**Analýza a implementace firewallu a systému NDR pro optimalizaci bezpečnosti počítačové sítě**

**Analysis and implementation of firewall and NDR system to optimize computer network security**

Projekt V

Studijní program: Informatika a kybernetika ve zdravotnictví

Autor práce: Šimon Kochánek

Vedoucí práce: RNDr. Dagmar Brechlerová, Ph.D

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství

Katedra informačních a komunikačních technologií v lékařství Akademický rok: 2023/2024

**Z a d á n í P r o j e k t V**

Student: **Šimon Kochánek**

Obor: Informatika a kybernetika ve zdravotnictví

Téma: **Analýza a implementace firewallu a systému NDR pro optimalizaci bezpečnosti počítačové sítě**

Téma anglicky: **Analysis and implementation of firewall and NDR system to optimize computer network security**

Z á s a d y p r o v y p r a c o v á n í :

Student zkoumá současné metody a nástroje pro zabezpečení počítačových sítí s hlavním zaměřením na firewall a systémy Network Detection and Response (NDR). Cílem je analyzovat open source řešení a demo verze od vybraných komerčních dodavatelů, porovnat je z hlediska jejich efektivity, výkonu a kompatibility. Na základě zjištěných výsledků student navrhne optimální řešení pro vybudování efektivního a bezpečného firewallu a systému NDR. Výsledkem bude konkrétní doporučení pro implementaci těchto řešení v praxi.

Seznam odborné literatury:

MARTINÁSEK, Zdeněk. Bezpečnost ICT 2. Přednáška: Problematika logování, systémy IDS a IPS. Brno: Vysoké učení technické v Brně, 2022.

SPAM Titan. Network Segmentation Best Practices to Improve Security. [online] [cit. 23. 10. 2022]. Dostupné z: https://www.spamtitan.com/web-filtering/network-segmentation-best-practices/.

ALDEN, Alexis. Network Segmentation Best Practices. [online] [cit. 23. 10. 2022]. Dostupné z: https://www.dodbuzz.com/network-segmentation-security-best-practices/.

ESET. Co je firewall? [online] [cit. 20. 10. 2022]. Dostupné z: https://www.eset.com/cz/firewall/.

BOUŠKA, Petr. VLAN – Virtual Local Area Network. [online] [cit. 18. 10. 2022]. Dostupné z: https://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/.

Vedoucí: RNDr. Dagmar Brechlerová, Ph.D.

Konzultanti:

V Praze dne 6.11.2023

....................................................

studentka / student

....................................................

vedoucí práce

....................................................

vedoucí / zástupce ved. katedry

**PROHLÁŠENÍ**

Prohlašuji, že jsem práci s názvem „Analýza a implementace firewallu a systému NDR pro optimalizaci bezpečnosti počítačové sítě“ vypracoval samostatně a použil k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k práci.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu §60 Zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Kladně 10.1.2024 …...….………...………………...

Šimon Kochánek

**PODĚKOVÁNÍ**

Rád bych vyjádřil upřímné poděkování doktorce Brechlerové za její vedení mého semestrálního projektu. Cením si jejího přístupu, který mi umožnil pracovat na projektu s větší svobodou a bez přísných pravidel. Děkuji jí za vedení a motivaci, které mi pomohly rozvíjet své schopnosti a mé pracovní příležitosti v oblasti kyberbezpečnosti. Její přístup k mému zpracování byl otevřený a konstruktivní, a jsem jí za to velmi vděčný.

**ABSTRAKT**

**Analýza a implementace firewallu a systému NDR pro optimalizaci bezpečnosti počítačové sítě**

V této studii se zaměřujeme na analýzu současných metod a nástrojů pro zabezpečení počítačových sítí, s hlavním důrazem na technologie firewallu a systémů Network Detection and Response (NDR). Hlavním cílem je prozkoumat a porovnat různé open source řešení a demo verze poskytované vybranými komerčními dodavateli. Porovnání bude založeno na kritériích efektivity, výkonu a kompatibility s existujícími systémy. Na základě získaných dat a analýzy student navrhne optimální strategii pro implementaci efektivního a bezpečného firewallu a systému NDR.

**Klíčová slova**

Počítačové sítě, Firewall, Network Detection and Response (NDR), Bezpečnostní analýza

**ABSTRACT**

**Analysis and implementation of firewall and NDR system to optimize computer network security**

In this study, we focus on the analysis of current methods and tools for securing computer networks, with a main focus on firewall technologies and Network Detection and Response (NDR) systems. The main objective is to explore and compare different open source solutions and demos provided by selected commercial vendors. The comparison will be based on the criteria of efficiency, performance and compatibility with existing systems. Based on the collected data and analysis, the student will propose an optimal strategy for implementing an efficient and secure firewall and NDR system.

**Keywords**

Computer Networks, Firewall, Network Detection and Response (NDR), Security Analysis

Obsah

[Seznam symbolů a zkratek 8](#_Toc476327912)

[1 Úvod 9](#_Toc476327913)

[1.1 Přehled současného stavu 9](#_Toc476327914)

[1.2 Cíle práce 9](#_Toc476327915)

[1.2.1 Alternativní postup 9](#_Toc476327916)

[2 Metody 10](#_Toc476327917)

[3 Výsledky 11](#_Toc476327918)

[4 Diskuse 13](#_Toc476327919)

[5 Závěr 14](#_Toc476327920)

[Seznam použité literatury 15](#_Toc476327921)

[Příloha A: Požadavky na formátování práce 16](#_Toc476327922)

[Příloha B: Základní typografické zásady 17](#_Toc476327923)

[Příloha C: Další doporučení pro přehlednost textu 18](#_Toc476327924)

[Příloha D: Obsah přiloženého CD 19](#_Toc476327925)

# Seznam symbolů a zkratek

#### Seznam zkratek

|  |  |
| --- | --- |
| Zkratka | Význam |
| NDR | Network Detection and Response (Síťová detekce a reakce) |
| PID | Proporcionálně-integračně-derivační |

# Úvod

V současné éře digitální transformace je bezpečnost počítačových sítí zásadním pilířem pro udržitelný rozvoj a ochranu informačních aktiv jakékoliv organizace. S neustále se rozšiřujícím spektrem kybernetických hrozeb a rostoucí závislostí na digitální infrastruktuře se bezpečnostní řešení stávají nepostradatelnými pro zajištění integrity, dostupnosti a důvěrnosti citlivých dat. Tento projekt si klade za cíl hloubkově prozkoumat současné metody a nástroje pro zabezpečení počítačových sítí, přičemž klade důraz na dvě klíčové oblasti: firewally a systémy Network Detection and Response (NDR).

Motivace k tomuto výzkumu vychází z potřeby porozumět a efektivně reagovat na dynamicky se vyvíjející kybernetické hrozby. V dnešní době, kdy organizace čelí stále složitějším a promyšlenějším útokům, je nezbytné mít nejen robustní, ale i adaptabilní bezpečnostní řešení. Projekt se zaměřuje na komparativní analýzu různých typů firewallů a NDR systémů, včetně open source řešení a demo verzí od vybraných komerčních dodavatelů. Cílem je poskytnout detailní pohled na jejich výkonnost, efektivitu a kompatibilitu v rámci různých provozních prostředí.

Hloubkové porovnání a analýza těchto technologií umožní identifikovat klíčové faktory, které by měly být zohledněny při výběru bezpečnostního řešení pro organizace. Projekt bude také zkoumat, jak se tyto technologie vyvíjejí v reakci na neustále se měnící kybernetické prostředí a jak jsou schopny reagovat na nové typy hrozeb. Výsledkem tohoto výzkumu bude sada doporučení pro implementaci těchto technologií, která by měla pomoci organizacím zvýšit jejich schopnost odolávat proti kybernetickým hrozbám a zároveň udržet flexibilitu a škálovatelnost jejich bezpečnostních systémů.

Tento projekt by mohl přispět k lepšímu pochopení současných bezpečnostních výzev a nabídne praktické návrhy pro zlepšení bezpečnostních opatření v oblasti počítačových sítí, což je nesmírně důležité pro zachování důvěry a ochrany v digitálně propojeném světě.

## Přehled současného stavu

V současném prostředí zabezpečení počítačových sítí se klíčové role ujímají firewally, Network Detection and Response (NDR), Intrusion Prevention Systems (IPS), a nově se rozvíjející koncepty Security Service Edge (SSE) a Secure Access Service Edge (SASE). Tyto technologie a přístupy představují zásadní prvky v ochraně proti kybernetickým hrozbám, zvláště v kontextu rostoucího významu cloudových služeb a distribuovaných pracovních prostředí.

Zásadní myšlenkou tohoto projektu je, že ačkoliv existují rozsáhlé a sofistikované bezpečnostní řešení, stále se setkáváme s výzvami v oblasti jejich integrace, adaptace na nové hrozby a efektivní správy. Tyto výzvy se stávají ještě akutnějšími s příchodem SSE a SASE, které slibují vyšší míru integrace bezpečnostních funkcí přímo do síťové infrastruktury.

Výchozí podmínky pro řešení tohoto problému vyplývají z potřeby hloubkové analýzy současných bezpečnostních technologií, jejich možností, omezení a potenciálu pro integraci. Tento projekt se zaměří na posouzení, jak mohou různé bezpečnostní technologie, včetně firewallových systémů NDR spolupracovat a vytvořit komplexní bezpečnostní řešení, které je adaptabilní, efektivní a schopné čelit současným i budoucím kybernetickým výzvám.

## Cíle práce

Hlavním cílem této práce je provést komplexní analýzu současných metod Network Detection and Response (NDR) a navrhnout optimální řešení pro NDR a firewally, které bude vhodné pro implementaci v reálném prostředí. Pro dosažení tohoto hlavního cíle byla vytyčena následující specifická cílová nastavení:

Prozkoumat současné metody NDR: Tento podcíl zahrnuje detailní průzkum a zhodnocení stávajících metod NDR. Zaměříme se na jejich funkčnost, efektivitu a schopnost reagovat na nejnovější kybernetické hrozby. Cílem je poskytnout komplexní přehled současného stavu technologií NDR.

Analyzovat Open Source řešení NDR: Zde se zaměříme na detailní prozkoumání dostupných open source NDR řešení. Analyzovat budeme jejich výhody, nevýhody, možnosti implementace a efektivitu v porovnání s komerčními produkty.

Analyzovat komerční řešení: Tento podcíl se věnuje detailní analýze komerčně dostupných NDR řešení. Budeme hodnotit jejich funkčnost, výkonnost, kompatibilitu s existujícími systémy a celkovou efektivitu.

Vytvoření vlastního prototypu: V rámci praktické části projektu navrhneme a realizujeme prototyp založený na Mikrotik Routeru s Mirroring portem a Wiresharkem na Raspberry Pi. Cílem je demonstrovat praktickou aplikovatelnost teoretických znalostí a posoudit možnosti a omezení vlastního řešení.

Navrhnout optimální řešení pro NDR a firewall: Na základě získaných poznatků z analýzy a testování prototypu navrhneme optimální konfiguraci NDR a firewallu, která bude reflektovat aktuální bezpečnostní požadavky a trendů.

Konkrétní doporučení pro implementaci: Výstupem práce bude sada konkrétních doporučení pro implementaci navrženého řešení NDR a firewallu v reálném provozu. Tato doporučení budou sloužit jako průvodce pro organizace, které hledají efektivní a bezpečné řešení pro zabezpečení svých sítí.

# Metody

Kapitola obsahuje detailní popis způsobu řešení problému studentem. V závislosti na charakteru řešeného problému je tuto část práce možné rozdělit do více kapitol, kdy názvy kapitol jsou voleny konkrétněji s ohledem na jejich obsah.

Popisovány jsou postupy aplikované k dosažení výsledků práce a rovněž např. použité přístroje a materiál, metody zpracování dat a jejich statistického vyhodnocení apod. V případě měření s živými subjekty tato část práce obsahuje informaci, jak byly ošetřeny etické otázky výzkumu a charakteristiku subjektů dle zvyklostí v biomedicínských časopisech.

V případě, že text obsahuje matematický vzorec, na který se bude text později odkazovat, uvádějte vzorec na samostatném řádku, vycentrovaný na střed řádku a s číslem, které udává pořadí mezi číslovanými vzorci v kapitole, jako je tomu v příkladu vztahu pro elektrický odpor

, (2.1)

kde *U* je napětí a *I* je proud. Pokud je vzorec součástí věty, jako v předchozím vztahu (2.1), pokračujte za ním textem bez odsazení nového odstavce. V programu *Microsoft Word* doporučujeme pro sazbu vzorců a matematických symbolů namísto příkazu *Vložit rovnici* používat *Editor rovnic* (*Vložit*\*Objekt\Editor rovnic 3.0*) nebo doplněk *MathType*, který je ve verzi *Lite* volně k dispozici.

# Výsledky

Věnujte kapitolu pouze přehlednému podání výsledků, nikoliv jejich diskusi. Data uvádějte zejména v grafech a tabulkách. Preferovány jsou grafy – tabulky se všemi naměřenými hodnotami, ze kterých grafy vycházejí, lze umístit do příloh práce.

Výsledky mají vždy obsahovat hlavní text, který zasadí prezentované obrázky a tabulky do souvislosti s předchozím textem a čtenáře prezentovanými daty provede. Prezentování výsledků ve formě nekomentovaného obrázkového alba je v drtivé většině případů nevhodné.

Na každý obrázek musí být uveden odkaz v textu, který má formát jako v následující větě. Obrázek se vždy čísluje a popisuje pod obrázkem, viz příklad na Obr. 3.1.



**Obr. 3.1:** Tulipány před ozářením kryptonitem. Fotografie: autor.

Obrázky číslujte podle hlavní kapitoly, ve které se vyskytují. Podkapitoly se již neuvažují. To znamená, že obrázky v úvodu (typicky kap. 1) budou: Obr. 1.1, Obr. 1.2 atd. V metodách (typicky druhá velká kapitola) budou číslovány Obr. 2.1, Obr. 2.2, Obr. 2.3 atd.

Popis tabulky, na rozdíl od obrázku, je zpravidla nad tabulkou, viz Tabulka 3.1. Není nutné v něm opisovat celý obsah záhlaví tabulky, které následuje hned vzápětí. Jednotlivé proměnné v tabulce jsou řazeny do sloupců. V tabulce jsou nezávislé proměnné, kategorie probandů apod. řazeny vlevo, závislé proměnné vpravo. Jednotky uvádějte v kulatých závorkách v záhlaví tabulky, ne u každého čísla zvlášť. Vysvětlující poznámky (např. dosažená hladina významnosti, zda jsou data udávána jako průměr + směrodatná chyba průměru, jaký statistický test byl použit apod.) jsou umisťovány pod tabulku a odkaz na ně se udává jako horní index (symboly, čísla, písmena) na příslušném místě tabulky. Na každý obrázek a tabulku je třeba odkazovat z hlavního textu.

**Tabulka 3.1:** Reakční čas *T*20 signálu periferní saturace kyslíkem, *Sp*O2, měřený třemi různými přístroji.

|  |  |  |  |
| --- | --- | --- | --- |
|  | *T*20 (s) | | |
| Fáze | Root Radical-7 | Nellcor N-600 | Carescape B650 |
| Hypoxická | 52±15\* | 65±19\* | 56±15 |
| Hyperoxická | 43±14 | 55±28 | 49±15 |
| Hyperkapnická | 75±23 | 119±47# | 73±41# |

Data byla měřena pro shodnou skupinu 14 probandů a jsou uvedena jako aritmetický průměr ± směrodatná odchylka. Symboly \* a # značí statisticky významný rozdíl (*p*<0,05) časů pro shodnou fázi.

# Diskuse

V této části shrňte získané výsledky (hlavní zjištění práce) a následně tyto výsledky interpretujte s ohledem na cíle práce. Lze též získané výsledky a výstupy konfrontovat s výsledky a výstupy jiných autorů, výrobky jiných společností apod. Nezbytné je správné uvádění zdrojů (citace prací, které jsou zde porovnávány a diskutovány). Diskutují se rovněž limitace práce. Nakonec lze nastínit další směřování práce do budoucna, opatrně spekulovat o klinickém významu práce apod.

# Závěr

Závěr stručně shrnuje splnění vytyčených cílů práce.

Shrnutí splněných (nebo snad v menší míře nesplněných) cílů práce navazuje na úvod práce. Z dalších částí práce (metody, výsledky a diskuse) je přebíráno jen to nejpodstatnější a v minimální nutné míře – závěr práce nemá být zopakováním abstraktu, výsledků nebo diskuse. Konec závěru může obsahovat podložené spekulace o významu práce do budoucna nebo výrazná doporučení pro další výzkum nebo praxi, pokud z výsledků předkládané práce přímo vyplývají.

# Seznam použité literatury

V celém dokumentu je nezbytné dodržovat jednotný styl citací. Pokud jsou odkazy na bibliografické citace v textu práce uváděny v podobě čísel, např. [1], pak se čísla přiřazují jednotlivým citovaným dokumentům v tom pořadí, v jakém se na ně poprvé odkazuje v textu práce, a ve stejném pořadí jsou řazeny citace zdrojů v seznamu použité literatury.

Bibliografické citace doporučujeme formátovat podle normy ČSN ISO 690. Lze případně volit i jiný mezinárodně uznávaný formát citací. Příklady citací lze nalézt např. na následujících odkazech:

http://knihovna.cvut.cz/cs/seminare-a-vyuka/jak-psat/jak-psat-zaverecnou-praci

http://vutium.vutbr.cz/proautory/citace.doc

Pro spravování a formátování citací doporučujeme službu Citace PRO, kterou má ČVUT předplacenou. Služba je dostupná na adrese:

www.citace.com/citace-pro

1. GUYTON, Arthur C. a John E. HALL. *Textbook of medical physiology*. 11th ed. Philadelphia: Elsevier Saunders, 2006. ISBN 07-216-0240-1.

# Příloha A: Požadavky na formátování práce

* Pro hlavní text práce používejte patkové písmo (Times New Roman, Georgia, Garamond apod.), velikost 12. Rovnice, matematické symboly apod. by měly být sázeny stejným, nebo alespoň co nejpodobnějším písmem stejné velikosti. Popisy obrázků a tabulek sázejte stejným písmem se zmenšenou velikostí. Nadpisy, čísla stránek, případné záhlaví či zápatí apod. mohou být sázeny buď stejným písmem jako hlavní text, nebo písmem bezpatkovým (např. Calibri). **V celé práci musí být použity maximálně dvě různá písma.**
* Řádkování práce, odsazení odstavců, velikosti písma v nadpisech apod. definují přímo jednotlivé styly použité v této šabloně.
* Okraje stránek práce jsou vždy 2,5 cm na každé straně plus 1 cm u hřbetu práce (levá strana).
* Práce je tištěna jednostranně, na papír formátu A4.
* Stránky se číslují arabskými číslicemi počínaje první (titulní) stranou. Číslování stránek se zobrazuje až od první stránky obsahu, což znamená, že na titulní straně, v zadání, prohlášení, poděkování a abstraktech se číslo stránky neuvádí.
* Hlavní kapitoly práce, počínaje Úvodem a konče Závěrem, jsou číslovány arabskými číslicemi. Seznam použité literatury číslo nemá. Přílohy označujte velkými písmeny anglické abecedy.
* Každou hlavní kapitolu práce (nadpis 1. úrovně) začínejte na samostatné stránce.

# Příloha B: Základní typografické zásady

* Fyzikální a fyziologické veličiny a matematické proměnné se sázejí proloženě (kurzívou). Zkratky a symboly, pod kterými se neskrývá číselná hodnota, jsou sázeny normálním písmem – stejně jako označení fyzikálních jednotek.
* Jednotky veličin a symboly (například procenta) se v textu od číselných údajů oddělují nezlomitelnou mezerou. Zápis bez mezery má význam přídavného jména. Např. „10 Ω“ čteme „deset ohmů“ a „10Ω“ čteme „desetiohmový“.
* Nezlomitelnou mezeru je nutné v editoru textu vyznačit. Např. v aplikaci Microsoft Word se použije kombinace <Shift> + <Ctrl> + <mezerník>.
* Neslabičné předložky a spojky (netýká se „a“) nesmí zůstat na konci řádku. Proto za nimi používejte nezlomitelnou mezeru.
* Rozlišujte spojovník a pomlčku. Spojovník je krátká čára používaná ke spojení dvou slov (např. česko-anglický slovník). Pomlčka slouží k vyznačení prodlevy v textu, pak ji obvykle píšeme s mezerami, nebo k vyznačení rozsahu (5–10), kdy se píše bez mezer.

# Příloha C: Další doporučení pro přehlednost textu

* Obrázky a tabulky sázejte v textu samostatně, bez obtékání textu po stranách. Nevkládejte obrázky a tabulky na stránku před skončením odstavce. Zkontrolujte, že popis obrázku nebo tabulky zůstal na stejné straně jako vlastní obrázek nebo tabulka.
* První řádek odstavce by neměl zůstat sám na konci řádky (tzv. vdova) a poslední řádek odstavce by neměl zůstat sám na začátku nové stránky (tzv. sirotek).
* Veškeré zkratky, s výjimkou těch nejznámějších jako DNA, by měly být v práci vysvětleny při prvním výskytu v hlavním textu a současně také v abstraktu, pokud je nutné je v něm použít.
* Na rovnice odkazujte jejich číslem, a to až za jejich uvedením v textu práce.
* Všechny obrázky a tabulky v práci musí být odkazovány z hlavního textu pomocí svých čísel.

# Příloha D: Obsah přiloženého CD

Poslední přílohou práce je obsah přiloženého datového nosiče. Typ a povinný obsah datového nosiče je specifikován na stránkách FBMI ČVUT v Praze. Pro odevzdávané práce v předmětech typu Projekt X není odevzdání této přílohy nutné.

Dále na datový nosič umístěte přílohy, které není možné pro jejich rozsah nebo charakter umístit do výtisku práce, ale které mohou být důležité pro posouzení úplnosti a kvality splnění zadání práce, jako jsou různé konstrukční výkresy, zdrojový kód programů pro zpracování naměřených dat apod.