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

DNS FIREWALL A JEHO NASAZENÍ A INTEGRACE V RÁMCI KYBERNETICKÉHO CENTRA

DNS FIREWALL AND ITS DEPLOYMENT AND INTEGRATION IN CYBER CENTER

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Martin Doležal

AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. Jan Jeřábek, Ph.D.

SUPERVISOR

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Martin Doležal ***ID:*** 221270

Ročník: 3 ***Akademický rok:*** 2021/22

NÁZEV TÉMATU:

DNS firewall a jeho nasazení a integrace v rámci kybernetického centra

POKYNY PRO VYPRACOVÁNÍ:

V rámci bakalářské práce bude popsáno fungování DNS, firewallu a DNS firewallu, dále budou prozkoumány možnosti integrace DNS firewallu s využitím BIND DNS s dalšími nástroji používanými v kybernetickém operačním centru. Dále pak budou zmapovány možnosti implementace DNS firewallu do IT infrastruktury kybernetického operačního centra. Budou ověřeny způsoby vynucení využití DNS firewallu dotčenými stanicemi nehledě na momentálně využívanou síť či jejich aktuální lokaci. V rámci praktické části práce bude provedena implementace a nasazení firewallu BIND DNS v reálném kybernetickém operačním centru, včetně vyhodnocení vynucení využití DNS firewallu v praxi. Dále bude provedena jeho integrace s vhodnými dostupnými nástroji v rámci kybernetického operačního centra. Na základě toho bude provedeno stanovení vhodných metrik a atributů pro vyhodnocení provozu BIND DNS RPZ firewallu z hlediska využitelnosti v operačním kybernetickém centru. V rámci semestrálního projektu proveďte teoretický rozbor technologií a postupů. Dále proveďte praktické ověření fungování DNS klientů na platformách Windows, OS.x a Android při manuálním nastavení DNS serveru a změnách připojení.

DOPORUČENÁ LITERATURA:

[1] KUROSE, J. F., ROSS, K. W., Computer networking: a top-down approach. 7th global ed. Essex: Pearson, 2017, 852 s. ISBN 978-1-292-15359-9.

[2] JEŘÁBEK, J. Pokročilé komunikační techniky. Skriptum FEKT Vysoké učení technické v Brně, 2021. s. 1-180.

Termín zadání: 7.2.2022 ***Termín odevzdání:*** 31.5.2022

Vedoucí práce: doc. Ing. Jan Jeřábek, Ph.D.

Konzultant: Mgr. Lukáš Novák, Axenta, a.s.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Tato bakalářská práce se věnuje nasazení, integraci a testování DNS firewallu v kybernetickém operačním centru. Popisuje možnosti napojení koncových stanic a vzdálených místních sítí na DNS firewall umístěný v rámci kybernetického operačního centra. Dále je popsáno vynucení využívání DNS firewallu. Hlavním cílem práce bylo nasadit a integrovat DNS firewall v kybernetickém operačním centru. První kapitola obecně popisuje kybernetické operační centrum a jeho části. Druhá kapitola se věnuje systému DNS. V následující kapitole je popsáno zabezpečení systému DNS a zabezpečení DNS dotazů a čtenář je seznámen s pojmem DNS firewall a s technologiemi RPZ a VPN. Čtvrtá kapitola popisuje postup nasazení DNS firewallu a jeho integraci v reálném kybernetickém operačním centru. Další kapitola popisuje možnosti napojení koncových stanic a vzdálených místních sítí na DNS firewall umístěný v rámci kybernetického operačního centra a jeho vynucení. Poslední kapitola se věnuje testování výkonnosti a dostupnosti nasazeného DNS firewallu. Výsledkem práce je nasazený, integrovaný, funkční a otestovaný DNS firewall v reálném kybernetickém operačním centru. Pro implementaci a nasazení DNS firewallu byl využit softwarový balík BIND a technologie RPZ. Pro napojení stanic byla využita technologie VPN a pro testování byla využita síť RIPE Atlas.

KLÍČOVÁ SLOVA

Berkeley Internet Name Domain, bezpečnost, bezpečnostní dohled, blokování DNS dotazů, Domain Name System, DNS firewall, DNS over VPN, firewall, kybernetické operační centrum, Response Policy Zones, SOC jako služba, Threat Intelligence

ABSTRACT

This bachelor's thesis deals with the deployment, integration, and testing of a DNS firewall in a security operations center. It describes the connection of endpoints and remote local area networks to the DNS firewall located in the security operations center. Furthermore, the enforcement of the DNS firewall is described. The main goal of the thesis was to deploy and integrate a DNS firewall inside a security operations center. The first chapter describes the security operations center in general. The second chapter deals with the DNS system. The following chapter describes the security of the DNS system and security of DNS requests, the reader is informed of the term DNS firewall and RPZ and VPN technologies. The fourth chapter describes the DNS firewall deployment process and its integration in a real security operations center. The next chapter describes connection methods of endpoint and remote local area networks to the DNS firewall and its enforcement inside the security operations center. The last chapter deals with performance testing and deployed DNS firewall availability. The outcome of the thesis involves a deployed, integrated, fully-functional, and tested DNS firewall in a real-world security operations center. The Bind software package along with the RPZ technology was used to implement and deploy the DNS firewall. For testing and connection of endpoints, the VPN technology, and the RIPE Atlas network was used.

KEYWORDS

Berkeley Internet Name Domain, security, security monitoring, DNS query blocking, Domain Name System, DNS firewall, DNS over VPN, firewall, Security Operations Center, Response Policy Zones, SOC as a service, Threat Intelligence

Vysázeno pomocí balíčku `thesis` verze 4.07; `http://latex.feec.vutbr.cz`

DOLEŽAL, Martin. *DNS firewall a jeho nasazení a integrace v rámci kybernetického centra*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2022, 89 s. Bakalářská práce. Vedoucí práce: doc. Ing. Jan Jeřábek, Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Martin Doležal
VUT ID autora:	221270
Typ práce:	Bakalářská práce
Akademický rok:	2021/22
Téma závěrečné práce:	DNS firewall a jeho nasazení a integrace v rámci kybernetického centra

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

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

Brno ....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

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

Obsah

Seznam obrázků

Seznam výpisů

Úvod

V dnešní době je velká část elektrických zařízení připojená k síti Internet. Tato zařízení jsou v síti Internet adresována pomocí IP adres, díky kterým mezi sebou mohou komunikovat. Pro běžného uživatele není možné si zapamatovat adresy zařízení v Internetu a proto většina komunikace na Internetu začíná Domain Name System (DNS) dotazem. Tento DNS dotaz je vyhodnocen systémem DNS. Systém DNS je hierarchický jmenný systém, který si můžeme představit jako databázi navzájem propojených odkazů na IP adresy serverů. Síťovým adresám přiřazuje lehčeji zapamatovatelná doménová jména. DNS je vlastně celosvětově distribuovanou databází, která umožňuje uživatelům, ale i počítačům přístup k aktuální IP adrese dané služby bez její předchozí znalosti. Dnes DNS představuje základní službu Internetu.

Každé zařízení na síti Internet může být potenciálním cílem útoku, ale i útočníkem. Systém DNS může být například využit škodlivým softwarem ke komunikaci s ovládacím serverem nebo k jiné nežádoucí aktivitě, jelikož na většině místních sítí v rámci Internetu je DNS protokol povolen a nefiltrován. Pro filtraci a řízení DNS dotazů lze využít DNS firewall. DNS firewall dokáže pomocí mechanismu Response Policy Zone (RPZ) filtrovat potenciálně nebezpečné DNS dotazy a tím může zabránit vzniku potenciálně nebezpečné komunikace na Internetu. Mechanismus RPZ dokáže modifikovat DNS odpovědi dle definicí administrátora.

Dnes jsme svědky neustálých kybernetických útoků na soukromé organizace, státní správu a kritickou infrastrukturu státu. Z tohoto důvodu chce být čím dál více těchto organizací monitorováno pomocí kybernetického operačního centra (SOC). Tato kybernetická operační centra jsou budována v rámci dané organizace nebo tyto organizace využívají externích kybernetických operačních center, které jsou nabízeny jako služba organizacím. DNS firewall může dodat navíc větší vhled do monitorované sítě díky informacím o provedených DNS dotazech a jejich překladech. Při monitoringu provozu na síti můžou DNS dotazy dodat více informací než standardní IP toky.

Tato bakalářská práce se věnuje nasazení a integraci DNS firewallu v reálném kybernetickém operačním centru, které je nabízeno jako služba organizacím. Dále se věnuje možnosti připojení organizací a koncových stanic k DNS firewallu provozovaným v SOCu a popisuje možnosti vynucení využívání tohoto DNS firewallu.

Cílem této bakalářské práce je popsat postup nasazení DNS firewallu v SOCu a jeho integrace s ostatními technologiemi využívanými v SOCu, popsání a otestování

možností připojení koncových stanic a vzdálených sítí k tomuto DNS firewallu a navrhnutí postupu, který by vedl k vynucení využívání tohoto DNS firewallu. Dále by měla být ověřena možnost využitelnosti, výkonnosti a dostupnosti DNS firewallu a navrhovaných řešení.

1 Kybernetické operační centrum

Tato kapitola seznamuje čtenáře s pojmem kybernetické operační centrum, anglicky se tento výraz překládá jako Security Operations Center, zkráceně SOC. Dále jsou v kapitole stručně popsány procesy a technologie využívané v rámci provozu SOCu.

1.1 Popis kybernetického operačního centra

SOC se skládá z lidí, procesů a technologií, které dohromady vytváří centralizovaný tým pro prevenci, detekci, analýzu a monitoring kybernetické bezpečnosti organizací. Monitorovány jsou aktivity jednotlivých aplikací, serverů, databází, koncových stanic a jiných zařízení.[1, 2, 3, 4]

SOC je standardně budován pro monitoring interní sítě organizace. Zároveň si ho ale můžeme představit jako službu bezpečnostní společnosti, která ve svém SOCu monitoruje sítě jednotlivých připojených zákazníků. Výhodou interního SOCu je perfektní znalost technologií, infrastruktury dané sítě a rychlá komunikace s daným IT oddělením. Výhodou SOCu jako služby jsou menší vstupní náklady pro organizaci, která si přeje být SOCem monitorována. Zároveň tím získá rozsáhlý analytický tým a tým techniků. Organizace pak není nucena nabírat specialisty na kybernetickou bezpečnost a školit pracovníky odbornou problematikou, je postačující seznámit stávající IT oddělení se zpracováváním podnětů ze SOCu. Nevýhodou tohoto řešení je pak neúplná znalost prostředí zákazníka, což může vyvolávat mnoho falešných incidentů.[1, 2, 3, 4]

V případě využití SOCu jako služby probíhá sběr dat vzdáleně. Zpracování dat, jejich další vyhodnocení a případná analýza probíhá již v SOCu. Následně je nejčastěji využíváno tiketovacího systému, kde pracovníci SOCu informují zákazníka o vzniklých incidentech a doporučují následné kroky a řešení. SOC může nabídnout i svůj investigativní tým k řešení složitějších bezpečnostních incidentů.[1, 2, 3, 4]

1.2 Lidé, technologie a procesy v kybernetickém operačním centru

1.2.1 Procesy v kybernetickém operačním centru

Procesy v prostředí SOCu propojují lidi a technologie. Jedná se o seskupení postupů, aktivit apod., které jsou využívány při řešení různých bezpečnostních událostí. Výsledkem správného vytvoření postupů je funkční SOC, který dokáže reagovat na jakoukoliv situaci. Podle kvality jednotlivých procesů je možné určit i celkovou kvalitu SOCu. Jedná se například o postup při řešení incidentu.[1, 2, 3, 4]

1.2.2 Technologie v kybernetickém operačním centru

Základní funkcí SOCu je sběr a následné vyhodnocení logů. K tomu je určena technologie Log Management, zkráceně LM. Tato technologie se stará o sběr, archivaci a indexaci logů. Následně umožňuje nad logy vyhledávat a provádět případnou analýzu. S technologií LM souvisí technologie Security Information and Event Management, zkráceně SIEM. Na základě vytvořených korelačních pravidel technologie SIEM provádí další vyhodnocování logů, které může vést až k vytvoření bezpečnostních událostí, ze kterých se později mohou stát incidenty. Korelované události se na základě procesu třídění alertů následně zobrazují obsluze v SIEMu. Zde analytický tým Level 1 provádí prvotní vyhodnocení a danou událost buď vyřeší sám, nebo ji předá na další analýzu analytické skupině Level 2. [1, 2, 3, 4]

Typickou součástí SOCu je i provozní monitoring. Ten nám dodává aktuální informace o stavech jednotlivých, do něj napojených, zařízení, například vytížení CPU, využití RAM atd. Dalšími technologiemi využívanými v SOCu jsou například technologie typu Endpoint Detection and Response (EDR), Threat Intelligence a jiné.[1, 2, 3]

1.2.3 Lidé v kybernetickém operačním centru

Pracovníci SOCu jsou děleni do základních dvou skupin a to na technický tým a analytický tým. Technický tým se stará o nasazování a údržbu technologií v SOCu, ale i u zákazníků. Analytický tým je dělen na Level 1, Level 2 a Level 3. Níže popsané rozdělení pracovníků SOCu je v dlouhodobé praxi považováno za ověřené. Je možné, že schopnosti a vlastnosti některých týmů se mohou překrývat. Součástí SOCu může být i management nebo technický architekt.[1, 2, 3, 4]

Level 1 analytik, zkráceně L1, zpracovává události ze SIEMu v reálném čase. Tento tým často pracuje v nasazení 24/7. Právě L1 analytici jsou prvními, kdo řeší nově vzniklé události. Tyto události mohou být vyřešeny následujícími způsoby. Za prvé - na základě svých vlastních znalostí mohou být události vyhodnoceny jako falešně pozitivní a v SIEMu jsou uzavřeny nebo mohou být vyhodnoceny jako incident a v tomhle případě je obsluha povinná informovat o této skutečnosti zákazníka. Za druhé může být vzniklá událost řešena pomocí postupů předem vytvořených vyšším analytickým týmem. Pokud obsluha ani jednu z následujících možností nevyhodnotí jako bezpečnostní událost, je přistoupeno k poslední možnosti a to, že daná událost je určena k další analýze. V takovém případě je sesbíráno co nejvíce informací o dané události, která je posléze předána na analytický tým L2. L1 analytik by měl mít základní povědomí ohledně informačních technologií, počítačových sítí, programování a měl by umět provádět základní analýzu. Analytik zároveň dohlíží na stav provozního monitoringu.[1, 4]

Level 2 analytik, zkrácené L2, je nedílnou součástí SOCu. L2 analytický tým by měl mít nejširší znalost v oboru kybernetické bezpečnosti v SOCu, zároveň musí splňovat jednotlivé vlastnosti L1 analytika. L2 analytici by měli mít celkové povědomí o většině využívaných a monitorovaných technologií a měli by být schopni provádět detailní analýzu. Tým L2 analytiků vytváří postupy pro skupinu L1 analytiků, vytváří nebo upravuje korelace a detekční metody, které následně přidává do SIEMu a sepisuje dokumentace. Nedílnou součástí práce L2 analytika je i hledání potenciálních hrozeb v surových datech, ke kterým ještě zpravidla nemusí být vytvořeny detekční pravidla nebo korelace. Pokud při analýze události nemá L2 analytik dostatečné znalosti, přenechá řešení této události L3 analytikovi. Další nedílnou znalostí analytika je orientace v oblasti tzv. Threat Intelligence. Tato oblast se zabývá automatizovaným sběrem dat o aktuálních nebezpečných aktérech a bezpečnostních hrozbách v kyberprostoru, shromažďuje informace o aktuálních "trendech", které může předávat například do SIEMu a můžou se nad nimi vytvářet další korelace.[1, 4]

Level 3 analytik, zkráceně L3, je analytik, který má největší znalosti jedné nebo více konkrétních technologií v SOCu nebo v dané bezpečnostní oblasti. Je to například odborník na malware a pokud L2 analytik nedokáže vyřešit událost týkající se malwaru, předá ji k řešení právě tomuto analytikovi. Ten, jelikož má expertní znalosti této oblasti, by měl dokázat danou událost vyřešit.[1, 4]

2 Domain Name System

Tato kapitola se věnuje bližšímu popisu služby Domain Name System, jejím protokolům, historii a důvodům, proč tato služba vznikla. Popisuje princip DNS, hierarchii DNS a druhy DNS dotazů a záznamů.

2.1 Historie a současnost Domain Name System

Myšlenka využívání doménových jmen na místo adresy sahá až do počátku samotného Internetu. Tato idea se poprvé objevila u sítě ARPANET, předchůdci dnešní sítě Internet. Překlad adres na jména byl realizován na stanicích jednotlivě pomocí souboru `host`, ve kterém byly definovány jednotlivé záznamy a soubor musel být vytvořen na každé stanici ručně. Tím vznikl problém, při kterém nedocházelo ke sjednocení doménových jmen, což mělo za následek, že na jednotlivých stanicích mohla být adresa reprezentována různým doménovým jménem. Řešení sjednocení doménových jmen bylo vytvořit soubor, který bude následně distribuován do všech ostatních stanic. Tento sdílený soubor vznikl ve Stanford Research Institute a jeho kopie byla distribuována na stanice zapojené v síti ARPANET. Toto řešení není škálovatelné a distribuce probíhala z jednoho místa. V té době byl malý počet doménových jmen a k jejich změně docházelo zřídka. Daný typ řešení se již v dnešní době nevyužívá, přesto se ale soubor `host` dodnes nachází ve všech operačních systémech a lze v něm manuálně definovat překlad doménových jmen na IP adresy.[5, 6]

V roce 1983 Paul Mockapetris na původní žádost Johna Postela ve standardech RFC 882 a RFC 883 prvně popisuje hierarchickou strukturu doménových jmen a zároveň definuje protokol, který má být využíván k překladu doménových jmen na IP adresy. K překladu jmen se má využívat jmenný server na místo lokálních `host` souborů. V roce 1984 na základě standardu RFC 882 a RFC 883 vznikl první DNS jmenný server, který vyvinuli studenti Kalifornské univerzity. Tato interpretace se nazývala The Berkeley Internet Name Domain Server, zkráceně BIND, postavená na operačním systému UNIX. Tím bylo poprvé možné využít myšlenku Paula Mockapetrise. Softwarový balík BIND je dodnes vyvíjen Kalifornskou univerzitou jako opensource a kromě služby DNS serveru zastřešuje i jiné funkce, například funkci Response Policy Zone (RPZ), které se věnuje tato práce. V roce 1987 byl původní protokol aktualizován ve standardu RFC 1034, který tvoří základ dnešní struktury DNS protokolu. Do roku 1998 spravovala doménová jména a přidělování IP adres organizace IANA, ze které v roce 1998 vznikla organizace ICANN sídlící v Los Angeles v Kalifornii v USA. Organizace ICANN je dnes nadřazená organizaci IANA, která má stále na starost i mimo jiné přidělování a správu doménových jmen.[5, 6, 7, 8, 9]

2.2 Důvod využívání Domain Name System

Komunikace na Internetu probíhá pomocí přepojování paketů. Zpráva, která má být zaslána přes síť Internet je nejprve rozdělena na menší části, tzv. pakety, které jsou následně poslány přes síť Internet. Tyto pakety nemusí být vždy směrovány stejnou cestou a mohou využívat více linek. K jejich správnému směrování slouží IP protokol. IP protokol definuje, jak mají být jednotlivé pakety směrovány v síti. Základní poznávací znamení všech prvků na Internetu je IP adresa. IP adresa je unikátní číslo, které identifikuje jednotlivá zařízení a lze si ji představit jako kombinaci směrovacího čísla a čísla popisného na domech. IP adresa se může v čase pro jednotlivá zařízení v síti měnit, navíc je nemožné si zapamatovat IP adresy například všech serverů, na které je během dne přistupováno. Systém DNS řeší tyto problémy tak, že IP adresám jsou přiřazovány snadněji zapamatovatelná doménová jména. Systém DNS je decentralizovaný, hierarchický, škálovatelný a může dodávat různé druhy informací.[5, 10]

2.3 Doménová jména a jejich hierarchie

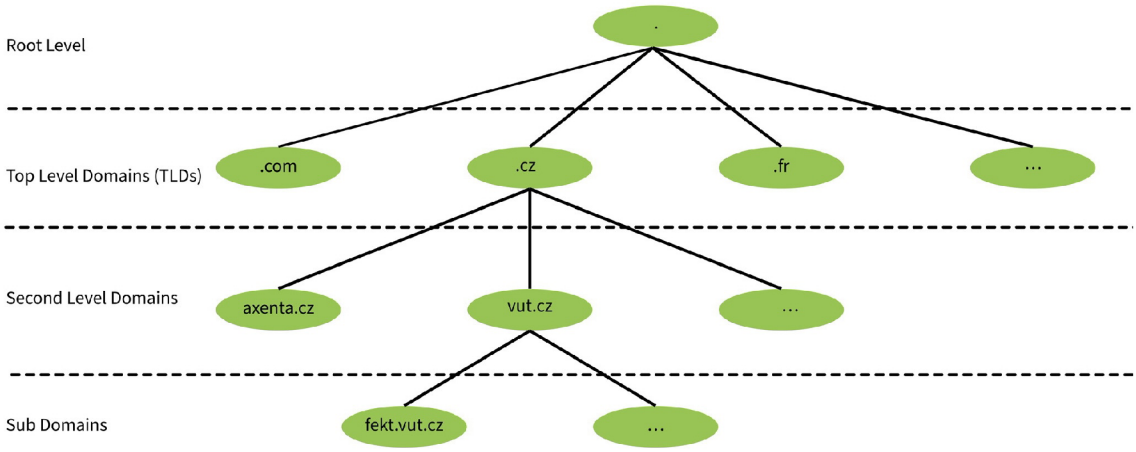
Doménové jméno, někdy označováno jako internetová doména, je jednoznačné označení prvku sítě, skupiny prvků nebo třeba služby. Příkladem doménového jména je www.vut.cz. Doménové jméno je rozděleno tečkami, které oddělují jednotlivé řády doménového jména. Na konci se nachází také tečka, která určuje kořenovou doménu a tato tečka je doplňována automaticky. Doménová jména jsou reprezentována stromovou strukturou, která byla zavedena standardem RFC 882, jak je znázorněno na obrázku 2.1.[5, 10]

Domény nejvyššího řádu, tzv. TLD (Top Level Domain), někdy označovány jako domény prvního řádu, jsou děleny do základních kategorií na národní a generické. Příkladem TLD jsou domény typu cz, org, net, com, gov atd. Tyto domény sdružují například národní domény nebo organizační domény. Domény druhého řádu, tzv. SLD (Second Level Domain), již reprezentují jednotlivé uzly na druhé úrovni hierarchické stromové struktury systému DNS. Spojením domény prvního a druhého řádu vzniká doménové jméno, například vut.cz, axenta.cz.[5, 10]

Domény prvního řádu jsou spravovány organizací IANA. Domény řádu druhého jsou spravovány většinou národní autoritou. V České republice je tímto správcem organizace CZ.NIC. Domény třetího a nižšího řádu jsou již spravovány firmou nebo organizací, která vlastní doménu druhého řádu.[9]

Aby se jednotlivé stanice na síti Internet dostaly k těmto doménovým jménům, existují ještě tzv. root servery (kořenové). Ty jsou rozmístěny různě po světě a mají v sobě záznamy o jednotlivých doménách prvního řádu. Tyto servery jsou považovány za základní část infrastruktury Internetu. Po celém světě distribuují základní databáze doménových jmen. Doménové jméno má maximální velikost 255 bytů. Část doménového jména mezi dvěma tečkami má maximální délku 63 bytů. [5, 10]

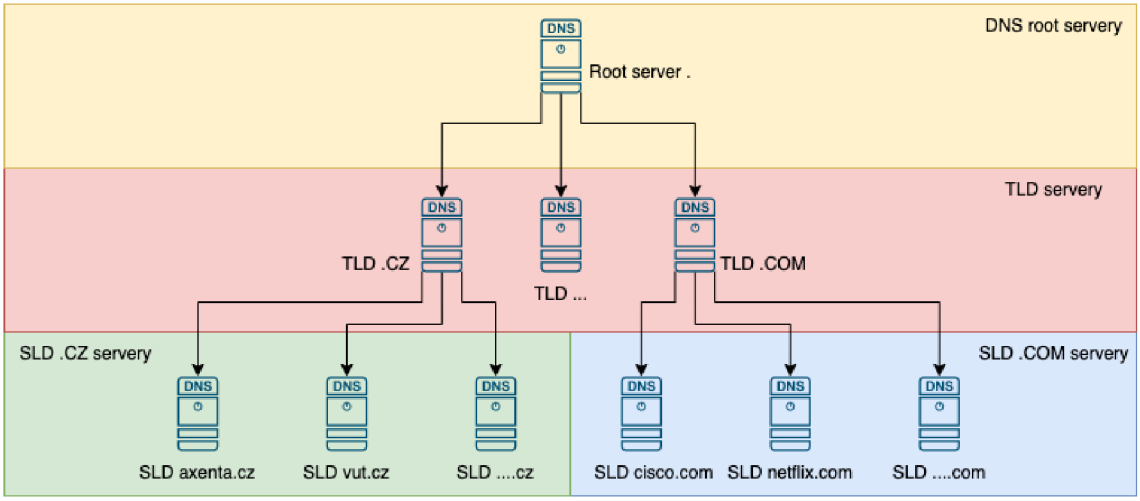
Specifikované doménové jméno, též FQDN (Fully Qualified Domain Name), označuje konkrétní zařízení v síti a vzniká spojením názvu stanice s jeho doménou, například `pc4.lab58.utko.fekt.vut.cz.` [10]



Obr. 2.1: Hierarchie doménových jmen v DNS

Hierarchie serverů protokolu DNS je jako struktura doménových jmen stromová, jak je znázorněno na obrázku 2.2. Na vrcholku stromu jsou kořenové (root) DNS servery, které spravují databáze IP adres serverů, které spravují domény prvních řádů. Na druhé úrovni se nachází servery, které spravují většinou státní organizace a ty mají databáze IP adres DNS serverů, které spravují domény druhých řádů. Servery, které spravují domény druhých a nižších řádů jsou již většinou vlastněny firmami, poskytovateli nebo organizacemi, které vlastní konkrétní domény druhého řádu a zároveň tyto servery spravují informace o doménách nižších řádů.[5, 10]

Systém DNS je dnes reprezentován 13 kořenovými servery, které běží na více než 1500 instancích po celém světě. Tyto kořenové servery jsou označeny písmeny A až M. Aktuální přehled funkčních instancí lze nalézt na stránce root-servers.org. K dnešnímu dni se v České republice nachází 9 instancí kořenových serverů.[11]



Obr. 2.2: Hierarchie doménových serverů v DNS

Jak již bylo řečeno, kořenové servery pod sebou mají servery, které spravují domény prvního řádu. Těmto serverům se říká TLD servery, jelikož spravují TLD domény.[5, 10]

Zóna je část hierarchie stromové struktury doménových jmen a může být oddělena na úrovni teček v doménovém jméně. S výjimkou kořenové domény je zóna vždy delegována výše nadřazené zóně.[4, 5, 10]

2.4 DNS Resolver

DNS Resolver, do češtiny přeložen jako DNS překladač, je server v místní síti nebo na Internetu, který se stará o převádění doménových jmen na adresy IP. DNS Resolver může fungovat v následujících základních módech:

- Forwarding - jde o typ nastavení serveru, při kterém DNS Resolver přepošle celý dotaz na jiný DNS Resolver.

- Recursion - jde o typ nastavení serveru, při kterém DNS Resolver vyhodnotí DNS dotaz podle obrázku 2.3.

2.5 Základní princip komunikace v systému DNS a vyhodnocení DNS dotazu

Systém DNS funguje na principu klient-server (dotaz-odpověď) a jak již bylo řečeno, směrování komunikace v síti Internet probíhá na základě číselných IP adres. Princip komunikace protokolu DNS je vysvětlen na následujícím příkladu. Uživatel počítače chce přes svůj webový prohlížeč navštívit webové stránky vut.cz. Tuto adresu zadá do prohlížeče a v tu chvíli začne počítač využívat DNS protokol, který musí vyřešit problém překladu doménového jména vut.cz na IP adresu. Na stanici musí být nastavena IP adresa DNS Resolveru, jenž je buď nastavena automaticky pomocí protokolu DHCP při připojení do sítě, nebo je nastavena manuálně uživatelem, administrátorem nebo pomocí politiky organizace. Stanice tedy položí dotaz DNS Resolveru, který má nastavený jako výchozí. V konečném důsledku se ho ptá, jaká IP adresa náleží doménovému jménu vut.cz. DNS Resolver má pak dvě možnosti. Buď tuto informaci již zná a vrátí ji stanici, nebo ji bude muset dotazem zjistit. Dotazy dělíme na:

- Rekurzivní - Pokud dotazovaný DNS Resolver odpověď nezná (tzn. není autoritativní pro doménu), standardním způsobem se dotáže na tuto doménu kořenového serveru a dalších DNS serverů podle obrázku 2.3, a následně odpověď zašle tazateli.

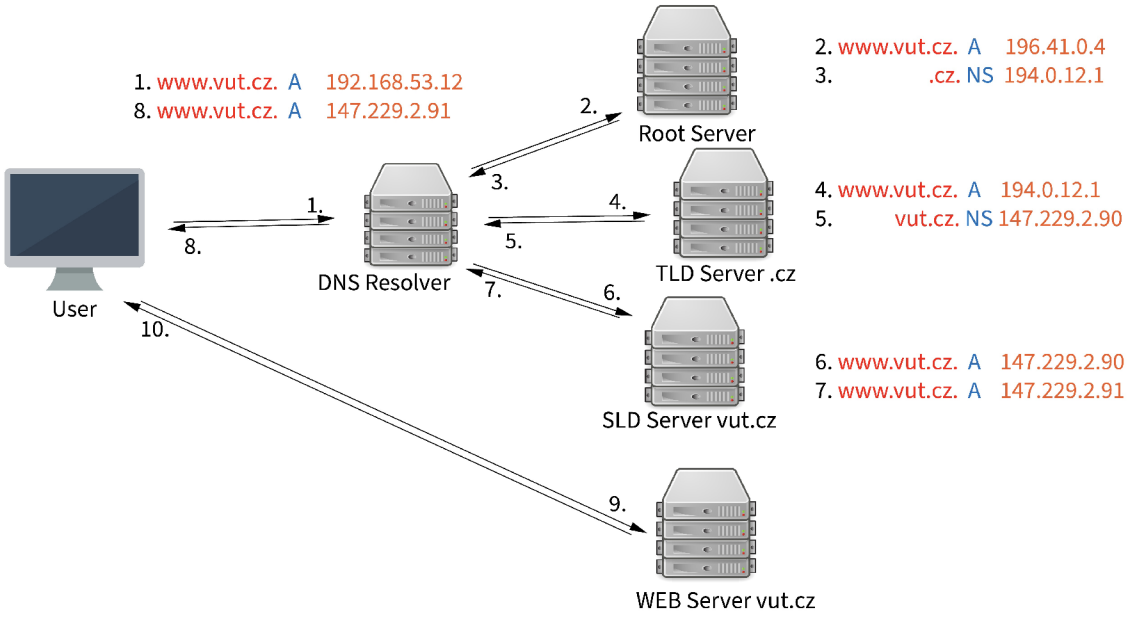
- Nerekurzivní - DNS server zná odpověď, jelikož je autoritativní pro danou doménu.

- Iterativní – DNS server vrátí nejbližší odpověď, kterou má k dispozici, tazateli. Neprovádí další dotazování a tím se minimalizuje počet dotazů.

DNS komunikace standardně probíhá na portu 53 pomocí protokolu UDP. Je možné tuto komunikaci provádět i přes spolehlivý protokol TCP, kde se taktéž využije port 53. TCP DNS komunikace se využívá například při přenosu většího objemu dat, například při přenosu zón mezi autoritativními servery. TCP komunikace se také využívá pokud je DNS odpověď příliš dlouhá. V tomto případě se od klienta očekává, že UDP odpověď zahodí a položí dotaz znovu, tentokrát pomocí TCP protokolu na který mu následně DNS server odpoví několika paketami. Při využívání TCP protokolu je také hovořeno o zvýšené spolehlivosti.[4, 5, 10]

Celý proces je popsán na obrázku 2.3 a následujícím příkladu. Uživatelská stanice se doptá svého DNS Resolveru na překlad doménového jména www.vut.cz. Je-

likož má DNS Resolver IP adresu 192.168.53.12, můžeme říct, že je součástí místní sítě, ve které se nachází i uživatelská stanice. DNS Resolver není autoritativní pro doménu vut.cz a ani nemá ve své paměti uložený překlad k tomuto doménovému jménu, proto se doptá Root serveru s IP adresou 196.41.0.4. Root server vrací DNS Resolveru adresu TLD serveru. Tento TLD server je autoritativní pro doménové jméno prvního řádu cz., v našem případě se jedná o IP adresu 194.0.12.1. DNS Resolver se nyní doptá TLD serveru opět na překlad doménového jména www.vut.cz., TLD server vrátí DNS Resolveru adresu SLD serveru, který je autoritativní pro doménovou zónu vut.cz. V dalším kroku se DNS Resolver doptá SLD serveru na doménové jméno www.vut.cz. a jelikož je tento SLD server autoritativní pro toto doménové jméno, vrátí pak DNS Resolveru IP adresu serveru, jenž odpovídá tomuto doménovému jménu. DNS Resolver pak předá uživatelskému PC IP adresu náležící doménovému jménu www.vut.cz a ten pak s ním již komunikuje dle potřeby.[4, 5, 10]



Obr. 2.3: Průběh vyhodnocení DNS dotazu

2.6 Typy DNS záznamů

Pojem Resource Record, zkráceně RR, reprezentuje jednotlivé záznamy v DNS databázi serveru nebo klienta. RR obsahuje vlastníka záznamu (Owner), třídu (IN - Internet, CH - Chaos, HS - Hesiod), typ záznamu, TTL a RDATA (Resource Data). Tyto informace se ukládají do tzv. zónových souborů. Následující typy DNS záznamů jsou relevantní pro tuto práci. [12]

2.6.1 A a AAAA záznam

Tento typ záznamu slouží pro přiřazení domény nebo subdomény k IP adrese a vždy obsahuje IP adresu ve formátu IPv4, pokud jde o záznam typu A, nebo IPv6 adresu, pokud jde o záznam typu AAAA.[12]

2.6.2 PTR záznam

PTR (Pointer Record) je takzvaný reverzní záznam, který je přesným opakem záznamu typu A nebo AAAA. PTR dotazem zjistíme, které doménové jméno odpovídá dané IP adrese.[12]

2.6.3 NS záznam

NS (Name server) záznam obsahuje IP adresu DNS serveru, který spravuje danou doménu nebo subdoménu. [12]

2.6.4 CNAME záznam

Záznam typu CNAME (Canonical Name) slouží pro nasměrování domény nebo subdomény na jinou doménu. V praxi je tento typ záznamu používán například pro přesměrování všech dotazů končících .vut.cz na adresu vut.cz.[12]

2.6.5 MX záznam

MX (Mail Exchange) záznam určuje, na jaký server se má směrovat emailová pošta pro danou doménu. Tyto záznamy jsou důležité pro komunikaci mailových serverů.[12]

2.7 Typy DNS odpovědí

Při vyhodnocení DNS dotazu zasílá DNS Resolver výsledek dotazovateli. Součástí tohoto výsledku je i DNS kód odpovědi. Následují typy kódů DNS odpovědí, které jsou relevantní pro tuto práci.[12]

2.7.1 NOERROR DNS odpověď

DNS odpověď typu NOERROR je nejčastější typ odpovědi v systému DNS. V podstatě říká, že daný DNS dotaz byl korektně vyhodnocen DNS Resolverem a zodpovězen dle dostupných dat.[12]

2.7.2 NXDOMAIN DNS odpověď

Odpověď typu NXDOMAIN je druhý nejčastější typ odpovědi v systému DNS. V případě, kdy DNS Resolver zašle odpověď NXDOMAIN, znamená to, že daná doména neexistuje nebo o ní DNS systém nemá veřejně dostupný záznam.[12]

2.7.3 SERVFAIL DNS odpověď

DNS odpověď SERVFAIL, oznamuje, že DNS Resolver nemohl dotaz vyhodnotit. Tuto odpověď může DNS Resolver zaslat v případě výkonnostních nebo jiných technických problémů.[12]

2.7.4 REFUSED DNS odpověď

Odpověď typu REFUSED zasílá DNS Resolver v případě, kdy z důvodů zásad nemůže dotaz vyhodnotit. Například když DNS dotaz dojde na DNS Resolver z jiného zařízení než z povoleného.[12]

3 DNS zabezpečení a Virtual Private Network

Tato kapitola se věnuje funkci DNSSEC, DNS over HTTPS, DNS firewallu, problematice jeho zabezpečení a monitoringu. Dále seznamuje s technologií RPZ a s BIND DNS. V poslední řadě je popsána technologie VPN.

3.1 Domain Name System Security Extensions

DNSSEC (Domain Name System Security Extensions) umožňuje v síti Internet zabezpečit informace poskytnuté systémem DNS proti podvržení nebo manipulaci. DNS Resolver může ověřit integritu poskytnutých dat pomocí elektronického podpisu. Nezajišťuje šifrování dat a využívá se asymetrické kryptografie. Správce domény vygeneruje soukromý a veřejný klíč. Soukromým klíčem podepisuje data, která posílá jako odpověď. Příjemce dat si může ověřit integritu a původ dat pomocí veřejného klíče. [13]

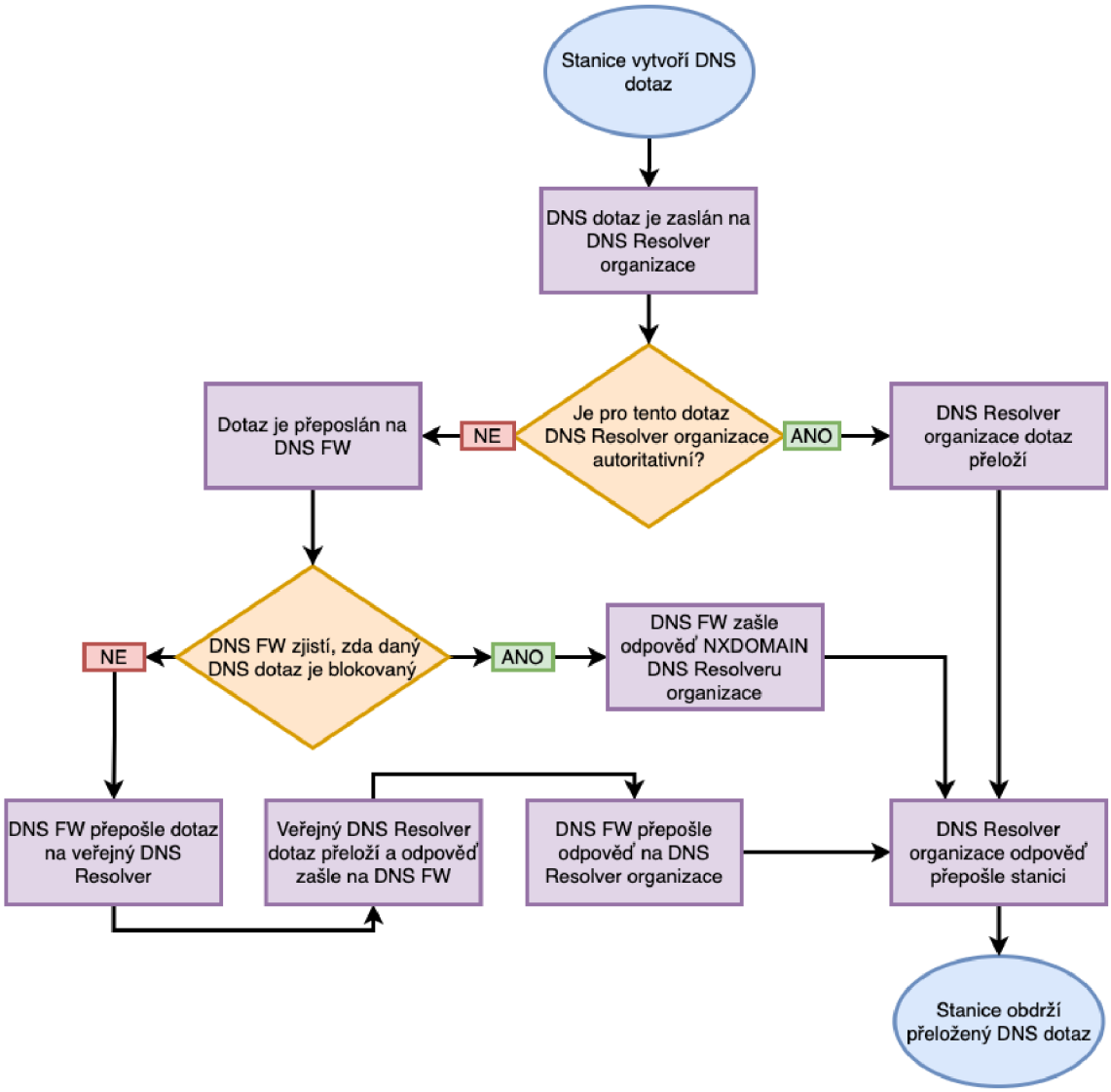
3.2 DNS over HTTPS

DoH (DNS over HTTPS) je protokol, který má za cíl zvýšit soukromí a bezpečnost tím, že zabrání odposlouchávání a manipulaci s daty DNS komunikace pomocí protokolu HTTPS, který zajišťuje šifrování dat mezi klientem a serverem. Webový prohlížeč se tedy pomocí šifrovaného protokolu HTTPS připojí na DNS Resolver a ten mu vrátí požadovaná data. V tomto případě je pro správce sítě nemožné filtrovat DNS dotazy z jednotlivých stanic. Funkce DoH je nastavována ve webovém prohlížeči a její zpřístupnění je závislé na regionu a verzi operačního systému. V dnešní době je možné nastavit DoH i v rámci některých operačních systémů.[14, 15]

3.3 DNS firewall

DNS firewall je bezpečnostní řešení, které umožňuje uživatelům, stanicím, serverům či aplikacím zabránit přístupu do škodlivých zón. DNS firewall funguje na stejném principu jako klasický firewall. Základem je filtrování DNS dotazů podle nastavených pravidel. Tím, na rozdíl od klasického firewallu, zabraňuje vzniknutí potenciálně škodlivé komunikaci, jelikož zablokuje překlad doménového jména a tudíž

nedojde ke komunikaci mezi stanicí a škodlivým serverem. Na obrázku 3.1 je zobrazeno zasazení DNS firewallu do systému vyhodnocení DNS dotazu. Pro DNS firewall není důležité, zda byl DNS dotaz zaslán spolehlivým TCP protokolem nebo nespolehlivým UDP protokolem a také není důležité, zda byl dotaz zaslán pomocí IPv4 nebo IPv6 protokolu. [16]



Obr. 3.1: Zasazení DNS firewallu do systému vyhodnocení DNS dotazu

Typický síťový firewall pracuje na třetí a čtvrté vrstvě ISO/OSI modelu a blokuje veškerou komunikaci, kromě komunikace povolené administrátorem sítě. DNS firewall funguje jako typický DNS Resolver, překládá veškeré DNS dotazy, kromě těch zakázaných, které jsou definovány jeho správcem. Blokované překlady mohou být nastavovány a stahovány automaticky z tzv. feedů. Z toho plyne, že kvalita a

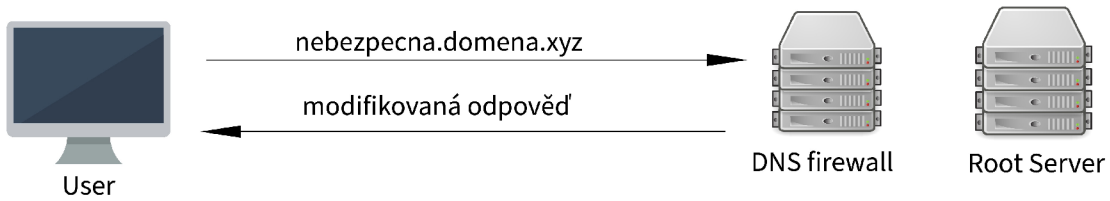
účinnost DNS firewallu je závislá na kvalitě a množství feedů. Právě z těchto feedů jsou stahována škodlivá doménová jména, která se následně nepřekládají. Zde se nabízí možnost využití placených feedů, ale ani u nich není zaručena jejich kvalita. Seznam některých poskytovatelů feedů je dostupný na adrese `dnsrpz.info`. [16]

DNS firewall dodává patřičný vhled do dění v místní síti, ve které je implementován. DNS firewall by měl umožňovat logování informací, jak o úspěšných, tak i o zamítnutých překladech doménových jmen. Tyto logy jsou pak užitečné pro další analýzu v rámci SOCu. Pro implementaci DNS firewallu lze využít technologii RPZ.[4]

3.3.1 Technologie Response Policy Zones (RPZ)

Technologie RPZ, neboli Response Policy Zones rozšiřuje funkce DNS Resolveru. Umožňuje rekurzivnímu DNS serveru vracet případně upravené výsledky. Úpravou výsledku lze zablokovat přístup k odpovídajícímu hostiteli. Mechanismus RPZ je publikován jako otevřený a multiplatformní standard pro výměnu informací o konfiguraci brány firewall DNS. RPZ umožňuje rekurzivnímu DNS serveru zvolit konkrétní akce, které mají být provedeny pro danou zónu. Pro každou zónu se služba DNS může rozhodnout provést standardní vyhodnocení DNS dotazu nebo jiné akce, včetně prohlášení, že požadovaná doména neexistuje, nebo dotaz přesměrovat na jinou doménu. RPZ je v podstatě filtrovací mechanismus. Vzhledem k tomu, že informace o zóně lze získat z externích zdrojů (prostřednictvím přenosu zóny), DNS serveru to umožňuje získat tyto informace o doméně od externí organizace. Tyto informace se nazývají reputační listy. Pro implementaci technologie RPZ lze využít programový balík BIND.[4, 17]

Na obrázku 3.2 je zobrazen DNS dotaz, který je potenciálně nebezpečný. Pomocí technologie RPZ je dotaz zablokován a uživateli byla vrácena upravená odpověď.



Obr. 3.2: Zablokování nebezpečného DNS dotazu DNS firewallem pomocí technologie RPZ

3.3.2 Berkeley Internet Name Domain (BIND)

Berkeley Internet Name Domain (BIND) je multiplatformní programový balík určený k interakci se systémem DNS. Jeho nejvýznamnější částí je komponenta pojmenovaná `named`. Tato komponenta plní role jak autoritativního DNS serveru, tak i rekurzivního DNS serveru. BIND je dnes nejpoužívanější software pro DNS servery. Byl navržen na University of California, Berkeley (UCB). Z názvu univerzity později vznikl i název softwaru Berkeley Internet Name Domain. Dnes je BIND vydáván a stále aktivně udržován konsorciem Internet Systems Consortium (ISC).[4, 18, 19]

BIND umožňuje personalizovat vyhodnocení DNS dotazů pomocí tzv. pohledů. Tyto pohledy umožní poskytovat konkretizované zóny specifikovaným zákazníkům SOCu jako služby. BIND umožňuje využití tzv. DNS RPZ. Dále umožňuje logovat rozsáhlé informace ohledně překladu doménových jmen a provozu DNS serveru.
[4, 18, 19]

BIND byl pro tuto práci zvolen na základě diplomové práce [4], ve které jsou porovnávána řešení Knot DNS Resolver, PowerDNS, Unbound DNS a BIND. Pouze BIND má všechny potřebné funkce pro fungování v SOCu jako služby. Jedná se o funkce jako je DNS forwarder, umožnění využívání různých pohledů, poskytování RPZ zón, whitelistování, blokování nebo pouze oznamování definovaných DNS dotaz a logování.

Konfigurace BINDu se provádí v konfiguračním souboru `named.conf` uloženém v adresáři `/etc/`. Obsah konfiguračního souboru je zobrazen ve výpisu 3.1.

```
options {
    // Definice portů a adres, na kterých server naslouchá.
    listen-on port 53 { 127.0.0.1; };
    listen-on-v6 port 53 { ::1; };
    // Pracovní adresář pro named.
    directory   "/var/named";
    // Cesta k souboru, do kterého bude vypsána databáze na
        vyžádání.
    dump-file   "/var/named/data/cache_dump.db";
    // Cesta k souboru, do kterého se vypisuje statistika
       pokud je k tomu named vyzván.
    statistics-file "/var/named/data/named_stats.txt";
    // Cesta k souboru, do kterého se vypisuje statistika o
```

```
        využití paměti po ukončení.
    memstatistics-file "/var/named/data/named_mem_stats.txt
        ";
    // Adresy, kterým má named vyhodnocovat dotazy.
    allow-query     { localhost; };
    // Nastavení named do rekurzivního módu.
    recursion yes;
    // Zapnutí funkce DNSSEC.
    dnssec-validation auto;
    bindkeys-file "/etc/named.bind.keys";
    managed-keys-directory "/var/named/dynamic";
    // Nastavení vyhodnocovacích limitů.
    rate-limit {
        responses-per-second 5;
        errors-per-second    5;
        nxdomains-per-second 40;
        qps-scale            300;
        exempt-clients { "localnets"; };
    };
    fetches-per-server 30;
    fetches-per-zone   20;
};
// Nastavení logování
logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};
// Definování zóny
zone "." IN {
    type hint;
    file "named.ca";
};
include "/etc/named.rfc1912.zones";
```

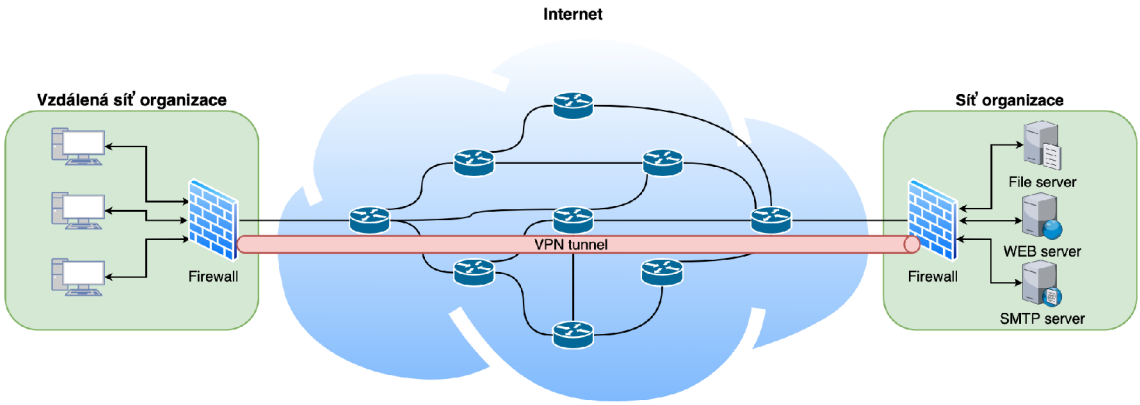
Výpis 3.1: Výchozí konfigurační soubor BIND doplněný o komentáře

3.4 Virtual Private Network

Technologie VPN, v češtině virtuální privátní síť, vytváří virtuální propojení nad jinou sítí. Umožňuje připojení do místní sítě, například sítě organizace, skrz síť Internet. Zařízení, které je připojeno přes VPN do místní sítě, se chová jako kdyby se v této síti nacházelo. Při využití VPN se vytváří spojení mezi zařízením a krajním bodem místní sítě, kde toto spojení může být šifrované. VPN se vytváří navázáním virtuálního spojení typu Point-to-Point nebo Point-to-Multipoint pomocí vyhrazených okruhů nebo tunelových protokolů přes stávající sítě. Z pohledu uživatele lze ke zdrojům dostupným v místní síti přistupovat vzdáleně. V některých sítích nebo státech může být technologie VPN blokována. [10, 20]

3.4.1 VPN typu Site-to-Site

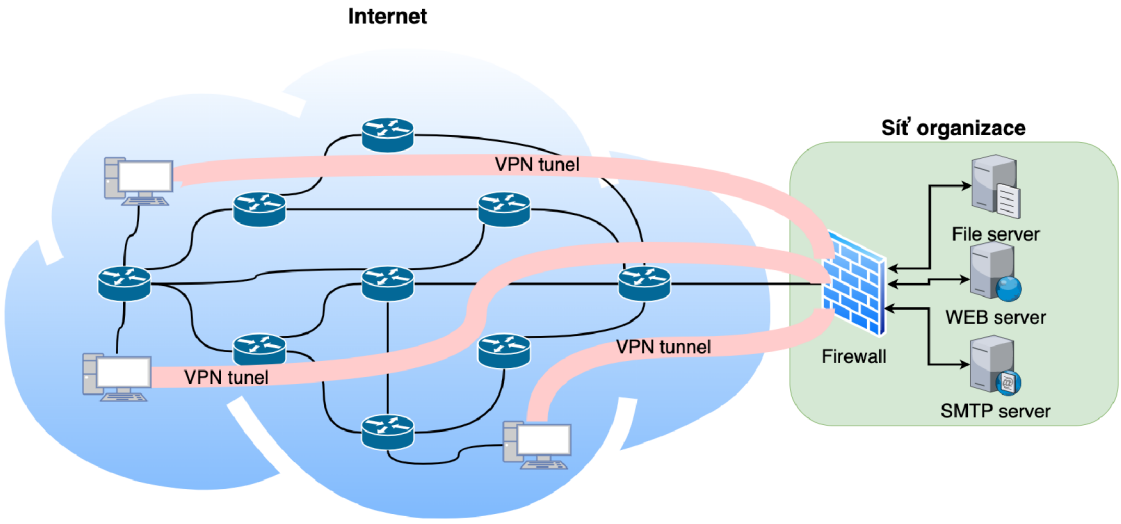
VPN sítě typu Site-to-Site umožňují propojit vzdálené místní sítě virtuálním tunelem. Vznikají vytvořením tunelu mezi hraničními uzly, typicky firewally, propojených sítí viz obrázek 3.3. Typickým protokolem využívaným v Site-to-Site VPN je IPsec. [20]



Obr. 3.3: Znázornění propojení dvou firemních sítí pomocí Site-to-Site VPN

3.4.2 Přístupové VPN sítě

Přístupové VPN sítě slouží k připojení vzdálených koncových zařízení do místní sítě přes síť Internet viz obrázek 3.4. Zde je nejčastěji využívaná technologie OpenVPN.[20]



Obr. 3.4: Znázornění připojení stanic do firemní sítě pomocí přístupové VPN

4 Nasazení DNS firewallu v kybernetickém operačním centru

Tato kapitola popisuje prostředí, ve kterém probíhalo nasazování DNS firewallu. Dále popisuje postup implementace DNS firewallu a jeho integraci s ostatními službami kybernetického operačního centra v testovacím prostředí.

4.1 Popis prostředí

V testovacím prostředí firmy AXENTA a.s. byla vytvořena testovací síť s virtuálním serverem. Na tento server byl nainstalován operační systém CentOS ve verzi 7. Dále byl nainstalován programový balík BIND ve verzi 9.16.23. Následně byl do tohoto testovacího subnetu vytvořen přístup ze sítě Internet pomocí OpenVPN. OpenVPN je technologie pro vytvoření šifrovaného spojení mezi zařízením nacházejícím se na Internetu a interní místní sítí. Testovací server má 4 CPU, 8 GB RAM a 70 GB HDD.

4.2 Nasazení DNS firewallu

Pro DNS FW na virtuálním serveru je využívána komponenta `named` z programového balíčku BIND 9. Konfigurace probíhá pomocí souboru `named.conf` umístěným v adresáři `/etc/`.

DNS FW byl nastaven do módu forwarder, tudíž bude v případě potřeby překladu doménového jména dotaz předávat na jiný DNS Resolver. Pro aktuální testování byl BIND DNS nastaven na přeposílání všech DNS dotazů na veřejné DNS Resolvery s IP adresami 1.1.1.1 a 8.8.8.8 od společností Cloudflare Inc. a Google LLC. DNS FW byl nastaven do tohoto módu, jelikož má na starost pouze filtrování DNS dotazů. Překlad těchto dotazů mají tedy na starost veřejné DNS Resolvery. Toto nastavení se provede zadáním následujících příkazů do konfiguračního souboru `named.conf`:

```
options {
    forward only;
    forwarders {
        1.1.1.1; 8.8.8.8;
    };
};
```

V případě, kdy je definováno více IP adres DNS Resolverů v konfiguračním nastavení `forwarders`, využívá komponenta `named` algoritmus SRTT. Jedná se o algoritmus váženého vyvažování zátěže, který vybírá nejrychleji reagující server a upřednostňuje jeho použití. Více o využívání algoritmu SRTT komponentou `named` je popsáno v dokumentu [24].

Dále bylo nutné definovat, jakým zdrojovým adresám má DNS FW vyhodnocovat DNS dotazy. Pro aktuální testovací nasazení bylo povoleno vyhodnocování DNS dotazů VPN klientům a adresám ze subnetu DNS FW. V případě připojení zákazníka SOCu nebo místní sítě je nutné toto nastavení upravit. Nastavení je provedeno zadáním následujících příkazů do konfiguračního souboru `named.conf`:

```
options {
    allow-query { trusted-IP-queries; };
    allow-recursion{ trusted-IP-queries; };
    allow-query-cache { trusted-IP-queries; };
};
acl trusted-IP-queries {
    127.0.0.1/32;
    192.168.53.0/24;
    192.168.239.0/24;
    };
```

Pro jednodušší orientaci byl vytvořen acl list `trusted-IP-queries`, ve kterém je definováno, kterým adresám má DNS FW vyhodnocovat dotazy. IP adresy mohou být typu IPv4 i IPv6. Funkce DNSSEC na DNS firewallu byla ponechán ve výchozím nastavení tudíž bez ohledu na požadavek klienta DNS firewall verifikuje DNS dotazy pomocí technologie DNSSEC.

Ke zjednodušení správy komponenty `named` na DNS FW je v softwarovém balíku BIND utilita `rndc`. Tato utilita umožňuje lokálně, ale i vzdáleně spravovat komponentu `named`. Pomocí utility `rndc` je možné například obnovit informace ze zónových souborů. Pro použití utility `rndc` je nutné povolit v konfiguračním souboru `named.conf` tuto utilitu a to přidáním následujících příkazů:

```
include "/etc/rndc.key";
controls {
   inet 127.0.0.1 port 953
   allow { 127.0.0.1; } keys { "rndc-key"; };
   };
```

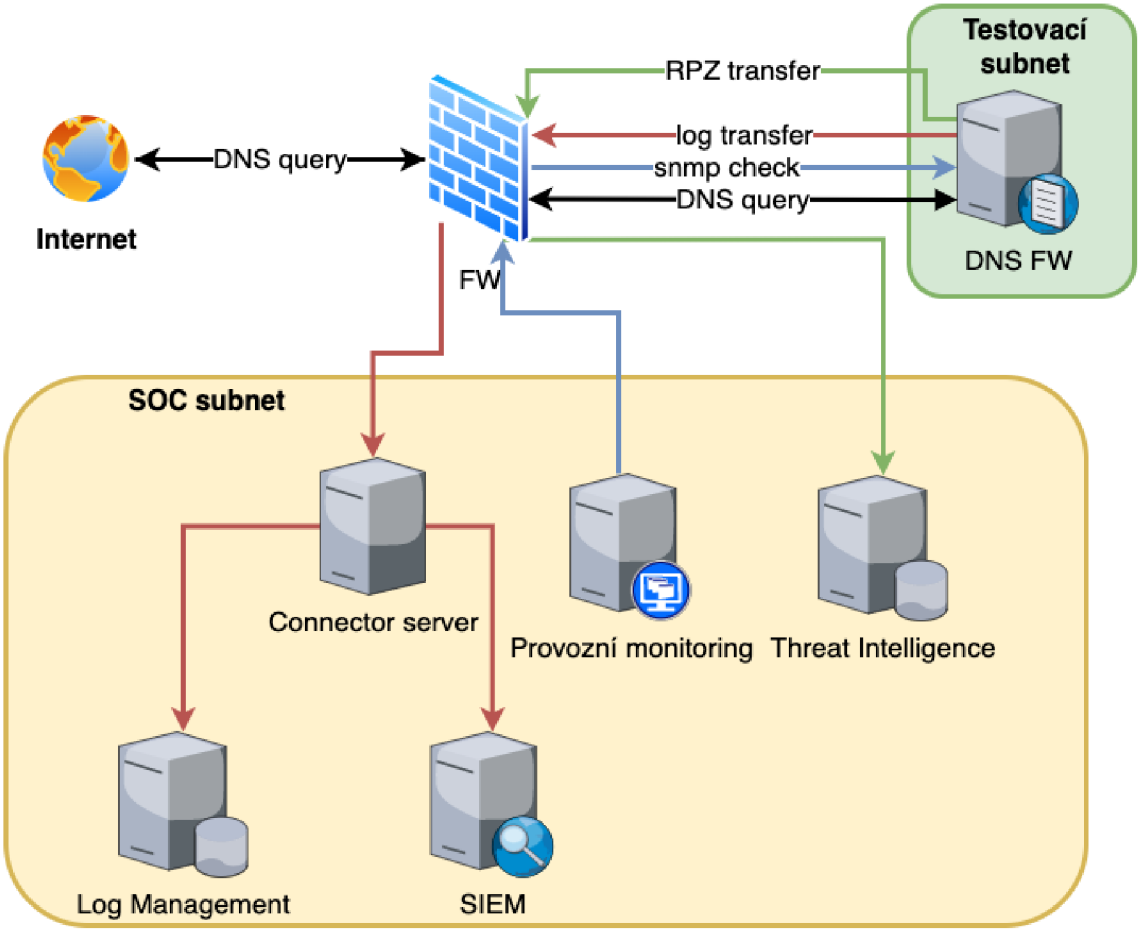
Tím je povoleno ovládání komponenty `named` pomocí utility `rndc` a to pouze z rozhraní DNS FW. Soubor `rndc.key` je vygenerován automaticky utilitou `rndc` při prvotním nastavení.

Pro zajištění větší bezpečnosti DNS FW je povoleno sdílení zónových souborů pouze definovaným IP adresám v acl listu `trusted-IP-transfer`. Dále jsou zakázány dynamické aktualizace zón příkazem `allow-update none;`. Následně je pomocí `allow-notify none;` zakázáno přijímat upozornění na změny v zónových souborech, jelikož tyto funkce jsou pro DNS FW zbytečné. Taktéž je vypnuta funkce `allow-update -forwarding none;`. Z bezpečnostního hlediska je zakázáno DNS firewallu sdílet informace o aktuálně nainstalované verzi BIND pomocí nastavení `version "Not available"`. Tím bylo zajištěno, že potenciálnímu útočníkovi DNS FW nesdělí aktuální nainstalovanou verzi BINDu. Příkazem `blackhole` jsou definovány IP adresy, kterým DNS FW nemá umožnit překlad DNS dotazů. Výše popsané nastavení je definováno přidáním následujících příkazů do konfiguračního souboru `named.conf`:

```
options {
    allow-transfer {trusted-IP-transfer ;};
    allow-update {none;};
    allow-notify { none; };
    allow-update-forwarding {none;};

    version "Not available";

    blackhole { blackhole-IP; };
    };

acl trusted-IP-transfer {
    none;
    };

acl blackhole-IP {
    none;
    };
```

4.3 Integrace DNS firewallu s ostatními technologiemi v kybernetickém operačním centru

Jelikož je DNS FW součástí SOCu, bylo nutné ho napojit i na ostatní technologie v SOCu. Na obrázku 4.1 je zobrazeno testovací prostředí, které je rozděleno na testovací subnet, ve kterém se nachází DNS FW a na SOC subnet, ve kterém se nachází ostatní technologie SOCu. Před samotnou integrací bylo nutné na firewallu nastavit prostupy k jednotlivým službám. DNS FW se doptává technologie Threat Intelligence na aktuální RPZ data, tudíž bylo nutné udělat prostup z DNS FW na Threat Intelligence technologii. Dále musí DNS FW přeposílat logy na Connector server, tudíž bylo nutné vytvořit prostup z DNS FW na Connector server. V poslední řadě se provozní monitoring doptává na aktuální stav DNS FW. Z toho plyne, že je nutné vytvořit prostup z provozního monitoringu na DNS FW. Následně bylo možné pokračovat s integrací DNS FW s ostatními technologiemi SOCu.



Obr. 4.1: Schéma rozvržení testovacího prostředí

4.3.1 Integrace DNS firewallu s technologií Log Management

Na začátek bylo nutné zajistit správné logování událostí DNS firewallu. Jelikož DNS FW je součástí kybernetického operačního centra, bylo nastaveno logování všech událostí vzniklých na DNS FW. K tomuto účelu byla navrhnuta následující konfigurace, která je aplikována v konfiguračním souboru `named.conf`:

```
logging {
        channel named           { file "log/named.log"
           versions 3 size 100M; severity dynamic;  print-time
           yes; print-severity yes; print-category yes; };
        channel security        { file "log/security.log"
           versions 3 size 100M; severity dynamic;  print-time
           yes; print-severity yes; print-category yes; };
        channel dnssec          { file "log/dnssec.log"
           versions 3 size 100M; severity dynamic;  print-time
           yes; print-severity yes; print-category yes; };
        channel resolver        { file "log/resolver.log"
           versions 3 size 100M; severity dynamic;  print-time
           yes; print-severity yes; print-category yes; };
        channel query_log       { file "log/query.log"
           versions 3 size 100M; severity dynamic;  print-time
           yes; print-severity yes; print-category yes; };
        channel query-errors    { file "log/query-errors.log"
           versions 3 size 100M; severity dynamic;  print-time
           yes; print-severity yes; print-category yes; };
        channel lame_servers    { file "log/lame-servers.log"
           versions 3 size 100M; severity dynamic;  print-time
           yes; print-severity yes; print-category yes; };
        channel capacity        { file "log/capacity.log"
           versions 3 size 100M; severity dynamic;  print-time
           yes; print-severity yes; print-category yes; };
        channel rpz             { file "log/rpz.log"
           versions 3 size 100M; severity dynamic;  print-time
           yes; print-severity yes; print-category yes; };
        channel other           { file "log/other.log"
           versions 3 size 100M; severity dynamic;  print-time
           yes; print-severity yes; print-category yes; };

        category default        { named; };
        category general        { named; };
        category security       { security; };
        category queries        { query_log; };
        category lame-servers   { lame_servers;};
        category dnssec         { dnssec; };
        category edns-disabled  { named; };
```

```
        category config          { named; };
        category resolver        { resolver; };
        category edns-disabled   { resolver; };
        category cname           { resolver; };
        category serve-stale     { resolver; };
        category spill           { capacity; };
        category rate-limit      { capacity; };
        category database        { capacity; };
        category client          { named; };
        category network         { named; };
        category dnstap          { other;};
        category unmatched       { named; };
        category client          { named; };
        category network         { named; };
        category dnstap          { other;};
        category unmatched       { named; };
        category client          { named; };
        category network         { named; };
        category delegation-only { named;};
        category dispatch        { named; };
        category trust-anchor-telemetry { named; };
        category rpz             { rpz;};
        category xfer-in         { other; };
        category xfer-out        { other; };
        category notify          { other; };
        category client          { other; };
        category query-errors    {query-errors; };
        category update          { other; };
        category update-security { other; };
        category zoneload        { other; };
};
```

Tímto nastavením v souboru `named.conf` bylo zajištěno, že komponenta `named` bude logovat veškeré informace do adresáře `log` do desíti souborů. Jelikož tyto logy jsou přeposílány na Connector server, bylo by dostačující všechny logy ukládat do jednoho souboru. Connector server Pro snazší orientaci byly různé kategorie logů rozděleny do různých souborů.

Proměnná `category` definuje, jaký typ logů komponenty `named` má být ukládán do kanálu popsaného ve složené závorce.

Proměnná `channel` popisuje, do jakého souboru má kanál ukládat logy a s jakými parametry. Pomocí následujících parametrů je definována maximální velikost souborů na 100 MB a server uloží maximálně tři tyto soubory. Dále jsou logy oboha-

ceny o závažnost, čas a typ logu. Toto nastavení je zajištěno následující konfigurací:

```
versions 3 size 100M; severity dynamic;  print-time yes; print-
   severity yes; print-category yes;
```

K zasílání logů na Connector server byl zvolen program **syslog-ng**. Jedná se o opensource implementaci protokolu syslog. Syslog je standardem pro protokolování logů. Konfigurace **syslog-ng** probíhá v souboru **syslog-ng.conf** umístěném v adresáři **/etc/syslog-ng/**. Instalace **syslog-ng** byla provedena příkazem **yum install syslog-ng**.

Po instalaci bylo nutné definovat zdroj logů, které mají být pomocí programu **syslog-ng** přeposílány na Connector server. To je provedeno přidáním následujícího nastavení do konfiguračního souboru **syslog-ng.conf**:

```
source s-file-named {
   wildcard-file(
        base-dir("/var/named/log") //Umístění logů DNS firewallu.
        filename-pattern("*.log") //Výběr všech souborů s končící
            .log.
        log_fetch_limit(20000) ); //Maximální počet načtených
           logů najednou.
};
```

Tímto byla definována proměnná **s-file-named**, která určuje zdroj logů. Hodnota **base-dir** určuje adresář, ze kterého má **syslog-ng** zpracovávat soubory s logy. Proměnnou **filename-pattern** je definováno, že soubory musí končit příponou .log.

Dále bylo nutné nastavit, kde má **syslog-ng** přeposílat logy. V testovacím prostředí se nachází Connector server **cstest1** s IP adresou 192.168.52.72. Následujícím nastavením je popsána cesta ke Connector serveru:

```
destination d-cstest1 {
        tcp("192.168.52.72" port(6999) // Definování IP adresy a
           portu Connector serveru.
        disk-buffer(disk-buf-size(2684354560) // Maximálně 2,5GB
           využití paměti na cílovém disku.
        mem-buf-size(512000) // Maximálně 500kB využití paměťové
           části vyrovnávací paměti místního disku.
        reliable(yes)) // Povolit spolehlivého ukládání do
           vyrovnávací paměti na disku.
```

```
        throttle(5000) // Povoleno zaslání maximálně 5000 logů za
            sekundu.
        );
};
```

V poslední řadě bylo nutné zadat programu `syslog-ng` informaci, že logy z umístění `s-file-named` má zasílat na destinaci `d-cstest1`. Toto nastavení bylo provedeno přidáním následující konfigurace do souboru `syslog-ng.conf`:

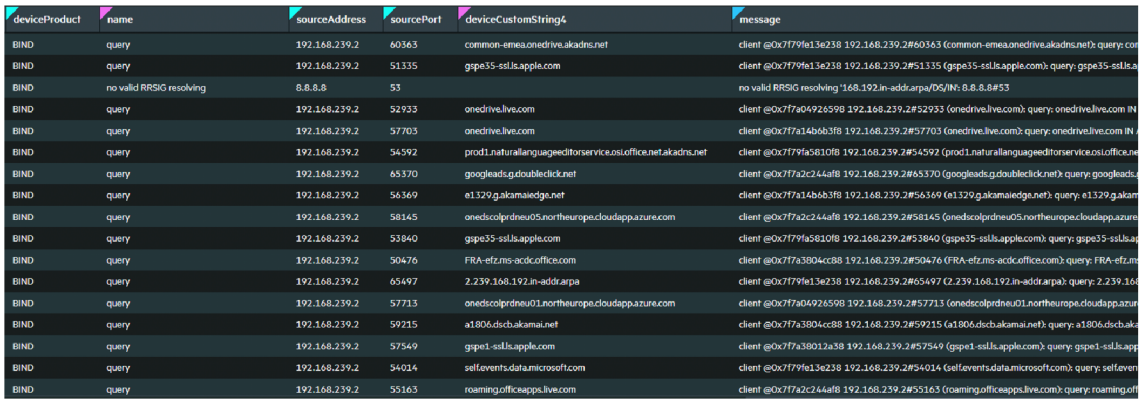
```
log { source(s-file-named); //Zdroj logů.
    destination(d-cstest1); //Definování cíle - Connector server.
};
```

Na Connector serveru dochází k normalizaci logů přijatých z DNS FW pomocí parserů. Po jejich normalizaci jsou logy dále přeneseny do systému Log managementu a SIEMu viz obrázek 4.1. Ve výpisu 4.1 je zobrazen log z DNS firewallu před normalizací. Jedná se o log, který informuje o zablokování překladu DNS dotazu pomocí technologie RPZ.

```
22-May-2022 22:56:43.208 rpz: info: client @0x7f3db4071158
192.168.239.2#62708 (airtravelabroad.com): rpz QNAME
NXDOMAIN rewrite airtravelabroad.com/A/IN via
airtravelabroad.com.mispexport.rpz
```

Výpis 4.1: Log vytvořený komponentou `named` informující o žádosti překladu domény z RPZ zóny

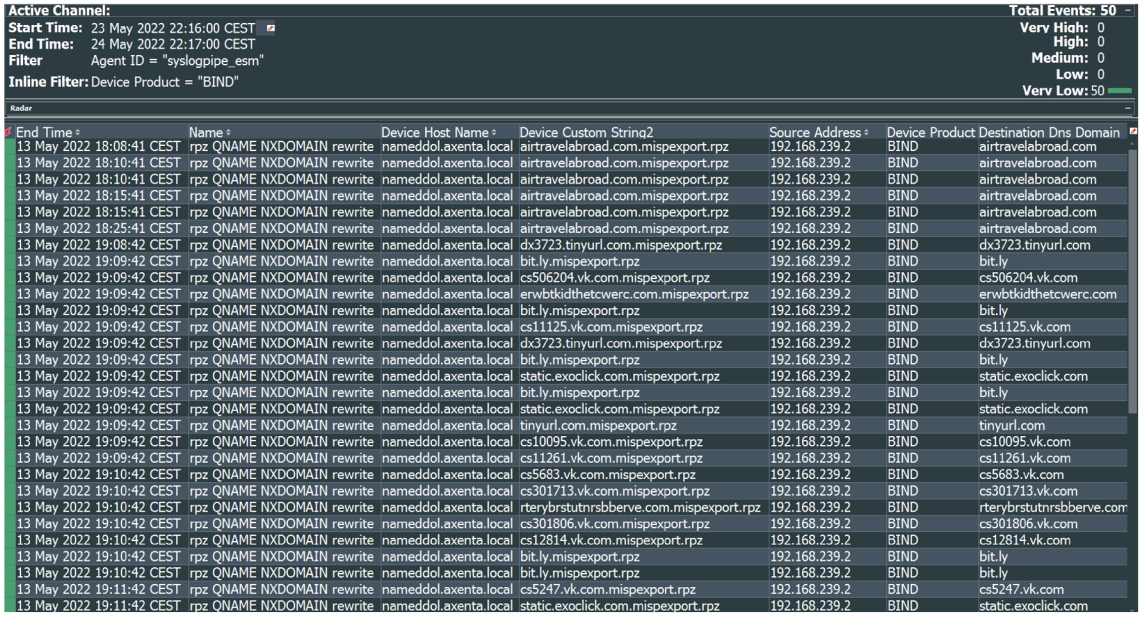
Pro Log Management se v testovacím prostředí SOCu využívá technologie ArcSight Logger. Jak již bylo řečeno v první kapitole, Log Management má na starost archivaci a správu logů. Po normalizaci logů vypadá jejich výpis v Loggeru viz obrázek 4.2.



deviceProduct	name	sourceAddress	sourcePort	deviceCustomString4	message
BIND	query	192.168.239.2	60363	common-emea.onedrive.akadns.net	client @0x7f79fe13e238 192.168.239.2#60363 (common-emea.onedrive.akadns.net): query: co
BIND	query	192.168.239.2	51335	gspe35-ssl.ls.apple.com	client @0x7f79fe13e238 192.168.239.2#51335 (gspe35-ssl.ls.apple.com): query: gspe35-ssl.ls.a
BIND	no valid RRSIG resolving	8.8.8.8	53		no valid RRSIG resolving '168.192.in-addr.arpa/DS/IN': 8.8.8.8#53
BIND	query	192.168.239.2	52933	onedrive.live.com	client @0x7f7a04926598 192.168.239.2#52933 (onedrive.live.com): query: onedrive.live.com IN
BIND	query	192.168.239.2	57703	onedrive.live.com	client @0x7f7a14b6b3f8 192.168.239.2#57703 (onedrive.live.com): query: onedrive.live.com IN
BIND	query	192.168.239.2	54592	prod1.naturallanguageeditorservice.osi.office.net.akadns.net	client @0x7f79fa5810f8 192.168.239.2#54592 (prod1.naturallanguageeditorservice.osi.office.ne
BIND	query	192.168.239.2	65370	googleads.g.doubleclick.net	client @0x7f7a2c244af8 192.168.239.2#65370 (googleads.g.doubleclick.net): query: googleads.g
BIND	query	192.168.239.2	56369	e1329.g.akamaiedge.net	client @0x7f7a14b6b3f8 192.168.239.2#56369 (e1329.g.akamaiedge.net): query: e1329.g.akam
BIND	query	192.168.239.2	58145	onedscolprdneu05.northeurope.cloudapp.azure.com	client @0x7f7a2c244af8 192.168.239.2#58145 (onedscolprdneu05.northeurope.cloudapp.azure
BIND	query	192.168.239.2	53840	gspe35-ssl.ls.apple.com	client @0x7f79fa5810f8 192.168.239.2#53840 (gspe35-ssl.ls.apple.com): query: gspe35-ssl.ls.ap
BIND	query	192.168.239.2	50476	FRA-efz.ms-acdc.office.com	client @0x7f7a3804cc88 192.168.239.2#50476 (FRA-efz.ms-acdc.office.com): query: FRA-efz.ms
BIND	query	192.168.239.2	65497	2.239.168.192.in-addr.arpa	client @0x7f79fe13e238 192.168.239.2#65497 (2.239.168.192.in-addr.arpa): query: 2.239.168
BIND	query	192.168.239.2	57713	onedscolprdneu01.northeurope.cloudapp.azure.com	client @0x7f7a04926598 192.168.239.2#57713 (onedscolprdneu01.northeurope.cloudapp.azur
BIND	query	192.168.239.2	59215	a1806.dscb.akamai.net	client @0x7f7a3804cc88 192.168.239.2#59215 (a1806.dscb.akamai.net): query: a1806.dscb.aka
BIND	query	192.168.239.2	57549	gspe1-ssl.ls.apple.com	client @0x7f7a38012a38 192.168.239.2#57549 (gspe1-ssl.ls.apple.com): query: gspe1-ssl.ls.app
BIND	query	192.168.239.2	54014	self.events.data.microsoft.com	client @0x7f79fe13e238 192.168.239.2#54014 (self.events.data.microsoft.com): query: self.even
BIND	query	192.168.239.2	55163	roaming.officeapps.live.com	client @0x7f7a2c244af8 192.168.239.2#55163 (roaming.officeapps.live.com): query: roaming.off

Obr. 4.2: Zobrazení logů po normalizaci v technologii ArcSight Logger

SIEM, celým názvem Security Information and Event Management, umožňuje z jednotlivých logů vytvořit bezpečnostní událost pomocí korelačních pravidel. Logy mohou pocházet z různých zdrojových zařízení a lze je v korelačních pravidlech kombinovat. Těmto událostem se pak může věnovat obsluha SOCu. V testovacím prostředí se jako SIEM využívá technologie ArcSight Enterprise Security Manager (ESM). Na obrázku 4.3 jsou zobrazeny logy v ESM z DNS firewallu, které informují o zablokování nebezpečného DNS dotazu pomocí technologie RPZ. Díky již proběhlé normalizaci logů pomocí parseru na Connector serveru jsou informace z původního logu rozděleny do jednotlivých sloupců.



Active Channel:
Start Time: 23 May 2022 22:16:00 CEST
End Time: 24 May 2022 22:17:00 CEST
Filter Agent ID = "syslogpipe_esm"
Inline Filter: Device Product = "BIND"

Total Events: 50
Very High: 0
High: 0
Medium: 0
Low: 0
Very Low: 50

Radar

End Time	Name	Device Host Name	Device Custom String2	Source Address	Device Product	Destination Dns Domain
13 May 2022 18:08:41 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	airtravelabroad.com.mispexport.rpz	192.168.239.2	BIND	airtravelabroad.com
13 May 2022 18:10:41 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	airtravelabroad.com.mispexport.rpz	192.168.239.2	BIND	airtravelabroad.com
13 May 2022 18:10:41 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	airtravelabroad.com.mispexport.rpz	192.168.239.2	BIND	airtravelabroad.com
13 May 2022 18:15:41 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	airtravelabroad.com.mispexport.rpz	192.168.239.2	BIND	airtravelabroad.com
13 May 2022 18:15:41 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	airtravelabroad.com.mispexport.rpz	192.168.239.2	BIND	airtravelabroad.com
13 May 2022 18:25:41 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	airtravelabroad.com.mispexport.rpz	192.168.239.2	BIND	airtravelabroad.com
13 May 2022 19:08:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	dx3723.tinyurl.com.mispexport.rpz	192.168.239.2	BIND	dx3723.tinyurl.com
13 May 2022 19:09:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	bit.ly.mispexport.rpz	192.168.239.2	BIND	bit.ly
13 May 2022 19:09:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	cs506204.vk.com.mispexport.rpz	192.168.239.2	BIND	cs506204.vk.com
13 May 2022 19:09:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	erwbtkidthetcwerc.com.mispexport.rpz	192.168.239.2	BIND	erwbtkidthetcwerc.com
13 May 2022 19:09:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	bit.ly.mispexport.rpz	192.168.239.2	BIND	bit.ly
13 May 2022 19:09:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	cs11125.vk.com.mispexport.rpz	192.168.239.2	BIND	cs11125.vk.com
13 May 2022 19:09:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	dx3723.tinyurl.com.mispexport.rpz	192.168.239.2	BIND	dx3723.tinyurl.com
13 May 2022 19:09:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	bit.ly.mispexport.rpz	192.168.239.2	BIND	bit.ly
13 May 2022 19:09:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	static.exoclick.com.mispexport.rpz	192.168.239.2	BIND	static.exoclick.com
13 May 2022 19:09:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	bit.ly.mispexport.rpz	192.168.239.2	BIND	bit.ly
13 May 2022 19:09:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	static.exoclick.com.mispexport.rpz	192.168.239.2	BIND	static.exoclick.com
13 May 2022 19:09:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	tinyurl.com.mispexport.rpz	192.168.239.2	BIND	tinyurl.com
13 May 2022 19:09:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	cs10095.vk.com.mispexport.rpz	192.168.239.2	BIND	cs10095.vk.com
13 May 2022 19:09:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	cs11261.vk.com.mispexport.rpz	192.168.239.2	BIND	cs11261.vk.com
13 May 2022 19:10:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	cs5683.vk.com.mispexport.rpz	192.168.239.2	BIND	cs5683.vk.com
13 May 2022 19:10:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	cs301713.vk.com.mispexport.rpz	192.168.239.2	BIND	cs301713.vk.com
13 May 2022 19:10:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	rterybrstutnrsbberve.com.mispexport.rpz	192.168.239.2	BIND	rterybrstutnrsbberve.com
13 May 2022 19:10:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	cs301806.vk.com.mispexport.rpz	192.168.239.2	BIND	cs301806.vk.com
13 May 2022 19:10:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	cs12814.vk.com.mispexport.rpz	192.168.239.2	BIND	cs12814.vk.com
13 May 2022 19:10:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	bit.ly.mispexport.rpz	192.168.239.2	BIND	bit.ly
13 May 2022 19:10:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	bit.ly.mispexport.rpz	192.168.239.2	BIND	bit.ly
13 May 2022 19:11:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	cs5247.vk.com.mispexport.rpz	192.168.239.2	BIND	cs5247.vk.com
13 May 2022 19:11:42 CEST	rpz QNAME NXDOMAIN rewrite	nameddol.axenta.local	static.exoclick.com.mispexport.rpz	192.168.239.2	BIND	static.exoclick.com

Obr. 4.3: Zobrazení logů o zablokování nebezpečného DNS dotazu pomocí technologie RPZ v technogii ArcSight Enterprise Security Manager

Jelikož je DNS FW nasazován v rámci kybernetického operačního centra, které své služby nabízí různým organizacím, je nutné zajistit funkci DNS FW i ve formě pouhého informování o skutečnosti, že stanice žádá o překlad nebezpečné domény. Někteří zákazníci SOCu nemusí chtít automaticky blokovat překlad nebezpečné domény, ale mohou chtít být pouze informováni o této skutečnosti. Proto bylo navrhnuto pravidlo v SIEMu, které vytvoří událost, pokud stanice zašle DNS dotaz na DNS firewall, který se nachází na seznamu nebezpečných domén. Dále bylo navrhnuto pravidlo, které vytvoří událost v SIEMu, pokud z více jak 10 stanic vzejde v jedné minutě požadavek na DNS firewall, ve kterém bude stejná nebezpečná doména.

4.3.2 Integrace DNS firewallu s technologií provozního monitoringu

V testovacím prostředí spravuje provozní monitoring služba Centreon. Jedná se o opensource software pro monitorování systémů a sítí. Pro napojení DNS FW na již existující Centreon bylo nutné doinstalovat následující balíčky `net-snmp net-snmp-utils net-snmp-devel` na DNS FW. Jedná se o sady aplikací, které umožňují implementovat SNMP protokol na Linux systémech a tato data posílat pomocí IP protokolu. Instalace byla provedena příkazem: `yum install net-snmp net-snmp-utils net-snmp-devel`.

Po instalaci bylo nutné vytvořit SNMP uživatele. To bylo provedeno následujícím příkazem, který definoval uživatelské jméno a heslo:

```
net-snmp-create-v3-user -ro -A [authpassword] -a SHA -X
[privpassword] -x AES [user] -u[user] --authpassword
[authpassword] --privpassword [privpassword] --snmp 3
--authprotocol sha --privprotocol AES
```

Po spuštění služby SNMP na DNS FW následovala integrace DNS FW do provozního monitoringu technologie Centreon. Tuto činnost provedl technik provozního monitoringu v SOCu. Bylo nutné vytvořit na firewallu prostup mezi Centreonem a DNS FW, aby Centreon mohl přistupovat na DNS FW a aktuální SNMP data mohl stahovat viz obrázek 4.1. Na obrázku 4.4 jsou zobrazeny kontroly DNS firewallu v provozním monitoringu Centreon.

Status	Resource	Parent	N	A	G	Duration	Tries	Last check	Information
OK	S Time: Uptime	DNS_FW_BIND				1d 3h	1/3 (H)	54m 14s	OK - Uptime (in day): 1
OK	S CPU: Usage	DNS_FW_BIND				1d 4h	1/3 (H)	14s	CPU utilization percentage : 1%
OK	S Traffic: eth0	DNS_FW_BIND				1d 4h	1/3 (H)	14s	OK - The Traffic In is 0.0Mbps, Out is 0.0Mbps, Total is 0.0
OK	S Traffic: ens192	DNS_FW_BIND				1d 4h	1/3 (H)	1m 6s	OK - The Traffic In is 0.0Mbps, Out is 0.0Mbps, Total is 0.0
OK	S [K1-T1] Process Status: SYSLOG-NG	DNS_FW_BIND				1d 4h	1/3 (H)	1m 14s	Number of current processes: 1
OK	S Ping	DNS_FW_BIND				1d 4h	1/3 (H)	1m 14s	OK - 192.168.53.12 rta 7.806ms lost 0%
OK	S Load	DNS_FW_BIND				1d 4h	1/3 (H)	1m 14s	Load average: 0.00, 0.01, 0.05.
OK	S Memory	DNS_FW_BIND				1d 4h	1/3 (H)	1m 14s	OK
UP	H DNS_FW_BIND					1d 4h	1/3 (H)	3m 6s	OK - 192.168.53.12 rta 1.438ms lost 0%
OK	S [K3-T0] CPU: Usage Detailed	DNS_FW_BIND				1d 4h	1/3 (H)	3m 14s	OK: CPU Usage: Wait 0.00 %, Guest 0.00 %, User 0.03 %
OK	S [K3-T3] TCP Connections	DNS_FW_BIND				1d 4h	1/3 (H)	3m 14s	OK: Total connections: 1
OK	S [K3-T3] Disk: I/O Operations	DNS_FW_BIND				1d 4h	1/3 (H)	3m 14s	OK: All devices [Read I/O : 0.00 B/s, Write I/O : 4.78 KB/s,
OK	S Time: LocalTime	DNS_FW_BIND				1d 4h	1/3 (H)	2m 14s	OK: Offset = 0s
OK	S Disk Usage: /	DNS_FW_BIND				1d 4h	1/3 (H)	3m 14s	Disk OK - / TOTAL: 19.990GB USED: 1.587GB (7%) FREE
OK	S Swap	DNS_FW_BIND				1d 4h	1/3 (H)	3m 14s	Disk OK - Swap space TOTAL: 4.000GB USED: 0.000GB (
OK	S Disk Usage: /var	DNS_FW_BIND				1d 4h	1/3 (H)	3m 14s	Disk OK - /var TOTAL: 9.990GB USED: 5.172GB (51%) FF
OK	S Disk Usage: /opt	DNS_FW_BIND				1d 4h	1/3 (H)	3m 14s	Disk OK - /opt TOTAL: 9.990GB USED: 0.031GB (0%) FRI
OK	S Top Processes: CPU	DNS_FW_BIND				1d 4h	1/3 (H)	14s	No Such Instance currently exists at this OID
OK	S Top Processes: RAM	DNS_FW_BIND				1d 4h	1/3 (H)	14s	No Such Instance currently exists at this OID

Obr. 4.4: Zobrazení kontrol DNS firewallu v provozním monitoringu Centreon

4.3.3 Integrace DNS firewallu s technologií Threat Intelligence

Součástí testovacího SOCu je i technologie Threat Intelligence. Jedná se o znalosti a informace týkající se kybernetické bezpečnosti. Pro sdílení a správu těchto znalostí v testovacím prostředí SOCu slouží platforma MISP. Jde o opensource projekt, který umožňuje shromažďovat a sdílet informace ohledně kybernetické bezpečnosti. Správce MISPu má možnost nastavit, jaké zdroje těchto dat si přeje stahovat z ostatních platforem. V rámci testovacího nasazení byla využita platforma MISP pro generování RPZ zón, které jsou potenciálně rizikové a DNS FW blokuje překlad doménových jmen z těchto zón. Pomocí skriptu `misp-export-all.sh`, který je spouštěn na DNS FW, se přes API platformy MISP generuje RPZ soubor se všemi zónami, které jsou potenciálně rizikové a tento soubor je stažen na DNS FW. Jelikož platforma MISP v testovacím prostředí slouží jako tzv. agregátor TI dat tím, že sbírá data z většiny dostupných zdrojů pro Threat Intelligence, je jediná využívaná pro generování RPZ souboru a není tedy potřeba využívat další TI zdroje. Obsah skriptu `misp-export-all.sh` je ve výpisu 4.2. Skript vytváří RPZ soubor s názvem `mispexport.rpz` do adresáře `/var/named/`.

```
sudo -u named curl -X POST -k -H 'Accept: application/json'
-H 'Authorization:'[KEY]'' -H 'Content-Type: application/
json' 'https:/[IP adresa MISPu]/attributes/restSearch'
--data '{"returnFormat": "rpz","type":"domain",
"requested_attributes" :["value"]}' -o
/var/named/mispexport.rpz
```

Výpis 4.2: Obsah skriptu `misp-export-all.sh`

Bylo nutné zajistit, aby měl DNS FW tento RPZ soubor vždy aktuální. K tomu byl využit software `cron`. Jedná se o program, který umožňuje automatizovat spouštění různých úloh a je součástí systému CentOS. Jeho konfigurace probíhá v souboru `crontab` umístěném v adresáři `/etc`. Přidáním následujícího nastavení do konfiguračního souboru bylo zajištěno, že skript `misp-export-all.sh` je spouštěn každou první minutu v hodině: `1 * * * * root /root/misp-export-all.sh > /dev/null`. Synchronizace RPZ souboru mispexport.rpz byla nastavena na každou hodinu. V testovacím prostředí dochází v MISPu k synchronizaci zdrojových dat aktuálně 2x denně. Pokud by k aktualizaci dat v MISPu docházelo častěji než 1x za hodinu, pak by bylo nutné upravit konfiguraci cronu. Ve výpisu 4.3 je zobrazen začátek souboru `mispexport.rpz`, který byl vygenerován MISPem.

```
$TTL 1w;
@               SOA localhost. root.localhost (2022052200 2
   h 30m 30d 1h)
                NS localhost.

; The following domain names and all of their sub-domains
   will timeout.
gulfc.haifa.ac.il CNAME rpz-drop.
*.gulfc.haifa.ac.il CNAME rpz-drop.
www.iabg.de CNAME rpz-drop.
*.www.iabg.de CNAME rpz-drop.
alkavkaz.com CNAME rpz-drop.
*.alkavkaz.com CNAME rpz-drop.
cihaderi.net CNAME rpz-drop.
*.cihaderi.net CNAME rpz-drop.
airtravelabroad.com CNAME rpz-drop.
```

```
*.airtravelabroad.com CNAME rpz-drop.
beijingnewsblog.net CNAME rpz-drop.
*.beijingnewsblog.net CNAME rpz-drop.
deervalleyassociation.com CNAME rpz-drop.
*.deervalleyassociation.com CNAME rpz-drop.
greencastleadvantage.com CNAME rpz-drop.
*.greencastleadvantage.com CNAME rpz-drop.
```

Výpis 4.3: Začátek vygenerovaného souboru `mispexport.rpz`

Dále bylo zajištěno, aby DNS FW blokoval překlady doménových jmen obsažených v souboru RPZ `mispexport.rpz` uloženým v adresáři `/var/named/`. V konfiguraci komponenty `named` byla vytvořena zóna `mispexport.rpz` přidáním následujícího nastavení do konfiguračního souboru `named.conf`:

```
zone "mispexport.rpz" {
  type master;
  file "mispexport.rpz";
};
```

Tím bylo definováno, že zóna `mispexport.rpz` je popsána v souboru `mispexport.rpz`. Dále bylo nutné definovat RPZ politiku přiřazenou této zóně. V testovacím nasazení bylo nastaveno, že DNS dotaz ze zóny `mispexport.rpz` nemá být korektně vyhodnocován a při odpovědi DNS FW je zasílána zpráva s kódem `NXDOMAIN`:

```
options {
    response-policy {
        zone "mispexport.rpz" policy nxdomain;
  } qname-wait-recurse no break-dnssec yes;
};
```

Pokud by bylo potřeba zajistit konfiguraci, která umožňuje pouze informování o přístupu na potenciálně nebezpečnou doménu, ale ne tento překlad blokovat, pak by muselo být nastavení politiky RPZ zóny z `NXDOMAIN` změněno na `PASSTHRU`. To by znamenalo, že DNS FW by tento DNS dotaz pouze logoval, ale neblokoval. Toto nastavení lze personalizovat pro jednotlivé zákazníky SOCu.

Jelikož se soubor `mispexport.rpz` každou hodinu aktualizuje, bylo nutné zajistit opakované načtení jeho obsahu i do programu `named`. To bylo zajištěno následujícím skriptem `named-reload.sh`:

```
sudo -u named rndc reload
```

Následně bylo nutné zajistit, aby tento skript byl spouštěn každou desátou minutu v hodině. Toto je zajištěno přidáním následujícího nastavení do souboru `crontab`: `10 * * * * root /root/named-reload.sh > /dev/null`.

4.4 Landing page

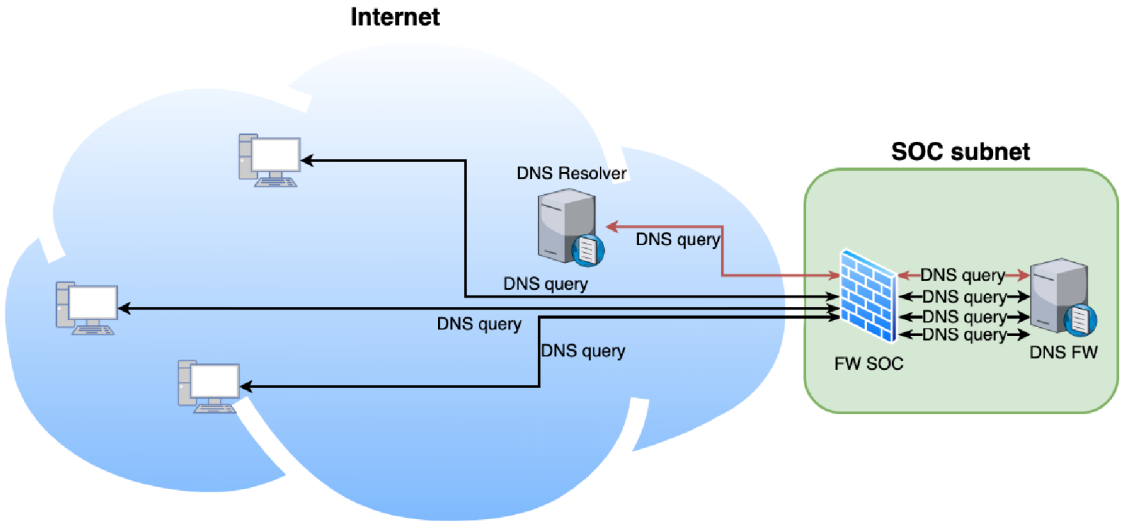
Landing page je webová stránka, na kterou je přesměrován klient v případě žádosti o překlad nebezpečného DNS dotazu, jenž byl zablokován DNS firewallem. Klientovi je tato webová stránka zobrazena a může na ní být kontakt na osobu, kterou má informovat, pokud chce nebezpečnou doménu zpřístupnit. Tato webová stránka by se měla nacházet na jiném serveru než je DNS FW a měla by být dostupná z Internetu. V případě využití landing page je nutné změnit politiku RPZ zóny z `NXDOMAIN` na politiku `CNAME` a tím definovat, kam se mají dotazy přesměrovávat. Landing page může být individualizována pro jednotlivé klienty SOCu.

5 Možnosti napojení stanic a vzdálených místních sítí na DNS firewall a vynucení jeho využívání

Tato kapitola popisuje možnosti napojení koncových zařízení a vzdálených místních sítí na DNS firewall umístěném v SOCu. Následně je popsána možnost jeho vynucení v místní síti a na koncových stanicích.

5.1 Napojení koncových stanic na DNS firewall v rámci sítě Internet

Existují dva základní způsoby, kterými lze DNS firewall zpřístupnit stanicím v rámci sítě Internet. První variantou je jeho veřejné zpřístupnění z Internetu. V tomto případě nastává jeden zásadní problém a to ten, že na server se může připojit jakákoliv stanice nacházející se na síti Internet. Tato varianta je náchylná na hardwarové zdroje a potenciální útoky na DNS FW. Druhou variantou je omezení přístupu na DNS FW z Internetu jiným, než předem vydefinovaným IP adresám. Tím je omezen přístup na DNS FW nechtěným stanicím v síti Internet. Tato varianta ovšem není možná, jelikož není možné předem určit, jakou IP adresu bude mít koncová stanice připojená k síti Internet. Na obrázku 5.1 je vyobrazeno vyhodnocení DNS dotazu stanic připojených na DNS FW v rámci sítě Internet.

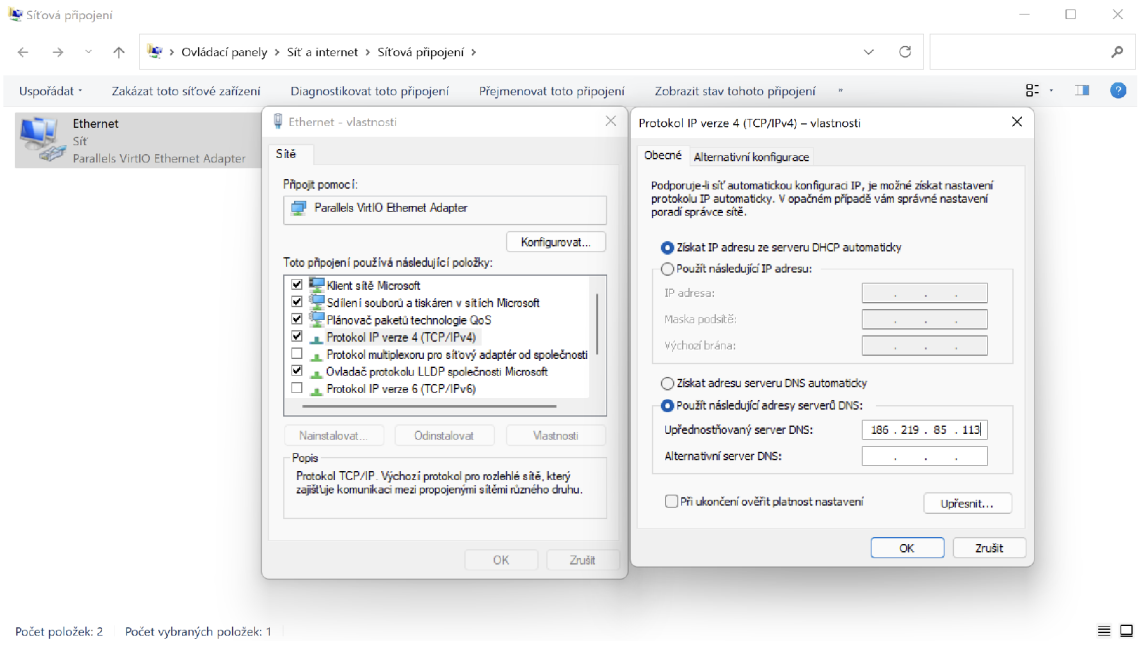


Obr. 5.1: Napojení koncových stanic na DNS firewall v rámci sítě Internet

Aby byl DNS firewall dostupný z Internetu, bylo nutné přesměrovat na firewallu port 53 protokolu TCP a UDP na DNS FW. V tomto případě, kdy byl DNS FW dostupný veřejně z Internetu, bylo možné koncovou stanici nakonfigurovat tak, aby využívala tento DNS FW jako DNS Resolver bez ohledu na její aktuální umístění v rámci Internetu.

5.1.1 Napojení koncových stanic se systémem Windows na DNS firewall dostupný z Internetu

Problematika napojení stanic s operačním systémem typu Windows tkví v tom, že operační systém si DNS Resolver nastavuje při každém připojení k síti pomocí DHCP protokolu, pokud není nastaveno jinak. Pomocí nastavení síťového adaptéru lze na stanici zvolit DNS Resolver, který bude využíván pro daný síťový adaptér bez ohledu na to, k jaké síti je připojen a jaká data dostane od DHCP serveru. Této konfigurace bylo docíleno nastavením síťového adaptéru podle obrázku 5.2.



Obr. 5.2: Nastavení DNS Resolveru pro síťový profil ve Windows 11

Dříve bylo možné nastavit DNS Resolver v operačních systémech Windows XP fixně, nehledě na aktuální síť a síťový adaptér pomocí GPO politiky. Bohužel se tato politika nedá využít v aktuálních verzích operačních systémů typu Windows.

Může nastat situace, kdy nebude DNS FW z dané místní sítě v rámci Internetu dostupný. V tom případě nebude stanice schopna vyhodnotit daný DNS dotaz. Tento problém lze řešit pouze změnou konfigurace síťového adaptéru. DNS Resolver na stanici je možné změnit pouze s administrátorskými právy. Během testovacího období nebyly zaznamenány žádné potíže a DNS dotazy byly zasílány pouze na DNS firewall.

5.1.2 Napojení koncových stanic se systémem Linux na DNS firewall dostupný z Internetu

Pro stanice s operačním systémem typu Linux bylo možné za pomocí utility `resolvconf` zajistit, aby stanice i po přepojení do jiné sítě zachovala definované nastavení DNS Resolveru. Při testování se potvrdila funkčnost této utility. V případě, kdy uživatel stanice má administrátorská práva, může DNS Resolver manuálně změnit. Utilitu bylo nutné doinstalovat. Pro systém Ubuntu probíhala instalace pomocí příkazu `apt install resolvconf`. Následně musela být v konfiguračním souboru `head` umístěném v adresáři `/etc/resolvconf/resolv.conf.d/` nastavena IP adresa DNS Resolveru:

```
nameserver [IP adresa DNS FW]
```

V poslední řadě bylo nutné nastavit spouštění utility `resolvconf` automaticky po startu operačního systému pomocí:

```
systemctl enable resolvconf.service
```

Opět může nastat situace, kdy DNS FW nebude z dané místní sítě dostupný a v tomto případě stanice není schopna vyhodnotit DNS dotaz. Problém je možné řešit navrženým postupem v podkapitole 5.1.1. Během testovacího období nebyly zaznamenány žádné potíže a DNS dotazy byly zasílány pouze na DNS firewall.

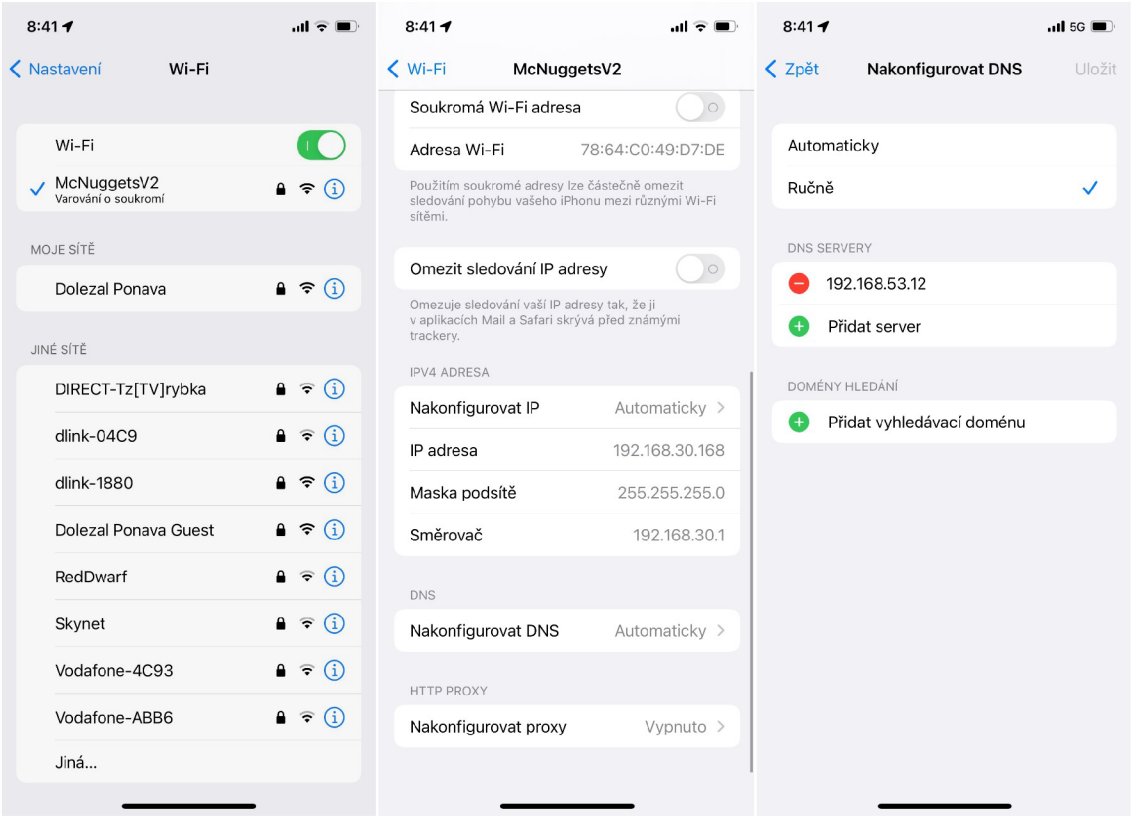
5.1.3 Napojení mobilních operačních systémů na DNS firewall dostupný z Internetu

Pro mobilní operační systémy iOS 15 a Android 12 se nepodařilo najít jednoduché řešení, které by zachovalo nastavení DNS FW i při změně sítě. Vždy jde nastavit DNS Resolver ke konkrétnímu síťovému připojení.

V případě systému iOS nebylo možné nijak zajistit využívání pouze DNS FW i při změnách síťového připojení. Na operačním systému Android existují aplikace,

které slibují, že zajistí využívání DNS Resolveru i při změnách připojení k síti. Bohužel v rámci jejich testování se tato funkce nepotvrdila.

Jediné schůdné řešení je manuální nastavení DNS Resolveru uživatelem vždy, když se připojí k nové síti, nebo ve chvíli, kdy chce být chráněn DNS firewallem. Tento postup je zobrazen na obrázku 5.3.



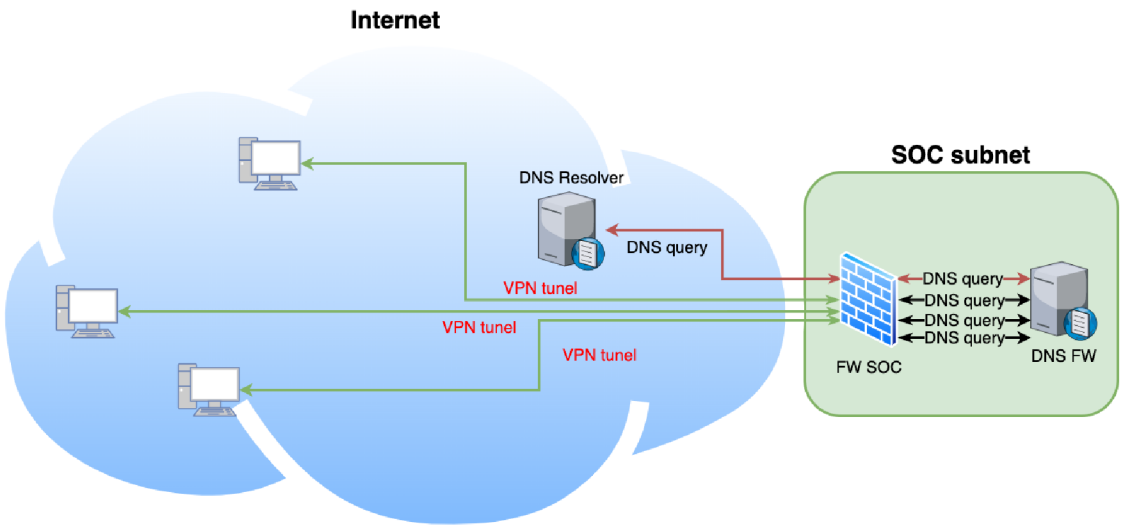
Obr. 5.3: Konfigurace DNS Resolveru na iOS 15

5.2 Napojení koncových stanic na DNS firewallu pomocí VPN

V předešlé podkapitole bylo zmíněno, že veřejně dostupný DNS FW z Internetu je náchylný na potenciální útoky a z toho důvodu bylo navrženo řešení připojení stanic k DNS FW pomocí VPN.

Díky technologii VPN se vytvoří tunel mezi stanicí, umístěné kdekoliv v rámci sítě Internet, a DNS firewallem viz obrázek 5.4. Toto spojení je umožněno pouze autentizovaným zařízením. DNS over VPN využívá tento VPN tunel, přes který je

možné zasílat DNS komunikaci. Stačí pouze na jednotlivých stanicích nastavit VPN klienta a jako DNS Resolver nastavit IP adresu DNS firewallu. Tím je zajištěno, že všechny DNS dotazy na překlad doménových jmen z konfigurovaných zařízení probíhají přes DNS firewall i při změnách připojení.



Obr. 5.4: Napojení koncových stanic na DNS FW pomocí VPN

Může nastat situace, kdy není možné využít technologii VPN z dané místní sítě v rámci Internetu. V tomto případě nelze využít funkci DNS over VPN a pak ani funkci DNS firewallu, jelikož stanice není schopna ustanovit VPN tunel a vyhodnotit daný DNS dotaz přes DNS firewall. DNS dotazy v tomto případě zasílá na DNS Resolver nastavený systémem nebo DHCP protokolem.

Výhodou DNS over VPN je, že pokud chce být uživatel stanice chráněn DNS firewallem, stačí, když ustanoví VPN tunel a tím se automaticky připojí i na DNS FW. Ustanovení VPN tunelu je pro uživatele stanice intuitivní a jednoduché.

5.2.1 Nastavení VPN klientů a připojení na DNS firewall

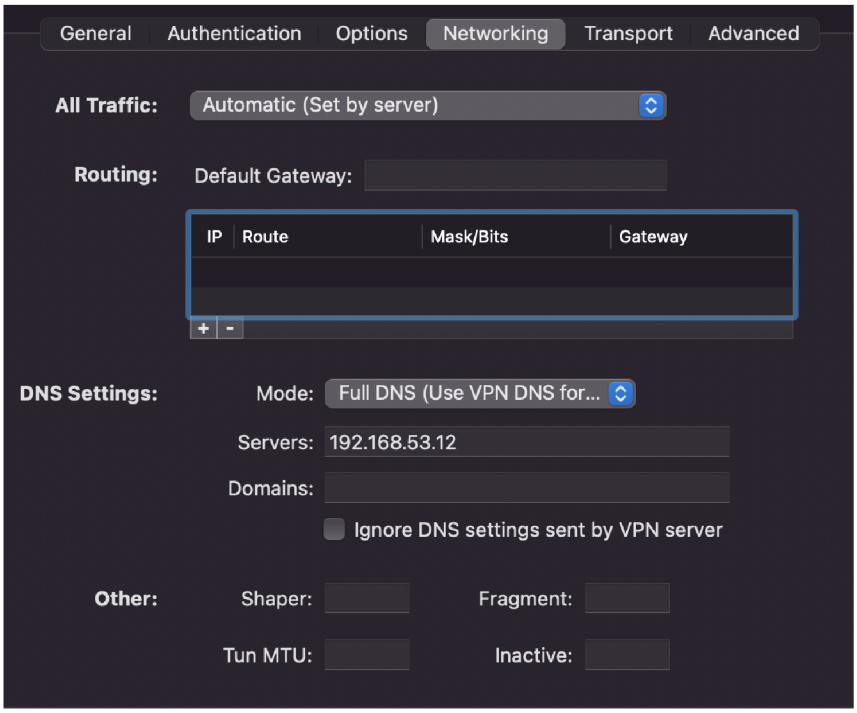
V této části je popsáno, jak nastavit VPN klienta na stanici a vynutit využívání DNS firewallu přes VPN tunel. Nastavení OpenVPN klienta probíhá na všech platformách velmi podobně. Administrátor sítě dodá konfigurační soubor s podpisovým certifikátem, který zabezpečí šifrování dat. Pro VPN klienta může být využit software OpenVPN[21] nebo Viscosity[22]. Jedná se o programy pro vytvoření VPN tunelu.

Do VPN konfiguračního souboru bylo nutné přidat vynucení DNS firewallu přes daný VPN tunel. To bylo zabezpečeno přidáním následujícího kódu do VPN konfigurace: `push "dhcp-option DNS 192.168.53.12"`, kde IP adresa 192.168.53.12 je privátní adresa DNS firewallu. Tato privátní adresa je směrována přes Internet vytvořeným VPN tunelem. Příkaz `push "dhcp-option DNS"` donutí stanici posílat DNS dotazy pouze na DNS firewall dostupný přes VPN tunel. Na obrázku 5.4 je vyobrazeno napojení stanice pomocí VPN tunelu na DNS firewall.

5.2.2 Testování DNS over VPN

Testování VPN klientů bylo provedeno na operačních systémech Windows 10, macOS 12, Linux CentOS 7, Android 12 a iOS 15.

Systémy Windows 10 a macOS 12 využívaly program Viscosity a připojovaly se ze třech různých sítí přes ethernetové a WiFi rozhraní. Pomocí programu Wireshark[23] byly monitorovány DNS odchozí dotazy. Ve všech pokusech směřovaly DNS dotazy na DNS firewall. Nenastal případ, kdy by systémy využily jiný DNS Resolver než testovací DNS firewall. Během testovacího období nebyly zaznamenány žádné potíže. Na obrázku 5.5 je vyobrazen postup nastavení DNS over VPN.



Obr. 5.5: Nastavení DNS over VPN v programu Viscosity

Na operační systém Linux CentOS 7 byl nainstalován program OpenVPN 3 Client for Linux. V rámci testování probíhalo připojování ze třech různých sítí přes ethernetové a WiFi rozhraní. Opět byly pomocí programu Wireshark monitorovány DNS odchozí dotazy. Ve všech pokusech směřovaly DNS dotazy na DNS firewall. Nenastal případ, kdy by systém využil jiný DNS Resolver než testovací DNS firewall. Během testovacího období nebyly zaznamenány žádné potíže. Ve výpisu 5.1 je zobrazen konfigurační soubor OpenVPN, ve kterém se nachází i nastavení konfigurace DNS over VPN.

```
dev tun
persist-tun
persist-key
data-ciphers AES-256-GCM:AES-128-GCM:AES-256-CBC
data-ciphers-fallback AES-256-CBC
auth SHA256
tls-client
client
resolv-retry infinite
remote [IP adresa] [port] udp4
verify-x509-name "pfsense.axenta.local" name
auth-user-pass
push "dhcp-option DNS 192.168.53.12"
pkcs12 pfsense1-UDP4-mdolezal.p12
tls-auth pfsense1-UDP4-mdolezal-tls.key 1
remote-cert-tls server
explicit-exit-notify
```

Výpis 5.1: Obsah konfiguračního souboru OpenVPN

Na mobilním systému iOS 15 byla využita aplikace OpenVPN Connect. Bohužel během testování docházelo při změnách připojení k Internetu k překladu doménových jmen i přes jiný DNS Resolver než DNS firewall. Problém spočíval v tom, že při změnách připojení k WiFi sítím nebo k mobilní síti často vypadnul VPN tunel a sám se již neustanovil. Toto chování bylo pozorováno i při testování aplikace na operačním systému Android 12.

Testování na platformách iOS 15, Android 12, Windows 10 a CentOS 7 probíhalo v rámci jednoho měsíce. Testování DNS over VPN na platformě macOS probíhalo půl roku a funkčnost a stabilita DNS over VPN byla potvrzena a může být doporučena k využití.

Funkce DNS over VPN tedy fungovala podle očekávání na operačních systémech typu Windows, macOS a Linux. Lze nastavit, aby VPN tunel byl ustanovován automaticky po připojení stanice k síti Internet. Zároveň je možné využívat jiný DNS Resolver v případě nemožnosti ustanovení VPN tunelu. U mobilních operačních systémů nelze využívat funkci DNS over VPN automaticky bez zásahu uživatele. V případě, kdy chce být uživatel mobilního telefonu chráněn DNS firewallem, je možné ustanovit VPN tunel manuálně.

5.3 Napojení vzdálených místních sítí na DNS firewall

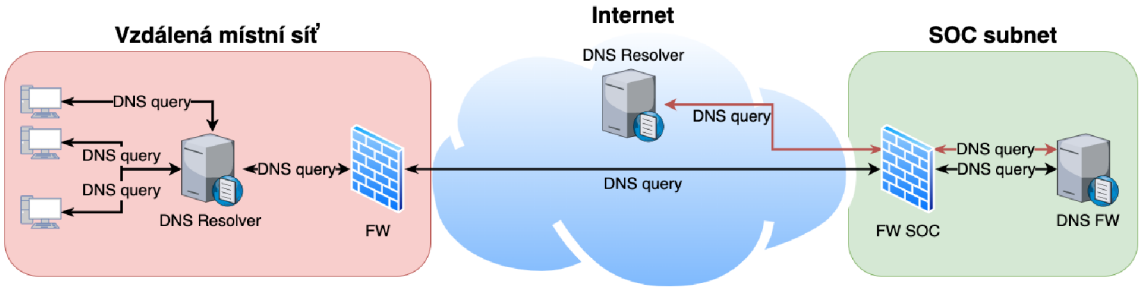
Napojení vzdálených místních sítí na DNS firewall SOCu jako služby by nemělo být obtížné. Připojení vzdálené místní sítě, ve které se nachází DNS Resolver, který je vynucen, probíhá následovně: DNS Resolver vzdálené místní sítě se nastaví tak, aby přeposílal DNS dotazy, pro které není autoritativní, na DNS firewall nacházející se v SOCu. Druhá možnost připojení vzdálené místní sítě na DNS firewall je pomocí funkce RPZ slave.

5.3.1 Napojení vzdálené místní sítě na DNS firewall bez VPN - Omezení přístupu pro konkrétní IP adresy

Na obrázku 5.6 je zobrazeno připojení DNS Resolveru vzdálené místní sítě na DNS firewall nacházející se v SOCu otevřeně přes Internet.

Na zajištění možnosti napojení DNS Resolveru vzdálené místní sítě na DNS firewall a zároveň, aby DNS firewall nebyl otevřen pro celý Internet, byl povolen přístup na DNS firewall pouze z veřejné IP adresy vzdálené místní sítě. Tím bylo zajištěno, že na DNS firewall prostoupily pakety pouze z veřejné IP adresy vzdálené místní sítě. Samozřejmě se zdrojová adresa dá podvrhnout a tak obejít tuto ochranu. V této variantě napojení DNS Resolveru vzdálené místní sítě na DNS firewall nejsou DNS dotazy šifrovány.

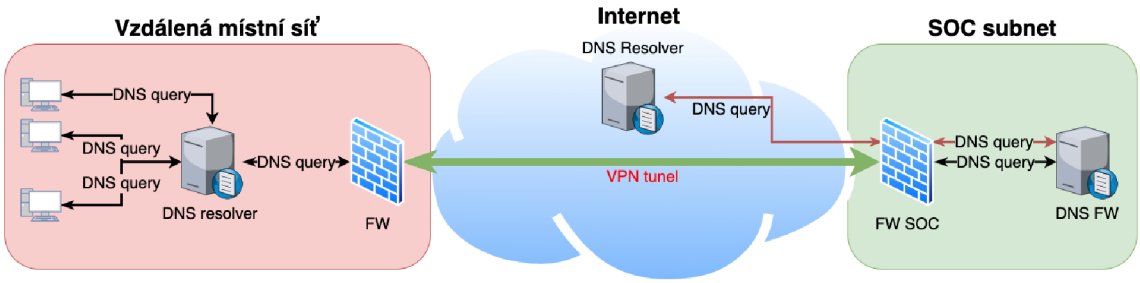
Nejprve bylo nutné vytvořit na SOC firewallu prostup na portu 53 pro protokol TCP a UDP z veřejné IP adresy vzdálené místní sítě. Dále je nutné upravit konfiguraci DNS FW a to přidáním veřejné IP adresy vzdálené místní sítě na seznam IP adres `trusted-IP-queries`, který definuje IP, kterým má DNS FW vyhodnocovat dotazy. Následně se DNS Resolver vzdálené místní sítě nastavil tak, aby DNS dotazy, pro které není autoritativní, zasílal na DNS FW. Vyhodnocení DNS dotazu pak probíhá podle obrázku 3.1. Během testovacího období nebyly zaznamenány žádné potíže a DNS dotazy byly zasílány pouze na DNS firewall.



Obr. 5.6: Připojení DNS Resolveru vzdálené místní sítě k DNS firewallu bez VPN

5.3.2 Napojení vzdálené místní sítě na DNS firewall pomocí VPN

Bezpečnější variantou, jak napojit vzdálenou místní síť na DNS firewall, je pomocí VPN tunelu. DNS firewall nemusí být dostupný otevřeně z Internetu, tudíž bude méně náchylný na potenciální útoky a DNS dotazy vzdálené místní sítě jsou při využití například IPsec technologie přenášeny šifrovaně. Na obrázku 5.7 je zobrazeno navrhované řešení napojení DNS Resolveru vzdálené místní sítě na DNS firewall SOCu pomocí VPN tunelu. Navrhované řešení spočívá v konfiguraci a sestavení VPN IPsec tunelu mezi firewallem SOCu a firewallem vzdálené místní sítě. Následně se na DNS Resolveru vzdálené místní sítě nastaví, aby DNS dotazy, pro které není autoritativní, přeposílal na DNS FW dostupný přes IPsec tunel. Opět bylo nutné upravit konfiguraci DNS FW a to přidáním IP adresy využívané vzdálené místní sítě na seznam IP adres `trusted-IP-queries`. Vyhodnocení DNS dotazu pak probíhá podle obrázku 3.1. Během testovacího období nebyly zaznamenány žádné potíže a DNS dotazy byly zasílány pouze na DNS firewall.

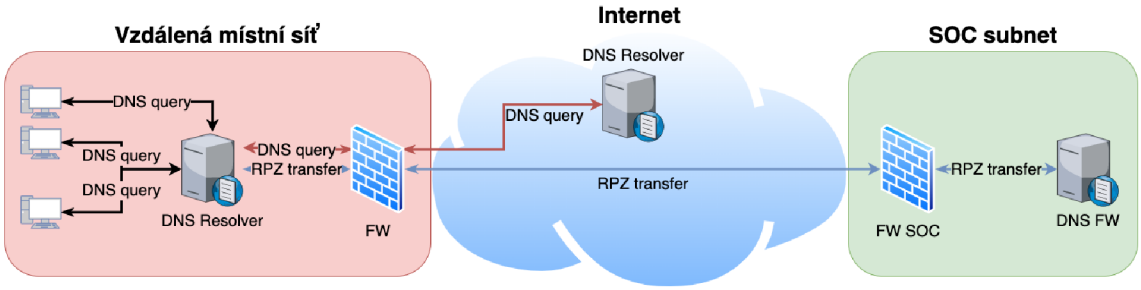


Obr. 5.7: Připojení DNS Resolveru vzdálené místní sítě k DNS firewallu pomocí VPN

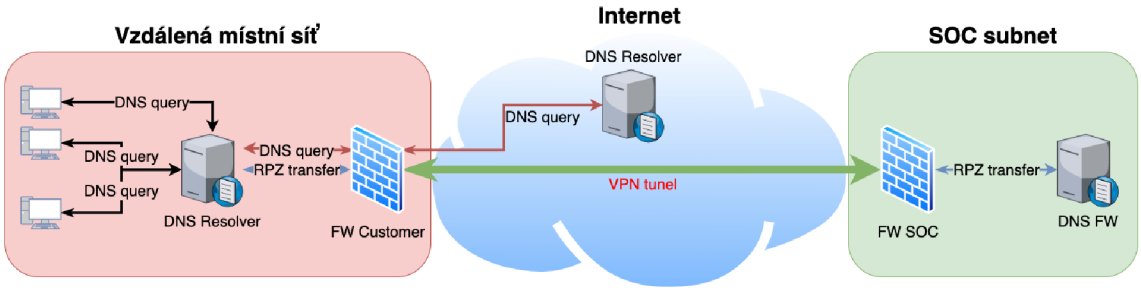
5.3.3 Napojení místní sítě na DNS firewall pomocí funkce slave RPZ

Další možností, jak napojit vzdálenou místní síť na DNS firewall umístěný v SOCu, je pomocí funkce slave RPZ. Tato funkce umožňuje sdílet RPZ soubory s DNS Resolvery. Využití funkce slave RPZ je možné bez ustanovování VPN tunelu mezi vzdálenou místní sítí a sítí, ve které se nachází DNS firewall, jak je zobrazeno na obrázku 5.8. V tomto případě jsou RPZ soubory přeposílány přes síť Internet nešifrovaně a DNS firewall musí být opět dostupný v rámci sítě Internet. Lze využít povolení přístupu na DNS firewall pouze z veřejné IP adresy vzdálené místní sítě. Zároveň je možné využít slave RPZ ve spojení s VPN tunelem. Tato varianta, například při využití technologie IPsec, umožňuje RPZ soubory přeposílat přes síť Internet šifrovaně a DNS firewall nemusí být přístupný veřejně z Internetu, jak je zobrazeno na obrázku 5.9. V obou těchto variantách je nutné nastavit DNS Resolver vzdálené místní sítě, aby stahoval RPZ soubory z DNS firewallu nacházejícího se v SOCu. Dále je zapotřebí nastavit DNS Resolveru místní sítě patřičnou RPZ politiku k RPZ souboru staženému z DNS firewallu.

Výhodou využití technologie slave RPZ je, že správce vzdálené místní sítě má možnost ovlivňovat RPZ politiku k danému RPZ souboru. Nevýhodou je menší vhled SOCu do dění ve vzdálené místní síti.



Obr. 5.8: Napojení DNS Resolveru vzdálené místní sítě pomocí funkce slave RPZ bez VPN



Obr. 5.9: Napojení DNS Resolveru vzdálené místní sítě pomocí funkce slave RPZ přes VPN

5.4 Vynucení využívání DNS firewallu koncovými stanicemi

Vynucení využívání DNS firewallu jako jediného DNS Resolveru pro koncovou stanici je možné zajistit pomocí technologie EDR. Testovací stanice využívá k technologii EDR řešení od firmy ESET. Konkrétně jde o produkt ESET Protect. ESET Protect dokáže na spravovaných stanicích pomocí funkce politik nastavit firewall pracovní stanice. Při testování se funkčnost politiky nastavení firewallu pracovní stanice potvrdila a je doporučena k využití.

Na firewallu pracovní stanice musí být povolena odchozí TCP a UDP komunikace pro port 53 na IP adresu DNS firewallu. Dále by měla být zakázána odchozí TCP

a UDP komunikace pro port 53 na všechny adresy. V případě implementace nastavení firewallu na pracovní stanici v pořadí navrženém výše bude zajištěna možnost zasílání DNS dotazu na portu 53 pouze na IP adresu DNS firewallu. Komunikace na ostatní IP adresy na portu 53 bude blokována firewallem pracovní stanice. Jak již bylo zmíněno v druhé kapitole, DNS komunikace probíhá primárně na portu 53. Tím je zajištěno, že bude možné pro zasílání standardních DNS dotazů možné využít pouze DNS firewall. V případě, kdy jsou DNS dotazy zasílány přes jiný port, nebude DNS firewall vynucen technologií EDR.

Dále musí být zabráněno využívání funkce DNS over HTTPS a DNS over TLS. Tyto funkce lze omezit pomocí nastavení firewallu na koncové stanici. Na firewallu koncové stanice je nutné zakázat odchozí komunikaci na portu 853 na všechny IP adresy. Tím bude zajištěna nemožnost využití služby DNS over TLS na standardním portu 853. Dále je na firewallu koncové stanice nutné zakázat odchozí komunikaci na portu 443 pro IP adresy nejběžnějších DNS Resolverů umožňující využívat funkci DNS over HTTPS.

V případě nastavení výše popsané konfigurace je zajištěné omezení využívání služby DNS over TLS na standardním portu 853 a omezení využívání DNS over HTTPS na standardním portu 443 pro rozsah DNS Resolverů definovaných na firewallu koncové stanice. Tyto služby ale nejsou zakázány pro ostatní porty.

5.5 Vynucení využívání DNS firewallu v rámci vzdálených místních sítí

Pro vynucení využívání DNS firewallu jako jediného DNS Resolveru pro vzdálenou místní síť musel být nastaven hraniční firewall vzdálené místní sítě podle níže popsaného návrhu.

Za prvé musela být omezena možnost využívání funkce DNS over TLS. Jelikož DNS over TLS standardně využívá port 853, bylo možné tuto funkci omezit přidáním pravidla na hraniční firewall vzdálené místní sítě, které zakázalo odchozí komunikaci na port 853 na všechny IP adresy.

Za druhé musela být omezena možnost využívání funkce DNS over HTTPS. DoH standardně využívá port 443. Tento port je využíván i jinými službami a proto ho není možné zablokovat stejně jako v předešlém kroku. Bylo nutné vytvořit seznam

veřejných DNS Resolverů, které umožňují využívat funkci DNS over HTTPS. Na hraničním firewallu vzdálené místní sítě musela být zablokována odchozí komunikace na IP adresy těchto veřejných DNS Resolverů na portu 443.

Implementací výše popsaného řešení byla omezena možnost využívání DNS over TLS a DNS over HTTPS ve vzdálené místní síti na standardních portech.

V posledním kroku vynucení využívání DNS firewallu v rámci vzdálené místní sítě muselo být na hraničním firewallu vzdálené místní sítě vytvořeno pravidlo, které povolilo odchozí TCP a UDP komunikaci pro port 53 na IP adresu DNS firewallu. Dále bylo nutné zakázat ostatní odchozí TCP a UDP komunikaci na portu 53. Tím byla zajištěna možnost překladu DNS dotazů na standardním portu 53 pouze DNS firewallem.

5.6 Shrnutí možných napojení koncových stanic a vzdálených místních sítí na DNS firewall a vynucení jeho využívání

V této kapitole byly popsány jednotlivé možnosti napojení koncových stanic a vzdálených místních sítí na DNS firewall provozovaným v SOCu. Následuje srovnání popsaných možností.

5.6.1 Shrnutí možných napojení koncových stanic na DNS firewall

Byly rozebrány dvě varianty připojení pracovních stanic k DNS firewallu ze sítě Internet. První variantou bylo připojení nešifrovaně skrz síť Internet a druhou bylo připojení koncových pracovních stanic na DNS Firewall pomocí VPN.

Mezi nevýhody připojení koncových stanic přes síť Internet bez využití VPN patří skutečnost, že DNS firewall musí být veřejně dostupný ze sítě Internet, jelikož se koncové stanice připojují z různých místních sítí světa a nelze předem určit jejich IP adresy. DNS firewall pak může vyhodnocovat DNS dotazy i neautorizovaným stanicím a je náchylný na útoky typu DoS. Další nevýhodou je, že pokud se koncová stanice nachází v místní síti, která blokuje odchozí komunikaci na DNS firewall a zároveň má DNS firewall nastaven jako DNS Resolver na síťovém adaptéru, dojde

k nemožnosti vyhodnocení DNS dotazů. Výhodou tohoto řešení je jednoduchá implementace.

V případě řešení napojení koncových stanic na DNS firewall pomocí VPN je hlavní nevýhodou složitější implementace řešení. Výhodou je, že v případě, kdy se nachází koncová stanice v místní síti, která neumožňuje využití VPN tunelu, stanice i nadále dokáže vyhodnotit DNS dotaz, pouze nebude využita funkce DNS firewallu. Další výhodou je, že DNS over VPN lze využít i na mobilních operačních systémech. DNS dotazy jsou ze zařízení na DNS firewall přenášeny šifrovaně. V případě, kdy chce uživatel využívat DNS firewall, vytvoří VPN tunel mezi koncovou stanicí nebo mobilním telefonem a firewallem a začne automaticky směrovat DNS dotazy na DNS firewall.

5.6.2 Shrnutí možností napojení vzdálených místních sítí na DNS firewall

Dále byly rozebrány tři varianty připojení vzdálených místních sítí na DNS firewall nacházející se v SOCu. První variantou připojení vzdálené místní sítě k DNS firewallu je přes Internet bez využití VPN. Nevýhodou této varianty je, že DNS dotazy se posílají přes Internet nešifrovaně a DNS firewall musí být otevřený do Internetu pro komunikaci z veřejné IP adresy vzdálené místní sítě. Hlavní výhodou této varianty je jednoduchá implementace.

Další variantou napojení vzdálených místních sítí na DNS firewall je využití VPN. Hlavní nevýhodou této varianty je složitá implementace. Hlavní výhodou je, že DNS dotazy jsou zasílány přes Internet šifrovaně. Další výhodou je, že DNS firewall nemusí být veřejně dostupný z Internetu.

Poslední popsanou variantou napojení vzdálených místních sítí na DNS firewall nacházející se v SOCu je využití funkce slave RPZ. Hlavní nevýhodou využití této varianty je menší vhled do dění na vzdálené místní síti a složitější implementace řešení. Hlavní výhodou je, že DNS dotazy jsou vyhodnocovány DNS Resolverem vzdálené místní sítě. Tím je docíleno, že správce vzdálené místní sítě může RPZ politiku upravovat.

5.6.3 Shrnutí využívání a vynucení DNS firewallu

Na konci této kapitoly byla popsána možná řešení, jak lze vynutit využívání DNS firewallu na koncových stanicích a v rámci vzdálených místních sítí. Toto řešení je implementováno pomocí technologie EDR, nasazením firewallu na koncových stanicích, který zajistí omezení využívání jiných DNS Resolverů než DNS firewallu umístěného v SOCu a omezení služeb typu DNS over TLS a DNS over HTTPS. Obdobně je toto řešení implementováno i pro vynucení využívání DNS firewallu v rámci vzdálených místních sítí.

6 Testování nasazeného DNS firewallu

V této kapitole jsou popsány výsledky testu výkonnosti DNS firewallu nasazovaného v kapitole 4. Dále jsou prezentovány výsledky dostupnosti DNS firewallu ze sítě Internet.

6.1 Testování výkonnosti nasazeného DNS firewallu

V rámci testovacího nasazení DNS firewallu v SOCu bylo provedeno testování výkonnosti DNS firewallu. Konkrétně se jednalo o testování propustnosti DNS firewallu za účelem zjištění maximálního počtu DNS dotazů, které DNS firewall dokáže vyhodnotit za sekundu. Testování probíhalo ze stanice s operačním systémem CentOS 7 připojené do subnetu DNS firewallu pomocí OpenVPN. Průměrná doba odezvy mezi stanicí a DNS firewallem byla 2 ms. K testování byl využit testovací nástroj `resperf`[25] ve verzi 2.9.0. Tento nástroj systematicky zvyšuje četnost DNS dotazů a sleduje rychlost odpovědí DNS firewallu na tyto dotazy. Test byl spuštěn pomocí příkazu:

```
resperf-report -s 192.168.53.12 -d test-queries.tsv -m 10000
```

Přepínač `-s` definuje adresu DNS Resolveru, na který má nástroj `resperf` zasílat DNS dotazy. Přepínačem `-d` je určen soubor s doménovými jmény, které `resperf` zasílá na DNS Resolver. Soubor doménových jmen `test-queries.tsv` byl stažen z webu Fedora Project [26]. Přepínač `-m` stanovuje maximální počet zaslaných dotazů za sekundu.

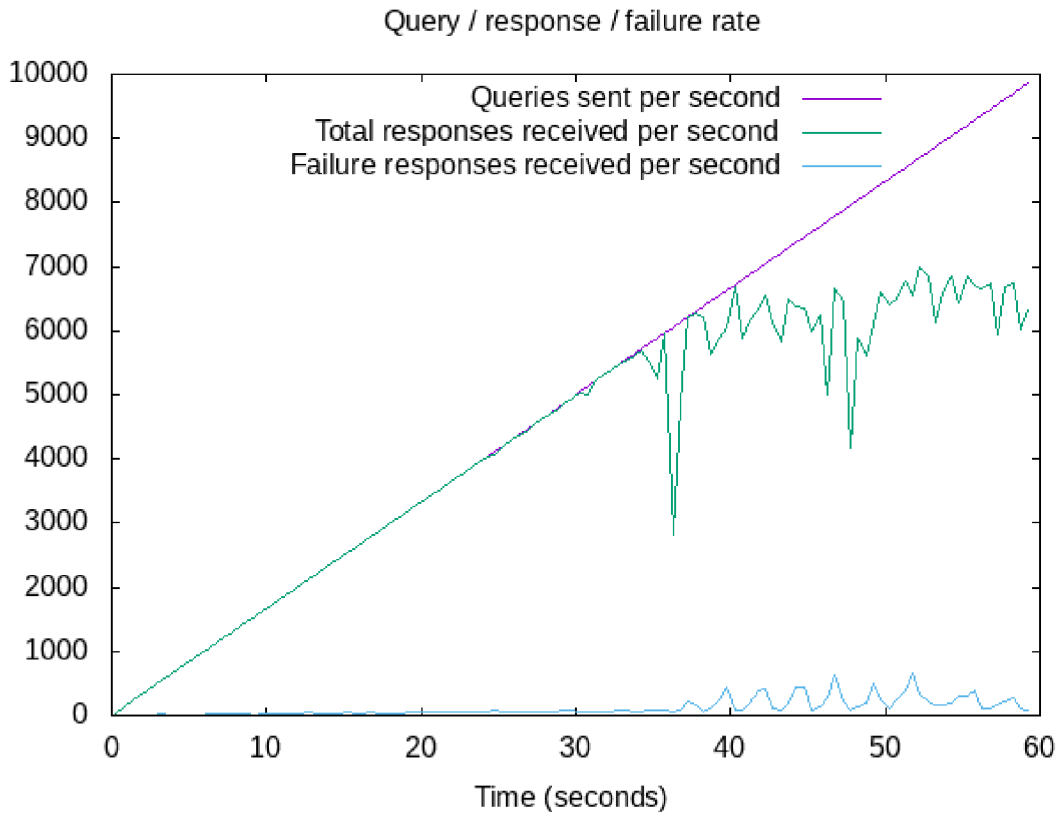
Testování proběhlo po restartování DNS firewallu, aby bylo zabráněno využívání odpovědí uložených v cache paměti DNS firewallu. Parametrem `-m` byl nastaven maximální počet DNS dotazů na 10000 za sekundu. Tato hraniční hodnota byla dostačující pro otestování hraniční propustnosti DNS firewallu nasazeného v kapitole 4.

Měření probíhalo 60 sekund a dalších 40 sekund nástroj `resperf` čekal na případné odpovědi. Tyto hodnoty jsou výchozími pro nástroj `resperf` viz manuál [27]. Výsledná statistika provedeného testu je vypsána ve výpise 6.1.

```
Dotazy zaslané:                 300000
Dotazy dokončené:               255558
Dotazy ztracené:                44442
Kódy odpovědí:                  NOERROR 181077 (70.86%)
                                SERVFAIL 6959 (2.72%)
                                NXDOMAIN 67522 (26.42%)
Doba běhu (s):                  100
Maximální propustnost:          6990 dotaz/s
Ztracené dotazy:                19.73%
```

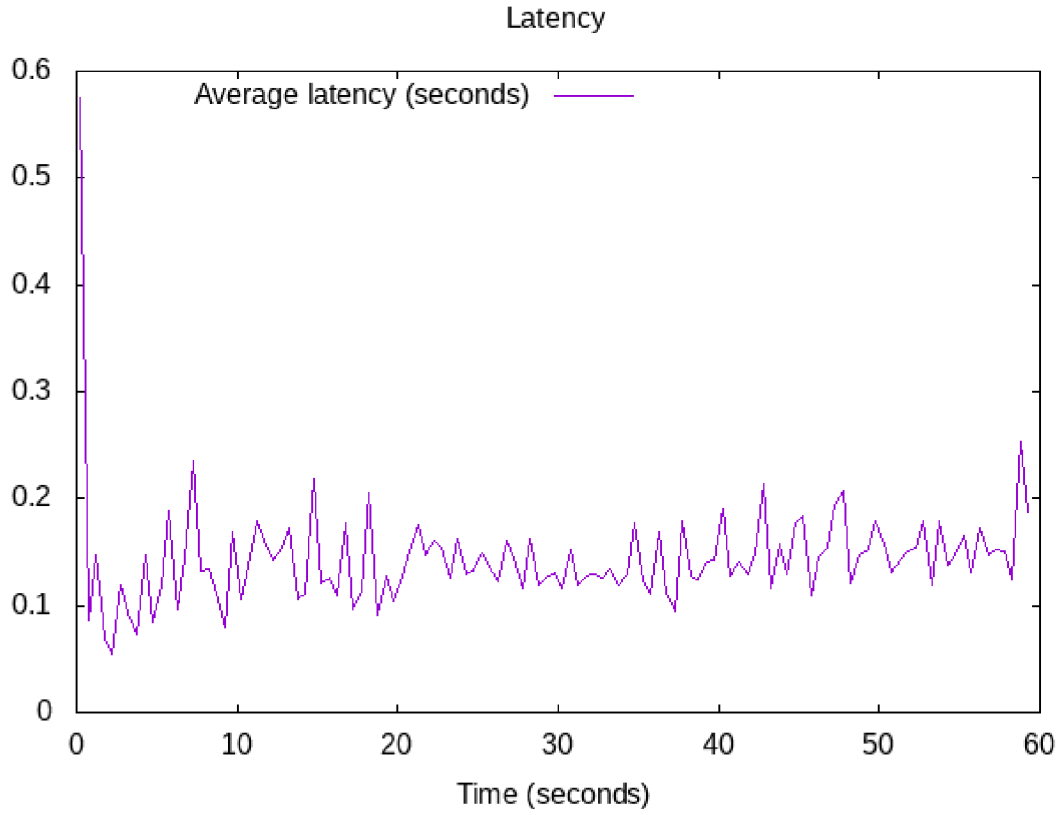
Výpis 6.1: Statistika testu propustnosti nasazeného DNS firewallu provedeného pomocí nástroje `resperf`

Na obrázku 6.1 je zobrazen graf vývoje propustnosti DNS firewallu. Tento graf ukazuje, že přibližně při sedmi tisících DNS dotazů za sekundu přestane DNS firewall vyhodnocovat další DNS dotazy. Ze statistiky ve výpisu 6.1 a z dat z grafu na obrázku 6.1 je zřejmá skutečnost, že implementace DNS firewallu v kapitole 4. umožňuje vyhodnocovat cca 7000 DNS dotazů za sekundu. Pro srovnání je možné uvést, že průměrný počet DNS dotazů vyhodnocených veřejným DNS Resolverem ODVR provozovaným sdružením CZ.NIC je 7500 DNS dotazů za sekundu [28]. Taktéž bylo ověřeno, zda výkonnost DNS firewallu neovlivní změna ze 4 jádrového CPU na 8 jádrový CPU. Bylo zjištěno, že přidáním jader CPU nevzrostla výkonnost nasazeného DNS firewallu.



Obr. 6.1: Graf vývoje propustnosti DNS firewallu a výsledků DNS dotazů

Součástí testu bylo i testování průměrného zpoždění DNS odpovědí. Na obrázku 6.2 je zobrazen graf průměrného zpoždění DNS odpovědí DNS firewallu na DNS dotazy. V průběhu testovací doby se hodnota průměrného zpoždění pohybuje okolo 150 ms. Pro srovnání podle DNSPerf.com[29] mají veřejné DNS Resolvery průměrné zpoždění okolo 20 ms.



Obr. 6.2: Graf průměrného zpoždění odpovědí DNS firewallu na DNS dotazy

6.2 Testování dostupnosti DNS firewallu v rámci sítě Internet

V rámci implementace DNS firewallu bylo provedeno testování jeho dostupnosti ze sítě Internet. K otestování byla využita globální síť sond RIPE Atlas [30]. Tyto sondy umožňují zjistit dostupnost prvků v síti Internet a dobu jejich odezvy. Pomocí této sítě lze získat informaci, jaká je průměrná doba odezvy mezi nasazeným DNS firewallem a sondami sítě RIPE Atlas. Tato informace je důležitá, aby bylo možné zjistit, zda se DNS firewall může využívat ze zařízení v rámci sítě Internet umístěných různě po světě. Pro provedení testů bylo nutné DNS firewall zpřístupnit veřejně v rámci sítě Internet. Nedostupnost DNS firewallu některým sondám mohla být způsobena blokací sítí, ve kterých byly sondy umístěny. V testech tyto sondy vracely odpověď `Error: Timeout: 5000`. DNS firewall zasílal odpovědi REFUSED, jelikož sondy zasílaly stejnou žádost o překlad doménového jména. Aby bylo zabráněno DoS útoku, při 900 stejných dotazech za sekundu omezil DNS firewall jejich vyhodnocování a vracel odpověď REFUSED. DNS firewall zaslal DNS odpověď typu SERVFAIL v případě, kdy veřejný DNS Resolver nebyl z výkonnostních důvodů

schopen dotaz v danou chvíli vyhodnotit. Hodnota `No recent report available` byla uveda v případě, kdy síť RIPE Atlas neobdržela odpověď od sondy. Tento problém nesouvisí s nasazeným DNS firewallem, ale jedná se o problém testovací sítě RIPE Atlas, který mohl být způsoben nedostupností sondy.

6.2.1 Testování dostupnosti DNS firewallu v rámci sítě Internet ze sond umístěných ve světě

První test dostupnosti DNS firewallu pomocí sítě RIPE Atlas byl proveden z 964 sond rozmístěných různě po světě viz obrázek 6.3. Sondy najednou zaslaly DNS dotaz na DNS firewall, konkrétně se jednalo o žádost o překlad doménového jména `www.google.com` na IPv4 adresu. Výsledkem bylo 95,85% dotazů vyhodnocených s DNS odpovědí `NOERROR` viz obrázek 6.4, pouze 2,28% sond nemělo dostupný DNS firewall. Na obrázku 6.5 jsou seřazeny testovací sondy podle doby odezvy a je zde zobrazená i průměrná doba odezvy dle měření z těchto sond. Průměrná doba odezvy sond byla 138,8 ms.

Testování dostupnosti veřejného DNS Resolveru CZ.NIC v rámci sítě Internet ze světa

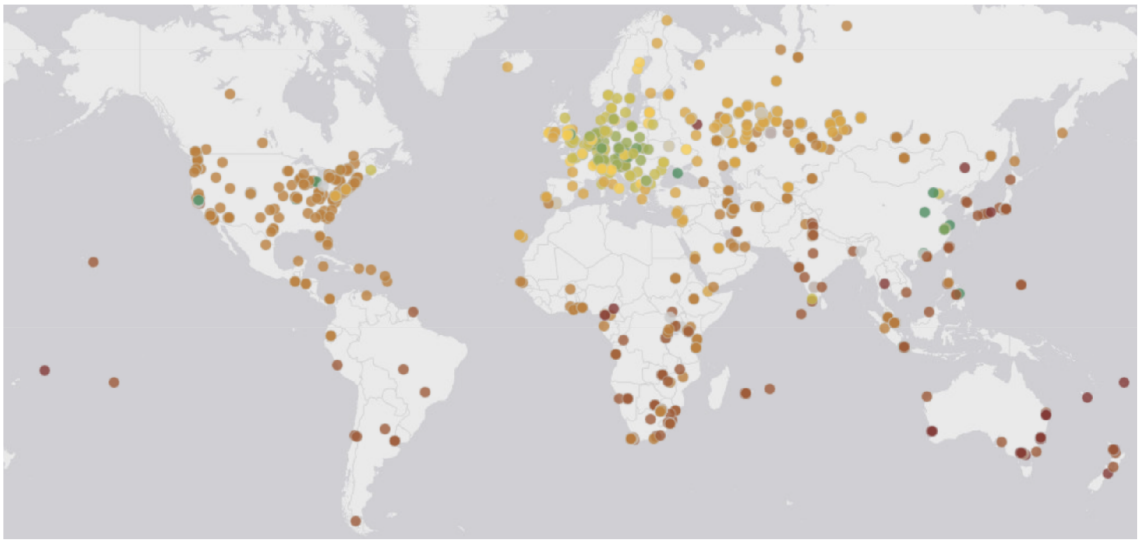
Pro porovnání dostupnosti nasazeného DNS firewallu byl proveden test dostupnosti ODVR DNS Resolveru provozovaného sdružením CZ.NIC. Test proběhl z 960 sond sítě RIPE Atlas rozmístěných různě po světě viz obrázek 6.6. Průměrná doba odezvy DNS Resolveru provozovaným sdružení CZ.NIC byla 128,6 ms viz obrázek 6.7. Rozdíl doby odezvy mezi nasazeným DNS firewallem a veřejným DNS Resolverem ODVR byl 10,2 ms. Pokud jsou zváženy přínosy, které přináší použití DNS firewallu, pak drobné zpoždění při překladu DNS dotazu není kritické.

6.2.2 Testování dostupnosti DNS firewallu v rámci sítě Internet ze sond umístěných v Evropské unii

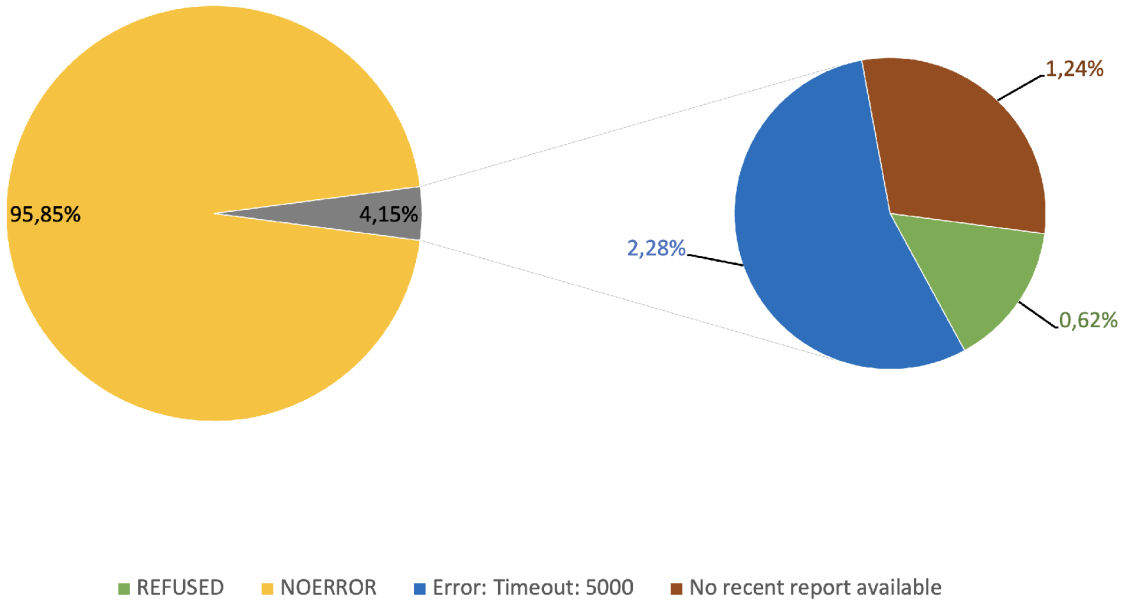
Další test pomocí sítě RIPE Atlas byl proveden z 929 sond. Sondy byly rozmístěny rovnoměrně po státech Evropské unie viz obrázek 6.8. Sondy poslaly DNS dotaz na DNS firewall, tentokrát se jednalo o žádost o překlad doménového jména www.axenta.cz na IPv4 adresu. Výsledkem bylo 96,02% dotazů vyhodnocených s DNS odpovědí `NOERROR` viz obrázek 6.9 a pouze 2,37% sond nemělo dostupný DNS firewall. Na obrázku 6.10 jsou seřazeny sondy podle doby odezvy a je zde

i zobrazená průměrná doba odezvy dle měření z těchto sond. Průměrná doba odezvy sond byla 45,3 ms.

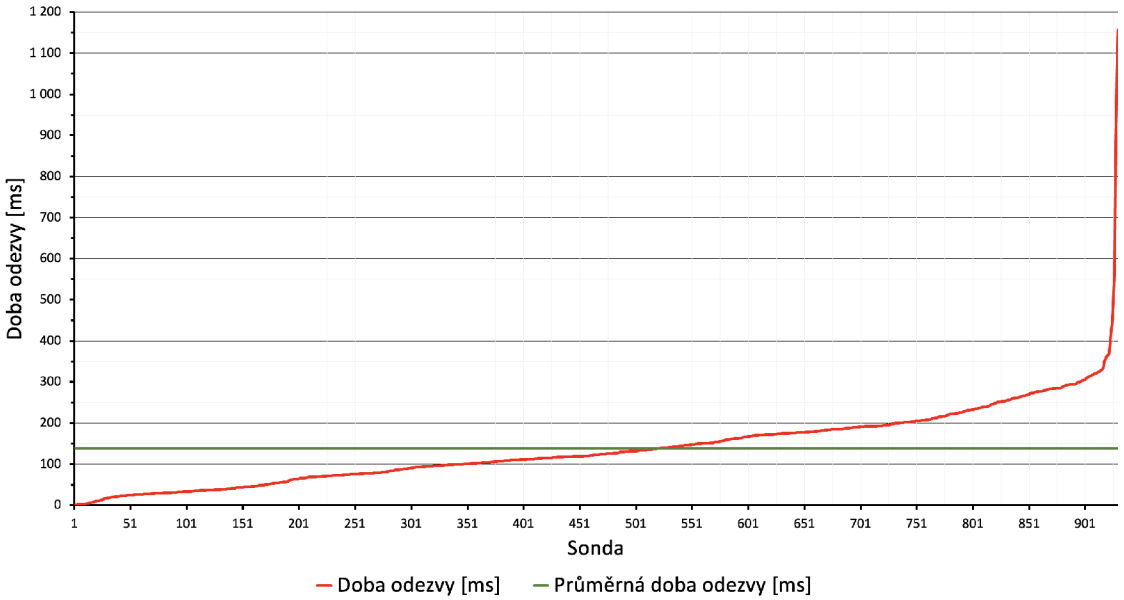
Poslední test pomocí sítě RIPE Atlas byl proveden z 929 sond. Sondy byly rozmístěny rovnoměrně po státech Evropské unie viz obrázek 6.11. Sondy najednou zaslaly DNS dotaz na DNS firewall se žádostí o překlad doménového jména na IPv4 adresu. Výsledkem bylo 96,12% dotazů vyhodnocených s DNS odpovědí `NOERROR` viz obrázek 6.12 a pouze 2,26% sond nemělo dostupný DNS firewall. Na obrázku 6.13 jsou seřazené sondy podle doby odezvy a je zde i zobrazená průměrná doba odezvy dle měření z těchto sond. Průměrná doba odezvy sond byla 49,7 ms.



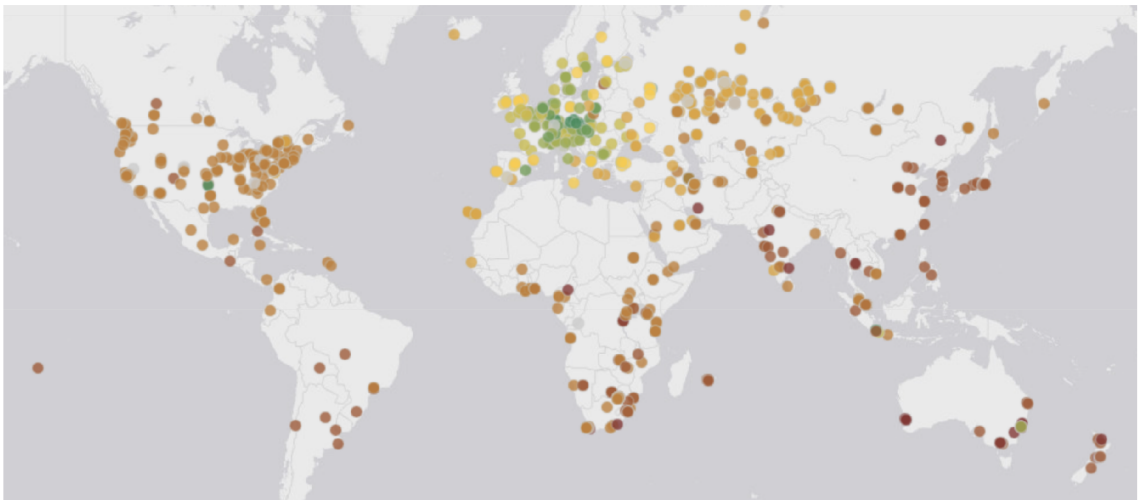
Obr. 6.3: Mapa využitých sond v rámci měření DNS firewallu ze sítě RIPE Atlas rozmístěných různě po světě



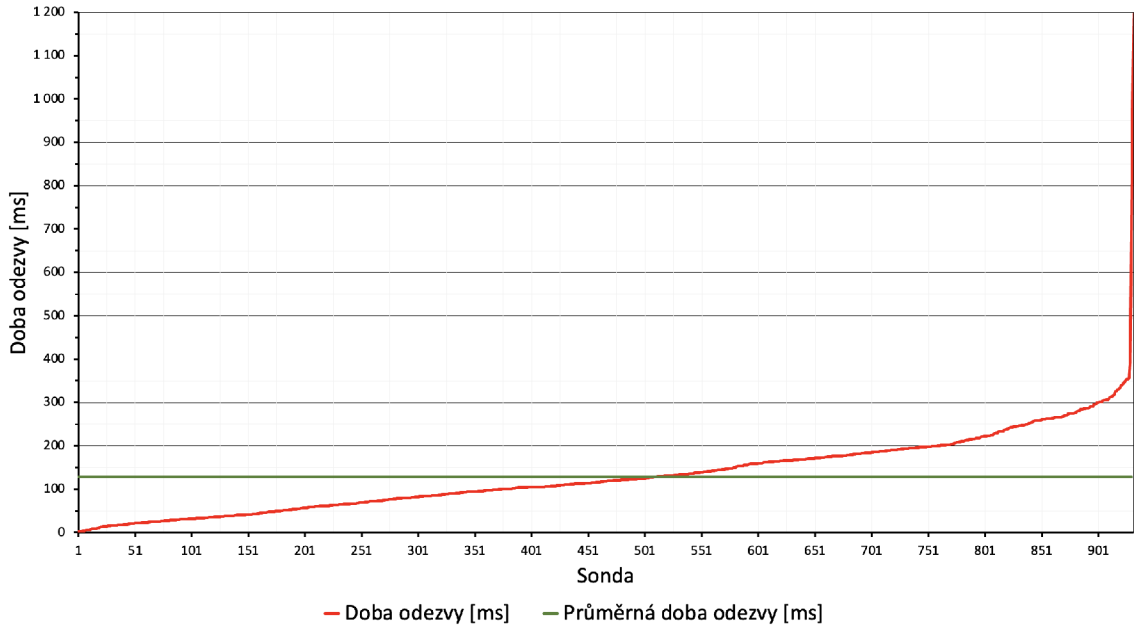
Obr. 6.4: Výsledné DNS odpovědi zaslané DNS firewallem při testování jeho dostupnosti ze sond ze sítě RIPE Atlas rozmístěných různě po světě



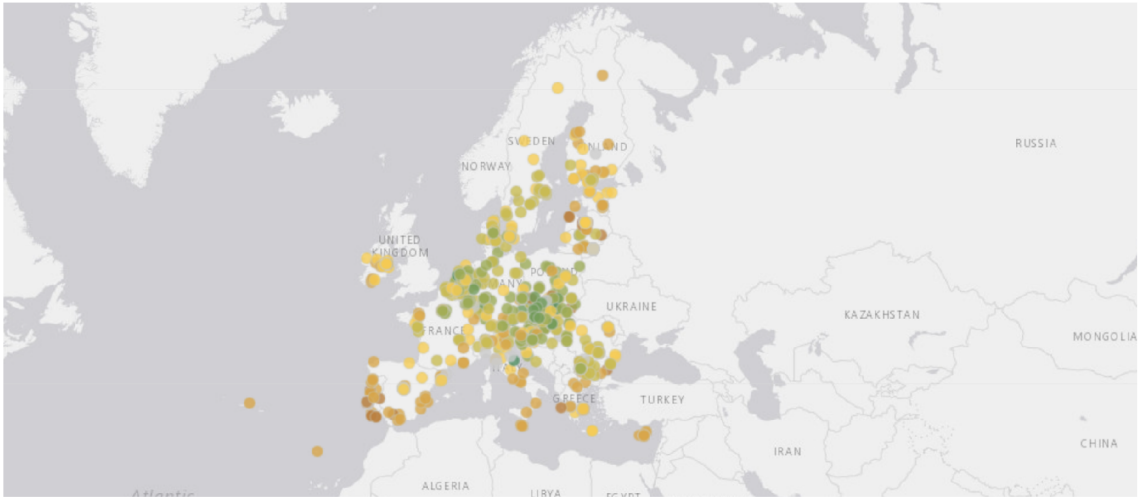
Obr. 6.5: Výsledný Response Time odpovědí zaslaných DNS firewallem při testování jeho dostupnosti ze sond ze sítě RIPE Atlas rozmístěných různě po světě



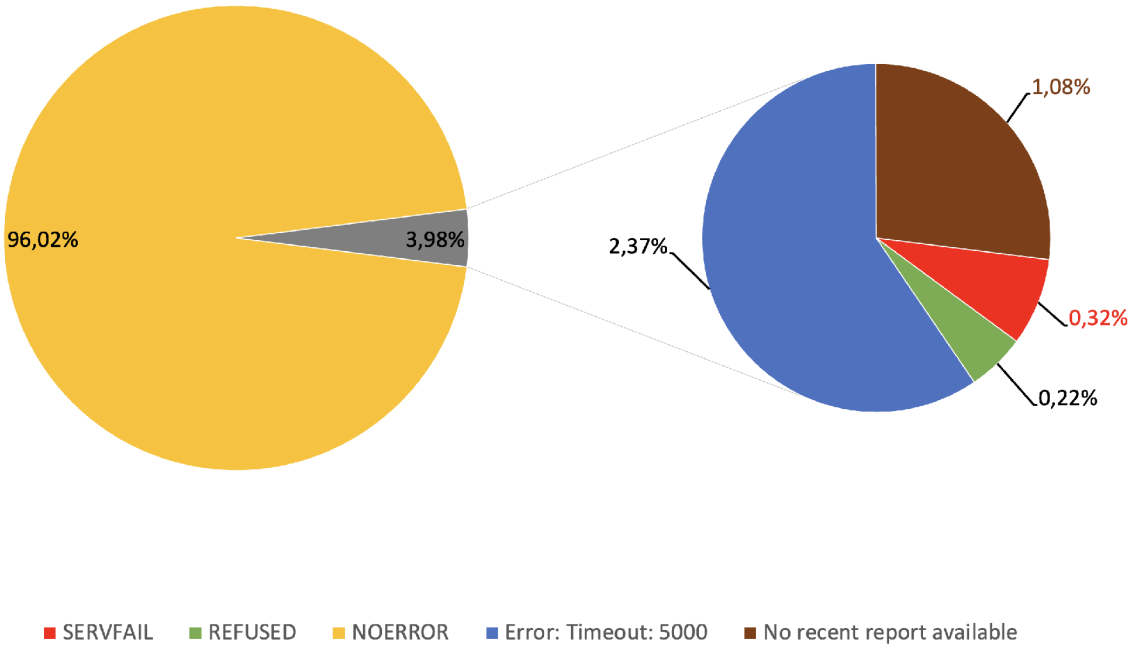
Obr. 6.6: Mapa využitých sond v rámci měření DNS resolveru CZ.NIC ze sítě RIPE Atlas rozmístěných různě po světě



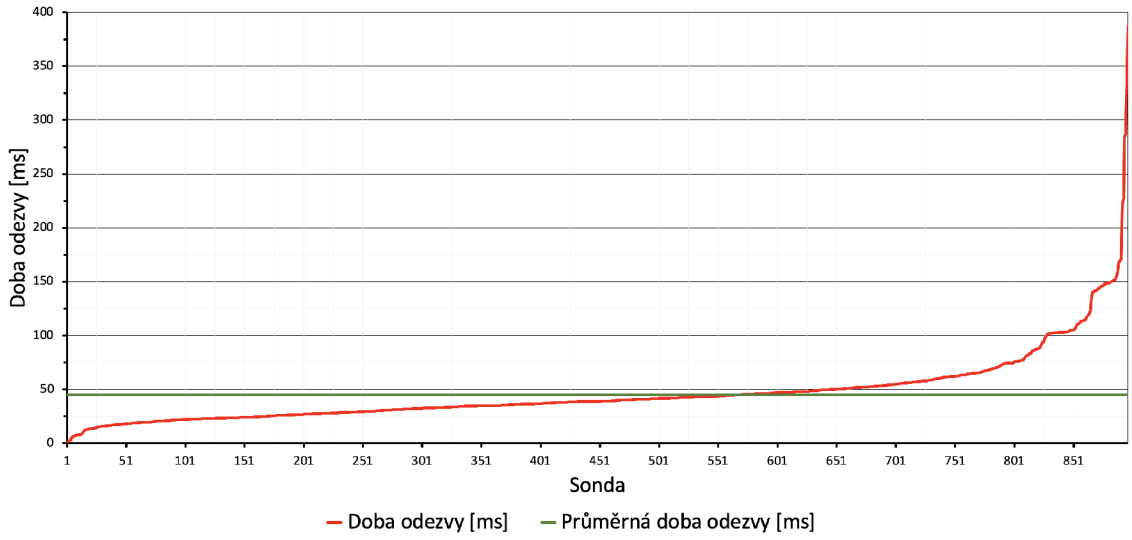
Obr. 6.7: Výsledný Response Time odpovědí zaslaných DNS Resolverem CZ.NIC při testování jeho dostupnosti ze sond ze sítě RIPE Atlas rozmístěných různě po světě



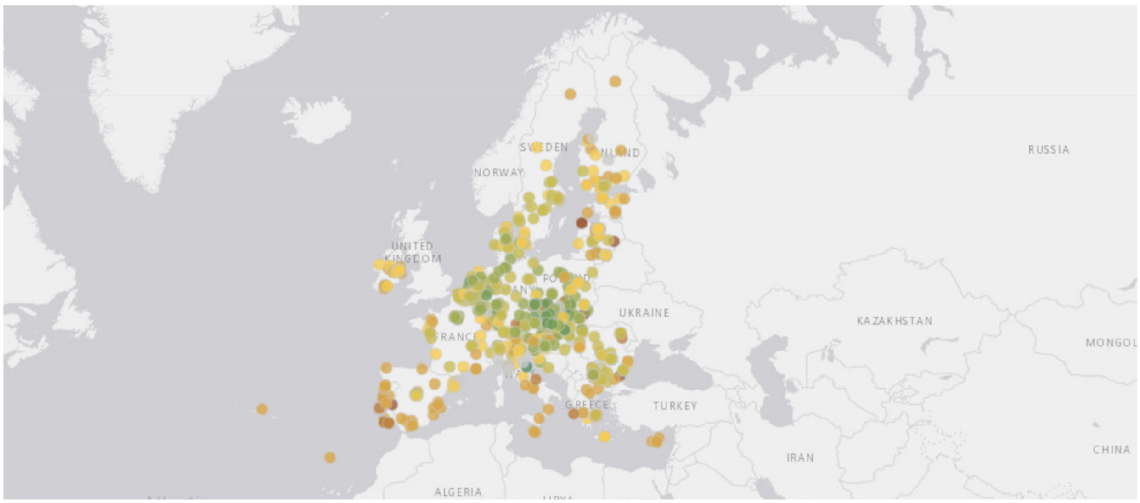
Obr. 6.8: Mapa využitých sond v rámci měření DNS firewallu ze sítě RIPE Atlas rozmístěných v zemích Evropské unie test 1



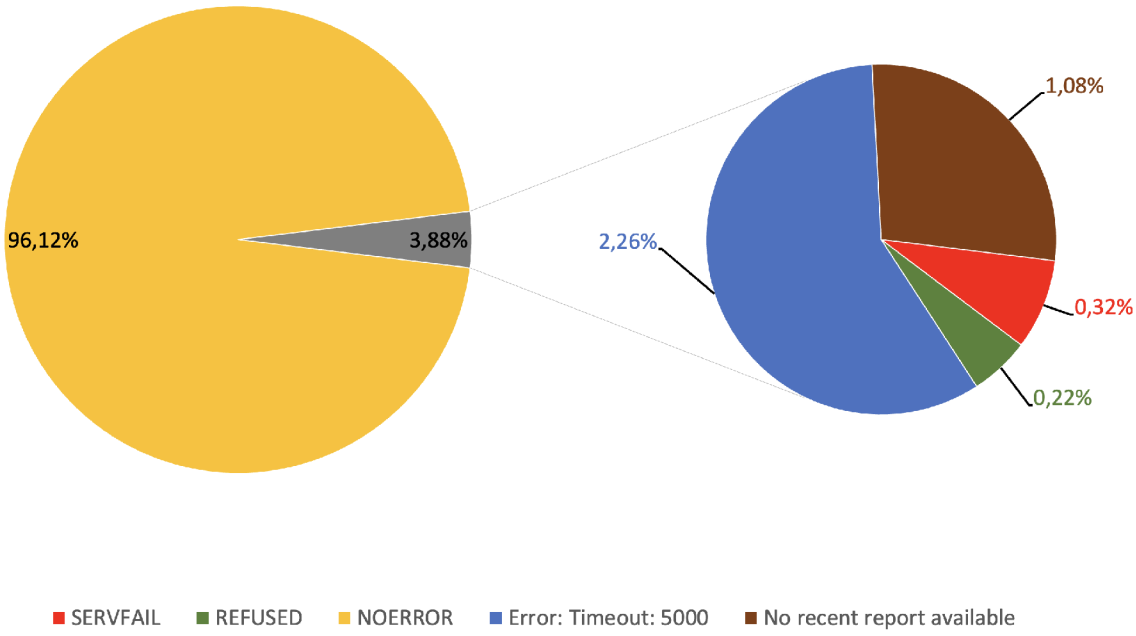
Obr. 6.9: Výsledné DNS odpovědi zaslané DNS firewallem při testování jeho dostupnosti ze sond ze sítě RIPE Atlas rozmístěných v zemích Evropské unie test 1



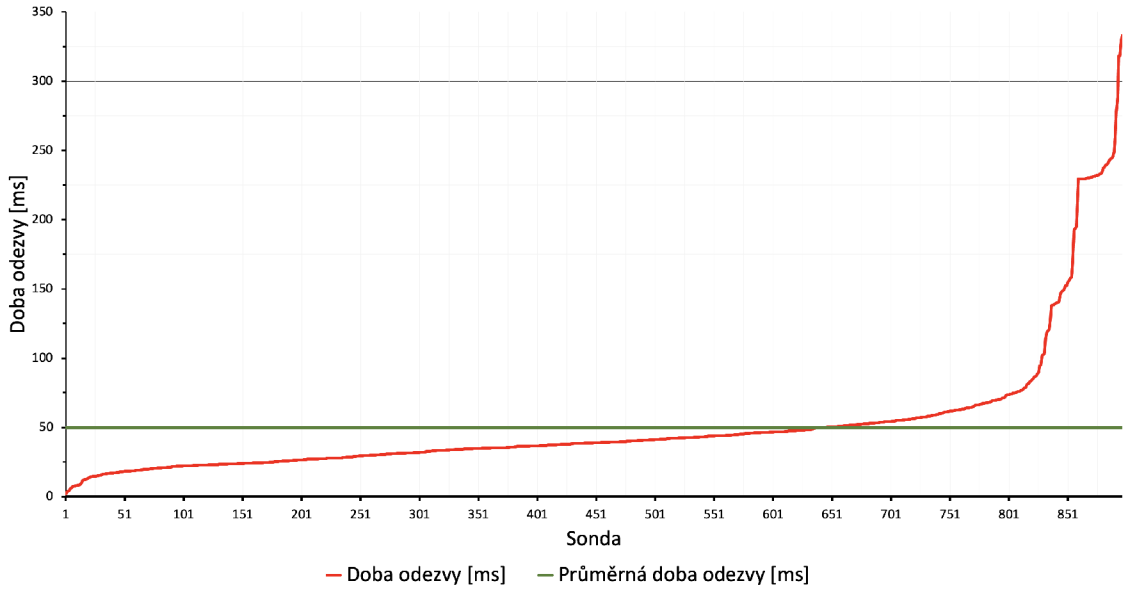
Obr. 6.10: Výsledný Response Time odpovědí zaslaných DNS firewallem při testování jeho dostupnosti ze sond ze sítě RIPE Atlas rozmístěných různě v zemích Evropské unie test 1



Obr. 6.11: Mapa využitých sond v rámci měření DNS firewallu ze sítě RIPE Atlas rozmístěných v zemích Evropské unie test 2



Obr. 6.12: Výsledné DNS odpovědi zaslané DNS firewallem při testování jeho dostupnosti ze sond ze sítě RIPE Atlas rozmístěných v zemích Evropské unie test 2



Obr. 6.13: Výsledný Response Time odpovědí zaslaných DNS firewallem při testování jeho dostupnosti ze sond ze sítě RIPE Atlas rozmístěných různě v zemích Evropské unie test 2

Závěr

Cílem této bakalářské práce bylo nasazení DNS firewallu v reálném kybernetickém operačním centru nabízeném jako služba. Pro DNS firewall měl být využit softwarový balík BIND a mechanismus RPZ. Dalším úkolem bylo provedení integrace nasazeného DNS firewallu s ostatními službami v SOCu. Hlavním úkolem bylo zmapování a otestování možností připojení koncových stanic a vzdálených místních sítí k nasazenému DNS firewallu. Posledním úkolem bylo navrhnutí postupu vynucení využívání nasazeného DNS firewallu jako jediného DNS Resolveru.

V první části práce bylo představeno kybernetické operační centrum a jeho prvky. Dalším tématem byla historie, důvody využívání a principy fungování DNS (Domain Name System). V kapitole byl popsán DNS Resolver, který má na starost překlad doménového jména na IP adresu. Byly definovány dva základní módy, ve kterých DNS Resolver může fungovat (Forwarding, Recursion). V poslední části kapitoly bylo znázorněno jak DNS Resolver vyhodnocuje DNS dotazy. Třetí kapitola byla věnována problematice zabezpečení DNS. Na začátek byl vysvětlen pojem DNSSEC, který má na starost zabezpečit integritu DNS odpovědí v systému DNS. Dále byla vysvětlena funkce DoH, která zajišťuje šifrování DNS dotazu. V rámci kapitoly byl také představen pojem DNS firewall. Ten umožňuje filtrovat DNS dotazy. Byl zasazen do systému DNS. Následně byl popsán mechanismus RPZ, který je využíván pro implementaci DNS firewallu. Dále byl objasněn programový balík BIND, který byl využit k nasazení DNS firewallu v SOCu a technologie VPN.

Kapitola čtyři představila testovací prostředí, ve kterém byl nasazen DNS firewall. Kapitola detailně popisuje nasazení DNS firewallu a jeho jednotlivá provedená nastavení. Další část byla věnována integraci nasazeného DNS firewallu s ostatními službami reálného testovacího kybernetického operačního centra. Byly podrobně rozebrány technologie nacházející se v testovacím SOCu a postup jejich integrace s nasazeným DNS firewallem. V přílohách A, B a C jsou umístěny vytvořené konfigurační soubory týkající se nasazeného DNS firewallu a jeho integrace. Pátá kapitola se zabývala testováním a popisem jednotlivých způsobů napojení koncových stanic a vzdálených místních sítí k nasazenému DNS firewallu. Byly popsány výhody a nevýhody jednotlivých řešení, které byly i testovány, a způsoby vynucení využívání DNS firewallu. Hlavními výhodami napojení koncových stanic a vzdálených místních sítí na DNS firewall pomocí technologie VPN je kombinace šifrovaného přenášení DNS dotazů a možnosti připojení koncových stanic a vzdálených místních sítí na DNS firewall i bez jeho veřejné dostupnosti ze sítě Internet. Zároveň při napojení pomocí technologie VPN a využívání DNS firewallu v SOCu pro překlad

DNS dotazů je výhoda většího vhledu do dění na koncových stanicích a vzdálených místních sítích. Na konci této bakalářské práce bylo provedeno testování nasazeného DNS firewallu v testovacím SOCu. Bylo zjištěno, že nasazený DNS firewall zvládá vyhodnotit cca 7000 DNS dotazů za sekundu. Průměrná doba odezvy DNS firewallu při testování ze stanice připojené pomocí VPN byla 150 ms. Nakonec byla ověřena dostupnost a průměrná doba odezvy DNS firewallu ze sond umístěných nejprve různě po světě a následně rozmístěných pouze po Evropské unii. Bylo zjištěno, že nasazená implementace má velmi podobné výsledky jako veřejný DNS Resolver, tím byla potvrzena využitelnost nasazeného DNS firewallu v testovacím SOCu.

Literatura

[1] *D*E GROOT, Juliana, 2020. What is a Security Operations Center (SOC)?. Digital Guardian [online]. [cit. 2021-12-12]. Dostupné z: https://digitalguardian.com/blog/what-security-operations-center-soc.

[2] *S*ecurity Operations Center. AEC [online]. [cit. 2021-12-12]. Dostupné z: https://www.aec.cz/cz/produkty-a-sluzby/Stranky/soc.aspx.

[3] *W*hat Is a Security Operations Center (SOC)?. McAfee [online]. [cit. 2021-12-12]. Dostupné z: https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-soc.html.

[4] NOVÁK, Lukáš, Brno 2020. DNS firewall jako služba SOCu. Diplomová práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Tomáš PITNER [online]. [cit. 2021-12-12]. Dostupné z: https://is.muni.cz/th/izihx/.

[5] ČERMÁK, Milan, Brno 2014. Bezpečnostní analýza provozu DNS. Diplomová práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Jan VYKOPAL. [online]. [cit. 2021-12-12]. Dostupné z: https://is.muni.cz/th/fbpfj/.

[6] ISI Names Dr. Paul Mockapetris Visiting Scholar. 2003 USC. [online]. [cit. 2021-12-12]. Dostupné z: https://web.archive.org/web/20120826032920/http:/www3.isi.edu/about-news_story.htm?s=54.

[7] Paul Mockapetris. Wikipedia [online]. [cit. 2021-12-12]. Dostupné z: https://en.wikipedia.org/wiki/Paul_Mockapetris.

[8] Internet Corporation for Assigned Names and Numbers. Wikipedia [online]. [cit. 2021-12-12]. Dostupné z: https://cs.wikipedia.org/wiki/Internet_Corporation_for_Assigned_Names_and_Numbers.

[9] The History of ICANN. ICANN [online]. [cit. 2021-12-12]. Dostupné z: https://www.icann.org/history.

[10] JEŘÁBEK, J. Pokročilé komunikační techniky. Skriptum FEKT Vysoké učení technické v Brně, 2021. s. 1-180.

[11] root-servers.org. [online]. [cit. 2021-12-12]. Dostupné z: https://root-servers.org/.

[12] MOCKAPETRIS, Paul, 1987. RFC 1035. Internet Assigned Numbers Authority [online]. [cit. 2022-05-23]. Dostupné z: https://www.rfc-editor.org/rfc/rfc1035

[13] BAU, Jason ; MITCHELL, John C, 2010. A Security Evaluation of DNSSEC with NSEC3. [online]. [cit. 2022-03-15]. Dostupné z: https://eprint.iacr.org/2010/115.pdf.

[14] KRČMÁŘ, Petr. DNS over HTTPS: nový standard pro bezpečné a soukromé DNS. ROOT.CZ [online]. [cit. 2021-12-12]. Dostupné z: https://www.root.cz/clanky/dns-over-https-novy-standard-pro-bezpecne-a-soukrome-dns/.

[15] HOFFMAN, P.; MCMANUS, P. DNS Queries over HTTPS (DoH). [online]. IETF, 2018 [cit. 2022-02-17]. Dostupné z: https:// tools.ietf.org/html/rfc8484.

[16] FAWCETT, Milly. What is DNS Firewall? A beginner's guide [online]. Spamhaus Technology, 2018 [cit. 2022-03-17]. Dostupné z: https://www.spamhaustech.com/resource-center/what-is- dns-firewall-a-beginners-guide/.

[17] DNS Response Policy Zones [online]. dnsrpz.info, 2019 [cit. 2022-02-10]. Dostupné z: https://dnsrpz.info/.

[18] BIND 9 Administrator Reference Manual [online]. ISC [cit. 2021-12-12]. Dostupné z: https://bind9.readthedocs.io/en/latest/index.html.

[19] BIND 9 [online]. ISC [cit. 2021-12-12]. Dostupné z: https://www.isc.org/bind/.

[20] T. Berger. Analysis of current VPN technologies. First International Conference on Availability, Reliability and Security (ARES'06), 2006, pp. [cit. 2021-12-12]. Dostupné z: https://ieeexplore.ieee.org/abstract/document/1625300?casa_token=ljJpgKCJ5vsAAAAA:R83_8tkqrwhtAjdWCo64nIW6494GhAzpDpTQFr_2ywf_vsCnoE90KvhPJ7PyaL4Xdg-P8sMjlQ

[21] OpenVPN [online]. [cit. 2021-12-12]. Dostupné z: https://openvpn.net/.

[22] Viscosity [online]. [cit. 2021-12-12]. Dostupné z: https://www.sparklabs.com/viscosity/.

[23] Wireshark [online]. [cit. 2021-12-12]. Dostupné z: https://www.wireshark.org/.

[24] Subverting BIND's SRTT Algorithm Derandomizing NS Selection [online]. [cit. 2022-05-23]. Dostupné z: https://www.usenix.org/system/files/conference/woot13/woot13-hay.pdf.

[25] resperf [online]. [cit. 2022-05-26]. Dostupné z: https://www.dns-oarc.net/tools/dnsperf.

[26] test-queries.tsv [online]. [cit. 2022-05-26]. Dostupné z: https://src.fedoraproject.org/lookaside/extras/dnsperf/queryfile-example-current.gz/851024fb2d6320ae126b0dcc4f5bb578/.

[27] resperf - Linux man page [online]. [cit. 2022-05-26]. Dostupné z: https://linux.die.net/man/1/resperf.

[28] Statistika CZ.NIC [online]. [cit. 2022-05-23]. Dostupné z: https://stats.nic.cz/dashboard/cs/Summary.html.

[29] DNS Performance Analytics and Comparison [online]. [cit. 2022-05-26]. Dostupné z: https://www.dnsperf.com.

[30] RIPE Atlas [online]. [cit. 2022-05-26]. https://atlas.ripe.net/.

Seznam zkratek

acl	Access Control List
ARPANET	Advanced Research Projects Agency Network
BIND	Berkeley Internet Name Domain
CNAME	Canonical Name
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoH	DNS over HTTPS
DoS	Denial of Service
EDR	Endpoint Detection and Response
ESM	Enterprise Security Manage
FQDN	Fully Qualified Domain Name
FW	Firewall
GPO	Group Policy
HDD	Hard Disk Drive
HS	Hesiod
HTTPS	Hypertext Transfer Protocol Secure
CH	Chaos
IANA	Internet Assigned Numbers Authority
ICANNA	Internet Corporation for Assigned Names and Numbers
IN	Internet
IP	Internet Protocol
IPv4	Internet Protocol version 4

IPv6	Internet Protocol version 6
LM	Log Management
MB	Megabyte
MISP	Malware Information Sharing Platform
MX	Mail Exchange
NS	Name Server
OS	Operating System
RAM	Random Access Memory
RDATA	Resource Data
RFC	Request for Comments
RNDC	Remote Name Daemon Control
RPZ	Response Policy Zone
RR	Resource Record
PTR	Pointer Record
SIEM	Security Information and Event Management
SLD	Second Level Domain
SNMP	Simple Network Management Protocol
SOC	Security Operation Center
SRTT	Smoothed Round Trip time
TCP	Transmission Control Protocol
TI	Threat Intelligence
TLD	Top Level Domain
TLS	Transport Layer Security
TTL	Time to Live
UDP	User Datagram Protocol

VPN Virtual Private Network

WWW World Wide Web

Seznam příloh

A Konfigurační soubor named.conf nasazeného DNS firewallu doplněný o komentáře

```
options {
    // Definice portů a adres, na kterých server naslouchá.
    listen-on port 53 { 127.0.0.1; 192.168.53.12; };
    listen-on-v6 port 53 { ::1; };

    // Pracovní adresář pro named .
    directory   "/var/named";

    // Cesta k souboru, do kterého bude vypsána databáze na
       vyžádání.
    dump-file   "/var/named/data/cache_dump.db";

    // Cesta k souboru, do kterého se vypisuje statistika pokud
       je k tomu named vyzván.
    statistics-file "/var/named/data/named_stats.txt";

    // Cesta k souboru, do kterého se vypisuje statistika
       o využití paměti po ukončení.
    memstatistics-file "/var/named/data/named_mem_stats.txt";

    // Nastavení do módu forwarder.
    forward only;

    // Určení DNS Resolverů, na které DNS firewall přeposílá
       dotazy.
    forwarders { 1.1.1.1; 8.8.8.8; };

    //Zapnutí loggování.
    querylog yes;

    // Definování IP adres, kterým má DNS firewall vyhodnotit DNS
        dotazy.
    allow-query { trusted-IP-queries; };
    allow-recursion{ trusted-IP-queries; };
    allow-query-cache { trusted-IP-queries; };

    // Definování IP adres, kterým má DNS firewall umožnit
       stažení zón.
    allow-transfer {trusted-IP-transfer ;};

```

```
35      // Zakání funkcí allow-update, allow-notify,allow-update-
            forwarding.
36      allow-update {none;};
37      allow-notify { none; };
38      allow-update-forwarding {none;};
39
40      // DNS firewall nebude sdílet informaci o instalované verzi
            BIND.
41      version "Not available";
42
43      // Definování IP adres, kterým DNS firewall nemá vyhodnocovat
             DNS dotazy.
44      blackhole { blackhole-IP; };
45
46      // Zapnutí funkce DNSSEC.
47      dnssec-enable yes;
48      dnssec-validation auto;
49      bindkeys-file "/etc/named.bind.keys";
50      managed-keys-directory "/var/named/dynamic";
51
52      // Nastavení RPZ politiky. DNS firewall bude vracet odpověď
            NXDOMAIN pro dotazy ze zóny mispexport.rpz.
53      response-policy {
54        zone "mispexport.rpz" policy NXDOMAIN;
55      } qname-wait-recurse no break-dnssec yes;
56  };
57
58  // Definování zóny mispexport.rpz.
59  zone "mispexport.rpz" {
60    type master;
61    file "mispexport.rpz";
62  };
63
64  // Nastavení logování událostí DNS firewallu.
65  logging {
66      channel named           { file "log/named.log"
            versions 3 size 100M; severity dynamic;  print-time yes;
            print-severity yes; print-category yes; };
67      channel security        { file "log/security.log"
            versions 3 size 100M; severity dynamic;  print-time yes;
            print-severity yes; print-category yes; };
68      channel dnssec          { file "log/dnssec.log"
            versions 3 size 100M; severity dynamic;  print-time yes;
            print-severity yes; print-category yes; };
69      channel resolver        { file "log/resolver.log"
            versions 3 size 100M; severity dynamic;  print-time yes;
            print-severity yes; print-category yes; };
```

```
70      channel query_log       { file "log/query.log"
           versions 3 size 100M; severity dynamic;  print-time yes;
           print-severity yes; print-category yes; };
71      channel query-errors    { file "log/query-errors.log"
           versions 3 size 100M; severity dynamic;  print-time yes;
           print-severity yes; print-category yes; };
72      channel lame_servers    { file "log/lame-servers.log"
           versions 3 size 100M; severity dynamic;  print-time yes;
           print-severity yes; print-category yes; };
73      channel capacity        { file "log/capacity.log"
           versions 3 size 100M; severity dynamic;  print-time yes;
           print-severity yes; print-category yes; };
74      channel rpz             { file "log/rpz.log"
           versions 3 size 100M; severity dynamic;  print-time yes;
           print-severity yes; print-category yes; };
75      channel other           { file "log/other.log"
           versions 3 size 100M; severity dynamic;  print-time yes;
           print-severity yes; print-category yes; };
76
77      category default        { named; };
78      category general        { named; };
79      category security       { security; };
80      category queries        { query_log; };
81      category lame-servers   { lame_servers;};
82      category dnssec         { dnssec; };
83      category edns-disabled  { named; };
84      category config         { named; };
85      category resolver       { resolver; };
86      category edns-disabled  { resolver; };
87      category cname          { resolver; };
88      category serve-stale    { resolver; };
89      category spill          { capacity; };
90      category rate-limit     { capacity; };
91      category database       { capacity; };
92      category client         { named; };
93      category network        { named; };
94      category dnstap         { other;};
95      category unmatched      { named; };
96      category client         { named; };
97      category network        { named; };
98      category delegation-only { named;};
99      category dispatch       { named; };
100     category trust-anchor-telemetry { named; };
101     category rpz            { rpz;};
102     category xfer-in  { other; };
103     category xfer-out { other; };
104     category notify         { other; };
```

```
105         category query-errors   {query-errors; };
106         category update         { other; };
107         category update-security { other; };
108         category zoneload       { other; };
109     };
110
111     zone "." IN {
112         type hint;
113         file "named.ca";
114     };
115
116     include "/etc/named.rfc1912.zones";
117
118     // Povolení ovládání DNS firewallu pomocí rndc.
119     include "/etc/rndc.key";
120     controls {
121         inet 127.0.0.1 port 953
122         allow { 127.0.0.1; } keys { "rndc-key"; };
123     };
124
125     // Forward zóna
126     zone "testbind.local" IN {
127         type master;
128         file "testbind.local.db";
129     };
130
131     // Backward zóna
132     zone "53.168.192.in-addr.arpa" IN {
133         type master;
134         file "testbind.local.rev";
135     };
136
137     // Seznam IP adres trusted-IP-queries, kterým má DNS firewall
        vyhodnocovat dotazy.
138     acl trusted-IP-queries {
139         127.0.0.1/32;
140         192.168.53.0/24;
141         192.168.239.0/24;
142     };
143
144     // Seznam IP adres trusted-IP-transfer, kterým má DNS firewall
        umožnit stažení zón.
145     acl trusted-IP-transfer {
146         none;
147     };
148
149     // Seznam IP blackhole-IP, kterým má DNS firewall odepřít přístup
```

```
150 acl blackhole-IP {
151     none;
152 };
```

B Konfigurační soubor crontab

```
1  SHELL=/bin/bash
2  PATH=/sbin:/bin:/usr/sbin:/usr/bin
3  MAILTO=root
4
5  # For details see man 4 crontabs
6
7  # Example of job definition:
8  # .---------------- minute (0 - 59)
9  # |  .------------- hour (0 - 23)
10 # |  |  .---------- day of month (1 - 31)
11 # |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
12 # |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,
       mon,tue,wed,thu,fri,sat
13 # |  |  |  |  |
14 # *  *  *  *  * user-name  command to be executed
15 1 * * * * root /root/misp-export-all.sh > /dev/null
16 10 * * * * root /root/named-reload.sh > /dev/null
```

C Konfigurace doplněná do výchozího konfiguračního souboru syslog-ng.conf

```
source s-file-named {
   wildcard-file(
        base-dir("/var/named/log") //Umístění logů DNS firewallu.
        filename-pattern("*.log") //Výběr všech souborů s končící
            .log.
        log_fetch_limit(20000) ); //Maximální počet načtených
           logů najednou.
};

destination d-cstest1 {
        tcp("192.168.52.72" port(6999) // Definování IP adresy a
           portu Connector serveru.
        disk-buffer(disk-buf-size(2684354560) // Maximálně 2,5GB
           využití paměti na cílovém disku.
        mem-buf-size(512000) // Maximálně 500kB využití paměťové
           části vyrovnávací paměti místního disku.
        reliable(yes)) // Povolit spolehlivého ukládání do
           vyrovnávací paměti na disku.
        throttle(5000) // Povoleno zaslání maximálně 5000 logů za
            sekundu.
        );
};

log { source(s-file-named); //Zdroj logů.
    destination(d-cstest1); //Definování cíle - Connector server.
};
```