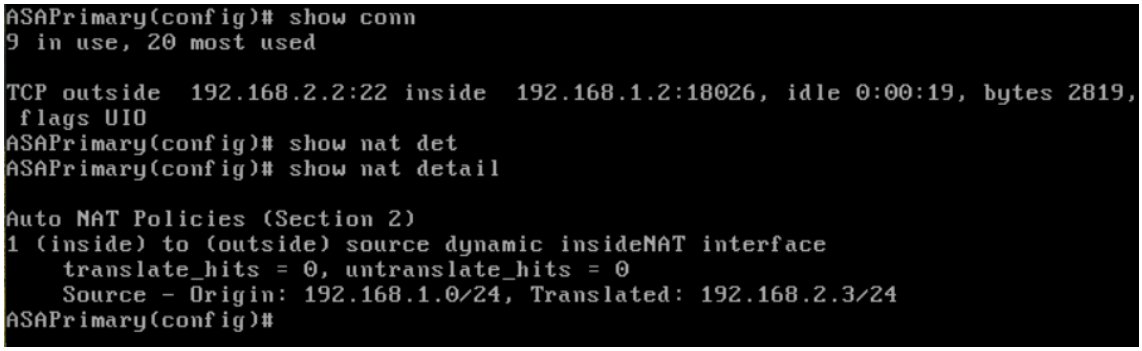
Obr. č.6.43 Konfigurácia SSH

Na obrázku č.6.44 je zobrazené na primárnom ASAv firewalle úspešné SSH pripojenie spolu s NAT zo smerovača RouterInside na RouterOutside. Kde je vidieť, že bol použitý TCP port 22. Tiež je vidieť aj aktuálny port 18026 na strane smerovača RouterInside. Cieľom bolo aby sa po prepnutí tieto porty vôbec nemenili. Zaujímavosťou je aj výpis po príkaze *show nat detail*, kde je vidieť aktuálny preklad IP adries pomocou NAT. IP adresa smerovača RouterInside 192.168.1.2 bola prekladaná na IP adresu 192.168.2.1. Práve IP adresa 192.168.2.1 predstavovala na primárnom ASAv firewalle rozrhanie g0/0 podľa obrázka č.6.37.

Na obrázku č.6.45 je zobrazené na sekundárnom ASAv firewalle úspešné SSH pripojenie spolu s NAT zo smerovača RouterInside na RouterOutside. Kde je vidieť, že TCP porty boli rovnaké ako v prípade smerovača RouterInside. Väčší dôraz treba dať na NAT. Na sekundárnom ASAv firewalle bola prekladaná adresa smerovača RouterInside 192.168.1.2 na standby IP adresu 192.168.2.3. Dôvod bol ten, že sekundárny ASAv firewall bol v režime „Standby ready“ a mal nastavenú IP standby adresu.



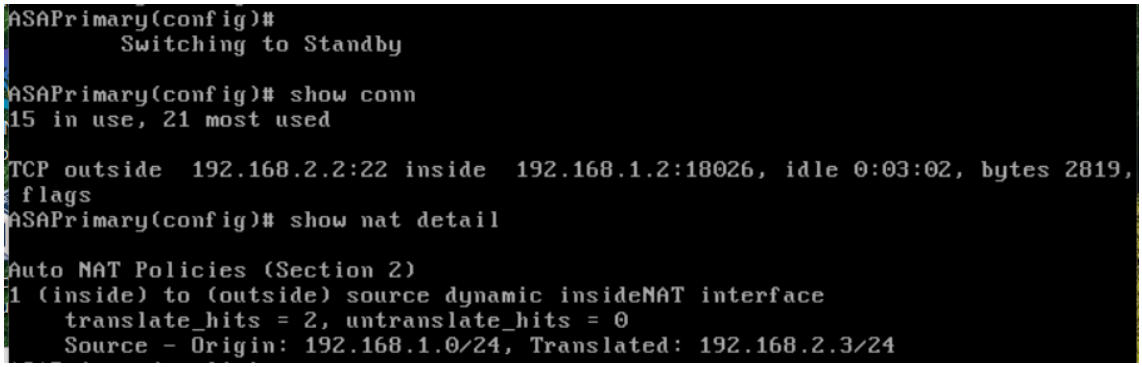
Obr. č.6.44 TCP spojenie + NAT – primárny ASAv firewall



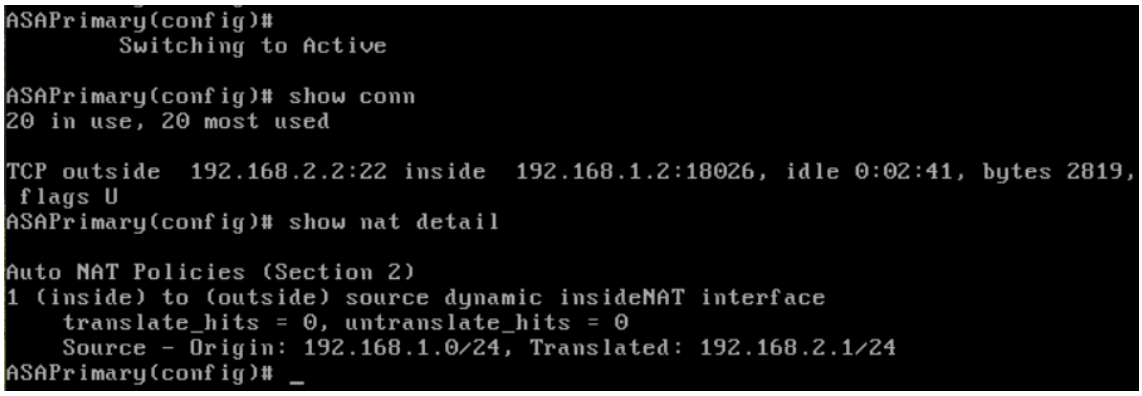
Obr. č.6.45 TCP spojenie + NAT – sekundárny ASAv firewall

Následne nasledovalo vypojenie požadovaných liniek medzi primárny ASAv firewallom a obi dvoma prepínačmi. Overenie správnosti konfigurácie je na obrázkoch č.6.46, č.6.47 a č.6.48. Na obrázku č.6.46 je zobrazený výpis primárného firewallu po vypojení daných liniek a prepnutí sieťovej prevádzky na sekundárny firewall. Je vidieť, že TCP porty zostali tie isté, čiže 22 a 18026, a tiež, že čas TCP spojenia sa neobnovil a pokračoval aj po prepnutí sieťovej prevádzky. Dôležitým príkazom je príkaz *show nat detail*, kde je vidieť, že primárny firewall po zmene sieťovej prevádzky mal zmenený preklad IP adries. Pred vypnutím požiadovaných liniek sa IP adresa smerovača RouterInside prekladala na IP adresu 192.168.2.1, no po vypnutí liniek prešiel primárny firewall do stavu „Standby ready“ a IP adresa smerovača RouterInside sa už prekladala na standby IP adresu 192.168.2.3 – obrázok č.6.46.

Na druhej strane u sekundárneho firewallu sa po vypnutí daných liniek IP adresa smerovača RouterInside prekladala na IP adresu 192.168.2.1 – obrázok č.6.47. Dôvodom bol ten, že sekundárny firewall prešiel do stavu „active“. Ako dôkaz správnosti nastavenia konfigurácie a urdžania trvalého TCP spojenia je aj to, že jednotlivé porty pri SSH pripojení zostali také isté ako pred vypnutím daných liniek – obrázok č.6.47.



Obr. č.6.46 Nezmenené TCP spojenie, zmenený NAT – primárny ASAv firewall



Obr. č.6.47 Nezmenené TCP spojenie, zmenený NAT – sekundárny ASAv firewall

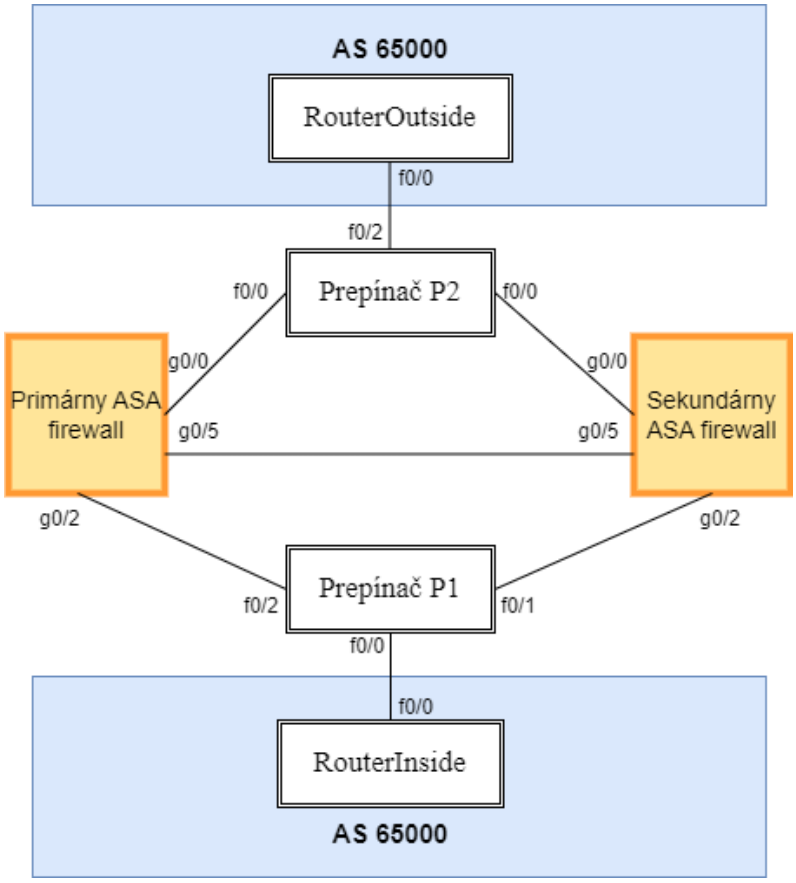
Posledná kontrola správnosti prebiehala na smerovači RouterOutside. Na obrázku č.6.48 je zobrazený výpis príkazu *show tcp brief* pred a po vypnutí daných liniek medzi primárnym ASAv firewallom a obi dvoma prepínačmi. Kde je vidieť, že dané porty sa po prepnutí sieťovej prevádzky na sekundárny firewall vôbec nezmenili.

```
RouterOutside#show tcp brief
TCB         Local Address          Foreign Address        (state)
674AAD58    192.168.2.2.22         192.168.2.1.18026      ESTAB
RouterOutside#
*Apr 29 23:19:58.151: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor
192.168.2.1 (FastEthernet0/0) is down: peer restarted
*Apr 29 23:19:58.167: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor
192.168.2.1 (FastEthernet0/0) is up: new adjacency
RouterOutside#show tcp brief
TCB         Local Address          Foreign Address        (state)
674AAD58    192.168.2.2.22         192.168.2.1.18026      ESTAB
```

Obr. č.6.48 Nezmenené SSH TCP spojenie – smerovač RouterOutside

6.6 Realizácia ASAv firewallu v programe GNS3 – TCP spojenie typu BGP

Okrem TCP spojenia typu Telnet a SSH bolo vyskúšané aj TCP spojenie prostredníctvom smerovacieho protokolu BGP. Ako je už z teórie zo strany 28 zrejmé, tak BGP protokol používa TCP port s číslom 179. Cieľom tejto konfigurácie bolo nakonfigurovať a overiť správnosť nastavenia HA pri ASAv firewalle, tak aby komunikácia počas prepnutia na sekundárny firewall nebola prerušená a aby nedošlo k prepnutiu TCP portov. Experimentálna počítačová sieť s BGP protokolom je na obrázku č.6.49. Konfigurácia BGP protokolu pre smerovač RouterInside je na obrázku č.6.50. IP adresy pre jednotlivé rozhrania sú v tabuľke č.8. Smerovač RouterInside mal IP adresu 192.168.2.2 na rozhraní f0/0. Smerovač RouterOutside mal IP adresu 200.200.200.2 na rozhraní f0/0. Obi dva smerovače boli v rovnakom autonómnom systéme s číslom 65000. Primárny a aj sekundárny ASAv firewall neboli v žiadnom autonomnóm systéme. Kvôli tomu musela byť nakonfigurovaná statická smerovacia cesta na obi dvoch smerovačoch. Čiže konfiguráciou BGP smerovacieho protokolu a statickej smerovacej cesty na obi dvoch smerovačoch bola zaistená konektivita medzi týmito smerovačmi.



Obr. č.6.49 Experimentálna sieť – ASAv BGP

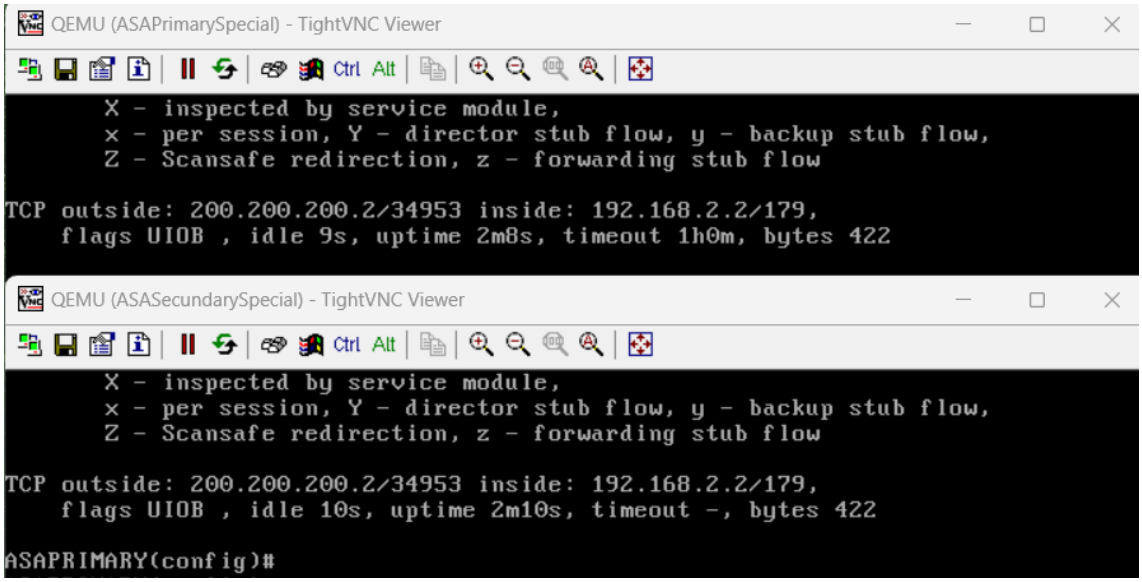
Názov	Port + IP adresa + zóna	Port + IP adresa + zóna	Port + IP adresa
Primárny ASA firewall	G0/2 192.168.2.1 Inside zóna	G0/0 200.200.200.1 Outside zóna	G0/5 1.1.1.1
	192.168.2.3 (Standby)	200.200.200.3 (Standby)	1.1.1.2 (Standby)

Tab. 8 IP adresy a rozhrania – ASAv BGP

```
router bgp 65000
bgp log-neighbor-changes
network 192.168.2.0
neighbor 200.200.200.2 remote-as 65000
neighbor 200.200.200.2 update-source FastEthernet0/0
exit
ip route 200.200.200.0 255.255.255.0 192.168.2.1
```

Obr. č.6.50 Nastavenie BGP – RouterInside

Po konfigurovaní BGP protokolu na obi dvoch smerovačoch a režimu failover na obi dvoch firewalloch následovalo otestovanie TCP spojenia. Toto otestované TCP spojenie je vidieť z obrázka č.6.51, kde zobrazené na obi dvoch firewalloch TCP spojenie s portom 179. To znamenalo, že bolo synchronizované TCP spojenie medzi obi dvoma firewallami. Pred vypojením daných liniek bol na smerovači RouterInside zapnutý príkaz *show tcp brief*, kde sa zobrazili aktuálne TCP spojenia. Následovalo vypojenie požadovaných liniek medzi primárnym ASAv firewallom a obi dvoma prepínačmi. Potom bol príkaz *show tcp brief* opäť zapnutý. Na obrázku č.6.52. je vidieť výpis príkazu *show tcp brief* na smerovači RouterInside pred a po vypojení daných liniek. Ako je vidieť, tak TCP spojenie pre BGP zostalo počas prepnutia sieťovej prevádzky na sekundárny firewall neporušené. Následne bol otestovaný aj ping, ktorý bol taktiež úspešný – obrázok č.6.52.



Obr. č.6.51 BGP TCP spojenie – firewally

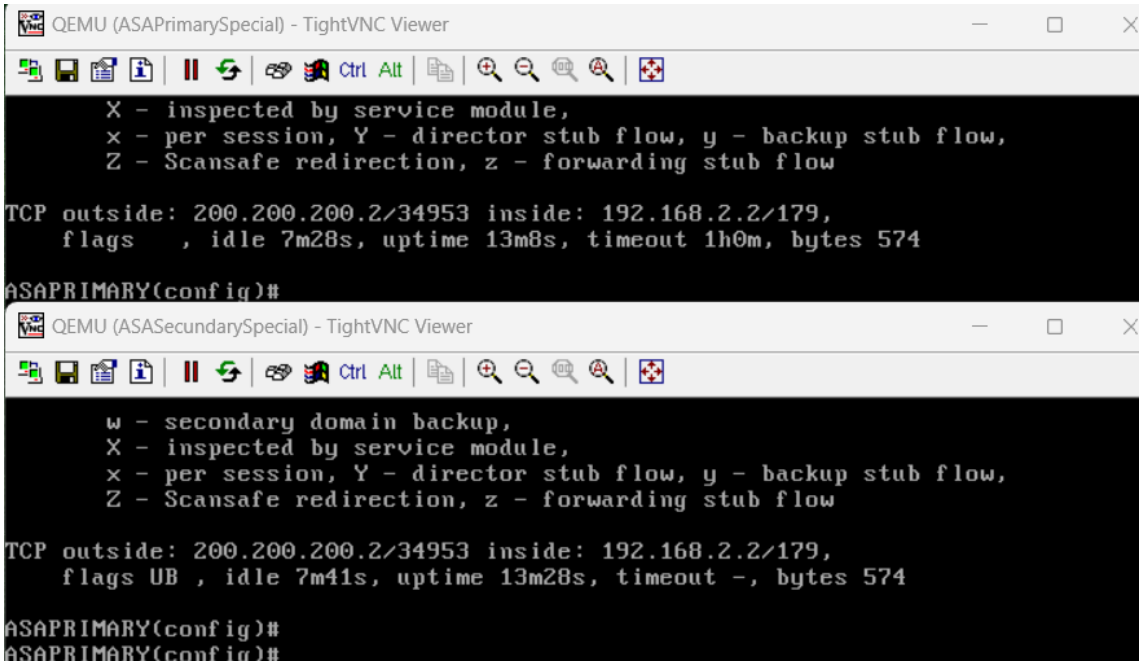
```
RouterInside#show tcp brief
TCB         Local Address          Foreign Address        (state)
68CB07BC    192.168.2.2.179        200.200.200.2.34953    ESTAB
RouterInside#show tcp brief
TCB         Local Address          Foreign Address        (state)
68CB07BC    192.168.2.2.179        200.200.200.2.34953    ESTAB
RouterInside#ping 200.200.200.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.200.200.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/10/11 ms
```

Obr. č.6.52 BGP TCP spojenie – Smerovač RouterInside

Na smerovači RouterOutside bol pred a po zmene prepnutím sieťovej prevádzky na sekundárny firewall zapnutý príkaz *show ip bgp summary* – obrázok č.6.53. Kde je vidieť, že čas BGP spojenia medzi obi dvoma smerovačmi sa neobnovil počas režimu failover – položka Up/Down. To znamenalo, že TCP spojenie s BGP protokolom nebolo prerušené. Ako posledné overenie správnosti neporušeného BGP TCP spojenia bolo cez príkaz *show conn detail* na obi dvoch firewallov – obrázok č.6.54. Kde je vidieť, že BGP spojenie sa naozaj neobnovilo, a taktiež, že aj TCP porty zostali úplne rovnaké.

```
RouterOutside#show ip bgp summary
BGP router identifier 200.200.200.2, local AS number 65000
BGP table version is 7, main routing table version 7
2 network entries using 288 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 272 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 720 total bytes of memory
BGP activity 4/2 prefixes, 4/2 paths, scan interval 60 secs

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.2.2     4      65000      10      10        7    0    0 00:05:21        1
RouterOutside#show ip bgp summary
BGP router identifier 200.200.200.2, local AS number 65000
BGP table version is 7, main routing table version 7
2 network entries using 288 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 272 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 720 total bytes of memory
BGP activity 4/2 prefixes, 4/2 paths, scan interval 60 secs

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.2.2     4      65000      11      11        7    0    0 00:06:18        1
RouterOutside#
```

Obr. č.6.53 BGP TCP spojenie – kontrola správnosti

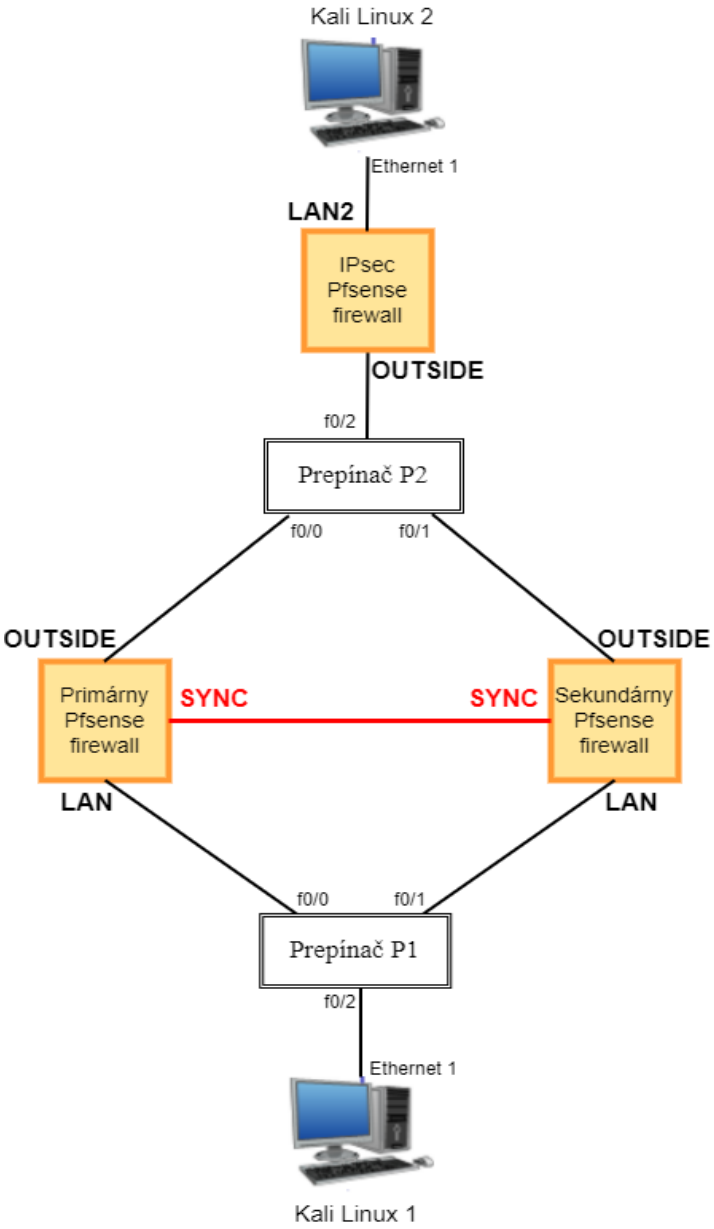


Obr. č.6.54 Nezmenené BGP TCP spojenie – firewally

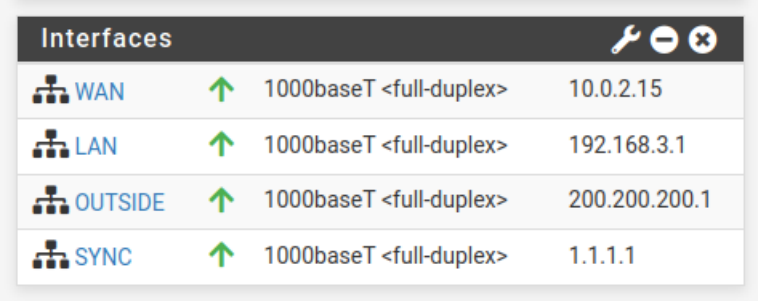
6.7 Realizácia Pfsense firewallu v programe GNS3 – IPsec VPN

Druhý v poradí firewall, ktorým bola nakonfigurovaná problematika HA bol firewall Pfsense. Cieľom bolo nakonfigurovať a overiť funkčnosť HA u tohto firewallu. Ďalším cieľom bolo porovnať výsledky so softvérovým firewallom ASAv a tiež aj s hardvérovým ASA firewallom. Pre toto overenie funkčnosti konfigurácie bolo nakonfigurované IPsec VPN spojenie v programe GNS3. Grafický návrh konfigurácie IPsec VPN s Pfsense firewallami je zobrazený v obrázku č.6.55. Rozloženie IP adries k daným rozhraniam pre jednotlivé firewally je zobrazené v na obrázku č.6.56, č.6.57 a na obrázku číslo č.6.58. Na týchto obrázkoch je vidieť aj rozhranie WAN, no toto rozhranie bolo nastavené len pre prístup do siete internet a nemalo žiadný vplyv na realizáciu IPsec VPN a HA. Počítač Kali Linux 2 mal IP adresu 192.168.2.2 na rozhraní Ethernet 1. Kali Linux 1 mal IP adresu 192.168.3.2 na rozhraní Ethernet 1.

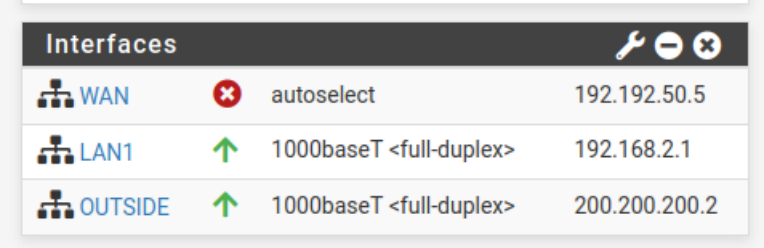
Obi dva Pfsense firewally boli v tejto a aj v ďalších konfiguráciách ako virtuálne stroje vo Virtualboxe. Oproti firewallom ASAv išlo o razantný rozdiel, keďže ASAv firewally boli virtuálne sieťové zariadenie. Treba zobrať do úvahy aj to, že virtuálne stroje majú vačšie nároky na operačnú pamäť alebo procesor ako virtuálne sieťové zariadenia, čo vo výsledku môže viešť aj ku skresľovaniu výsledkov tejto diplomovej práce. Osobný notebook na ktorom bola vypracovaná diplomová práca mal operačnú pamäť 8 Gb a procesor bol 11th Gen Intel(R) Core(TM) i3-1115G4 @ 3.00GHz 3.00 GHz. Tiež treba zobrať do úvahy, že napr. konfigurácia IPsec VPN pri Pfsense firewalle obsahovala celkovo až 5 virtuálnych strojov: 2 – Kali Linux, 3 – Pfsense firewally. Oproti tomu konfigurácia IPsec VPN pri ASAv firewalle neobsahovala ani jeden virtuálny stroj.



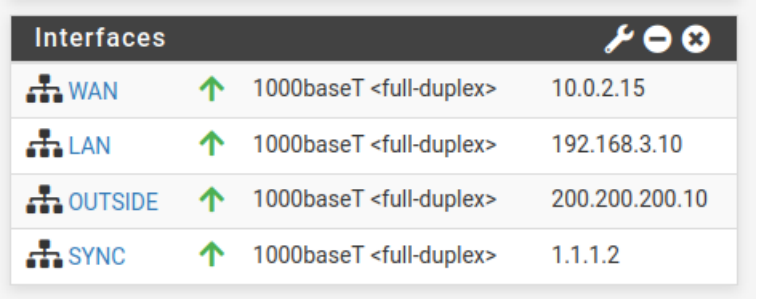
Obr. č.6.55 Návrh topológie IPsec VPN – Pfsense



Obr. č.6.56 Primárny Pfsense – IP adresy na rozhraniach

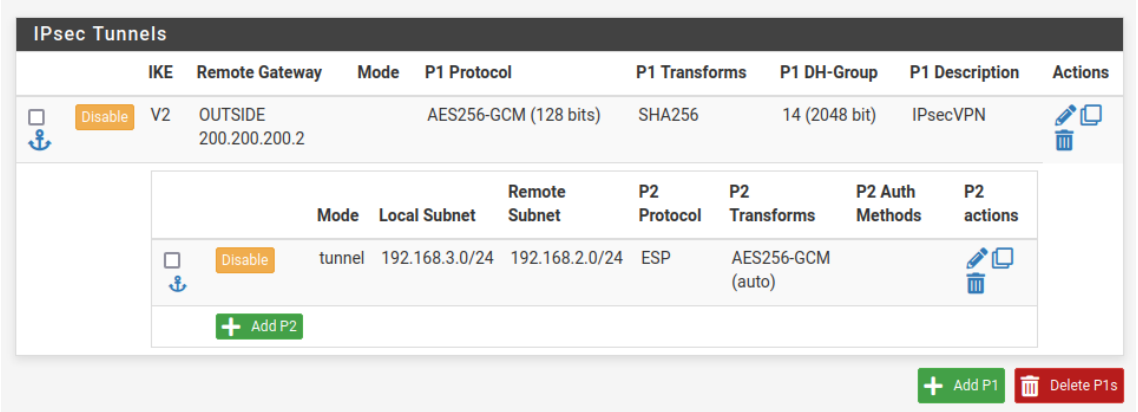


Obr. č.6.57 IPsec Pfsense – IP adresy na rozhraniach

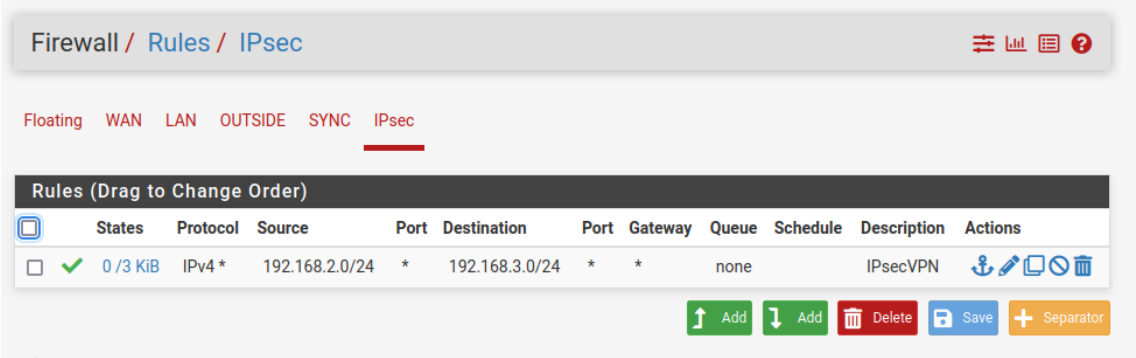


Obr. č.6.58 Sekundárny Pfsense – IP adresy na rozhraniach

Nastavenie IPsec VPN bolo veľmi podobné ako pri nastavení u ASAv firewallu. Tiež bola nastavená šifra AES, hash SHA256, Diffie-Hellman protokol, tunel alebo IP adresy k vzdialenej a lokálnej sieti. Vzorové nastavenie IPsec VPN je zobrazené na obrázku č.6.59. Na druhej strane oproti ASAv firewallu bolo veľmi dôležitým krokom nastaviť a povoliť pravidlo prevádzky v nastaveniach pravidiel firewallu. Na obrázku č.6.60 je nastavené pravidlo prevádzky na primárnom Pfsense firewalle. Kde ako zdrojová sieť bola nakonfigurovaná lokálna sieť LAN2 a ako vzdialená sieť bola nakonfigurovaná lokálna sieť LAN. IPsec VPN a pravidlo prevádzky bolo podobné nakonfigurované aj na IPsec firewallu, len bol rozdiel oproti konfigurácií primárného Pfsense firewallu vo vzdialenej a lokálnej IP adrese.

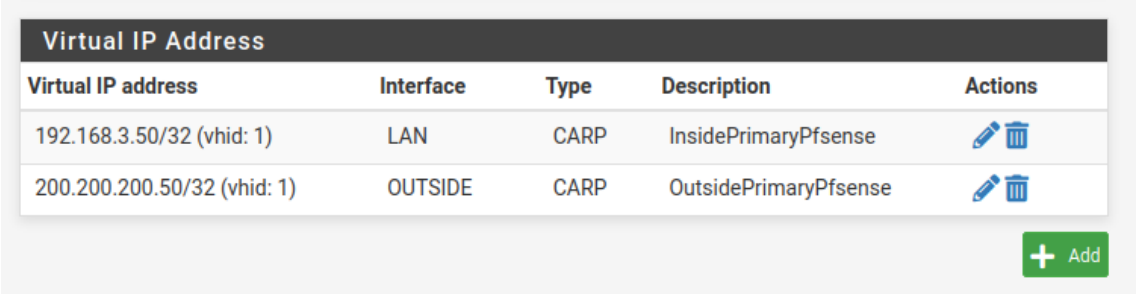


Obr. č.6.59 Primárny Pfsense – Nastavenie IPsec VPN



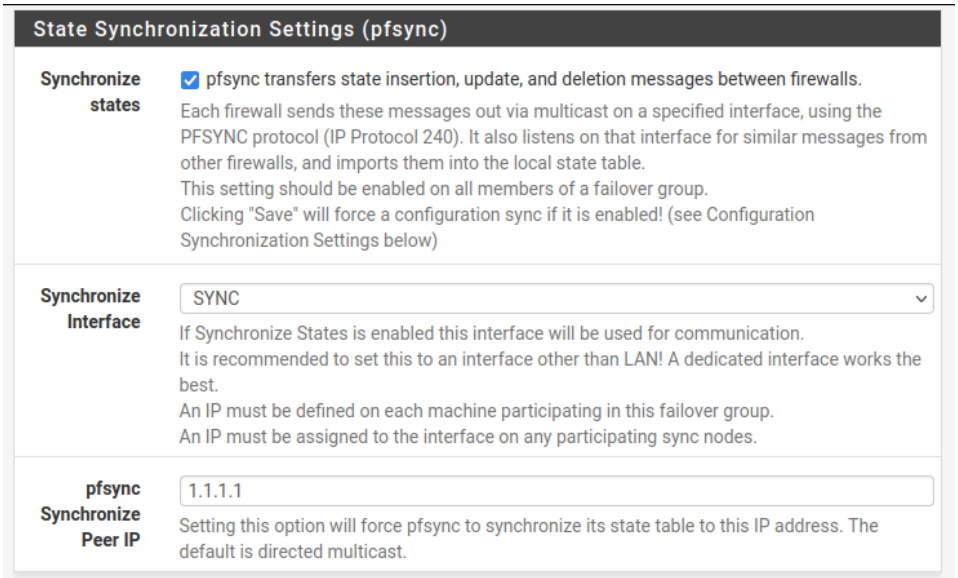
Obr. č.6.60 Primárny Pfsense – Nastavenie pravidla prevádzky

Tým boli nakonfigurované pravidlá pre IPsec VPN na obi dvoch Pfsense firewallov. Následovala konfigurácia HA. Ako prvé boli nastavené IP adresy typu CARP. Toto nastavenie bolo rovnaké na primárnom a sekundárnom firewalle. Avšak táto konfigurácia sa nastavovala len na primárnom firewalle. Sekudárny firewall získal toto nastavenie automaticky z primárneho firewallu. Nastavenie IP adries typu CARP pre primárny firewall je na obrázku č.6.61.

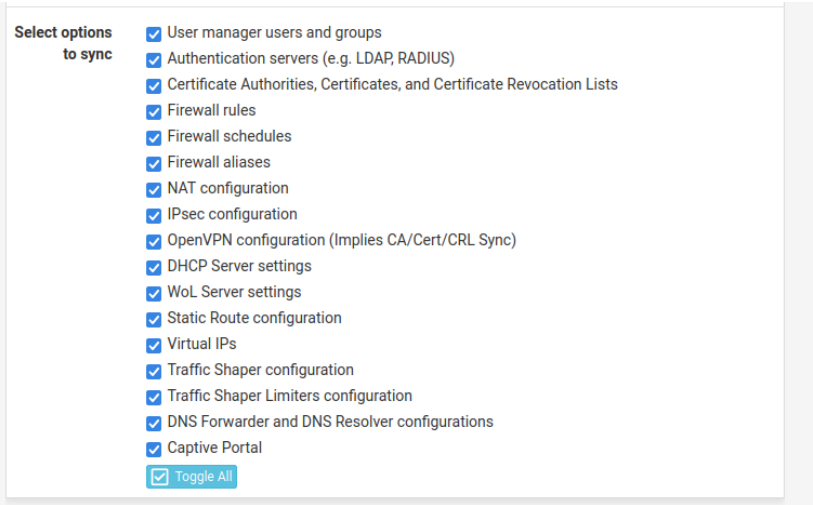


Obr. č.6.61 Primárny Pfsense – CARP adresy

V druhom kroku bolo nastavené SYNC rozhranie. Vzorové nastavenie SYNC rozhrania pre sekundárny Pfsense firewall je nakonfigurované na obrázku č.6.62 a č.6.63. Na obrázku č.6.62 bolo vybrané na synchronizáciu SYNC rozhranie a IP adresa SYNC rozhrania na primárnom Pfsense firewalle. Na obrázku č.6.63 bolo pre synchronizáciu povolené všetko. Nakoniec sa primárny firewall stal aktívnym firewallom a sekundárny firewall sa stal záložným firewallom.



Obr. č.6.62 Sekundárny Pfsense – Nastavenie SYNC rozhrania, časť 1



Obr. č.6.63 Sekundárny Pfsense – Nastavenie SYNC rozhrania, časť 2

Po nakonfigurovaní HA bol spustený ping z klienta Kali Linux 1 na rozhranie LAN2 u IPsec firewallu. Tento ping je vidieť na obrázku č.6.64. Neskôr boli vypnuté požadované linky. Ako je vidieť z tohto obrázka, tak skutočne došlo k prepnutiu, a to medzi paketami so sekvenčnými číslami 7 a 11. Od paketu so sekvenčným číslom 12 fungovala sieťová prevádzka podľa normalného charakteru. Toto spojenie bolo otestované aj druhý krát, ako si je možné všimnúť na obrázku č.6.65. Tu tiež nachvíľku vypadla sieťová prevádzka medzi paketami so sekvenčnými číslami 8 a 13. Od sekvenčného čísla 14 bola sieťová prevádzka obnovená. Vo výsledku to znamenalo, že síce došlo k malému výpadku, ale na druhej strane došlo k výpadku len malého počtu paketov a tiež, že reakcia sieťovej prevádzky na časovú odozvu nebola taká veľká ako pri

anyconnect spojení u softvérového ASAv firewallu. Samozrejme dá sa aj porovnať IPsec VPN pri ASAv a Pfsense firewalle. Na toto porovnanie slúžia prevažne obrázky č.6.64 a č.6.17. Pri skúmaní si je možné všimnúť, že sieťová prevádzka u ASAv firewallu reagovala na HA nepatrne lepšie ako sieťová prevádzka u Pfsense firewallu pri rovnakom režime IPsecVPN.

```
┌──(root2㉿kali)-[~]
└─$ └─$ ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=2 ttl=63 time=6.59 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=63 time=4.57 ms
64 bytes from 192.168.2.1: icmp_seq=6 ttl=63 time=4.32 ms
64 bytes from 192.168.2.1: icmp_seq=12 ttl=63 time=8.42 ms
64 bytes from 192.168.2.1: icmp_seq=13 ttl=63 time=4.99 ms
64 bytes from 192.168.2.1: icmp_seq=14 ttl=63 time=3.87 ms
64 bytes from 192.168.2.1: icmp_seq=15 ttl=63 time=4.33 ms
```

Obr. č.6.64 Testovanie HA – Pfsense, časť 1

```
┌──(root2㉿kali)-[~]
└─$ └─$ ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=63 time=13.13 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=63 time=4.22 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=63 time=7.52 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=63 time=5.93 ms
64 bytes from 192.168.2.1: icmp_seq=5 ttl=63 time=5.29 ms
64 bytes from 192.168.2.1: icmp_seq=6 ttl=63 time=5.93 ms
64 bytes from 192.168.2.1: icmp_seq=7 ttl=63 time=5.50 ms
64 bytes from 192.168.2.1: icmp_seq=13 ttl=63 time=9.88 ms
64 bytes from 192.168.2.1: icmp_seq=14 ttl=63 time=6.74 ms
64 bytes from 192.168.2.1: icmp_seq=15 ttl=63 time=5.31 ms
64 bytes from 192.168.2.1: icmp_seq=16 ttl=63 time=4.66 ms
64 bytes from 192.168.2.1: icmp_seq=17 ttl=63 time=4.28 ms
```

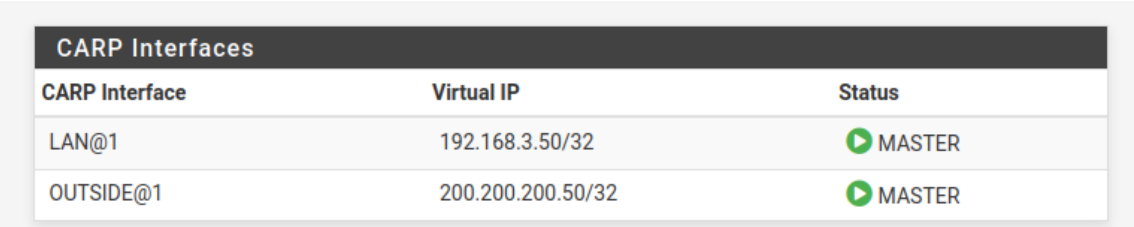
Obr. č.6.65 Testovanie HA – Pfsense, časť 2

Zároveň prešiel primárny Pfsense firewall do stavu „BACKUP“, čiže sa stal záložným firewallom a sekundárny Pfsense firewall prešiel do stavu „MASTER“, čiže sa stal aktívnym firewallom.

CARP Interfaces

CARP Interface	Virtual IP	Status
LAN@1	192.168.3.50/32	BACKUP
OUTSIDE@1	200.200.200.50/32	BACKUP

Obr. č.6.66 Primárny Pfsense – BACKUP

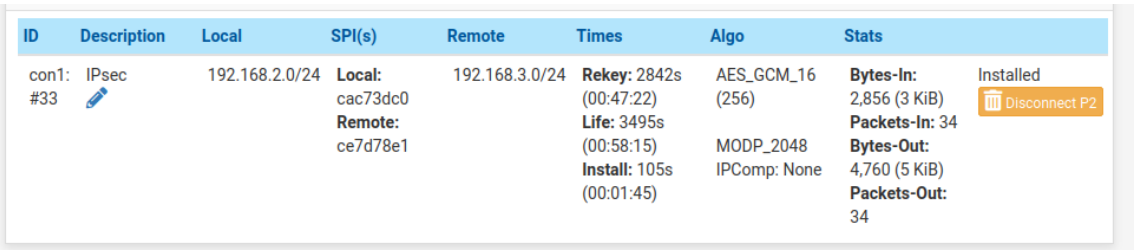


CARP Interfaces

CARP Interface	Virtual IP	Status
LAN@1	192.168.3.50/32	MASTER
OUTSIDE@1	200.200.200.50/32	MASTER

Obr. č.6.67 Sekundárny Pfsense – MASTER

Testovanie správnosti prebiehalo aj na IPsec firewalle, kde bol zapnutý monitoring IPsec VPN spojenia. Na obrázku č.6.68 je ukázaná správnosť konfigurácie HA a IPsec VPN spojenia na IPsec firewallu. Kde je znázornené, že niekto zo siete z IP rozsahu 192.168.3.0/24 sa pokúsil o ping do siete z IP rozsahu 192.168.2.0/24. A tiež, že tento ping bol úspešený – položka Stats.

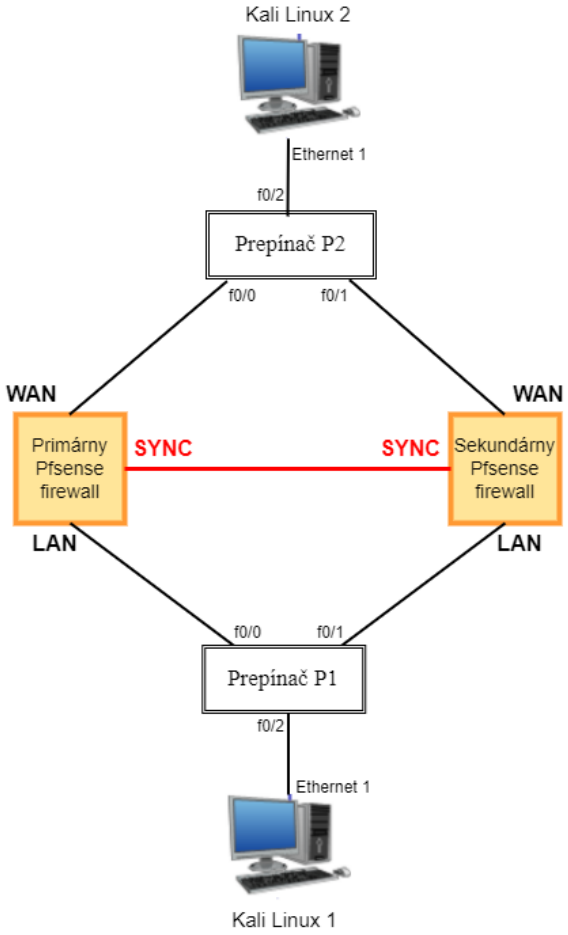


ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats	
con1: #33	IPsec	192.168.2.0/24	**Local:** cac73dc0 **Remote:** ce7d78e1	192.168.3.0/24	**Rekey:** 2842s (00:47:22) **Life:** 3495s (00:58:15) **Install:** 105s (00:01:45)	AES_GCM_16 (256) MODP_2048 IPComp: None	**Bytes-In:** 2,856 (3 KiB) **Packets-In:** 34 **Bytes-Out:** 4,760 (5 KiB) **Packets-Out:** 34	Installed Disconnect P2

Obr. č.6.68 IPsec Pfsense – kontrola IPsec pripojenia

6.8 Realizácia Pfsense firewallu v programe GNS3 – NAT

Ako druhá konfigurácia u PFsense firewallu pre otestovanie HA bola nakonfigurovaná problematika NAT. Grafický návrh konfigurácie je na obrázku č.6.69 a rozloženie IP adries pre dané rozhrania je v tabuľke č.9. Kali Linux 2 mal IP adresu 192.168.2.2 a Kali Linux 1 mal IP adresu 192.168.3.2.



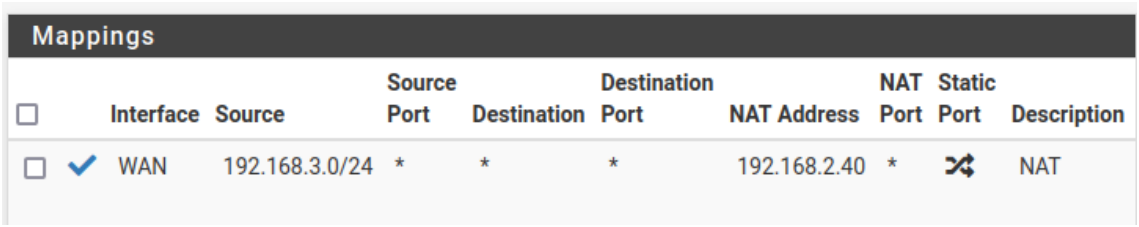
Obr. č.6.69 Návrh topológie NAT – Pfsense

Názov	IPv4 WAN	IPv4 LAN	IPv4 SYN
Primárny Pfsense firewall	192.168.2.1	192.168.3.1	1.1.1.1
Sekundárny Pfsense firewall	192.168.2.10	192.168.3.10	1.1.1.2

Tab. 9 IP adresy a rozhrania – NAT PFsense

Okrem IP adries na rozhraní Pfsense firewallov boli nastavené aj CARP adresy. Pre rozhranie WAN bola nastavená CARP adresa 192.168.2.40 a pre rozhranie LAN bola nastavená CARP adresa 192.168.3.40.

Následne bolo nastavené pravidlo NAT – obrázok 6.70, kde mal prebiehať preklad IP adries v rozhraní LAN 192.168.3.0/34 na IP CARP 192.168.2.40 na WAN rozhraní firewallov.



Mappings

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
☐	✔ WAN	192.168.3.0/24	*	*	*	192.168.2.40	*	⇄	NAT

Obr. č.6.70 Nastavenia NAT – Pfsense

Neskôr boli vypnuté linky medzi primárnym Pfsense firewallom a prepínačom P1 a tiež medzi primárnym Pfsense firewallom a prepínačom P2. Na obrázku č.6.71 je vidieť zapnutý ping z Kali Linux 1 na Kali Linux 2. Na obrázku č.6.72 je vidieť debugovanie icmp paketov na klientovi Kali Linux 2.

```
┌──(root2㉿kali)-[~]
└─$ ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=4 ttl=63 time=2.22 ms
64 bytes from 192.168.2.2: icmp_seq=8 ttl=63 time=1.59 ms
64 bytes from 192.168.2.2: icmp_seq=10 ttl=63 time=1.86 ms
64 bytes from 192.168.2.2: icmp_seq=11 ttl=63 time=2.71 ms
64 bytes from 192.168.2.2: icmp_seq=12 ttl=63 time=2.60 ms
64 bytes from 192.168.2.2: icmp_seq=13 ttl=63 time=2.58 ms
64 bytes from 192.168.2.2: icmp_seq=16 ttl=63 time=2.95 ms
64 bytes from 192.168.2.2: icmp_seq=17 ttl=63 time=2.80 ms
64 bytes from 192.168.2.2: icmp_seq=18 ttl=63 time=2.28 ms
64 bytes from 192.168.2.2: icmp_seq=19 ttl=63 time=1.88 ms
64 bytes from 192.168.2.2: icmp_seq=20 ttl=63 time=2.08 ms
```

Obr. č.6.71 Ping z Kali Linux 1 na Kali Linux 2 – Pfsense NAT

```
┌──(root4㉿kali)-[~]
└─$ sudo tcpdump -i eth1 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
15:14:57.899836 IP 192.168.2.40 > 192.168.2.2: ICMP echo request, id 15688, seq 2,
length 64
15:14:59.947881 IP 192.168.2.40 > 192.168.2.2: ICMP echo request, id 15688, seq 4,
length 64
15:14:59.947904 IP 192.168.2.2 > 192.168.2.40: ICMP echo reply, id 15688, seq 4, length
64
15:15:01.963638 IP 192.168.2.40 > 192.168.2.2: ICMP echo request, id 15688, seq 6,
length 64
15:15:04.011275 IP 192.168.2.40 > 192.168.2.2: ICMP echo request, id 15688, seq 8,
length 64
15:15:04.011306 IP 192.168.2.2 > 192.168.2.40: ICMP echo reply, id 15688, seq 8, length
64
15:15:05.013839 IP 192.168.2.40 > 192.168.2.2: ICMP echo request, id 15688, seq 9,
length 64
15:15:06.026858 IP 192.168.2.40 > 192.168.2.2: ICMP echo request, id 15688, seq 10,
length 64
15:15:06.026889 IP 192.168.2.2 > 192.168.2.40: ICMP echo reply, id 15688, seq 10, length
64
15:15:07.027829 IP 192.168.2.40 > 192.168.2.2: ICMP echo request, id 15688, seq 11,
length 64
15:15:07.027856 IP 192.168.2.2 > 192.168.2.40: ICMP echo reply, id 15688, seq 11, length
64
15:15:08.029644 IP 192.168.2.40 > 192.168.2.2: ICMP echo request, id 15688, seq 12,
length 64
15:15:08.029668 IP 192.168.2.2 > 192.168.2.40: ICMP echo reply, id 15688, seq 12, length
64
15:15:09.031566 IP 192.168.2.40 > 192.168.2.2: ICMP echo request, id 15688, seq 13,
length 64
15:15:09.031588 IP 192.168.2.2 > 192.168.2.40: ICMP echo reply, id 15688, seq 13, length
64
15:15:11.583310 IP 192.168.2.40 > 192.168.2.2: ICMP echo request, id 15688, seq 15,
length 64
15:15:12.586087 IP 192.168.2.40 > 192.168.2.2: ICMP echo request, id 15688, seq 16,
length 64
15:15:12.586117 IP 192.168.2.2 > 192.168.2.40: ICMP echo reply, id 15688, seq 16, length
64
15:15:13.586788 IP 192.168.2.40 > 192.168.2.2: ICMP echo request, id 15688, seq 17,
length 64
15:15:13.586807 IP 192.168.2.2 > 192.168.2.40: ICMP echo reply, id 15688, seq 17, length
64
```

Obr. č.6.72 Debug icmp na Kali Linux 2 – Pfsense NAT

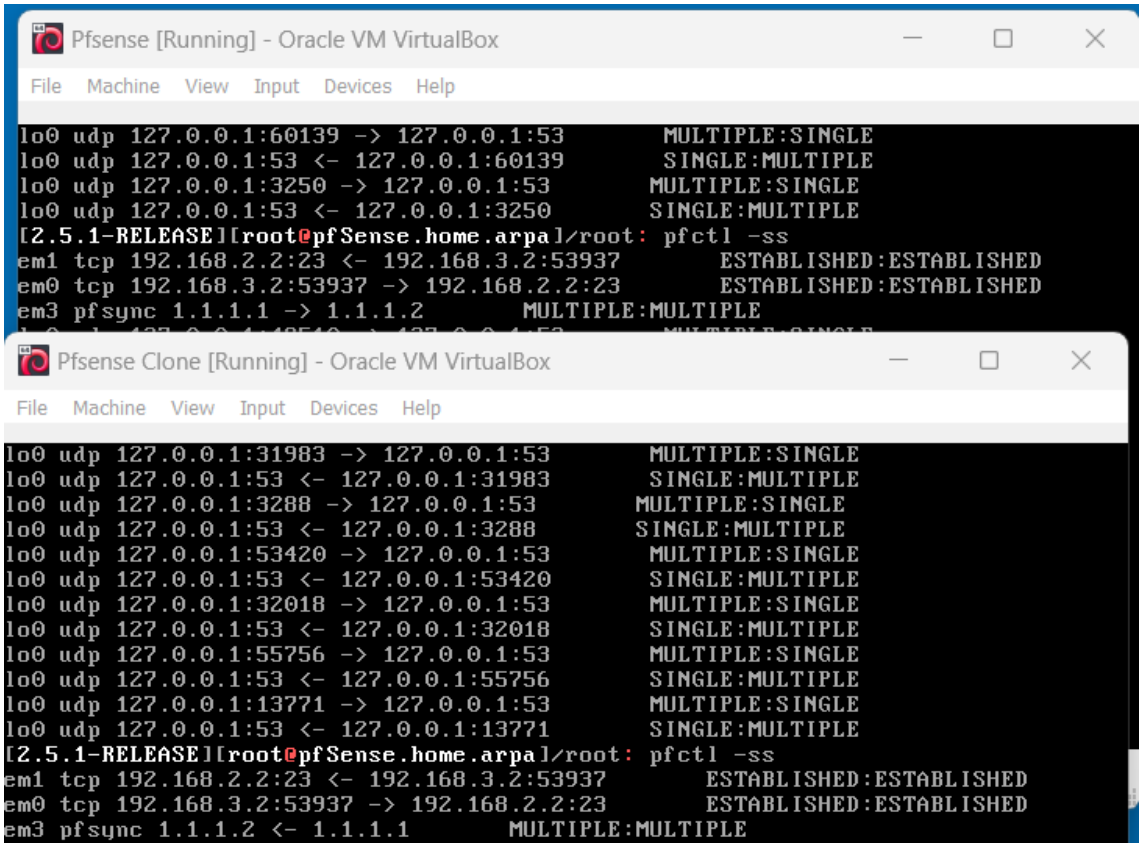
Z obrázka č.6.71 je vidieť, že sieťová prevádzka pre NAT u Pfsense firewallu nebola výrazne narušená počas prepnutia na sekundárny firewall. U tohto pingu je vidieť, že úplne prepnutie na sekundárny Pfsense firewall nastalo pri pakete so sekvenčným číslom 16. Samotné prepnutie sieťovej prevádzky pri NAT na sekundárny Pfsense firewall je označené v červenom rámčeku v obrázku č.6.71.

Avšak pre lepšiu predstavu čo sa stalo v počítačovej sieti pri prepnutí na sekundárny firewall slúži obrázok č.6.72, kde je znázornený debug icmp paketov na klientovi Kali Linux 2. Samotné prepnutie v tomto obrázku nastalo vo vyznačenom červenom rámčeku, kde je vidieť, že posledný odoslaný icmp echo reply paket z Kali Linux 2 na Kali Linux 1 pred prepntutím na sekundárny Pfsense firewall mal sekvenciu 13. Na druhej strane prvý odoslaný icmp echo reply paket po prepnutí sieťovej prevádzky na sekundárny firewall mal sekvenciu 16. Veľmi dôležitá je IP adresa, ktorá obsahuje zdroj komunikácie. Kali Linux 1 predstavoval tento zdroj komunikácie a mal IP adresu 192.168.3.2. Ale pri konfigurácií pravidel NAT bolo určené, že IP adriesy z rozsahu 192.168.3.0/24 sa budú prekladať na IP adresu typu CARP 192.168.2.40. Tento preklad IP adries je vidieť v obrázku č.6.72. V tomto obrázku je vidieť červený rámček, ktorý slúži na lepšiu orientáciu na tomto obrázku, kde je vidieť, že samotné prepnutie sieťovej prevádzky na sekundárny firewall nastalo práve v tomto červenom rámčeku. Taktiež je si možné všimnúť, že sieťová prevádzka nebola výrazne ovplyvnená po prepnutí na sekundárny firewall. Čo je ešte zaujímavejšie, tak je to, že IP adresa na ktorú sa mal preložiť klient Kali Linux 1, to je IP adresa CARP pre WAN 192.168.2.40, nebola vôbec zmenená pri prepnutí na sekundárny firewall, čiže zostala stále tá istá IP adresa, a to 192.168.2.40. Tak ako to platilo pri IPsec VPN, tak to isté platí aj pre NAT, že prepnutie sieťovej prevádzky na sekundárny firewall u Pfsense firewallu má nepatrne horšie výsledky ako u ASAv firewallu, kde pri NAT bola úspešnosť až 100%. Ale v konečnom hodnotený, prepnutie sieťovej prevádzky na sekundárny firewall nemá zásadný vplyv pre obi dva firewally v režime NAT. Existujú len zanedbateľné rozdiely.

6.9 Realizácia Pfsense firewallu v programe GNS3 – TCP spojenie

Poslednou úlohou bolo nakonfigurovať vo firewalle Pfsense trvalé TCP spojenie pri prepnutí sieťovej prevádzky na sekundárny firewall. Ako TCP spojenie bolo vybrané Telnet spojenie. Návrh počítačovej siete je podobný ako na obrázku č.6.69, len Kali Linux 1 bol nahradený smerovčom RouterInside a Kali Linux 2 bol nahradený smerovačom RouterOutside. Tabuľka IP adries je rovnaká ako v tabuľke č. 9. Princíp konfigurácie Telnet na smerovači RouterOutside bol rovnaký ako pri konfigurcácií Telnetu u ASAv firewallu. Funkčná synchornizácia TCP spojenia z primárného Pfsense firewallu na sekudnárny Pfsense firewall je na obrázku č.6.73. Z tohto obrázku je zreteľné, že na obi dvoch firewalloch bolo zaznamenané a synchronizované Telnet spojenie zo smerovača RouterInside na smerovač RouterOutside. Toto Telnet spojenie bolo zaznamenané na rozhraní WAN a aj LAN rozhraní. Avšak z tohto obrázka WAN

rozhranie predstavovalo rozhranie em1 a LAN rozhranie predstavovalo rozhranie em0. Tieto rozhrania em1 a em0 predstavovali ethernetové rozhrania. Len vo výpise cez príkaz *pfctl -ss* nie sú zobrazené názvy WAN a LAN, ale len skratky ethernetových rozhraní. Avšak vo výsledku, že na obrázku sú pomenované ethernetové rozhrania ako em0, em1 a nie ako WAN a LAN nemalo zásadný vplyv na funkčnosť režimu HA. Preto sa pracovalo v následujúcich častiach s pojmami WAN a LAN. Z obrázka č.6.73 je vidieť, že smerovač RouterInside s IP adresou 192.168.3.2 sa pripojil cez Telnet s TCP portom 23 na smerovač RouterOutside s IP adresou 192.68.2.2. A tiež je vidiež, že toto spojenie bolo zaznamenané aj na sekundárnom PFsesne firewalle, čo vo výsledku zanemnalo, že existovala medzi firewallami synchronizácia. Obi dva Pfsense firewally boli nainštalované ako virtuálne stroje vo Virtualboxe. Primárny Pfsense firewall mal pomenovanie vo Virtualboxe ako „Pfsense“. Sekundárny Pfsense firewall mal vo Virtualboxe pomenovanie ako „Pfsense Clone“. Tieto názvy si je možné všimnúť aj na obrázku č.6.73. Správnosť nakonfigurovania režimu HA bola otestovaná aj na smerovači RouterInside, kde bol zapnutý pred vypnutím liniek príkaz *show tcp biref* a po vypnutí liniek bol tento príkaz znovu zapnutý. Ako je vidieť na obrázku č.6.74, tak po odpojení daných liniek medzi primárnym PFsense firewallom a obi dvoma prepínačmi zostalo Telnet spojenie stále to isté, čiže sa nezmenili TCP porty. Vo výsledku to znamenalo, že bola overená správnosť TCP Telnet spojenia pri Pfsense firewalloch v režime HA.



Obr. č.6.73 Funkčná synchornizácia TCP spojenia – Pfsense

```
RouterOutside#show tcp  brief
TCB          Local Address         Foreign Address       (state)
649AEEA4  192.168.2.2.23        192.168.3.2.53937     ESTAB
RouterOutside #
RouterOutside #show tcp  brief
TCB          Local Address         Foreign Address       (state)
649AEEA4  192.168.2.2.23        192.168.3.2.53937     ESTAB
RouterOutside #
```

Obr. č.6.74 Nezmenené TCP Telnet spojenie – Pfsense

7. ZÁVER

Diplomová práca bola rozdelená na dve časti: teoretická časť a praktická časť. Teoretická časť bola primárne zameraná na firewally a HA problematiku. Boli zistené rôzne možnosti nasadenia HA u jednotlivých firewallov. Čo sa týka firewallov, tak bol bližšie v teoretickej časti popísaný a rozobraný ASA firewall.

V rámci mojej diplomovej práce som sa zoznámil s problematikou HA firewallov. V prostredí GNS3 som implementoval testovacie prostredie na overovanie a porovnanie HA vlastností firewallov ASA a Pfsense ako reprezentantov komerčných a opensource firewallových platforiem. ASA firewall bol reprezentovaný ako seťové virtuálne zariadenie, čiže ako ASAv. Oproti tomu Pfsense firewall bol reprezentovaný ako virtuálny stroj. Cieľom bolo nakonfigurovať v režime HA jednotlivé VPN spojenia, či už IPsec alebo anyconnect spojenie, ako aj skúmať problematiku NAT a TCP spojení v režime HA. Ďalej ako cieľom bolo aj tieto jednotlivé výsledky konfigurácie porovnať medzi ASAv a Pfsense firewallami. Ako výsledok bola nakonfigurovaná a otestovaná základná konfigurácia HA pre VPN, NAT a pre TCP spojenia.

Testovaním a skúmaním sa prišlo k záveru, že napr. IPsec VPN spojenie pre sotfvérový ASAv a Pfsense firewall v režime HA pri výpadku primarného firewallu reaguje na výpadok sieťovej prevádzky lepšie ako anyconnect VPN spojenie u softvérového ASAv firewallu, kde pri výpadku primarného ASAv firewallu dochádza k väčšej časovej odozve, a to až približne 40-45 sekúnd.

U IPsec VPN spojenia je možné porovnať aj ASAv spolu s PFsense firewallami. Pred samotným porovnaním treba zobrať do úvahy fakt, že sieťové virtuálne zariadenia majú menšie nároky na operačnú pamäť a procesor ako virtuálny stroj, čo mohlo pri výsledkoch viesť ku miernému skresleniu. Z výsledok merania vyplýva, že pre IPsec VPN spojenie je vhodnejší ASAv firewall, kde sieťová prevádzka pri prepnutí na sekundárny firewall reagovala o niečo lepšie ako u Pfsense firewallu.

U NAT výsledky boli podobné. Tiež mal ASAv firewall o málo lepšiu reakciu na prepnutie sieťovej prevádzky na sekundárny firewall ako Pfsense firewall. Tiež bolo dokázané, že výpadok primarného ASAv alebo Pfsense friewallu nemá zásadný vplyv na sieťovú prevádzku a reakcia sieťovej prevádzky u obi dvoch firewallov bola lepšia pri NAT ako pri IPsec VPN. Na druhej strane stále platí, že najhoršie výsledky dosiahol ASAv firewall pri anyconnect VPN.

Na overenie správnej funkčnosti synchronizácie tabuľky otvorených TCP spojení primárneho a sekundárneho firewallu boli použité aplikácie Telnet, SSH a BGP. Na protokole BGP je veľmi dobre vidieť, že pri prepnutí na sekundárny firewall nedôjde k rozpadu TCP spojenia. Navyše som v rámci riešenia diplomovej práce získať skúsenosti s týmto smerovacím protokolom. Z výsledkov sa môže potvrdiť, že obi dva firewally podporujú TCP spojenie. Čiže obi dva firewally sú v synchronizácií stavových TCP tabuliek rovnocenné.

V samotnom zhrnutí obi dvoch firewallov, či už komerčného firewallu – ASAv alebo opensource firewallu – Pfsense sa môže z vyskúmaných výsledkov definitívne určiť, že obi dva firewally podporujú pri režime HA synchronizáciu VPN, NAT a aj TCP spojenia. V podrobnom zhrnutí bolo výskúmané, že sieťová prevádzka pri IPsec VPN a NAT u ASAv firewallov reagovala pri prepnutí firewallov nepatrne lepšie ako pri Pfsense firewallov. Toto malé zhoršenie u Pfsense firewallov mohlo byť spôsobené prevažne tým, že Pfsense firewall bol reprezentovaný ako virtuálny stroj, naproti tomu ASAv firewall bol reprezentovaný ako sieťové virtuálne zariadenie. Pri konfigurácií IPsec VPN u Pfsense firewallu bolo použitých až päť virtuálných strojov, dva reprezentovali klientov, ktorí mali operačný systém Kali Linux a tri reprezentovali firewall Pfsense. Päť súčasne spustených virtuálnych strojov na jednom fyzickom notebooku malo veľké požiadavky na operačnú pamäť a procesor.

LITERATÚRA

[1] In: UPPAL, Shveta a Bijnan SUTAR. *Computer Science: Computer Networks* [online]. Delhi: NCERT, 2020, s. 182-202 [cit. 2022-12-07]. ISBN 978-93-5292-338-0. Dostupné z: https://ncert.nic.in/textbook/pdf/lecs110.pdf

[2] STOJANOVSKI, Nenad a Marjan GUSEV. Analysis of Computer Network Attacks [online]. Skopje, 2018, s. 21-28 [cit. 2022-11-19]. Dostupné z: https://www.researchgate.net/publication/258778792_Analysis_of_Computer_Network_Attacks

[3] KUMAR, Gulshan, Amanjeet KAUR a Sania SETHI. Computer Network Attacks - A Study [online]. 2014, s. 24-31 [cit. 2022-11-19]. Dostupné z: https://www.researchgate.net/publication/311108218_Computer_Network_Attacks-A_Study

[4] ÚTOKY NA SIEŤ [online]. [cit. 2022-11-19]. Dostupné z: https://www.kis.fri.uniza.sk/~ludo/simona/ponuka/utokynasiet.html

[5] SHI, Junyan a Juanjuan LI. The Security and Protection Strategy Study of Computer Network Information [online]. 2016, 34-37 [cit. 2022-11-19]. Dostupné z: https://www.researchgate.net/publication/308629254_The_Security_and_Protection_Strategy_Study_of_Computer_Network_Information

[6] HE, Xinzhou. *Research on Computer Network Security Based on Firewall Technology* [online]. Wuhan, 2020, s. 1-4 [cit. 2022-11-19]. Dostupné z: https://iopscience.iop.org/article/10.1088/1742-6596/1744/4/042037/pdf

[7] A. SHAJI, George a George HOVAN. A Brief Study on The Evolution of NextGeneration Firewall and Web ApplicationFirewall [online]. Chennai, 2021, 32-36 [cit. 2022-11-19]. Dostupné z: https://www.researchgate.net/publication/351637754_A_Brief_Study_on_The_Evolution_of_Next_Generation_Firewall_and_Web_Application_Firewall

[8] The History of the Firewall [online]. [cit. 2022-11-19]. Dostupné z: https://www.aureon.com/services/it-management/it-services/security/firewall/the-history-of-the-firewall/

[9] Understand the evolution of firewalls [online]. [cit. 2022-11-19]. Dostupné z: https://www.techrepublic.com/article/understand-the-evolution-of-firewalls/

[10] KONIKIEWICZ, Wojciech a Marcin MARKOWSKI. Analysis of Performance and Efficiency of Hardware and Software Firewalls [online]. Wroclaw, 2017, s. 50-52 [cit. 2022-11-19]. Dostupné z: https://www.researchgate.net/publication/322857184_Analysis_of_Performance_and_Efficiency_of_Hardware_and_Software_Firewalls

[11] SCARFONE, Karen a Paul HOFFMAN. Guidelines on Firewalls and Firewall Policy: Firewall Planning and Implementation [online]. Gaithersburg, 2009, s. 51-58 [cit. 2022-11-19]. Dostupné z: https://www.govinfo.gov/content/pkg/GOVPUB-C13-

f52fdee3827e2f5d903fa8b4b66d4855/pdf/GOVPUB-C13-f52fdee3827e2f5d903fa8b4b66d4855.pdf
[12] *About HA* [online]. [cit. 2022-11-19]. Dostupné z: https://docs.sophos.com/nsg/sophos-firewall/18.5/Help/en-us/webhelp/onlinehelp/HighAvailablityStartupGuide/AboutHA/index.html
[13] High Availability (HA) Firewall [online]. [cit. 2022-11-19]. Dostupné z: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/high-availability-ha-firewall/
[14] In: PAN-OS® Administrator's Guide: High Availability [online]. Version 10.1. Santa Clara: Palo Alto Networks, 2023, s. 363-450 [cit. 2023-04-22]. Dostupné z: https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-1/pan-os-admin/pan-os-admin.pdf Cisco Switching and Spanning Tree Protocol (STP) Basics [online]. [cit. 2022-11-02]. Dostupné z: https://www.pluralsight.com/blog/it-ops/switching-and-stp
[15] Common Types of Routing Protocols: A Complete Guide [online]. [cit. 2022-11-05]. Dostupné z: https://www.indeed.com/career-advice/career-development/routing-protocols
[16] What is Open Shortest Path First (OSPF)? [online]. [cit. 2022-11-05]. Dostupné z: https://www.metaswitch.com/knowledge-center/reference/what-is-open-shortest-path-first-ospf
[17] RIP Protocol [online]. [cit. 2022-11-05]. Dostupné z: https://www.javatpoint.com/rip-protocol
[18] Border Gateway Protocol (BGP) [online]. [cit. 2023-04-22]. Dostupné z: https://www.imperva.com/learn/ddos/border-gateway-protocol-bgp/
[19] Border Gateway Protocol [online]. [cit. 2023-04-22]. Dostupné z: https://www.javatpoint.com/border-gateway-protocol
[20] *Princíp HSRP* [online]. [cit. 2022-11-20]. Dostupné z: http://tech.sosthe.sk/index.php/ccna/cisco-ios/16-hsrp-hot-standby-routing-protocol/
[21] VRRP (Virtual Router Redundancy Protocol) [online]. [cit. 2023-04-22]. Dostupné z: https://networklessons.com/cisco/ccie-routing-switching/vrrp-virtual-router-redundancy-protocol
[22] In: ELTAEIB, Tarik a Sahithi SAHITHI. Journal of Multidisciplinary Engineering Science and Technology [online]. Vol. 2 Issue 3. 2015, s. 408-410 [cit. 2022-11-20]. ISBN 3159-0040. Dostupné z: https://www.jmest.org/wp-content/uploads/JMESTN42350531.pdf
[23] PfSense - introduction to the most powerfull router operating system [online]. [cit. 2022-10-26]. Dostupné z: https://teklager.se/en/pfsense-introduction-open-source-router-firewall/
[24] The pfSense Documentation. : HIGH AVAILABILITY [online]. 2022, 801-814 [cit. 2022-11-20]. Dostupné z:

https://docs.netgate.com/manuals/pfsense/en/latest/the-pfsense-documentation.pdf
[25] FortiOS - Cookbook. In: : High availability [online]. Version 6.0.0. 2020, s. 133-134 [cit. 2022-11-20]. ISSN 01-600-000000-20200624. Dostupné z: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a4a06ec3-12a7-11e9-b86b-00505692583a/FortiOS-6.0.0-Cookbook.pdf
[26] High Availability. In: PAN-OS® Administrator's Guide [online]. Version 10.1. Santa Clara: Palo Alto Networks, 2022, s. 361-445 [cit. 2022-10-18]. Dostupné z: https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-1/pan-os-admin/pan-os-admin.pdf
[27] Next-Generation Firewall [online]. [cit. 2022-11-20]. Dostupné z: https://www.juniper.net/us/en/solutions/next-gen-firewall.html
[28] WHAT IS THE CISCO ADAPTIVE SECURITY APPLIANCE (ASA)? - CXTEC [online]. [cit. 2023-04-22]. Dostupné z: https://www.cxtec.com/blog/what-is-cisco-asa-security-appliance/
[29] Cisco Adaptive Security Virtual Appliance (ASAv) - BYOL [online]. [cit. 2023-04-22]. Dostupné z: https://www.exoscale.com/marketplace/listing/cisco-adaptive-security-virtual-appliance-byol/
[30] In: CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.6: How to Implement Firewall Services [online]. San Jose: Cisco Systems, 2016, s. 23-27 [cit. 2023-04-22]. Dostupné z: https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-1/pan-os-admin/pan-os-admin.pdf
[31] In: CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.6: Network Address Translation (NAT) [online]. San Jose: Cisco Systems, 2016, s. 171-196 [cit. 2023-04-22]. Dostupné z: https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-1/pan-os-admin/pan-os-admin.pdf
[32] What is IPsec? | How IPsec VPNs work [online]. [cit. 2023-04-22]. Dostupné z: https://www.cloudflare.com/learning/network-layer/what-is-ipsec/
[33] CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.7 [online]. [cit. 2023-04-23]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/vpn/asa-97-vpn-config/vpn-ike.html
[34] What is a remote access VPN and how does it work? [online]. [cit. 2023-04-23]. Dostupné z: https://nordvpn.com/blog/remote-access-vpn/
[35] What is a site-to-site VPN? How it works [online]. [cit. 2023-04-23]. Dostupné z: https://nordvpn.com/blog/site-to-site-vpn/

[36] CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.8 [online]. [cit. 2023-04-23]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/configuration/general/asa-98-general-config/ha-failover.html

ZOZNAM SYMBOLOV A SKRATIEK

AH	Authentication Header
ACL	Access Control List
ARP	Address Resolution Protocol
ASA	Adaptive Security Appliance
ASAv	Adaptive Security Virtual Appliance
BGP	Border Gateway Protocol
BPDU	Bridge protocol Data Unit
CARP	Common Address Redundancy Protocol
CDA	Context Directory Agent
COPS	Computer Oracle and Password Systém
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
eBGP	Exterior Border Gateway Protocol
ESP	Encapsulating Security Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
FGCP	FortiGate Clustering Protocol
FTP	File Transfer Protocol
HA	High Availability
HMAC	Hashed Message Authentication
HSRP	Hot Standby Router Protocol
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
iBGP	Interior Border Gateway Protocol
ICMP	Internet Control Message Protocol
ID	Identification Number
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IPSEC	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISAKMP	Internet Security Association and Key Management Protocol
LSA	Link State Agreement).
NAPR	Napríklad
NAT	Network Address Translation
NGFW	Next-Generation Firewalls
OSPF	Open Shortest Path First
PAT	Dynamic Port Address Translation
RAM	Random Access Memory

RFC	Request For Comments
RIP	Routing Information Protocol
RSA	Rivest-Shamir-Adleman
SA	Security Association
SDN	Software Defined Networks
SIP	Session Initiation Protocol
SMLI	Stateful multiplayer inspection firewalls
SSH	Secure Shell Protocol
SSL	Secure Sockets Layer
SCTP	Stream Control Transmission Protocol
STP	Spanning Tree Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	Time To Live
TZV	Takzvane
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAF	Web Aplication Firewall