Využití segmentace LAN pro zabezpečení infrastruktury

Lubomír Langer

Bakalářská práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Lubomír Langer**
Osobní číslo:	**A20919**
Studijní program:	**B1032A020001 Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Využití segmentace LAN pro zabezpečení infrastruktury**
Téma práce anglicky:	**Using LAN Segmentation for Infrastructure Security**

Zásady pro vypracování

1. Popište současné hrozby v kyberprostoru, které je schopna segmentace sítě eliminovat.
2. Popište infrastrukturu, kterou chcete chránit. Specifikujte kritické body infrastruktury.
3. Navrhněte model segmentace pro vaši infrastrukturu.
4. Implementujte vaše řešení v testovací infrastruktuře.
5. Otestujte funkčnost vašeho řešení vůči vybraným útokům.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. REICHENBERG, Nimy a Mark WOLFGANG. Segmentace sítě: Pět kroků k lepší ochraně podnikové sítě. SecurityWorld. Praha: IDG Czech Republic, a.s., Seydlerova 2451, 2015, 2015(1), 48.
2. AKAMAI TECHNOLOGIES. Network Segmentation and Micro Segmentation in Modern Enterprise Enviroments [online]. Cambridge, Massachusetts, U.S.: Akamai Technologies, 2019 [cit. 2022-12-01]. Dostupné z: [https://www.akamai.com/site/en/documents/white-paper/akamai-network-segmentation-and-microsegmentation-in-modern-enterprise-environments-white-paper.pdf.](https://www.akamai.com/site/en/documents/white-paper/akamai-network-segmentation-and-microsegmentation-in-modern-enterprise-environments-white-paper.pdf.
3. ADAHMAN, Zillah, Asad WAQAR MALIK a Zahid ANWAR. An analysis of zero-trust architecture and its cost-effectiveness for organizational security. Computers & Security [online]. North Dakota State University (NDSU), USA; National University of Sciences and Technology (NUST), Islamabad, Pakistan: Elsevier, 2022, 5 May 2022, Revised 28 June 2022, 2022(122), 1-13 [cit. 2022-12-01]. Dostupné z: doi:[https://doi.org/10.1016/j.cose.2022.102911](https://doi.org/10.1016/j.cose.2022.102911 'https://doi.org/10.1016/j.cose.2022.102911')
4. FRIEDMAN, Jon a Bassam KHAN, SHUTTLEWORTH, Susan, ed. CYBEREDGE GROUP, LLC. Definitive GuideTM to Complete Network Visibility: How to Get High-Performing, Secure Networks While Staying Within Budget [online]. 1. Annapolis, USA: CyberEdge Group, 2020, 62 s. [cit. 2022-12-01]. ISBN 978-1-948939-10-2. Dostupné z: [https://cyber-edge.com/resources/definitive-guide-to-complete-network-visibility/](https://cyber-edge.com/resources/definitive-guide-to-complete-network-visibility/ 'https://.
5. DUBE, R., DIAMOND, Stephanie a Rev VARADHARAJ, ed. Internal Firewalls For Dummies®, VMware Special Edition [online]. 1. Hoboken, New Jersey, USA: John Wiley & Sons, 2021, 60 s. [cit. 2022-12-01]. ISBN 978-1-119-77296-5 (pbk); 978-1-119-77298-9 (ebk). Dostupné z: [https://www.vmware.com/content/dam/learn/en/apj/fy22/Internalfirewalls.pdf].

Vedoucí bakalářské práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **16. prosince 2022**
Termín odevzdání bakalářské práce: **5. června 2023**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 16. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne …….

Lubomír Langer v.r.

ABSTRAKT

V této bakalářské práci se zaměřením na vysvětlení konceptu segmentace, popíši aktuální hrozby v kyberprostoru a jak nás může segmentace sítě chránit před těmito hrozbami. Specifikuji kritické body infrastruktury. Dále popíšu infrastrukturu, kterou se snažím chránit, a ukáži na její kritické body. Představím vhodný model pro segmentaci této infrastruktury. Poté se pokusím tento model implementovat v testovací infrastruktuře a následně provedu několik testů, které ověří zabezpečení segmentované sítě.

Klíčová slova: Segmentace LAN, Síťová infrastruktura, Bezpečnost sítě, Kybernetické hrozby, Firewall, Kybernetická bezpečnost, Ochrana infrastruktury, Testování bezpečnosti

ABSTRACT

In this bachelor's thesis, I will primarily focus on elucidating the concept of segmentation. I will discuss the current threats in the cyberspace and demonstrate how network segmentation can help protect against these threats. I will identify the critical points in the infrastructure, and describe the specific infrastructure that I aim to protect, highlighting its potential vulnerabilities. I will propose a suitable model for the segmentation of this infrastructure. Subsequently, I will attempt to implement this model in a test infrastructure, followed by conducting several tests to verify the security of the segmented network.

Keywords: LAN segmentation, Network infrastructure, Network security, Cyber threats, Firewall, Cybersecurity, Infrastructure protection, Security testing

Úvodem bych rád poděkoval svému vedoucímu bakalářské práce Ing. Davidu Malaníkovi, Ph.D. za odborné vedení, pomoc a rady při zpracování této práce.

OBSAH

ÚVOD

„*Spoléhat se na demilitarizovanou zónu při ochraně sítě a dat je podobné jako uložit peníze do banky, která chrání vklady jedněmi vrátky a jedním strážným.*“ [1, str. 20].

Aby banky tyto zločince odradily volí vícestupňovou ochranu, peníze nejsou položeny volně, ale zamčené v bezpečnostních schránkách, ty jsou zase uzamčeny v trezoru, který chrání ostraha a nachází se v budově, která je sledována a za bránou, jež je zabezpečena. [1]

Na druhou stranu, když schránku zavřeme do další schránky a tu zavřeme do trezoru, který bude uložen ve větším trezoru za nespočtem dveří, tak jistě odradíme každého zloděje, ale to abychom si v případě, že potřebujeme získat obsah schránky, vzali na týden volno.

Proto je potřeba uvažovat o efektivitě dané ochrany, protože každá další překážka snižuje rychlost, s jakou je možno se k prostředkům dostat. Této efektivity docílíme tím, že nejdříve provedeme důkladnou bezpečnostní kontrolu příchozího. Následně má každý zaměstnanec přesně vymezená oprávnění, kam smí přistupovat a co může dělat. Toto hlídají čtečky karet, kamery a u velmi cenných prostorů hlídači. V případě neoprávněného jednání ihned informují velín, který proti takovému pokusu zakročí. Tím i při nižším počtu hlídačů a dveří jsme schopni odradit případné zločince.

Přesně takovým způsobem funguje i segmentace sítě. Jen si místo peněz představíme data, hlídači jsou Intruder Protection System (IPS) a Intruder Detection System (IDS) , kamerami různé nástroje pro sledovaní sítě, oprávnění jsou uložena v Active Direcory (AD) a čtečkami jsou Identity provider IDP servery.

Jak je z předešlého zřejmé, segmentování ochrany do více úrovňových stupňů s přísným režimem přístupu a ochrany je v případě ochrany dat nutností. Přesto se dodnes najde velké množství společností, které na toto bezpečnostní opatření stále nekladou dostatečný důraz.

Příkladem z nedávné doby je ransomwarový útok na Ředitelství Silnic a Dálnic (ŘSD). Tomuto programu se podařilo proniknout opravdu hluboko do sítě a na velmi dlouhý čas se mu podařilo zcela vyřadit nejen tok dopravních informací, ale i ekonomické, účetní a další systémy ŘSD. Problém byl, že tento ransomware dokázal zašifrovat i zálohy a způsobil škody z nichž některé mohou být i nevratné.[2]

Tomuto by se dalo předejít, pokud by zálohování bylo naprosto odděleno a nebylo možné v určitém časovém období tyto zálohy jakkoli měnit a mazat. Řešení by sice bylo finančně náročnější, protože by bylo potřeba platit externí úložiště, případně zřídit izolované

zálohovací datové centrum. Při zpětném pohledu by bylo, ale neocenitelné a řádově mnohonásobně levnější, něž kolik útok nakonec podnik, (tedy i nás, daňové poplatníky) stál.

Správné segmentování se netýká jen společností, ale i domácností. Protože s tím, jak jde doba kupředu, dnes čím dál tím větší podíl domácností používá techniku, která má přímé napojení na internet. Ať již jde o různé pomocníky Alexa, Goggle assist, ledničku, která vám je schopna objednat docházející potraviny, nebo televizi kterou ovládáte na základě hlasu. Toto souhrnně nazýváme IoT (internet of things). Díky každé z těchto věcí se útočník může dostat k potenciálně citlivým a zneužitelným datům, proto je i v tomto případě nutno mít se na pozoru a ani zde zabezpečení nepodceňovat.

I. TEORETICKÁ ČÁST

1 ÚVOD DO SEGMENTACE SÍTÍ

1.1 Pochopení struktury

Prvním, na co se musíme při správné segmentaci zaměřit, je pochopit strukturu firmy, nebo domácnosti. Tedy uspořádání toho, co se snažíme chránit. Toto je podobné klasickému zabezpečování objektu. [1]

Nejdříve si tedy provedeme bezpečnostní analýzu současného stavu. Zjistíme si, jaká data jsou pro nás nejcennější, jakým způsobem je možné je odcizit a identifikujeme bezpečnostní hrozby. To pro nás bude základním odrazovým můstkem pro to, jak toto riziko maximálně snížit.

1.1.1 Struktura domácnost

Jako příklad první uvedu domácnost. Vezmeme si rodinný dům s IP kamerovým a poplachovým zabezpečením, který je vybaven chytrými spotřebiči, televizí s hlasovým ovládáním, chytrým osvětlením, termostatem a solárními panely, které jsou ovládány inteligentní elektrickou sítí.[3] V domácnosti jsou tři členové s vlastním telefonem, herním PC se systém Windows, PlayStationem a dvěma pracovními notebooky s přístupem k elektronickému bankovnictví.

Nejvíce kritické pro nás v takovém případě bude zajištění elektrické energie a internetového připojení. Záznam a přístup ke kamerovému systému a také schopnost zabezpečovacího systému vyvolat poplach. Dalším je zajištění přístupu a bezpečnosti sítě a notebooků které mají přístup do bankovnictví.

Následuje zabezpečení sítě s chytrými spotřebiči, televizí, osvětlením, termostatem a bezpečným přístupem mobilních telefonů. Přístup PlayStationu a herního PC v rámci našich potřeb hraje nejmenší roli, ačkoli co se bezpečnostního rizika týká tak PC je tou největší hrozbou.

1.1.2 Struktura společnosti

Pokud se podíváme na strukturu společnosti, můžeme najít mnoho paralel se strukturou domácnosti, ale také mnoho specifických prvků, které vyžadují odlišné přístupy k zabezpečení. Mějme jako příklad bankovní instituci.

Stejně jako v domácnosti, kde jsme identifikovali kritické systémy, (elektrická energie, internetové připojení, zabezpečovací systémy a zařízení s přístupem k citlivým informacím,

například k bankovním účtům), musíme také v bankovní instituci identifikovat kritické systémy a data. V našem případě jsou to data o finančních transakcích (vkladech, úvěrech, platbách, splátkách klientů atd.) a komunikace s kontrolním orgánem, což je v České republice Česká národní banka.

Dále komunikace s klienty, dodavateli, zajištění permanentního bezpečného přístupu na internet a do jednotlivých bankovních aplikací. Tento přístup musíme zajistit nejen z budovy, kde je zaměstnání standardně vykonáváno, ale i vzdáleně z notebooku, tabletu, mobilu. Tyto aplikace poté musí mít neustále přístup ke svým datům, která jsou uložená v databázích.

Musíme hlídat a chránit data uložená na našich serverech, která zaměstnanci denně využívají ke své práci a v případě jejich poškození, či neúmyslného smazání je v krátkém čase obnovit. V případě cloudových úložišť definovat role a kontrolovat přístupy.

Samostatnou kapitolou jsou osobní údaje klientů, dodavatelů a zaměstnanců. Tato data musí být chráněna s vysokou prioritou, protože jejich únikem by byly dané osoby vystaveny vysokému riziku zneužití těchto dat, ale došlo by i k poškození značky a žalobám, což by vedlo k velkým finančním ztrátám.

Nakonec je potřeba zajistit i funkčnost a bezpečnost webových stránek a internetového bankovnictví. Delší výpadek kterékoli z těchto služeb totiž způsobí instituci ztrátu kreditu a v případě opakovaných výpadků, pak následně i ztrátu finanční projevující nedůvěrou veřejnosti ve schopnosti organizace.

1.2 Plánování

Poté, co si určíme základní strukturu společnosti, či domácnosti a zjistíme, co potřebujeme chránit, přistoupíme k další části, kterou je plánování. Využijeme data, získaná prvotní analýzou a na jejich základě naplánujeme, jak co nejlépe zajistit přístupnost, bezpečnost a obnovitelnost těchto dat a zdrojů.

Nejdříve je tedy nutné zhodnotit, izolovat a následně ochránit nejdůležitější komponenty. Následně seskupit položky, které mají na sebe návaznost dohromady. Uvedu příklad, který se bude týkat organizací.[1]

1.2.1 Plánování organizace

Můžeme všechny servery Windows umístit do jedné virtuální sítě LAN (VLAN). Stejně tak toto můžeme provést pro Linux, Unix atd... Následně máme díky nástrojům jako vmware možnost mít tyto prvky pod kontrolou na jednom místě.[1]

Další, co bychom si měli segmentovat jsou prvky infrastruktury mezi něž se řadí směrovače, přepínače, VPN, VoIP (Voice over Internet Protocol), které si vložíme do jedné VLAN. Následně bezpečnostní aktiva jako IDS, firewally, webové filtry a skenery které uzavřeme do jiné. [1]

Samostatnou VLAN bychom měli věnovat serverům finančního oddělení a HR tedy oddělení lidských zdrojů, tyto severy obsahují, zpracovávají a ukládají osobní data, která jsou osobní povahy a podléhají GDPR, a tudíž již ze své povahy si vyžadují zvláštní zacházení. [1]

Zaměřit se musíme také na různé skupiny zaměstnanců. Oddělit si potřebujeme správce serverů, které si vložíme do samostatné sítě VLAN. Stejně jako správce zabezpečení, které vložíme do jiné. Výkonnému managmentu můžeme z povahy jejich funkce také určit jinou skupinu, než ostatním zaměstnancům. [1]

V neposlední řadě nesmíme zapomenout ani na data zvláštní povahy. Mezi tato data řadíme data o kreditních kartách, která musí splňovat předpis PCI-DSS (Datového bezpečnostního standardu pro obor platebních karet), jehož dodržování je požadováno od všech subjektů, které ukládají, zpracovávají, nebo předávají údaje majitelů platebních karet.[4] Z tohoto důvodu je nutné vytvořit těmto datům vlastní izolovanou síť VLAN. [1]

1.2.2 Plánování domácnosti

U domácností je rozdělení o poznání snazší už jen z toho důvodu, že jediná data, která chráníme jsou ta naše. To ale neznamená, že bychom jejich ochranu měli podceňovat.

Pokud se vrátíme k našemu příkladu z předešlé části, určitě bychom si měli vytvořit samostatnou VLAN pro inteligentní elektrickou síť, jakožto kritickou část naší infrastruktury. Do další samostatné sítě si uzavřeme bezpečnostní a kamerový systém.

Inteligentní prvky domácnosti IoT vložíme také do své samostatné sítě. Notebooky, využívané k práci a mající přístup do bankovnictví, by také měly být od ostatních prvků odděleny ve vlastní VLAN.

Jako další si vytvoříme VLAN pro herní zařízení PlayStation a mobilní telefony. Samostatně izolováno by mělo být herní PC se systémem Windows. Důvodem je především velká pravděpodobnost napadení tohoto systému a s tím hrozící riziko napadení dalších systémů.

Můžeme ještě vytvořit nezávislou VLAN pro hosty, která je také potenciálně napadnutelná.[5]

1.3 Přístupy

Přístupy jsou alfou a omegou při zavádění segmentace, je hezké že máte oddělené sítě VLAN, když do každé z nich mají přístup všichni, ze všech ostatních sítí. Proto je nutné přístupová oprávnění důkladně promyslet.

Abychom si s tímto co nejlépe poradili, je nutné si pokládat ty nejjednodušší otázky. Kdo a proč? Případně na jak dlouho? Kdo a proč potřebuje mít přístup na směrovače a přepínače? Kdo a proč potřebuje mít přístup k serverům nebo datům kreditních karet, či k systémům lidských zdrojů a finančním systémům. Kdo a proč potřebuje mít možnost ovládat bezpečnostní kamery?[1]

V těchto otázkách musíte být naprosto nelítostní. Pokud není důvodná potřeba, není přístup. Nesmíte se nechat ovlivnit myšlenkou, že v budoucnu to potřeba bude. Až tato potřeba nastane, tak se uživateli přístup udělí. Musíte být důslední: v případě, že uživatel přestane přístup potřebovat, musí mu být odebrán. Nelze kontrolovat nic. o čem nemáte přehled. Z tohoto důvodu je zásadní vždy vědět, kdo má do kterých systémů přístup. Neomezujte se ale pouze na vnitřní prvky. Pokud jste v organizaci fungující výhradně na vnitrostátní úrovni, můžete blokovat zahraniční IP adresy, popřípadě provést selekci zemí se, kterými nepřicházíte do styku. [1]

Obecně je v základu nejlepší přistoupit pro každou VLAN k blokaci všeho a následně, na základě přísně daných postupů, udělovat přístupy. Musíme si uvědomit, že cílem je, aby do jednotlivých prvků neměl přístup nikdo jiný, než kdo jej skutečně potřebuje.[1]

Cílem segmentování je vytvořit dostatečné množství překážek pro zastavení, v horším případě alespoň značné zpomalení nezvaných návštěvníků, kterým se podaří prolomit vrchní vrstvu zabezpečení a maximálně omezit možné škody.

1.4 Aplikování segmentace

Segmentace sítě je ve velké organizaci velice důležitým, dlouhodobým a samozřejmě i nákladným projektem. Při správné implementaci jednotlivých prvků a dodržení pravidel je ale každý krok, který po této cestě ujde, navýšením úrovně zabezpečení.[1]

Toto se však netýká jen organizací. Jak jsem zmínil dříve i v případě domácností nám segmentace dokáže pomoci zvýšit zabezpečení našeho domova. Řešení v případě domácnosti nemusí být nijak nákladné, bude nám stačit VLAN switch a Router, popřípadě L3 switch, který v sobě skrývá obojí. Obojí se dá pořídit v řádu několika stovek až tisíců korun – záleží na kvalitě výrobku a potřebě domácnosti. Co je náročnější, je následné nastavení jednotlivých sítí a podsítí, kde už se očekává znalost uživatele.

Ve firemních řešeních se bavíme o nákupech v řádech statisíců, ale u velkých společností i v řádech desítek milionů korun.

Při zavedení segmentace ve firmě začneme, například na úrovni správce sítě, či správce serverů Windows. Nastavíme si síť VLAN s názvem „net-admins-workstations“ pro pracovní stanice a „net-devices“ pro směrovače a přepínače.[1]

V rámci implementace protokolujeme veškerou komunikaci a přenosy mezi jednotlivými segmenty. Tím zjistíme standardy sítě a základ pro její efektivní využívání. Poté, co informace získáme, začneme s postupnou blokací veškerých přístupů k této VLAN z ostatních zařízení. Naším konečným cílem je dostat se do výchozího bodu blokování, to znamená do bodu, kdy jediné, co má do sítě VLAN přístup, jsou procesy a lidé, nutné pro provoz a bezproblémové fungování.[1]

Takto budeme postupovat u všech prvků, u kterých budeme segmentaci provádět. Základem je, abychom si zachovali možnost k vynucení segmentace a monitoringu, aby ji budoucí změny přístupu neohrozily. Toto zopakujeme pro každou skupinu aktiv, dat a personálu.

1.5 Údržba

Přestože postavíte dům z nejlepších materiálů s použitím nejmodernějších technologií, nelze reálně očekávat, že vydrží stát věčně. Dříve nebo později bude potřebovat údržbu a čím déle s ní budete otálet, tím větší úsilí a náklady vás očekávají v budoucnu.[1]

Podobným způsobem, avšak v kratším časovém horizontu, funguje segmentace. Nelze předpokládat, že v případě jejího vytvoření se již o ni nebudeme muset starat. Toto si můžeme na určitou chvíli dovolit v případě domácí sítě, ale v případě společnosti, která je vlastně živým organismem, to možné není.

Na základě požadavků a potřeb organizace se budou měnit zásady přístupu k síti, pravidla definované na firewallech, směrovačích, nebo souvisejících zařízeních.

Úkolem je ohlídat, aby takové změny nenarušily strategii segmentace. To bude vyžadovat vysokou míru monitoringu a automatizace. Monitoring je také velmi důležitý v případě výpadku, nebo přerušení provozu z důvodu nesprávné konfigurace. K takové kontrole můžeme využít třeba program Zabbix. Což je dohledový software pro sítě, servery, virtuální stroje a cloudy.[1]

Pro velké množství společností jsou bohužel náklady spojené s tímto monitoringem, ať již v souvislosti s lidskými zdroji nebo s licencemi, dostatečným důvodem k tomu, aby se správné segmentaci vyhýbali. Tím se však vystavují vysokému riziku, jelikož špatná a špatně monitorovaná segmentace je skoro stejná jako žádná.[1]

Pokud se vrátím k úvodu, tak se to dá přirovnat k bance, která má sice zaměstnance, hlídače, dveře, trezory a bezpečnostní schránky, ale netušíte, kdo je kdo, kde se nachází a které dveře jsou otevřené a které zavřené. Ztráta nebo únik dat je pak jen otázkou času.

2 KYBERNETICKÉ HROZBY

Slovo „kybernetika“ známe již od padesátých let dvacátého století, tehdy však značilo kontrolování a ovládání pohybu strojů a zvířat, až poté následovalo slovo „kybernetické“ tedy počítačové. V devadesátých letech, na základě zvyšujícího se počtu kybernetických útoků vzniklo slovo kyberprostor, aby vymezilo místo odkud k útokům dochází.[6]

Kybernetické hrozby jsou velký problém. Kybernetické útoky mohou způsobit výpadky elektřiny, selhání vojenského vybavení a porušení národních bezpečnostních tajemství. Mohou vést ke krádeži cenných, citlivých dat, jako jsou lékařské záznamy. Mohou narušit telefonní a počítačové sítě nebo paralyzovat systémy, takže data nebudou dostupná. Není přehnané tvrzení, že kybernetické hrozby mohou ovlivnit fungování života, jak jej známe.[6]

Na základě dat ČSÚ (český statistický úřad) má v roce 2022 počítač již 78% českých domácností. Pokud do této statistiky zahrneme ještě uživatele tabletů číslo se nám zvýší na 81%. Celkově má u nás přístup na Internet 85% domácností a i když se toto číslo zdá vysoké, v celoevropském průměru z roku 2021 jsme lehce pod průměrem. ČR 89 %, průměr EU 92 % a Lucembursko dokonce 99% [7]

Podívejme se na data NÚKIB (Národní úřad pro kybernetickou bezpečnost) a CSIRT.CZ (Computer Security Incident Response Team), který je provozován sdružením CZ.NIC z roku 2021. NÚKIB obdžel 476 hlášení o kybernetických incidentech, z nichž řešil 157. Znamenalo to meziroční nárůst o 58 incidentů. Z těchto celkem 157 incidentů bylo 8 velmi významných. Nejčastějšími útoky byly phishing, podvodné e-maily a skenování vnější sítě. CSIRT.CZ řešil 1726 bezpečnostních incidentů a 1281 phishingových útoků. Celkově bylo spácháno 9518 trestných činů v oblasti kybernetické kriminality a kriminality páchané na internetu. Nejvážnějšími hrozbami pak byly nově zveřejněné zranitelnosti, phishing, nebo spear-phishing a ransomwarové útoky.[8]

2.1 Typy hrozeb a ochrana pomocí segmentace

Prakticky se kybernetické hrozby dělí na tři kategorie záměrů. První z nich je motivována finančním ziskem. Druhá získáním informací o podnicích, lidech, strategiích atd. Třetí kategorií je narušení. Může se jednat o výpadek webové služby, stejně jako o narušení chodu nemocnice. Obecně vzato, každá kybernetická hrozba patří do jedné z těchto kategorií. Pokud jde o technickou stránku věci, tam již mají útočníci daleko širší pole možností.[6]

2.1.1 Malware

Malware, je zkratka pro „škodlivý software“. Tento pojem označuje jakýkoli rušivý software vyvinutý kyberzločinci (často nazývanými „hackeři“) za účelem krádeže dat a poškození nebo zničení počítačů a počítačových systémů. Příkladem malwaru mohou být viry, červi, trojské viry, spyware, adware a ransomware.[9]

Ochrana:

V případě malwaru nám segmentace pomůže omezit jeho šíření oddělením jednotlivých částí sítě. Tím se zamezí přenosu malwaru z jedné části sítě do další, sníží se riziko širokého rozšíření malwaru a minimalizují se možné škody, způsobené infekcí [9]. Použití antivirových programů a pokročilých detekčních nástrojů může také posílit ochranu proti malwaru [10].

2.1.1.1 Virus

Základní definicí počítačového viru je, že je to program nebo software, připojený k jinému softwaru nebo počítačovému programu, aby narušil, nebo poškodil počítačový systém. Po stažení bude virus nečinný do té doby, dokud jej nespustíme. Pokud počítačový virus spustíme, bude narušovat chod systému nebo například mazat soubory. Důležitou vlastností viru je, že nelze dálkově ovládat. [9]

Ochrana:

Segmentace sítě snižuje riziko šíření virů tím, že odděluje různé části sítě a zabraňuje přenosu těchto škodlivých programů mezi jednotlivými částmi sítě. Tím se snižuje možnost širokého šíření virů a trojských koní a minimalizují se škody způsobené infekcí [9]. Pravidelné aktualizace antivirových programů a provádění bezpečnostních aktualizací systému mohou posílit ochranu proti těmto hrozbám [10].

2.1.1.2 Červ (worm)

Hlavní rozdíl mezi červem a virem je že lze dálkově ovládat, a především se velmi rychle replikuje na každé další zařízení v sítí. Oproti virům červ ke svému šíření nepotřebuje hostitelský program. Jinak se v zásadě od viru ve své funkci neliší. [9]

Ochrana:

2.1.1.3 Trojský virus/kůň

Trojský virus, více známý jako trojský kůň, pojmenovaný po Trojském koni z antické řecké historie, je specifickou podkategorií klasického viru. Maskuje se na první pohled jako užitečný program, který po svém stažení může získat přístup k citlivým informacím a následně je upravovat, zablokovat nebo odstranit. Trojské koně však nejsou navrženy k samostatné replikaci. [9]

Ochrana:

Viz 2.1.1.1 Virus

2.1.1.4 Spyware

Jak již jeho názvu plyne jedná se o software, který má za účel špehovat. Po jeho spuštění na počítači se hlásí vzdálenému uživateli a zasílá citlivé informace. Také může zajistit vzdálený přístup na stanici. Nejčastěji se s ním setkáváme při krádeži finančních údajů a přístupů k bankovnictví. Nejznámějším typem je tzv. keylogger, který zaznamenává stisky jednotlivých kláves. [9]

Ochrana:

Jak jsem již zmínil v předešlých případech i zde segmentace sítě pomáhá omezit šíření spywaru tím, že odděluje jednotlivé části sítě a zabraňuje přenosu škodlivého softwaru mezi segmenty. To může zamezit širokému šíření spywaru a minimalizovat možné škody způsobené infekcí [9]. Použití antivirových a antimalwarových řešení a sledování síťového provozu může zlepšit detekci a odstranění spywaru. [10]

2.1.1.5 Adware

Je dnes běžně využívaný především u reklamních agentur a na sociálních sítích. Sleduje váš pohyb a na základě toho vám nabízí různé produkty. Kromě toho, že může zpomalovat váš počítač, dá se využít i ke zločinným účelům. Například když vás přesměruje na nebezpečné stránky a v některých případech může obsahovat i trojské koně a spyware. [9]

Ochrana:

Segmentace sítě je účinným opatřením pro ochranu proti adware. Rozdělením sítě na samostatné segmenty umožňuje oddělit uživatele a zařízení s podobnými potřebami a oprávněními. Tím minimalizuje šíření adware mezi segmenty a chrání tak ostatní části sítě. [10]

2.1.1.6 Ransomware

Tento software získá přístup k vašim datům v systému a postupně tato data zašifruje a zamezí k nim přístup. Může se jednat o celý disk nebo datové pole. Následně se ozve skupina, která za odšifrování požaduje značnou částku. Data odemknou až po zaplacení výkupného. [9]

Ochrana:

I v tomto případě segmentace sítě přispívá k ochraně proti ransomwarovým útokům tím, že omezuje šíření škodlivého softwaru mezi jednotlivými segmenty. Pokud je ransomware omezen na jeden segment sítě, snižuje se jeho schopnost infikovat další systémy a získat kontrolu nad celou sítí. Kromě toho může segmentace usnadnit zotavení z ransomwarového útoku, protože jen omezený počet systémů je ovlivněn [11]. Použití pokročilých firewallů a IDS/IPS může také pomoci zlepšit detekci a blokování ransomwarových útoků [12].

2.1.1.7 Bezsouborový Malware

Tento typ malwaru zůstává v paměti RAM, je mnohem těžší jej odhalit protože se nenachází na pevném zisku a standartní sken jej nenajde. Tento malware má ale také omezenou životnost, protože zůstává v paměti jen do restartování počítače. To ale značně ztěžuje i možnosti případného vyšetřování. Příkladem je DNSMessenger, který umožňuje na stanici spouštět útočníkovi vlastní příkazy a následně získávat výsledky z jejich spuštění. [9]

Ochrana:

Ochrana proti bez-souborovému malwaru pomocí segmentace je zajištěná tím, že znemožňuje díky rozdělením jednotlivých částí sítě jejich napadení a případnou replikaci v systému. Tím se snižuje riziko rozšíření tohoto druhu malwaru a minimalizují se škody způsobené infekcí [9]. Použití pokročilých detekčních a ochranných nástrojů může zlepšit schopnost odhalit a blokovat bez-souborový malware [10].

2.1.2 Phishing

Útok přenášený e-mailem, který zahrnuje oklamání příjemce e-mailu, aby vyzradil důvěrné informace nebo stáhl malware kliknutím na hypertextový odkaz ve zprávě. [6] Nejčastější formou je snaha o získání citlivých informací o bankovní kartě nebo snaha o získání přístupů do internetového bankovnictví. V takovém případě nám útočník zašle podvodný email, který

se vydává za oficiální instituci (banku, poštu, státní instituci) a žádá nás o zadání těchto údajů.[13]

Ochrana:

I když segmentace sítě nemusí přímo chránit proti phishingovým útokům, může přispět k omezení dopadu útoku, pokud se útočníkovi podaří získat přístupové údaje k systémům nebo sítím [14]. Segmentace může zamezit útočníkovi přístup k dalším citlivým informacím nebo systémům, tím že omezuje jeho pohyb mezi segmenty [11]. Školení zaměstnanců v oblasti bezpečnosti a povědomí o hrozbách phishingu, spolu s použitím e-mailových filtrů a pokročilých detekčních nástrojů, mohou posílit ochranu proti těmto útokům [15].

2.1.3 Spear Phishing

Metoda phishingu, která se zaměřuje na konkrétní jednotlivce nebo skupiny v rámci organizace. Jedná se o účinnou variantu phishingu, zákeřné taktiky, která využívá e-maily, sociální média, rychlé zasílání zpráv a další platformy k tomu, aby přiměla uživatele prozradit osobní údaje nebo provádět akce, které způsobují kompromitaci sítě, ztrátu dat nebo finanční ztrátu. Zatímco phishingové taktiky mohou spoléhat na brokovnicové metody, které doručují hromadné e-maily náhodným jednotlivcům, spear phishing se zaměřuje na konkrétní cíle a zahrnuje předchozí výzkum.[14]

Ochrana:

Viz. 2.1.2 Phishing

2.1.4 Útok „Muž uprostřed“ (MitM).

Typ klamavého útoku. Útočník se usadí na pozici mezi odesílatelem a příjemcem elektronických zpráv a zachytí je. Útočník může tyto zprávy nejen přečíst, ale také pozměnit. Takže máte pocit, že komunikujete s příjemcem, ale informace které odesíláte a dostáváte jsou pozměněné. Tento útok se používá jak v armádě ke zmatení nepřítele, tak například ke způsobení finanční ztráty společnosti.[6]

Ochrana:

I když segmentace sítě snižuje riziko útoků typu Man-in-the-Middle tím, že odděluje komunikační cesty mezi různými segmenty sítě, je třeba zdůraznit, že zabezpečení neskončí pouze segmentací. Je důležité řešit také zabezpečení uvnitř jednotlivých segmentů, například v

rámci jedné VLAN nebo na úrovni jednoho switche. To znamená, že je třeba implementovat opatření, která zabraňují Man-in-the-Middle útokům i v rámci těchto menších segmentů. Taková opatření mohou zahrnovat použití šifrované komunikace, autentizace a kontrolu integrity dat. Tímto způsobem je možné posílit celkovou bezpečnost sítě a zajistit důvěrnost komunikace na všech úrovních sítě. [11;12]

2.1.5 Útok Denial of Service nebo Distributed Denial of Service Attack (DDoS)

Kde útočník převezme mnoho (možná tisíce) zařízení a použije je k vyvolání funkcí cílového systému, např. webové stránky, což způsobí jeho pád z přetížení poptávky. Cílem tohoto útoku je ostatním uživatelům odepřít, nebo znepřístupnit nějakou službu. K tomuto útoku nejdříve útočník infikuje velké množství počítačů z celého světa, čímž si vytvoří vlastní síť útočníků.[6]

Ochrana:

Odolnost vůči DDoS útokům může segmentace sítě zlepšit tím, že rozdělí síť na více částí, které mohou být lépe chráněny a spravovány [11]. Pokud je jedna část sítě napadena, ostatní části mohou zůstat v provozu, což zvyšuje celkovou odolnost sítě [11]. Navíc segmentace může usnadnit identifikaci a řešení útoků DDoS, protože zjednodušuje sledování provozu v jednotlivých segmentech [10]. Aplikace techniky scrubbingu (funkce údržby dat, která opraví nebo odebere nesprávná či nekompletní data.) a použití cloudových služeb pro odražení DDoS útoků může také posílit ochranu sítě [15].

2.1.6 Útoky na zařízení IoT

Poměrně novým odvětvím jsou útoky na zařízení IoT. Zařízení internetu věcí, jsou zranitelná vůči mnoha typům kybernetických hrozeb. Patří mezi ně i možnost, že hackeři převezmou zařízení, aby se stalo součástí výše zmíněného DDoS útoku. Nebezpečí představuje i neoprávněný přístup k datům která zařízení shromažďuje. Vzhledem k jejich počtu, geografickému rozložení a často zastaralým operačním systémům jsou IoT zařízení jedním z hlavních cílů.[6]

Ochrana:

Segmentace sítě může pomoci chránit zařízení IoT před útoky tím, že odděluje IoT zařízení do samostatných segmentů a zabraňuje přenosu škodlivého softwaru mezi různými částmi sítě. Tím se snižuje riziko kompromitace zařízení IoT a minimalizují se škody způsobené

infekcí [11]. Aplikace zásad nejmenších oprávnění, aktualizace firmwaru a pravidelné zabezpečení zařízení IoT mohou posílit ochranu proti těmto hrozbám [10].

2.1.7 Piggybacking

Piggybacking je využití cizího bezdrátového připojení, k přístupu k internetu bez autorizace. Cílem je získat bezplatný přístup k síti, což je často zneužíváno pro pokusy o škodlivé aktivity, jako je narušení dat a šíření malwaru. To může také vést ke zpomalení internetové rychlosti pro všechny systémy připojené k síti. I když k piggybackingu nedojde s úmyslem škodit, je stále nelegální, protože uživatel získává neoprávněnou výhodu ze služby, za kterou neplatil. [16].

Ochrana:

Pokud někdo provede piggybacking a získá neoprávněný přístup k síti, segmentace omezuje škodlivý dopad tím, že omezí pohyb útočníka v síti. I když se útočník dostane do jedné části sítě, nebude schopen přistoupit k ostatním částem bez dalších oprávnění nebo hesel. To znamená, že citlivé informace a důležité systémy budou lépe chráněny. [15].

2.1.8 Únik dat

Je účelová krádež dat třetí osobou, buď zvenčí, nebo takovou, která v instituci pracuje. Motivy pro úniku dat zahrnují zločin (krádež identity, vydírání), touhu poškodit instituci. Můžou v něm hrát roli i morální aspekty viz. Edward Snowden, či Panama pappers, ale rovněž také špionáž.[6]

Ochrana:

Segmentace sítě může pomoci předcházet úniku dat tím, že odděluje citlivé informace a systémy do samostatných segmentů a zamezuje přenosu těchto informací mezi různými částmi sítě. Tím se snižuje riziko úniku dat a zvyšuje ochranu citlivých informací. Může také přispět k ochraně proti hrozbám zevnitř organizace tím, že omezuje přístup k citlivým informacím a systémům na základě role a oprávnění uživatelů. Tím se snižuje možnost, že neautorizovaný uživatel získá přístup k citlivým informacím nebo systémům [11]. Implementace řízení přístupu, sledování uživatelského chování a pravidelné revize uživatelských oprávnění mohou posílit ochranu. [15]

3 KRITICKÉ BODY INFRASTURY

Jak je z předešlé části zřejmé hrozeb v kyberprostoru je opravdu veliké množství a segmentace je důležitou zbraní v tomto boji. K tomu, aby byla účinná, budeme ale potřebovat ještě další moduly, které nám s ochranou pomůžou.

Většina firem dnes využívá při ochraně svých IT systémů firewall společně s VLAN a systémem řízení vstupů ACL (Acces Control List). Doba se však mění a s nárustem virtualizace, SDN (Software Defined Networks) a větším využitím veřejné multi-cloudové infrastruktury, vznikla nová sada bezpečnostních problémů, které je třeba řešit. [11]

3.1.1 Firewall

Při hledání ideálního řešení se může podnik v rámci svých finančních prostředků při ochraně perimetru nejdříve zaměřit na tzv. Legacy Device (starší zařízení, která jsou sice plně funkční, ale již nemusí být podporována). Bohužel, tato zařízení jsou konstruována tak, aby monitorovala provoz, který se pohybuje klienta na server (North to South). Což ve své době bylo jistě dostačující, ale dnes kdy se velká část komunikace z důvodu virtualizace odehrává v rámci datového centra tedy ze serveru na server (East to West), je tato technologie nedostačující. [11]

Tradiční firewally, které jsou zaměřeny na zabezpečení perimetru, mohou mít omezenou schopnost chránit firmu před již infikovanými zařízeními. Historicky nebyly schopny zabránit útočníkům, kteří se již dostali do sítě pomocí infikovaného zařízení, v pohybu ze serveru na server. Rovněž s nárůstem šifrování TLS (Transport Layer Security) a snadným skrýváním škodlivého provozu piggybackingem přes otevřené legitimní porty aplikací, byla ztížena možnost odhalení a reakce na tato narušení [11].

Vývoj moderních firewallů nicméně vedl ke zlepšení těchto schopností. Nyní jsou často vybaveny vylepšenými funkcemi pro detekci a prevenci hrozeb, což umožňuje hlubší kontrolu paketů a lepší identifikaci a blokování škodlivého provozu i v případě, že je skrytý technikami jako je piggybacking nebo šifrován pomocí TLS [11].

Avšak samotný firewall, ať už je sebevyspělejší, neposkytuje dostatečnou ochranu v kontextu stále se vyvíjejících hrozeb kybernetické bezpečnosti. Navzdory vylepšením ve funkčnosti firewallů je stále důležité provádět další bezpečnostní opatření, jako je segmentace LAN, aby se další posílilo zabezpečení infrastruktury.

3.1.2 Řešení pomocí segmentace

S vědomím, že firewally, i virtualizované, samy o sobě nestačí pro ochranu hybridních cloudových datových center se podniky snaží uplatnit segmentaci v rámci east to west infrastruktury třemi základními způsoby. Jak jsem již uvedl výše, ve chvíli, kdy útočník prolomí firewall a má možnost se pohybovat mezi servery, nejúčinnějším způsobem jak mu tento pohyb maximálně ztížit, je právě segmentace. V zásadě existují tři základní typy segmentace sítě s využitím mikrosegmentace. Tyto tři typy lze navíc dohromady kombinovat a vytvářet tak mnohem sofistikovanější řešení. [11]

3.1.2.1 Segmentace prostředí

První a klíčovou fází každé strategie segmentace je segmentace prostředí. Jak již název napovídá jedná se rozdělení prostředí na dvě a více částí. Základem je oddělení vývojového a produkčního prostředí. Po tomto rozdělení, by mělo následovat vytvoření podrobnějších zásad. [11]

3.1.2.2 Segmentace aplikací

Pokud máme oddělené prostředí, můžeme se zaměřit dále. Řekněme, že máme aplikaci, která je pro chod podniku klíčová. Takovou aplikaci potřebujeme chránit, proto ji oddělíme v rámci prostředí od ostatních. Toto můžeme provést s každou kritickou aplikací. [11]

3.1.2.3 Segmentace úrovní

Při nejvyšší úrovni mikrosegmentace jsme schopni aplikaci kontrolovat dokonce na úrovni jednotlivých procesů. Můžeme zde vytvářet zásady pro správu komunikace mezi jednotlivými úrovněmi v rámci stejného aplikačního clusteru. Například řízením provozu mezi webovými servery, aplikačními servery a databázovými servery. [11]

3.1.3 VLAN

V rámci mnoha globálních vlivů, dnes velká část firem začíná, nebo již aktivně používá VLAN. Tyto virtuální místní sítě podnikům umožňují své prostředí rozdělit na různé části a následně každé z těchto částí přidělit svou komunikační cestu. K tomu lze využít již výše zmíněný firewall, přístupové brány, nebo kontrolu přístupů (ACL) na samotném směrovači. V každém případě, i když je VLAN dnes běžnou, nemusí být vždy tou správnou volbou. Důležitým aspektem jsou požadavky na ochranu vašeho prostředí. [11]

Důvod, který vede většinu firem do spárů segmentování za pomoci VLAN dokážeme pochopit opravdu snadno. Segmentaci lze totiž většinou provést i se stávající architekturou, a to na první pohled vyvolává pocit nižších nákladů a jednoduché implementace. Jenže jak už tomu bývá všechno není takové, jak se na první pohled zdá. [11]

Zavedení segmentace sítě pomocí VLAN rozhodně nezvládne malá, ale ani střední firma, pokud není specializovaná na IT, pomocí vlastních sil. Tudíž se řešení prodraží o síťové specialisty, kteří budou danou architekturu vytvářet. Ti, aby mohli začít, potřebují znalost serverů a jejich závislosti v jednotlivých segmentech, následně nám vytvoří a realizují požadovanou síťovou konfiguraci. Tím se cesta k implementaci segmentace pomocí tohoto řešení nejen prodlužuje, ale i znatelně prodražuje, a to se nebavíme o správě, případných rekonfiguracích a úpravách. [11]

3.1.4 Segmentace VLAN a internet

Nejdříve je dobré se zamyslet, z jakých důvodů VLAN byly vytvořeny. Jejich prvotním účelem bylo snížení přetížení sítě, nikoli její omezení. Proto v rámci segmentace není chytré je k tomuto účelu využívat, jelikož to spolu sebou nese spoustu omezení. [11]

3.1.4.1 Cloudová technologie

První, co je dobré si uvědomit je že VLAN ani jiné tradiční politiky segmentace nelze rozšířit na cloud. V případě, že pro kontrolu přístupu uživatelů používáte interní segmentované brány ISFW (Internal Segmented Firewall) nebo kontrolu uživatelských přístupů ACL, bude lepší pro cloud využít softwarově definované sítě SDN. Obvykle bývá toto řešení zajištěno dodavatelem třetích stran. [11]

3.1.4.2 Kontejnery

Jak sám název napovídá, jedná se o něco společného, uzavřeného v jednom boxu. V tomto případě je to kernell (jádro operačního systému), na kterém běží operační systém a jsou odděleny pouze části uživatelského prostoru. Proto vystavení takového kontejneru do cloudu by znamenalo veliké riziko, které segmentací vyřešit nelze. [11]

3.1.4.3 Omezení protokolů

Jak jsem napsal již na začátku této části, VLAN nebyly vytvořeny pro segmentaci, proto mají omezení na 4096 segmentů. To naneštěstí znamená že jejich využití ve velkých

datových centrech není optimální. Ještě je dobré zmínit, že podrobnější přístupy k segmentaci tato omezení nemají. [11]

3.1.5 Segmentace aplikací – řízení na 4. aplikační vrstvě

K vyřešení značné části problémů zmíněných dříve, pomáhá právě segmentace na 4. aplikační vrstvě. V cloudových prostředích nám pomáhá pomocí bezpečnostních skupin. V lokálních virtualizovaných prostředí pomocí firewallů, kde se pravidla aplikují na hypervizory a není tedy potřeba samostatná konfigurace pro zařízení. [11]

Tím, že nám nabízí možnost řízení přístupu aplikace na jednotlivých úrovních služeb, jsme schopni ovlivnit, že každá služba aplikace bude mít přístup pouze tam, kam to opravdu potřebuje (load balancery, databáze, aplikační servery). Tím, že každá z těchto úrovní dostane svoje vlastní pravidla, snížíme možnost kompromitace mezi nimi na minimum. To znamená, že můžeme například zabránit určitým databázím v komunikaci s internetem, nebo zajistit, aby útočník, který se dostal do prostoru prostřednictvím jednoduchého load balanceru, nedokázal získat přístup k citlivým informacím v databázové vrstvě. [11]

I toto řešení má však své limity. Nejdříve je třeba si uvědomit, že ve 4. aplikační vrstvě se pohybujeme na úrovni portů a IP adres. V případě dnešních hrozeb, kdy útočník dokáže podvrhnout systému svoji IP adresu, nebo využít piggibacking na povolených portech, aby pronikl do naší sítě, potřebujeme řešení, které bude ještě více sofistikované. Navíc toto řešení nám nedokáže pokrýt boční pohyb v rámci sítě. Útočníci jsou tedy schopni zaútočit přes otevřený port a následně se díky pohybu na 7. aplikační vrstvě dostat kam, potřebují.

Jak tedy již většina společností zjistila, ačkoli je segmentace na 4. aplikační vrstvě krok správným směrem, sama o sobě nestačí. [11]

3.1.6 Mikro-segmentace až do 7. aplikační vrstvy

Naproti tomu je 7. aplikační vrstva velice účinná při omezování bočního pohybu a to i v rámci aplikačního clusteru. Na této vrstvě dochází k integraci síťových služeb s operačním systémem. Mezi protokoly, které tato vrstva využívá, patří HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SMTP (Simple Mail Tranfer Protokol), RIP (Routing Information Protocol) a další. Nejnovější pokroky v segmentaci jsou tedy schopny kontrolovat aktivity nejen na 4. aplikační vrstvě ale i na této 7. vrstvě. Tím se samozřejmě benefit tohoto řešení násobí a umožnuje odhalit potenciální

hrozby už podle špatného hashe (unikátní otisk souboru, který se mění pokaždé, když se změní jeho obsah) a to i v případě, že útočník zrcadlí nějaký proces nebo cestu. [11]

Segmentace na 7. aplikační vrstvě nám navíc umožňuje provádět velmi specifický seznam pravidel povolených procesů a komunikací (whitelisting), kde všechny ostatní jsou principiálně zablokované. [11]

3.1.7 Architektura nulové důvěry (Zero Trust Architecture, ZTA)

Pojem „nulová důvěra“ ZTA zavedl Kindervag et al. [17]. Kdy John Kindervag publikoval zprávu Forrester Research, která se zabývala modelem nulové důvěry podporující přísnější snahy o kybernetickou bezpečnost. Ačkoli tedy tato koncepce není nic nového a její popularita neustále roste, přesto se organizace do tohoto řešení zdráhají investovat. Zvýšenou pozornost vzbudila až nyní Bidenova administrativa, když podepsala nařízení o mandátu národní kybernetické bezpečnostní centrály (2021). [12]

Architektura nulové důvěry spočívá, jak už z název napovídá z konceptu „nikdy nevěř, vždy ověřuj“ (Never trust, always verify), který zajišťuje kybernetickou bezpečnost eliminací důvěry a průběžným ověřováním síťových požadavků. Tato architektura je zde proto, aby nahradila VPN a poskytla osamocený přístup k aplikacím a datům. [12]

ZTA je forma zabezpečení kde je základem identita. Teprve až základě ověření identity získáváte přístup ke zdrojům organizace. Z tohoto důvodu je veškerý provoz dovnitř i ven organizace kontrolován a zaznamenáván. Každá identita je také průběžně ověřována při pobytu v síti. [12]

II. PRAKTICKÁ ČÁST

4 POPIS CHRÁNĚNÉ INFRASTRUKTURY

V předešlých částech práce jsme se dozvěděli, jakým nebezpečím musíme čelit a jakým způsobem můžeme, nebo spíše potřebujeme chránit naši síť, pokud ji chceme zabezpečit proti vnějším, ale i vnitřním útokům.

Pro lepší představu se budu snažit zajistit ochranu třeba menší až střední bankovní instituce, ale tento model by měl být aplikovatelný i na jiné společnosti.

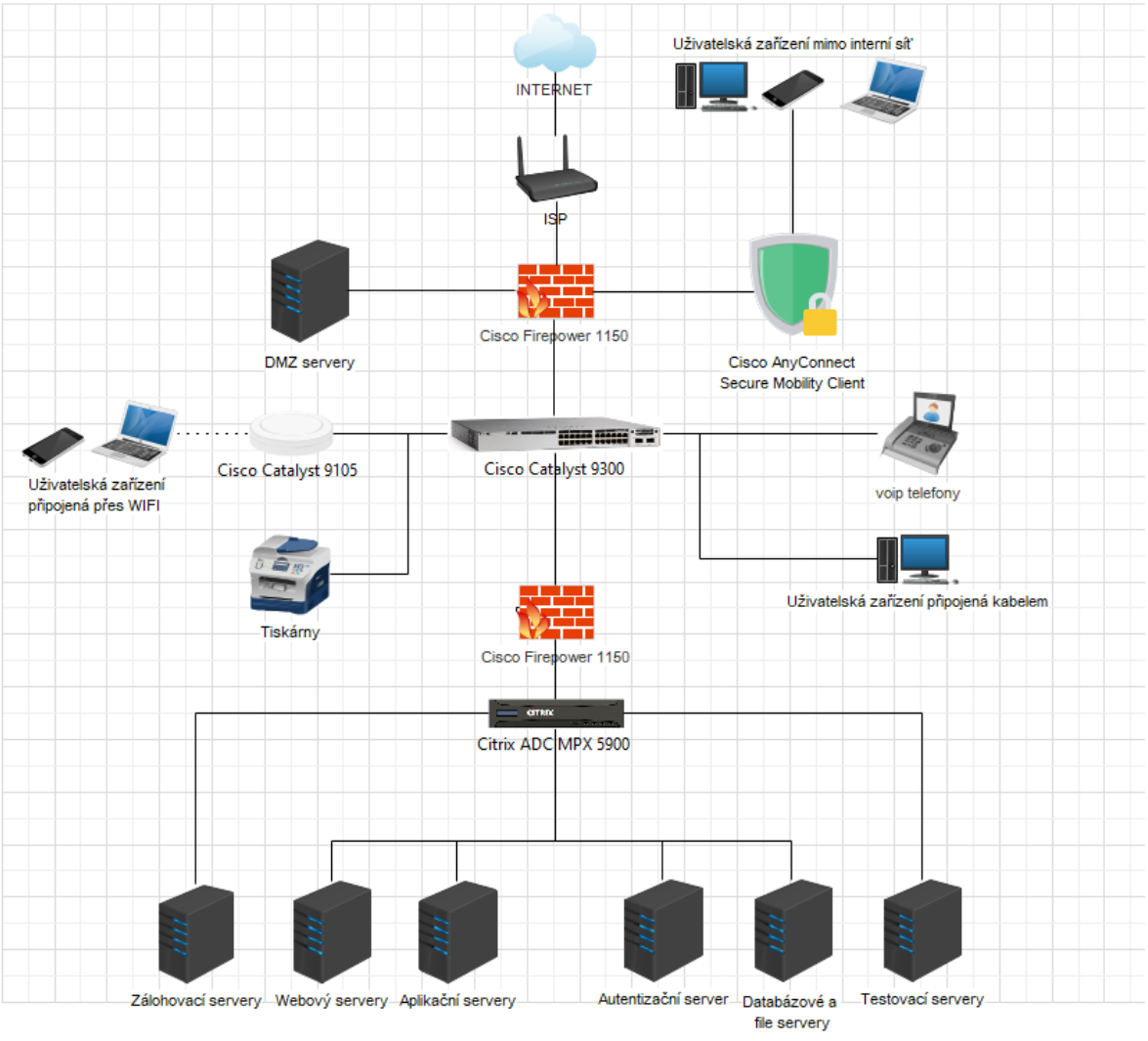
V tomto konkrétním případě musím brát v potaz požadavek, aby se uživatelé mohli připojit do sítě nejen přímo v sídle společnosti, ale i vzdáleně. Ve společnosti bude možnost připojení jak kabelem, tak bezdrátově. Vzdálené připojení bude zajištěno VPN. Společnost bude používat VoIP telefony a sdílené tiskárny. Dalším požadavkem bude testovací prostředí a dostatečně zabezpečený zálohovací server. Společnost spravuje velké množství dat, takže bude potřeba i pro ně najít vhodné místo. Používá velké množství aplikací a webových služeb, takže bude nutné najít vhodné řešení pro jejich optimalizaci a zabezpečení.

5 MODEL SEGMENTACE

Rozhodl jsem se navrhnout hvězdicovou topologii pro střední společnost. Jako hlavní switch použiji řadu Cisco Catalyst 9300, která poskytuje vysoký výkon, míru škálovatelnosti a pokročilé funkce pro zabezpečení a analýzu sítě.

V mé architektuře se o bezpečnost bude starat externí a interní NG (new generation) firewall Cisco Firepower 1150 společně s netscalerem Citrix ADC MPX 5900, který bude fungovat zároveň i jako load balancer pro servery.

Možnost připojení do sítě bude pomocí VPN Cisco AnyConect Secure Mobility Client přes externí firewall. Přes ten půjdou i veškeré DMZ (demilitarizovaná zóna) servery. Samostatnou VLAN bude mít i testovací server a zálohovací server, abych zajistil maximální bezpečnost zálohovaných dat.



Obrázek 1. Model sítě v aplikaci Wondershare EdrawMax - vlastní tvorba

5.1 Architektura systému

Na počátku mého systému je ISP router, který je připojen k cloudu. Tento router je prvním bodem připojení k této síti a umožňuje přístup k internetu. Za tímto routerem je umístěn externí firewall Cisco Firepower 1150, který chrání síť před nebezpečnými hrozbami z internetu.

Externí firewall je připojen k switchi Cisco Catalyst 9300, který je jádrem této sítě. Tento switch umožňuje připojení různých zařízení k síti, včetně APs, VOIP zařízení, tiskáren a počítačů. Každé z těchto zařízení je připojeno do vlastní VLAN, což umožňuje izolaci a řízení provozu mezi nimi.

Switch je dále také připojen k internímu firewallu Cisco Firepower 1150, který poskytuje další důležitou vrstvu zabezpečení pro tuto síť. Za tímto firewallem je umístěn Citrix ADC MPX 5900, který je zodpovědný za optimalizaci provozu mezi různými servery.

Na Citrix ADC jsou připojeny různé servery, včetně aplikačního, webového, zálohovacího, databázového, souborového, testovacího a autentizačního serveru. Každý z těchto serverů je připojen do své vlastní VLAN pro izolaci a řízení provozu.

5.2 Nastavení systému

1. **Konfigurace routeru ISP:**
   Router bude konfigurován tak, aby poskytoval přístup k internetu pro naši síť. Bude nastaven tak, aby blokoval veškerý nežádoucí provoz a povolil pouze nezbytnou komunikaci.

2. **Konfigurace firewallů:**
   Externí a interní firewall budou konfigurovány tak, aby blokovaly veškerý nežádoucí provoz a povolovaly pouze nezbytnou komunikaci. Budou také konfigurovány tak, aby monitorovaly a hlásily jakékoli podezřelé aktivity.

3. **Konfigurace switchů a VLAN:**
   Switch bude konfigurován tak, aby správně směroval provoz mezi různými VLAN. Každá VLAN bude mít svá vlastní pravidla pro izolaci a řízení provozu. Pro dosažení tohoto cíle budeme muset provést několik kroků. Nejprve vytvoříme potřebné VLANy na switchi a přiřadíme porty k jednotlivým VLANám.

Poté definujeme a implementujeme ACLs pro ovládání komunikace mezi VLANami, kde konfigurujeme pravidla, která povolují nebo blokují určitý provoz mezi VLANami. Dále aktivujeme funkci Port Security, abychom zabránili neautorizovanému přístupu k portům, a nakonfigurujeme maximální počet povolených MAC adres na portu. Kromě toho povolíme DHCP Snooping, abychom zabránili neoprávněnému poskytování DHCP služeb v síti, a nakonfigurujeme ARP Inspection pro ochranu proti ARP spoofingu a dalším útokům.[18]

4. **Konfigurace APs, VOIP, tiskáren a počítačů:**

   Tato zařízení budou konfigurována, aby zahrnovala následující prvky. Zařízení budou konfigurována tak, aby komunikovala pouze s povolenými službami a zařízeními v příslušných VLAN. Pro zabezpečení připojení budou využity různé metody autentizace, jako je standard WPA2/WPA3 pro bezdrátovou autentizaci, protokol 802.1X pro autentizaci na síťové úrovni a použití uživatelských jmen a hesel. Šifrování bude zajištěno pomocí AES pro zabezpečení dat v síti a vytvořením šifrovaného tunelu pomocí VPN pro komunikaci mezi vzdálenými sítěmi nebo zařízeními. Takto nakonfigurovaná síť bude poskytovat bezpečnou komunikaci a ochranu dat.[19]

5. **Konfigurace VPN:**

   Při nastavování Cisco AnyConnect Secure Mobility Clienta zvolím silné autentizační metody, včetně dvoufaktorové autentizace (2FA) a použití certifikátů pro ověření identity klienta i serveru. Nastavím integraci RADIUS autentizace pro centrální správu autentizace a autorizace uživatelů a využiji také možnosti integrované Windows autentizace pro pohodlné přihlašování. Tímto způsobem zajistím vysokou úroveň zabezpečení a ochrany při vzdáleném přístupu k síti pomocí Cisco AnyConnect Secure Mobility Clienta.

6. **Konfigurace Citrix ADC a serverů:**

   Citrix ADC bude konfigurován tak, aby optimalizoval provoz mezi různými servery. Každý server bude konfigurován tak, aby komunikoval pouze s povolenými službami a zařízeními a byl chráněn před neoprávněným přístupem.

5.3 Funkčnost systému

Po dokončení výše uvedených kroků bude můj systém plně funkční a připravený k použití. Každé zařízení nebo server bude moci komunikovat s ostatními zařízeními nebo servery v rámci své vlastní VLAN, a komunikace mezi různými VLAN bude řízena pomocí ACLs.

Připojení k internetu bude zabezpečeno prostřednictvím routeru ISP a externího firewallu, zatímco interní firewall a Citrix ADC budou chránit naše servery a optimalizovat jejich provoz. VPN klient umožní bezpečný vzdálený přístup do naší sítě.

Výsledkem tedy nakonec bude robustní, bezpečný a výkonný systém, který bude schopen zvládnout širokou škálu aplikací a služeb. Systém bude navržen tak, aby byl snadno spravovatelný, škálovatelný a odolný vůči výpadkům.

5.4 Popis jednotlivých částí

5.4.1 Switch Cisco Catalyst 9300

Přepínače řady Cisco Catalyst 9300 jsou navrženy pro podnikové prostředí a patří do rodiny Catalyst 9000. Tyto přepínače slouží k transformaci sítě pro hybridní svět, kde se pracoviště nachází na kterémkoli místě, koncové body mohou být různé a aplikace jsou hostovány na různých místech. [17]

Klíčové vlastnosti:

- Až 1 TB šířky pásma pro stackování s technologií Stackwise-1T
- Flexibilní a husté uplinkové možnosti s modulárními uplinky, včetně SFP, SFP+, QSFP, QSFP+, RJ-45 a další.
- Smíšené stackování s kompatibilitou zpětně
- Vysoký počet Multigigabit portů
- Vysoká hustota 90W UPoE(Universal Power over Ethernet) + portů
- Technologie StackPower s kompatibilitou zpětně
- 100G IPsec v hardwaru
- Bezpečné tunelové připojení
- Zvýšené možnosti hostování aplikací
- Integrace s ThousandEyes pro lepší dohled nad sítí
- Ochrana investic díky kompatibilitě s Catalyst 9300

Přepínače Cisco Catalyst 9300 Series jsou základem pro softwarově definovaný přístup (SD-Access) v rámci Cisco Digital Network Architecture (Cisco DNA). Cisco DNA poskytuje zjednodušené nasazení zařízení, sjednocené správy drátových a bezdrátových sítí, virtualizaci sítě a segmentaci, skupinové politiky a kontextovou analýzu. Cisco DNA Software umožňuje flexibilní modely licencování a snazší správu a aktualizaci softwaru. [20]

5.4.2 Firewall Cisco Firepower 1120

Cisco Firepower 1150 je firewall platforma, která poskytuje pokročilou ochranu proti hrozbám, snadnou správu a vysokou odolnost pro podnikové prostředí. Tento model nabízí rychlosti 5,3 Gbps a 6,1 Gbps a je vybavený 8x RJ45, 2x SFP s 2x 10G SFP+ porty pro konektivitu. [21]

Klíčové vlastnosti:

- Centralizované řízení
  centralizovaná konfigurace, záznamy, sledování a hlášení jsou prováděny správcem Threat Defence (FMC) nebo alternativně z cloudu pomocí Cisco Defense Orchestrator.
- Vysoká propustnost
  Model 1150 nabízí 5,3 Gbps propustnost pro firewall a AVC (Application Visibility and Control), 4,9 Gbps pro FW + AVC + IPS (Intrusion Prevention System), pro IPSec VPN 2,4 Gbps a 1,4 Gbps pro TLS.
- AVC (Aplication Visibility and Control)
  podpora více než 4 000 aplikací, stejně jako geolokace, uživatelů a webových stránek.
- Cisco Security Intelligence –
  služba, která poskytuje informace o bezpečnostních hrozbách v reálném čase. Využívá globální sítě senzorů a poskytuje informace o známých hrozbách, sítích s vysokým rizikem a škodlivých IP adresách.
- Cisco IPS (Intrusion Prevention System)
  může pasivně detekovat koncové body a infrastrukturu pro korelaci hrozeb a indikátory kompromisu (IoC).
- Cisco Malware Defense pro sítě
  umožňuje detekci, blokování, sledování, analýzu a obsažení cíleného a trvalého malwaru, řeší útoky během a po nich.

Může být také doplněna o integrovanou korelaci hrozeb s Cisco AMP (Advanced Malware Protection) pro koncové body.

Mezi další patří Cisco Malware Analytics sandboxing, URL filtrování, automatické aktualizace hrozeb a IPS signatur, integraci s ekosystémem třetích stran a otevřených zdrojů, vysokou dostupnost a sdružování a technologie Cisco Trust Anchor. Tyto funkce zajišťují, že Cisco Firepower 1150 je schopen poskytnout kompletní a efektivní řešení pro ochranu podnikových sítí. [21]

5.4.3 Netscaler Citrix ADC MPX 5900

Netscaler MPX 5900 nabízí výkonné hardwarové řešení pro doručování aplikací a vyvažování zátěže. Kromě toho poskytuje možnosti pro zvýšení bezpečnosti webových aplikací a SSL offloading. Toto řešení je ideální pro správu webových aplikací s několika gigabity provozu a poskytuje vysoké zabezpečení webových aplikací spolu s podporou SSL. Navíc je Netscaler MPX vybaven integrovaným WAF (Web Application Firewall), který ještě více zvyšuje zabezpečení vašich webových aplikací. [22]

Funguje jako flexibilní all-in-one platforma pro doručování a zabezpečení aplikací, která automatizuje doručování aplikací na velkém měřítku pomocí přístupu IaC (Infrastructure as Code) při nasazení vašich ADC (Aplication Delivery Controler). S jednotným operačním systémem pro všechny formy a centralizovanou správou je snadné udržovat konzistentní správu vašich ADC napříč hybridními a více-cloudovými prostředími. Netscaler je vybaven 6x RJ45 a 2x SFP+ porty. [22; 23]

Klíčové vlastnosti:

- Zrychlení webových stránek a snížení latence díky architektuře s jedním průchodem.
- Komplexní zabezpečení pro všechny aplikace a koncové body API ve všech prostředích, včetně integrovaného WAF.
- Bohatá analytika a reálné vhledy pro optimalizaci výkonu a rychlejší řešení problémů.
- Vysoký výkon doručování aplikací a řízení provozu L4-L7.
- Integrace s hlavními veřejnými cloudy, platformami Kubernetes, správci kontejnerů a populárními nástroji pro IaC a sledování.
- Škálovatelné DNS rozlišení na hranici sítě místo v datovém centru pro rychlejší reakci na uživatelské DNS dotazy až do 1 milionu požadavků za sekundu.

- Snadná automatizace a správa ADC na základě definovaných politik, které nevyžadují znalosti programování.

Velkou výhodou je také NetScaler Intelligent Traffic Management, který používá telemetrické údaje, a umožňuje tak obejít přetížené části sítě a směrovat provoz do míst s nejnižším vytížením. Tím zajišťuje optimální uživatelský zážitek z aplikací. [22]

5.4.4 AP – Cisco Catalyst 9105

Řada Cisco Catalyst 9105 Access Points jsou vysoce flexibilní, odolné, zabezpečené a inteligentní zařízení pro podnikové sítě. Tyto přístupové body jsou ideální pro sítě všech velikostí a nabízejí škálovatelnost pro růst požadavků IoT. Navíc, podporují nejnovější inovace a technologie. [24]

Klíčové vlastnosti:

- Wi-Fi 6 (802.11ax) - podpora nejnovějšího standardu pro vyšší efektivitu a výkon
- Uplink/downlink OFDMA (Orthogonal Frequency-Division Multiple Access) – snižuje režii a latenci díky lepšímu rozdělení šířky pásma
- Downlink MU-MIMO – zlepšuje propustnost díky rozdělení prostorových proudů mezi zařízeními
- BSS (Basic Service Set) coloring – umožňuje simultánní přenosy a zlepšuje výkon sítě
- Target Wake Time – šetří energii u bateriově napájených zařízení
- Intelligent Capture – poskytuje hlubokou analýzu a sledování více než 240 anomálií
- Aplikační hosting – zjednodušuje a zefektivňuje nasazení IoT
- Bluetooth 5 - umožňuje polohové služby a sledování majetku
- Cisco Embedded Wireless Controller – zjednodušuje správu a nasazení sítě
- Kontejnerová podpora pro aplikace – umožňuje výpočetní operace na okraji sítě pro IoT aplikace
- Bezpečná infrastruktura – zabezpečení založené na Cisco Trust Anchor Technologies
- Podpora Cisco DNA Software – poskytuje analýzu, zabezpečení a automatizaci pro celou síť

Catalyst 9105 Access Points jsou dostupné v různých variantách pro montáž na strop (9105i) nebo na zeď (9105w). Díky své škálovatelnosti, podpoře nejnovějších technologií a Wi-Fi 6 standardu, jsou tato zařízení ideální pro podnikové sítě různých velikostí. [24]

5.4.5 VPN Cisco AnyConnect Secure Mobility Client

Cisco AnyConnect® Secure Mobility Client je řešení pro zabezpečené připojení k firemním sítím, které je navrženo pro mobilní zařízení, notebooky a stolní počítače. Nabízí spolehlivé a snadno nasaditelné šifrované síťové připojení a trvalý přístup do firemních zdrojů pro zaměstnance na cestách. [25]

Klíčové vlastnosti produktu:

- Široká kompatibilita: Klient AnyConnect je dostupný pro Apple iOS, Android, Windows Phone 8.1 a novější, BlackBerry 10.3.2 a novější, vybraná zařízení Amazon Kindle a Fire Phone, Google Chrome OS, Windows 7, 8, 8.1, 10, macOS 10.10 (Yosemite) a novější, Linux (64bitové verze Ubuntu, Red Hat, CentOS a další).
- Optimalizovaný přístup k síti: Klient automaticky přizpůsobuje tunelování pro nejefektivnější metodu na základě síťových omezení a podporuje DTLS, IPsec IKEv2 a TLS (HTTP přes TLS/SSL) pro šifrovaný přístup k podnikovým aplikacím.
- Síťová viditelnost: Nabízí mobilní viditelnost prostřednictvím modulu Network Visibility a zachytávání toků koncových bodů s bohatým kontextem uživatele, koncového bodu, aplikace, místa a cíle.
- Přívětivost pro mobilitu: Klient automaticky obnovuje připojení po změně IP adresy, ztrátě konektivity nebo uspání zařízení.
- Šetrnost k baterii: Klient je kompatibilní s režimem spánku zařízení, což šetří baterii.
- Silné šifrování: Podporuje silné šifrování, včetně AES-256 a 3DES-168, a další pokročilé šifrovací algoritmy.
- Možnosti autentizace: Nabízí širokou škálu možností autentizace, včetně RADIUS, RSA SecurID, Active Directory, Kerberos, digitálních certifikátů a dalších.
- Konzistentní uživatelský zážitek: Poskytuje plně tunelovaný režim klienta, který podporuje uživatele vyžadující konzistentní zážitek podobný LAN.
- Centralizovaná kontrola politik a správa: Politiky mohou být předkonfigurovány nebo konfigurovány lokálně a mohou být automaticky aktualizovány z VPN bezpečnostní brány.
- Flexibilita při přiřazování IP adres: Klient podporuje různé mechanismy pro přiřazování IP adres, včetně statických adres, interního poolu, DHCP a RADIUS/LDAP.

Díky široké kompatibilitě, optimalizovanému přístupu k síti, silnému šifrování a centralizované správě je Cisco AnyConnect Secure Mobility Client ideálním řešením pro zabezpečení firemních sítí a ochranu dat zaměstnanců na cestách, ať už používají mobilní zařízení nebo notebooky. [25]

5.4.6 Servery

První servery, na které narazíme jsou DMZ servery, může se jednat například o emailové servery, různé FTP servery, webové servery. V praxi tyto servery bývají často napojeny na externí switch. V mém případě jsem ovšem zvolil napojení na externí firewall, a to hned ze dvou důvodů. Prvním je že Cisco Firepower 1150 je vybaven dostatečným počtem portů pro vytvoření oddělených VLAN. Druhým, že připojení přes firewall zajišťuje lepší kontrolu a vyšší bezpečnost datového toku.

Ostatní servery jsou schovány hluboko v nitru infrastruktury za interním firewallem a netscalerem. Důvodů je hned několik. Netscaler Citrix ADC MPX 5900 dokáže zajistit dostatečnou propustnost pro jednotlivé servery a navíc vyvážit jejich zatížení. Má dostatečný počet portů pro vytvoření dostatečného počtu VLAN a navíc je jeho součástí i WAF, který ještě zvýší samotnou bezpečnost sítě, což v kombinaci s interním firewallem snižuje při správném nastavení možnost napadení na minimum.

5.4.7 Uživatelé

Uživatelé mají tři možnosti, jak se do sítě přihlásit. První možností je využít zařízení připojená přes pevnou linku uvnitř společnosti, pro kterou je vytvořena na switchi samostatná VLAN. Druhou možností je využít uvnitř společnosti bezdrátové připojení přes VLAN Cisco Catalyst 9105. Poslední a třetí možností je přihlásit se z firemního zařízení mimo společnost. V tomto případě se o autentizaci a vytvoření tunelového připojení bude starat Cisco AnyConnect Secure mobility Client. O správnou IP adresu se postará Cisco Catalyst 9300, který je Layer 3 switch a má přímo v sobě DHCP integrováno.

5.4.8 VoIP telefony a tiskárny

Jako tiskárnu můžeme zvolit HP LaserJet Enterprise MFPs.
Společnost HP je dlouholetým hráčem v oblasti tiskáren a jejich LaserJet Enterprise multifunkční tiskárny jsou vhodné pro podnikové prostředí. Nabízí vysokou kvalitu tisku, robustní bezpečnostní funkce a snadnou integraci do sítí.

Z VoIP telefonů zvolíme Cisco 8800 Series IP Phones.

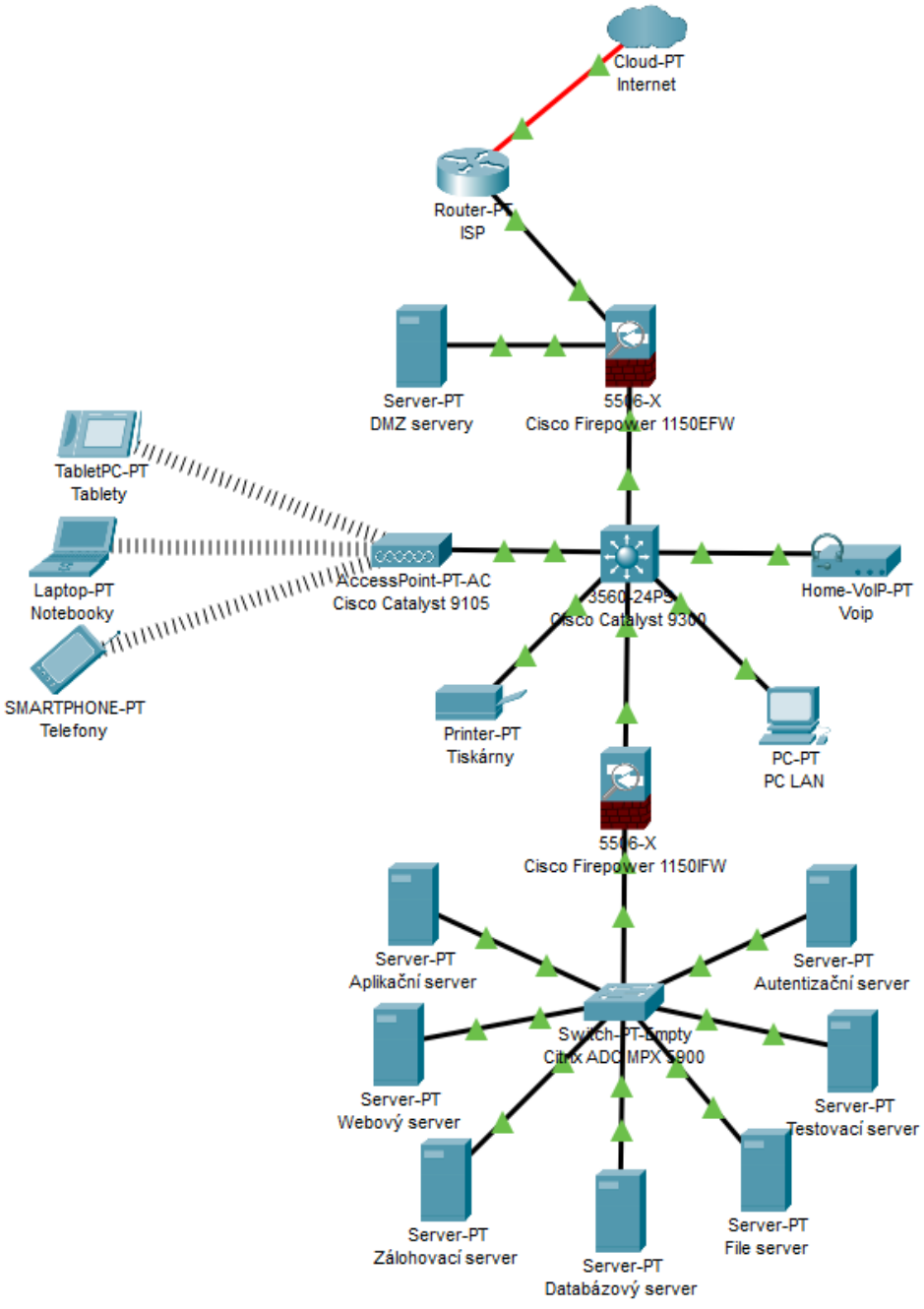
Tato řada telefonů nabízí vysokou kvalitu hlasu, robustní bezpečnostní funkce a širokou škálu modelů pro různé potřeby. Některé modely také podporují video hovory a mají vestavěné wifi.

Jak v případě tiskáren, tak VoIP telefonů, přiradíme každému z prvků vlastní VLAN a budou připojeni přímo ke switchi.

6 IMPLEMENTACE A TESTOVÁNÍ

Protože jsem používal především produkty Cisco a nedisponuji rozpočtem, který by mi dovoloval si zařízení pořídit, rozhodl jsme se pro otestování funkčnosti této sítě použít nastroj Cisco packet tracer, což je nástroj pro simulaci sítě. Jedním z hlavních důvodů byla i jednoduchost. Vytvořil jsem model své architektury v tomto programu viz. Obrázek 2.

6.1 Cisco Packet Tracer



Obrázek 2. Architektura sítě v aplikaci Citrix Packet tracer- vlastní tvorba

Měl jsem v plánu vytvořit hvězdicovou topologii pro středně velkou společnost, s Cisco Catalyst 9300 jako hlavním switchem, poskytujícím vysoký výkon, škálovatelnost a pokročilé funkce pro zabezpečení a analýzu sítě. Místo toho jsem byl nucen využít switch Cisco 3560-24PS. Ačkoli je to kvalitní zařízení, nedisponuje stejnou úrovní výkonu a škálovatelnosti jako Catalyst 9300.

Také jsem měl v plánu do architektury začlenit externí a interní NG firewall Cisco Firepower 1150, ale místo toho jsem se musel spolehnout na vlastnosti firewallu integrovaného v Packet Traceru 5506-X. Toto zařízení nemá pokročilé funkce NG firewallu, což znamená, že moje síť nebude mít stejnou úroveň ochrany. Navíc jsem měl v plánu využít Netscaler Citrix ADC MPX 5900 jako load balancer pro servery. Toto zařízení však program Cisco Packet Tracer nenabízí. Místo toho jsem byl nucen jeho funkci suplovat pomocí dostupného switche Switch-PT, což výrazně omezuje funkčnost a efektivitu sítě.

Při implementaci mého návrhu hvězdicové topologie jsem původně zamýšlel využít AccessPoint Cisco Catalyst 9105 pro jeho vysokou výkonnost, pokročilé bezpečnostní funkce a efektivní integraci do komplexních sítí. Avšak, kvůli omezením programu Cisco Packet Tracer, jsem byl opět nucen použít alternativu, AccessPoint-PT-AC.

V procesu konfigurace sítě jsem narazil na další omezení programu, tentokrát při pokusu o nastavení firewallu Cisco ASA 5506-X jako DHCP serveru, což bylo důležitou součástí mého původního plánu. Cisco ASA 5506-X je ve skutečnosti schopen tuto roli plnit, ale program Cisco Packet Tracer tuto funkci v plné míře nepodporuje.

Možnou variantou by bylo zařadit do architektury samostatný DHCP server. To jsem ale nezvolil. Abych zachoval jednoduchost a čistotu původního návrhu, rozhodl jsem se pro ruční přiřazení IP adres a výchozích bran jednotlivým zařízením, což je detailně popsáno v Tabulce1.

Tabulka 1. Přidělení IP

Zařízení	Rozhraní	IP adresa	Maska sítě
Router	Internet	10.0.0.1	255.255.255.252
Router	Externí FW	10.0.0.5	255.255.255.252
Externí firewall	Rozhraní k routeru	10.0.0.6	255.255.255.252
Externí firewall	DMZ rozhraní	10.0.1.1	255.255.255.0
Externí firewall	DMZ servery	10.0.2.10	255.255.255.0
Switch	AP	10.0.3.1	255.255.255.0
Switch	VoIP	10.0.4.1	255.255.255.0
Switch	Tiskárny	10.0.5.1	255.255.255.0

Switch	PC-Lan	10.0.6.1-10.0.6.254	255.255.255.0
Rozhraní k switchi	Rozhraní ke switchi	10.0.7.1	255.255.255.0
Interní firewall	Rozhraní k Net-scaleru	10.0.8.1	255.255.255.0
Netscaler	Aplikační servery	10.0.9.1	255.255.255.0
Netscaler	Webové servery	10.0.10.1	255.255.255.0
Netscaler	Zálohovací servery	10.0.11.1	255.255.255.0
Netscaler	Databázové servery	10.0.12.1	255.255.255.0
Netscaler	File servery	10.0.13.1	255.255.255.0
Netscaler	Testovací server	10.0.14.1	255.255.255.0
Netscaler	Autentizační server	10.0.15.1	255.255.255.0

V dalším kroku, jsem se rozhodl, že se podívám na provoz firewallů, nastavení ACL, povolování provozu ven a dovnitř, pravidla na DMZ a další konfigurace týkající se omezení provozu. V grafickém rozhraní, které program nabízel toto nebylo možné, tak jsem se o to pokusil přes CLI. I v tomto případě jsem však narazil na limitace programu, který mi toto nedovolil. Rozhodl jsem se nakonec od implementace přes Cisco packet tracer upustit. Možnost těchto nastavení byla totiž zásadní pro ověření bezpečnosti sítě v mé práci.

Přemýšlel jsem proto nad využitím pokročilejších nástrojů, jako je Cisco VIRL (Virtual Internet Routing Lab) nebo GNS3 (Graphical Network Simulator-3). Tyto sofistikované simulátory sítí nabízejí širší spektrum funkcí a možností konfigurace, jako jsou ACL, DMZ a firewall. Jsou to nástroje, které by mohly překonat omezení, na která jsem narazil při používání Cisco Packet Traceru.

6.2 GNS3

Nakonec jsem si vybral GNS3, který je zdarma a k vytvoření virtuální stanice využil VMware Workstation. Nicméně nepříjemný překvapením pro mne bylo, že naprostá většina zařízení, která jsem potřeboval pro své testování využít byla placená. To samo o sobě by byla jen další v řadě překážek a pokusil bych se použít zařízení podobná. Nepřekonatelným problémem se však stalo, že na mém osobním počítači, který jsem měl pro testování dedikovaný a který má dostačené prostředky RAM se mi GNS3 nepodařilo korektně zprovoznit. Jako poslední možnost jsem si vypůjčil notebook, který měl fungovat jen pro účel tohoto testování. Měl však pouhých 8 Gb paměti a při současném běhu Windows 10 bylo nereálné cokoli testovat.

6.3 Firemní prostředí

Rozhodl jsem se tedy pro tyto překážky a technické problémy najít jiné řešení. Díky svému zařazení mohu totiž nahlédnout pod pokličku systémům IT ve společnosti, kde pracuji. Protože v této práci chci seznámit čtenáře s fungováním sítí LAN a jejich využitím pro zabezpečení sítě, zkusím to demonstrovat na mnou navržených testech v reálné síti. Tyto se budou konat na mě přiděleném firemním zařízení a serveru který mám ve správě.

6.3.1 Představení prostředí

S ohledem na bezpečnost nemohu detailně popisovat jednotlivé prvky sítě. Popíšu tedy pouze hrubě architekturu. Ve společnosti využíváme dva switche externí a interní, Na externím jsou DMZ servery a jde přes něj i připojení VPN, na interním se nachází všechny ostatní servery, jako jsou databázové, aplikační, testovací, zálohovací a další s náležitě rozdělenými VLAN. Mezi nimi se nachází firewall s množstvím pravidel a samozřejmě korektně nastaveným ACL. K připojení na internet z vnitřní sítě musíte využít Proxy server v opačném směru pak potřebujete ještě VPN. Netscaler je využit především k loadbalancigu webových a aplikačních serverů. Zálohování je prováděno Imutabilně, tedy bez možnosti jakéhokoli zásahu. K ověření uživatelů a jejich přístupů na servery a do služeb se využívá IdP a ADFS.

O kontrolu zabezpečení se stará komplexní systém zabezpečení, v němž nechybí ani IPS/IDS, skeny zranitelností a SIEM. Na stanicích pak nalezneme, krom různých pravidel přes GPO (Group Policy Object) například DLP, šifrování disku a antivirový program. Omezení připojení do firemní sítě je pak limitováno navázání korektního připojení do VPN.

6.3.2 Testování

Provedu několik základních testů VPN a na serveru v DMZ za firewallem.

6.3.2.1 Testování VPN

K přístupu do VPN používáme 2FA autentizaci. Po ověření se již každý účet chová jako by byl v interní síti.

1. **Test přístupu do interní sítě**

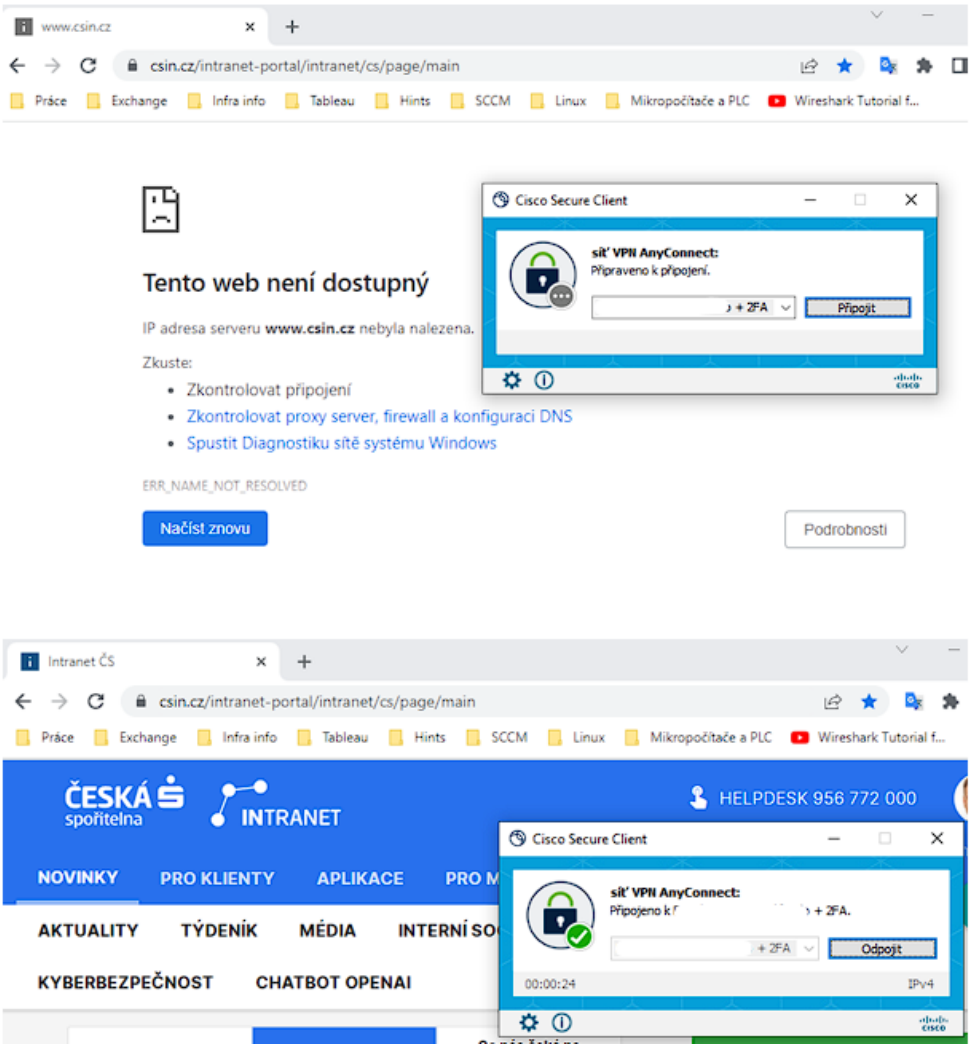
   Nejdříve provedu test přístupu na intranet bez VPN a s VPN

   Předpokládaný výsledek:

   Bez připojení k VPN zařízení nebude mít přístup do interní sítě.

Výsledek:

Vše proběhlo dle očekávání a přístup do interní sítě byl možný až po přihlášení k VPN.



Obrázek 3. Ukázka připojení do interní sítě před a po připojení do VPN

2. Test úniku IP adresy (IP Leak Test)

V tomto testu zjišťujeme, zda je IP adresa uživatele skutečně skryta při použití VPN.

Předpokládaný výsledek:

Uživatel by neměl vidět svou skutečnou IP adresu, ale místo toho IP adresu poskytnutou VPN službou. Důvodem je, že když uživatel používá VPN, jeho skutečná IP adresa by měla být skryta. Toto je klíčové pro zajištění uživatelova soukromí a bezpečnosti, chránění jeho identity, předcházení sledování, ochraně před potenciálními útoky a umožnění přístupu k obsahu s geografickými omezeními. Pokud tedy skutečná IP adresa uživatele není skryta, může to signalizovat problém s konfigurací VPN nebo potenciální bezpečnostní hrozbu.

Výsledek:

Po připojení se adresa změnila na adresu poskytnutou službou VPN

Obrázek 4. Ukázka IP adresy
před a po připojení do VPN
z webu https://ipleak.net/

3. Test úniku DNS (DNS Leak Test)

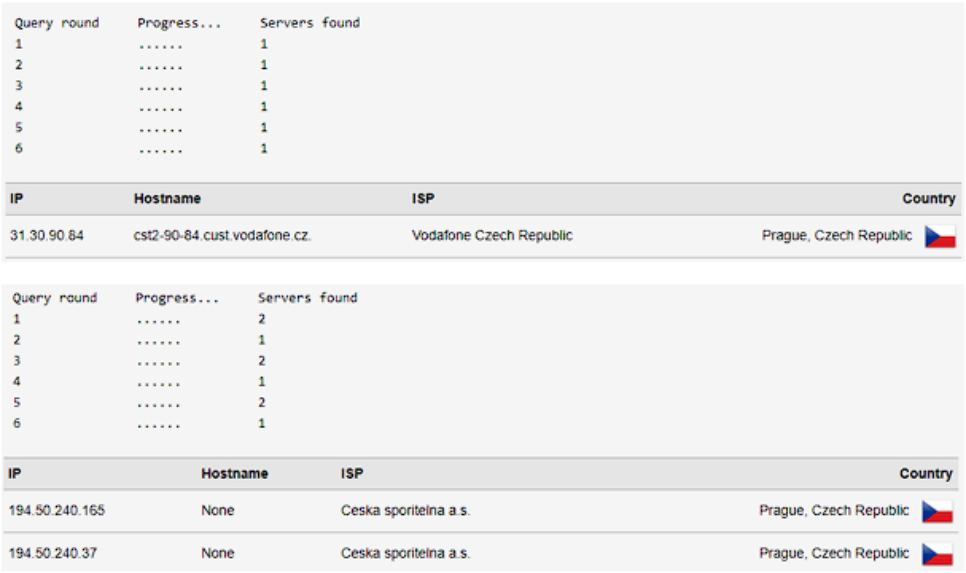
Podobně jako test úniku IP, tento test kontroluje, zda se veškerý DNS provoz odesílá přes VPN a nikoli přes standardního poskytovatele DNS.

Předpokládaný výsledek:

Všechny DNS požadavky by měly být směrovány přes VPN.

Výsledek:

Všechny dotazy byly efektivně směrovány přes interní DNS server společnosti, jak je patrné z provedeného testu, a to jak při pohledu z vnější, tak vnitřní perspektivy. Po navázání zabezpečeného spojení probíhala komunikace přes VPN tunel.



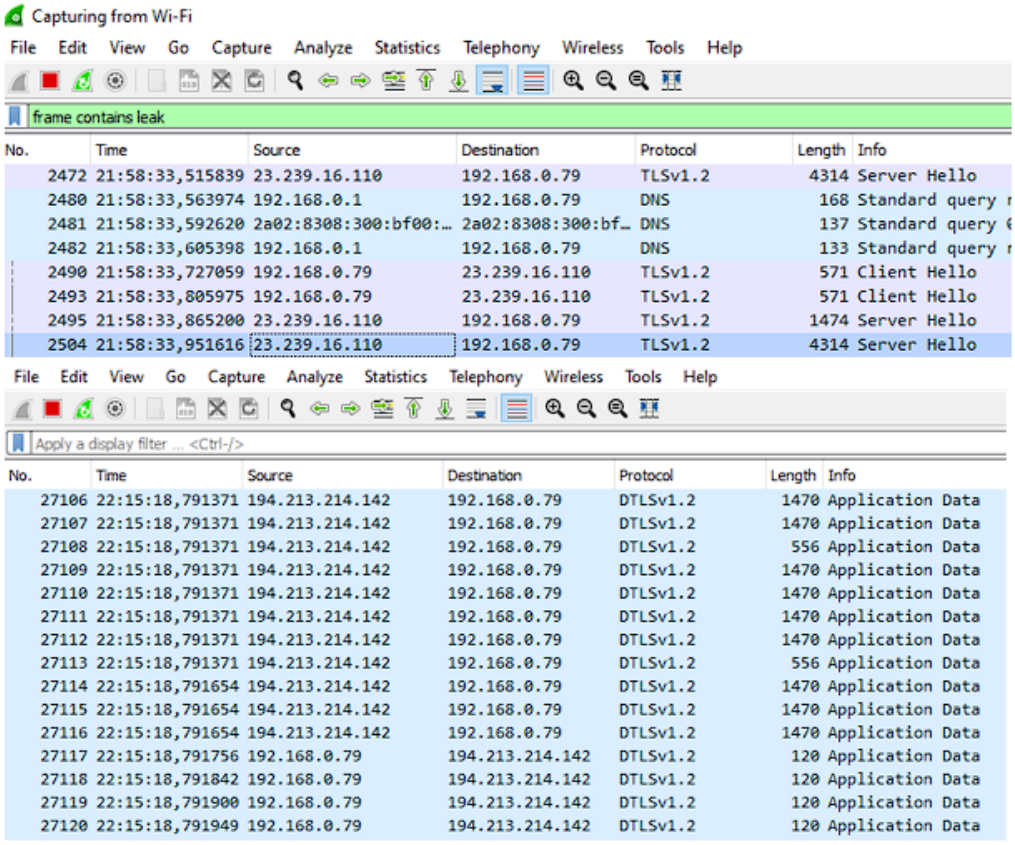
Query round	Progress...	Servers found
1	.....	1
2	.....	1
3	.....	1
4	.....	1
5	.....	1
6	.....	1

IP	Hostname	ISP	Country
31.30.90.84	cst2-90-84.cust.vodafone.cz.	Vodafone Czech Republic	Prague, Czech Republic

Query round	Progress...	Servers found
1	.....	2
2	.....	1
3	.....	2
4	.....	1
5	.....	2
6	.....	1

IP	Hostname	ISP	Country
194.50.240.165	None	Ceska sporitelna a.s.	Prague, Czech Republic
194.50.240.37	None	Ceska sporitelna a.s.	Prague, Czech Republic

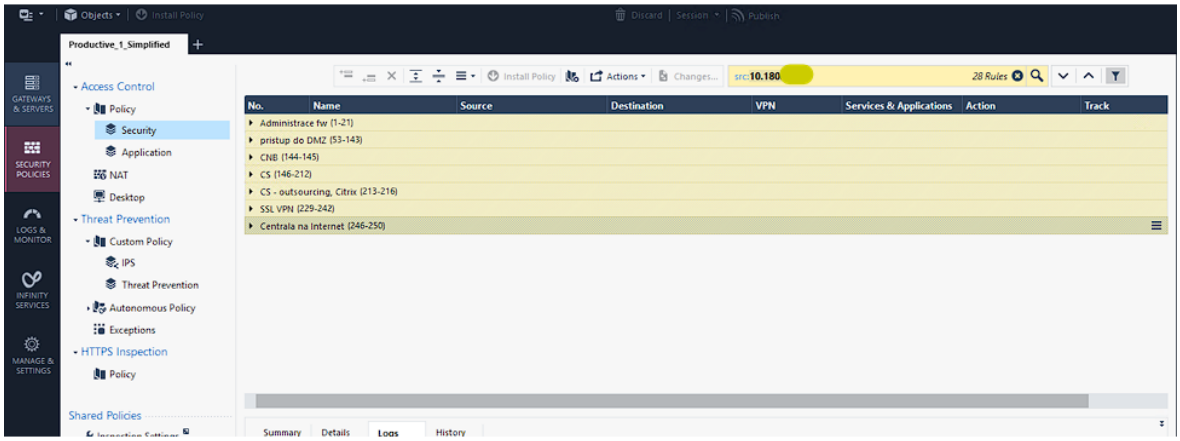
Obrázek 5. Ukázka DNS záznamu před připřipojením k VPN a po připojení z webu https://www.dnsleaktest.com/



Obrázek 6. Komunikace v průběhu testu před a po navázání spojení přes VPN
zdroj: WireShark

6.3.2.2 Test serveru

Nyní provedu testy na serveru. Na samotném serveru je nastaveno 28 bezpečnostních pravidel pro povolenou komunikaci. Vyzkoušíme však ty, které povolené nejsou. Tím je přímá komunikace do internetu mimo Proxy a přístup na DMZ.



Obrázek 7. Ukázka rozhraní pro správu ACL a pravidel na Firewallu v aplikaci Check Point SmartConsole

1. Skenování portů pomocí Nmap

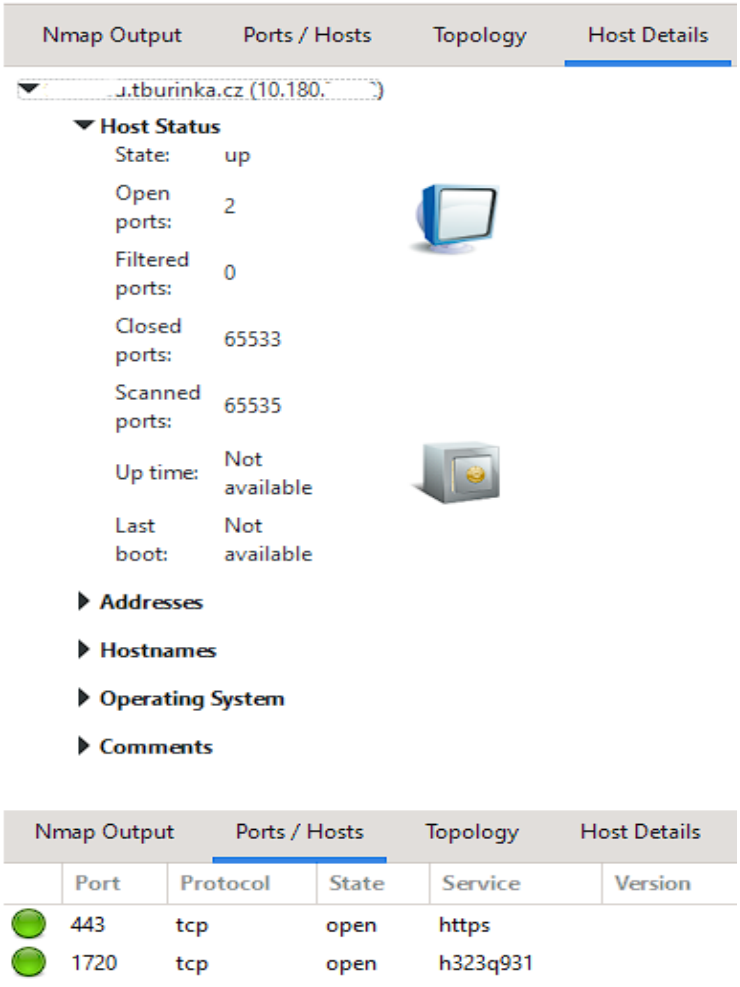
Začneme ale tím že se podíváme na to kolik portů je na serveru otevřeno. K tomu využijeme Nmap. Přesněji k tomuto účelu využiji program ZenMap a základě analýzy těchto portů poté určím, jestli je vše v pořádku nebo se zde nachází bezpečnostní riziko.

Předpokládaný výsledek:

V ideálním případě budou otevřeny pouze porty nezbytné pro provoz služeb serveru a všechny ostatní porty budou uzavřeny.

Výsledek:

Na serveru jsou otevřeny pouze dva porty. Port 443 zajišťující šifrovanou komunikaci a přenos dat a port 1720 který se používá pro H.323 protokol, který je určen pro audio a video komunikaci přes sítě. Vzhledem k povaze serveru jsou oba porty v pořádku a server je dostatečně zabezpečen.



Obrázek 8. Ukázka výsledku skenování portů na serveru v aplikaci Zenmap

2. Testování ping v síti

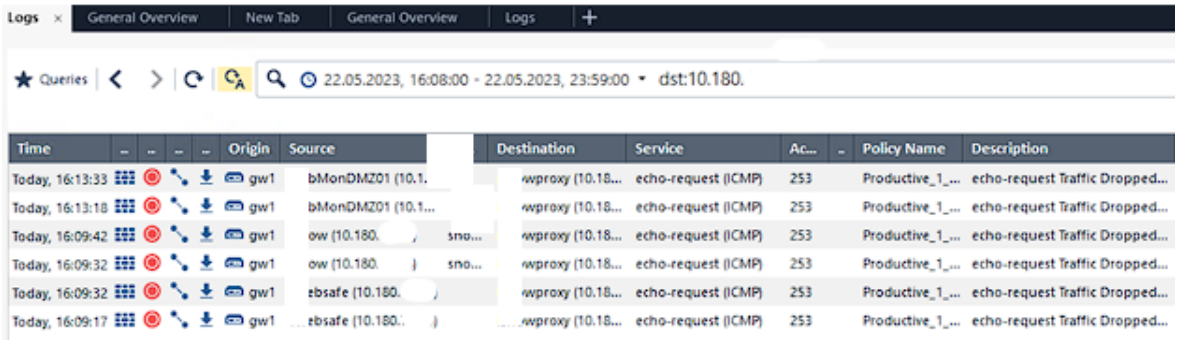
Otestuji ping na servery v DMZ, tento je dle pravidel zakázaný a firewall by jej měl zablokovat.

Předpokládaný výsledek:

Ping nebude možný.

Výsledek:

Test ping nebyl možný, jak je vidět na obrázku 9. přímo z firewallu.



Obrázek 9. Ukázka testu ping na FW v aplikaci Check Point SmartConsole

3. Testování přenosu dat v síti v rámci protokolu Https 443

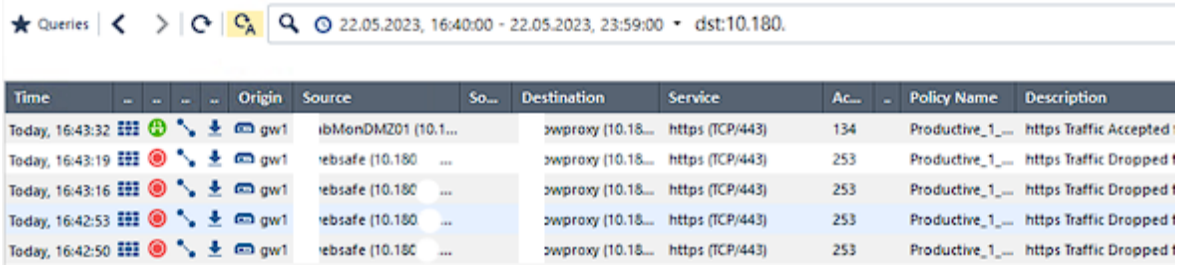
Otestuji přenos dat přes protokol HTTPS v rámci dvou serverů v DMZ, kde je přenos povolen. Následně provedu stejný přenos ze serveru v interní sítí, kde je zablokován.

Přepokládaný výsledek:

Přenos ze serveru v DMZ bude možný a přenos z interního serveru bude zablokován.

Výsledek:

Jak ukazuje Obrázek 10. přenos z interního serveru byl zablokován, naproti tomu přenos ze serveru DMZ byl povolen.



Obrázek 10. Ukázka testu Https na FW v aplikaci Check Point SmartConsole

4. Testování prostupu do internetu mimo proxy

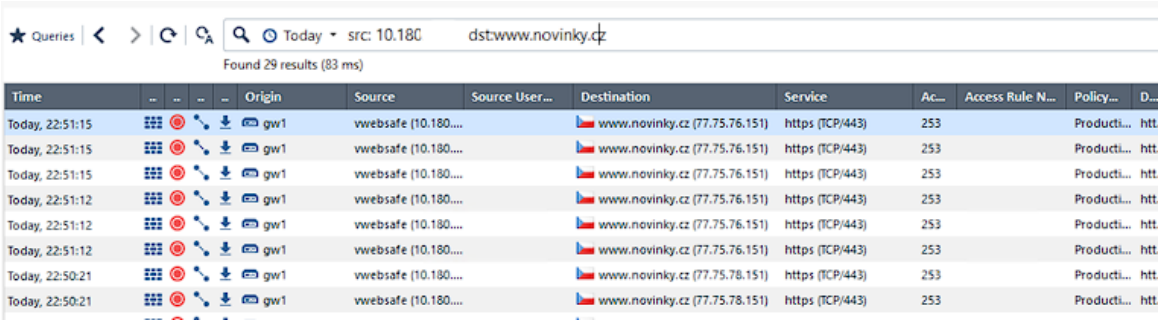
Na serveru vypnu Proxy a pokusím se o přímý přístup do internetu.

Přepokládaný výsledek:

Přístup do internetu nebude povolen a na Firewallu uvidíme jeho zablokování

Výsledek:

Přístup do internetu byl dle očekávání Firewallem zastaven.



Obrázek 11. Ukázka pokusu o přímý přístup na internet ze serveru z aplikace Check Point SmartConsole

6.3.2.3 Závěr Testování

Všechny provedené testy prokázaly správnou funkčnost VPN a serveru v DMZ za firewallem. Autentizace VPN prostřednictvím 2FA byla úspěšně ověřena, což umožňuje uživatelům přístup do interní sítě pouze po úspěšném ověření.

Test úniku IP adresy a test úniku DNS ukázaly, že při použití VPN je skutečná IP adresa a DNS provoz uživatele účinně maskován, což je zásadní pro zachování bezpečnosti a anonymity uživatele.

Skenování portů na serveru prokázalo, že jsou otevřeny pouze nezbytné porty, což minimalizuje potenciální bezpečnostní rizika. Ping na servery v DMZ byl úspěšně blokován firewallem, což opět ukazuje správnou konfiguraci bezpečnostních pravidel.

Testování přenosu dat v rámci protokolu HTTPS potvrdilo správnou konfiguraci pravidel pro přenos dat mezi servery. Přenos dat byl povolen mezi servery v DMZ a zablokován ze serveru v interní síti, což je v souladu s očekávaným výsledkem.

Konečně, test přístupu na internet mimo proxy potvrdil správnou funkci firewallu. Po vypnutí proxy na serveru byl veškerý přímý přístup na internet úspěšně blokován.

Celkově lze konstatovat, že provedené testy ukázaly, že konfigurace a bezpečnostní opatření jak pro VPN, tak pro server v DMZ za firewallem jsou správně nastaveny a fungují podle očekávání. To poskytuje solidní základ pro bezpečný a účinný provoz IT infrastruktury.

ZÁVĚR

Tato práce byla zaměřena na několik klíčových cílů. Prvním cílem bylo seznámit čtenáře s konceptem segmentace sítě a popsat současné hrozby v kyberprostoru, které lze pomocí správné segmentace sítě eliminovat. Druhým cílem bylo popsat infrastrukturu, kterou se snažím chránit, a specifikovat její kritické body. Třetí cíl spočíval v návrhu modelu segmentace pro danou infrastrukturu. Tyto první tři cíle jsem úspěšně splnil.

Následně jsem se zaměřil na implementaci navrženého řešení v testovacím prostředí a otestování jeho funkčnosti vůči vybraným útokům. Zde se však vyskytly komplikace. Nástroje, které jsem původně plánoval použít pro realizaci těchto cílů, Cisco Packet Tracer a GNS3, se ukázaly jako problematické kvůli různým omezením a technickým potížím.

Avšak místo toho, abych se vzdal, našel jsem alternativní řešení. Díky své pozici jsem měl přístup k IT systémům ve společnosti, kde pracuji, což mi umožnilo provést testování na reálných příkladech sítí namísto simulace.

Ačkoli tato práce nebyla realizována tak, jak bylo původně zamýšleno, stále poskytuje náhled do praktického využití segmentace sítě a jejího zabezpečení v reálném prostředí. Přestože jsem narazil na některé výzvy a omezení, byl jsem schopen najít alternativní způsoby, jak dosáhnout svých cílů. Tuto zkušenost a zjištění z ní vyplývající považuji za cenný přínos pro budoucí práce v oblasti sítí a kybernetického zabezpečení.

SEZNAM POUŽITÉ LITERATURY

[1] REICHENBERG, Nimy a Mark WOLFGANG. Segmentace sítě: Pět kroků k lepší ochraně podnikové sítě. *SecurityWorld*. Praha: IDG Czech Republic, a.s., Seydlerova 2451, 2015, **2015**(1), 48.

[2] *Podcast s generálním ředitelem ŘSD ČR - Kybernetický útok na ŘSD: Kyber útok na servery, aplikace a úložiště ŘSD ČR byl podle expertů dlouho připravován a velmi sofistikovaný.* [online]. Praha: ŘSD, 2022 [cit. 2023-02-26]. Dostupné z: https://www.rsd.cz/-/podcast-s-gener%C3%A1ln%C3%ADm-%C5%99editelem-%C5%98sd-%C4%8Cr-kybernetick%C3%BD-%C3%BAtok-na-%C5%98sd

[3] Chytrá elektřina: co jsou to inteligentní sítě a k čemu slouží. *EURACTIV.cz* [online]. Praha, 2017 [cit. 2022-11-17]. Dostupné z: https://euractiv.cz/section/all/linksdossier/chytra-elektrina-co-jsou-to-inteligentni-site-a-k-cemu-slouzi/

[4] Dodržování předpisů PCI DSS: Bezpečnostní standardy, z nichž mají prospěch všichni. *Visa* [online]. Praha: Visa, 2020, 16.6.2020 [cit. 2022-11-17]. Dostupné z: https://www.visa.cz/spojte-se-s-nami/dodrzovani-predpisu-pci-dss.html

[5] COPE, steve. VLANS on Home Networks. *Steve's Smart Home and Networking Guide* [online]. USA: 2017-2022 Steve's Smart Home Guide, 2022 [cit. 2022-11-17]. Dostupné z: https://stevessmarthomeguide.com/vlans-home-networks/

[6] TAYLOR, Hugh. What Are Cyber Threats and What to Do About Them: From infiltrations on infrastructure and data breaches to spear phishing and brute force. Online threats are varied and they don't discriminate organizations from individuals when looking for a target. In: *Prey Blog* [online]. San Francisco: PREY, 2021, June 16, 2021 [cit. 2022-12-18]. Dostupné z: https://preyproject.com/blog/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them

[7] Využívání informačních a komunikačních technologií v domácnostech a mezi osobami - 2022: 1. Počítače a internet v domácnostech. In: *ČSÚ* [online]. Praha: Český statistický úřad, 2022 [cit. 2022-12-17]. Dostupné z: https://www.czso.cz/csu/czso/1-pocitace-a-internet-v-domacnostech-4ebw3izyl9

[8] ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2021. In: *Národní úřad pro kybernetickou a informační bezpečnost - Zprávy o stavu KB* [online]. Praha: Národní úřad pro kybernetickou a informační

bezpečnost, 2022 [cit. 2022-12-17]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf

[9] What Is Malware?: Definition and Examples. In: *Cisco* [online]. San Jose, USA: Cisco, 2018 [cit. 2022-12-18]. Dostupné z: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html

[10] FRIEDMAN, Jon a Bassam KHAN, SHUTTLEWORTH, Susan, ed. CYBEREDGE GROUP, LLC. *Definitive GuideTM to Complete Network Visibility: How to Get High-Performing, Secure Networks While Staying Within Budget* [online]. 1. Annapolis, USA: CyberEdge Group, 2020, 62 s. [cit. 2022-12-01]. ISBN 978-1-948939-10-2. Dostupné z: https://cyber-edge.com/resources/definitive-guide-to-complete-network-visibility/

[11] AKAMAI TECHNOLOGIES. *Network Segmentation and Micro Segmentation in Modern Enterprise Enviroments* [online]. Cambridge, Massachusetts, U.S.: Akamai Technologies, 2019 [cit. 2022-12-01]. Dostupné z: https://www.akamai.com/site/en/documents/white-paper/akamai-network-segmentation-and-micro-segmentation-in-modern-enterprise-environments-white-paper.pdf. White paper.

[12] ADAHMAN, Zillah, Asad WAQAR MALIK a Zahid ANWAR. An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Computers & Security* [online]. North Dakota State University (NDSU), USA; National University of Sciences and Technology (NUST), Islamabad, Pakistan: Elsevier, 2022, 5 May 2022, Revised 28 June 2022, **2022**(122), 1-13 [cit. 2022-12-01]. Dostupné z: doi:https://doi.org/10.1016/j.cose.2022.102911

[13] Co je phishing?. In: *Eset* [online]. Praha: Eset, 2021 [cit. 2022-12-18]. Dostupné z: https://www.eset.com/cz/phishing/

[14] Spear phishing. In: *Trend Micro* [online]. Texas, USA: Trend Micro, 2022 [cit. 2022-12-18]. Dostupné z: https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing

[15] DUBE, R., DIAMOND, Stephanie a Rev VARADHARAJ, ed. *Internal Firewalls For Dummies®, VMware Special Edition* [online]. 1. Hoboken, New Jersey, USA: John Wiley, 2021, 60 s. [cit. 2022-12-01]. ISBN 978-1-119-77296-5 (pbk); 978-1-119-77298-9 (ebk). Dostupné z: https://www.vmware.com/content/dam/learn/en/apj/fy22/Internalfirewalls.pdf

[16] RUDRA, Ahona. What is Piggybacking?. POWERDMARC [online]. Delaware, USA: PowerDMARC, 2022, NOVEMBER 11, 2022 [cit. 2023-02-13]. Dostupné z: https://powerdmarc.com/what-is-piggybacking/

[17] KINDERVAG, John. Build Security Into Your Network's DNA: The Zero Trust Network Architecture. *FORRESTER* [online]. Cambridge, MA 02139 USA: Forrester Research, November 5, 2010, **2010**, 25 [cit. 2023-04-26]. Dostupné z: https://www.actiac.org/system/files/Forrester_zero_trust_DNA.pdf

[18] BOUŠKA, Petr. Cisco IOS 24 - zabezpečení komunikace na portech. *SAMURAJ-cz.com* [online]. Praha: Petr Bouška, 2016, 19.10.2016 [cit. 2023-05-23]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-24-zabezpeceni-komunikace-na-portech/

[19] ALISA. WPA vs WPA2 vs WPA3: WiFi Security Differences. *MiniTool* [online]. Vancouver, Canada: MiniTool® Software, 2022, October 21, 2022 [cit. 2023-05-23]. Dostupné z: https://www.minitool.com/news/wpa-vs-wpa2-vs-wpa3.html

[20] Cisco Catalyst 9300 Series Switches Data Sheet. *Networking, Cloud, and Cybersecurity Solutions - Cisco* [online]. San Jose, USA: Cisco Systems, 2023, February 28, 2023 [cit. 2023-05-03]. Dostupné z: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html

[21] Cisco Firepower 1000 Series Data Sheet. *Networking, Cloud, and Cybersecurity Solutions - Cisco* [online]. San Jose, USA: Cisco Systems, 2023, March 13, 2023 [cit. 2023-05-03]. Dostupné z: https://www.cisco.com/c/en/us/products/collateral/security/firepower-1000-series/datasheet-c78-742469.html

[22] *NetScaler: Application Delivery at Scale: Application delivery at scale can be complex. Make it simpler with NetScaler.* [online]. Kalifornie, USA: Citrix Systems, 2023 [cit. 2023-05-04]. Dostupné z: https://www.netscaler.com/

[23] MAJUMDER, Subbendu a Shipra SHARAD. NetScaler MPX 5900. *NetScaler: Application Delivery at Scale* [online]. Kalifornie, USA: Citrix Systems, 2023, May 2, 2023 [cit. 2023-05-04]. Dostupné z: https://docs.netscaler.com/en-us/citrix-hardware-platforms/mpx/netscaler-hardware-platforms/citrix-netscaler-mpx-5900.html

[24] Cisco Catalyst 9105 Series Access Points Data Sheet. *Networking, Cloud, and Cybersecurity Solutions - Cisco* [online]. San Jose, USA: Cisco Systems, 2022,

November 3, 2022 [cit. 2023-05-03]. Dostupné z: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/datasheet-c78-744062.html

[25] Cisco AnyConnect Secure Mobility Client v4.x. *Networking, Cloud, and Cybersecurity Solutions - Cisco* [online]. San Jose, USA: Cisco Systems, 2014, 20-OCT-2014 [cit. 2023-05-03]. Dostupné z: https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client-v4-x/model.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

2FA	Two-Factor Authentication
3DES	Triple Data Encryption Standard
ACL	Acces Control List
ADC	Aplication Delivery Controler
ADFS	Active Directory Federation Services
AES	Advanced Encryption Standard
AMP	Advanced Malware Protection
AP	Acces Point
ARP	Address Resolution Protocol
AVC	Aplication Visibility and Control
BSS	Basic Service Set
Cisco DNA	Cisco Digital Network Architecture
CLI	Command Line Interface
ČSÚ	Český Statistický Úřad
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name Systém
DTLS	Datagram Transport Layer Security
FMC	Firepower Management Center
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GNS3	Graphical Network Simulator-3
GPO	Group Policy Object

HDX	High Density Experience
HTTP	Hypertext Transfer Protocol
IdP	Identity Provider
IDS	Intrusion Detection System
IKEv2	Internet Key Exchange version 2
IoC	Indicator of Compromise
iOS	iPhone Operating System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISFW	Internal Segmented Firewall
ISP	Internet Service Provider
IT	Information Technology
LAG	Link Agregation Group
LAN	Local Area Network
LDAP	Lightweight Directory Acces Protocol
MitM	Man in the Middle
MPX	Multi-Processing eXtension
MU-MIMO	MultiUser Multiple-Input Multiple-Output
NG	New Generation
Nmap	Network Mapper
OFDMA	Orthogonal Frequency-Division Multiple Access
PC	Personal Computer
PCI-DSS	Payment Card Industry Data Security Standard
PT-AC	Packet Tracer-Access Point
QSFP	Quad Small Form-factor Pluggable

RADIUS	Remote Authentication Dial-In User Service
RAM	Random Acces Memory
RF	Radio Frequency
RIP	Routing Information Protocol
RJ-45	Registered Jack - 45
RSA	Rivest-Shamir-Aldeman
SD-Access	Software Defined Acces
SDN	Software Defined Networks
SFP	Small Form-factor Pluggable
SIEM	Security Information and Event Manager
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UPoE	Universal Power over Ethernet
URL	Uniform Resource Locator
VIRL	Virtual Internet Routing Lab
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAF	Web Application Firewall
WI-FI	Wireless Fidelity
WPA	Wi-Fi Protected Access
ZTA	Zero Trust Architecture

SEZNAM OBRÁZKŮ

SEZNAM TABULEK