Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra Informačních Technologií

Analýza využitelnosti simulačních nástrojů pro síťovou bezpečnost

Bakalářská práce

Autor: Martin Mičkech
Studijní obor: Aplikovaná informatika

Vedoucí práce: doc. Mgr. Josef Horálek, Ph.D.

Hradec Králové Duben 2024

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 18.4.2024 Martin Mičkech

Poděkování:

Děkuji vedoucímu bakalářské práce doc. Mgr. Josefu Horálkovi, Ph.D. za odborné vedení práce, ochotu a přínosné konzultace. Zároveň bych chtěl poděkovat rodině a přátelům za jejich podporu.

Abstrakt:

Tato bakalářská práce poskytuje ucelený pohled na testování a simulace počítačových sítí. Teoretická část zahrnuje popis nástrojů, jako je Packet Tracer od Cisco a Security Fabric, FortiTester a FortiGuard od Fortinet. Dále zkoumá kybernetické útoky, včetně neautorizovaného přístupu, Man-in-the-middle útoků, DDoS útoků a analyzuje hrozby síťových vrstev OSI. Práce se také zabývá zabezpečením sítě a popisuje prvky jako firewall, řízení přístupu k síti a detekce průniku. Praktická část je věnována analýze a testování bezpečnostní infrastruktury Security Fabric na síti vytvořené s využitím FortiGate, FortiAP a FortiSwitch. Jsou zde popsány nástroje nabízené těmito zařízeními v rámci Security Fabric a postupy jejich konfigurace.

Abstract:

Title: Analysis of the usability of simulation tools for network security

This bachelor thesis provides a comprehensive view of testing and simulation of computer networks. The theoretical part includes a description of tools such as Cisco's Packet Tracer and Fortinet's Security Fabric, FortiTester and FortiGuard. It also examines cyber-attacks, including unauthorized access, man-in-the-middle attacks, DDoS attacks, and analyzes OSI network layer threats. The thesis also discusses network security and describes elements such as firewall, network access control, and intrusion detection. The practical part is devoted to the analysis and testing of the Security Fabric infrastructure on a network created using FortiGate, FortiAP and FortiSwitch. It describes the tools offered by these devices within the Security Fabric and the procedures for their configuration.

Obsah

1. ÚVOD

V dnešní době digitalizace a internetu jsou počítačové sítě častým cílem konstantně se rozvíjejících útoků. Proto je kyberbezpečnost klíčovým tématem, které by nemělo být podceňováno. Útoky mohou postihnout jakoukoli počítačovou síť či zařízení a může vést k závažným následkům, mezi které může patřit ztráta citlivých dat, finanční ztráty, narušení síťového provozu a další, což může mít pro organizace fatální dopad.

Vzhledem k neustálému rozvoji kybernetických hrozeb, je pro organizace velmi důležité mít přístup k nástrojům pro simulaci a testování různých scénářů týkajících se zabezpečení a efektivity počítačových sítí. Tyto nástroje organizaci umožní připravit se na případné hrozby a scénáře, které by mohli nastat a zároveň může tvůrcům těchto systémů poskytnout zpětnou vazbu potřebnou pro další vývoj. Konkrétně se tyto nástroje dají využít pro plánování topologií sítí, testování efektivity provozu, nebo testování zabezpečení proti konkrétním hrozbám.

Ochrana počítačové sítě lze provést několika způsoby. Základní součástí každé dobře zabezpečené sítě je firewall, který pro síť monitoruje a filtruje datový provoz. Mezi další možnosti zabezpečení může patřit segmentace sítě pomocí rozdělení do podsítí, využití antivirových programů, nebo řízení přístupu k síti.

Pozornost je v práci z velké části věnována Security Fabric od společnosti Fortinet, který představuje centrálně řízenou bezpečnostní architekturu počítačové sítě. I přesto, že není primárně navržen jako simulační nástroj, hraje klíčovou roli v ochraně sítě proti hrozbám a lze jej využít pro testování a ověřování efektivity a zabezpečení počítačové sítě. Jeho vlastnost centrálního řízení a monitorování sítě umožňuje rychlou reakci na hrozby a následnou implementaci bezpečnostních opatření.

2. CÍL A METODIKA PRÁCE

Bakalářská práce je zaměřena na téma zabezpečení počítačových sítí á nástrojů pro jejich simulaci. Cílem práce je uvést několik simulačních a testovacích nástrojů síťové bezpečnosti a seznámit se základními koncepty síťových útoků a možností, jak se proti nim bránit.

Teoretická část je zaměřena na představení nástrojů určených pro simulaci, testování síťového provozu a kyberbezpečnosti. Následuje kapitola, která je věnována seznámením s tématem kybernetických útoků. Je uvedeno několik nejčastějších typů útoků, společně s jejich charakteristikami. Další kapitola navazuje na tématiku kybernetických útoků v podobě popsání hrozeb na jednotlivé síťové vrstvy OSI a nejčastější útoky prováděné na ně. Poslední část teoretické části je věnována tématice nástrojů a taktik určených pro zabezpečení počítačových sítí.

Praktická část se věnuje analýze nástrojů Security Fabric. Obsahuje postup tvorby počítačové sítě a jejího zabezpečení s využitím zařízení od společnosti Fortinet. Jsou zde popsány nabízené nástroje těmito zařízeními, jejich konfigurace a využití.

3. Testování a simulace počítačových sítí

Nástroje pro simulaci a testování počítačových sítí a zabezpečení představují klíčový prvek v rozvoji infrastruktury a zabezpečení moderních síťových infrastruktur. Simulační nástroje umožňují modelovat a testovat různé scénáře a problémy spojené s počítačovými sítěmi bez nutnosti fyzických zařízení. Na druhou stranu testovací nástroje jsou spíše určeny pro otestování funkčnosti a bezpečnosti již existujících sítí, či jejich částí. Těmito vlastnostmi napomáhají najít a odstranit případné slabiny v zabezpečení, či infrastruktuře počítačové sítě.

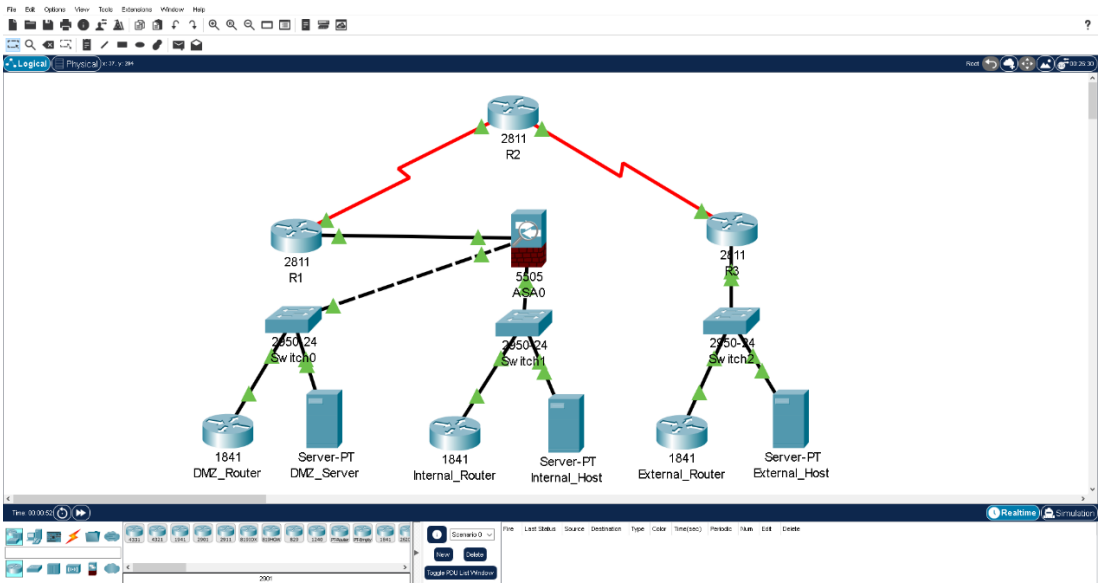
3.1. Nástroje Cisco

Cisco je nejspíše nejznámější společností nabízející produkty zaměřené na počítačové sítě. Do jejich nabídky patří síťový hardware a software, nástroje pro simulaci počítačových sítí, síťové zabezpečení, komunikační systémy a další.[1]

3.1.1. Packet Tracer

Cisco Packet Tracer je software vytvořený společností Cisco Systems a je nástrojem určeným spíše pro výuku a trénink tvoření počítačových sítí. Aplikace nabízí pouze omezené množství Cisco zařízení použitelných pro tvorbu simulované sítě. Jednotlivá zařízení lze libovolně konfigurovat a mezi sebou propojovat.[2]

Packet Tracer nabízí několik funkcí, které z něho dělají dobrý nástroj pro obecné testování sítí a vzdělávání. Jednou z těchto mechanik může být možnost práce několika uživatelů na jednom projektu současně z vlastních zařízení. Dále nabízí logický a fyzický mód, v tom logickém jsou zařízení zobrazována pouze jako jednoduchá miniatura zařízení. Zatímco ve fyzickém módu, jsou jednotlivá zařízení zobrazována tak, jak fyzicky vypadají, tudíž uživatel má možnost vyzkoušet si, jak by se pracovalo s reálným zařízením. Jednou z výhod tohoto softwaru je jeho nenáročnost na hardware, tudíž je možné jej zprovoznit na běžných počítačích.[3]



Obrázek 1 – Snímek obrazovky programu Packet Tracer Zdroj: Vlastní

3.2. Modelling Labs (CML)

CML je simulačním nástrojem od společnosti Cisco určený především pro síťové vývojáře. Oproti Packet Tracer, který je určen spíše pro vzdělávání, je CML mířeno spíše na vývojáře a inženýry sítí. Je možné setkat se s názvem Cisco Virtual Internet Modelling Labs neboli VIRL, což je starší verze CML.

Nabízí možnost použít velké množství zařízení nejen od společnosti Cisco, ale i od jiných výrobců pomocí licencovaných softwarových kopií jednotlivých zařízení. Pomocí těchto zařízení je možné tvořit rozsáhlé počítačové sítě a následně sledovat jejich chování při provozu, či změně některých konfigurací za chodu. Také je možné provádět útoky na simulovanou síť a otestovat tím, jak efektivní je zavedené zabezpečení.[4, 5]

3.3. Nástroje Fortinet

Fortinet, inc., je jedna z nejrozšířenějších společností zaměřující se na kyberbezpečnost. Je známa pro své firewally nové generace FortiGate, které jsou centrálním prvkem infrastruktury Security Fabric. Existuje také varianta FortiGate VM, který je virtuální variantou firewallu a je ideální možností otestování tvorby počítačové sítě a jejího zabezpečení bez nutnosti vlastnictví fyzického hardware. Fortinet dále nabízí širokou škálu jiných zařízení a nástrojů pro tvorbu a testování počítačových sítí s důrazem na zabezpečení. Výhodou produktů od Fortinet je dobrá interoperabilita se zařízeními a službami od jiných výrobců.[6]

3.3.1. Security Fabric

Security Fabric je integrovaná bezpečnostní infrastruktura od společnosti Fortinet, spočívající v řízení jednotlivých síťových prvků centrálně s cílem co nejlepšího zabezpečení pomocí softwaru FortiGuard. Do této infrastruktury jsou zahrnuty veškeré zařízení v síti, což zajišťuje jejich správnou koordinaci při detekci síťového útoku a jeho následné zamezení.[7] Jednou z jeho důležitých vlastností je škálovatelnost, tudíž není náročné síť požívající Security Fabric libovolně rozšiřovat. Všemu napomáhá automatizace tohoto systému pomocí umělé inteligence FortiGuard AI, která je schopná rychle reagovat na příchozí útoky, tím že je sleduje a v reálném čase se proti nim ochrana sítě přizpůsobuje.[8]

3.3.2. FortiTester

FortiTester je síťové zařízení, které má za úkol otestovat různé aspekty infrastruktury počítačové sítě a tím napomoci zvýšit její bezpečnost a výkon. Toto zařízení nabízí širokou škálu testů pro změření výkonu sítě. Výkon sítě měří pomocí testů na propustnost, odolnost proti výpadkům, kvalitu služeb a dalších.[9]

Dalším významným aspektem je možnost otestovat síťové zabezpečení, a to pomocí otestování funkčnosti jednotlivých síťových prvků, nebo simulace síťových útoků, kterých nabízí širokou škálu. Mezi útoky, které dokáže simulovat patří DDoS, malware, IPS, webové útoky a další. Další možností pro simulaci útoků je pomocí nástroje MITRE ATT&CK Framework, který útoky pouze neposílá na prvky sítě, ale dokáže simulovat průběh útoku po prolomení zabezpečení. Jedním z příkladů těchto útoků lze uvést plánování úloh, kdy útočník přinutí cílové zařízení spustit úlohy s cílem ukrást data, zneužít oprávnění, nebo v zařízení spustit škodlivý software.[10, 11]

3.3.3. FortiGuard

FortiGuard je software využívaný zařízeními Fortinet, na kterých zajišťuje co nejvyšší zabezpečení. Jeho součástí je například antivirus, IPS, kontrola aplikací, filtrace webů a spamu, nebo webový firewall. Ačkoliv není nutností pro funkčnost Fortinet zařízení, je doporučován pro jejich co nejlepší zabezpečení.

FortiGuard využívá umělou inteligenci k prevenci a boji proti kyberútokům. Dokáže se s její pomocí dynamicky přizpůsobovat probíhanému útoku, a to i proti neznámým typům útoků. Funkčnosti napomáhají i pravidelné aktualizace poskytující informace o nejnovějších

hrozbách, které byli pečlivě zkoumány ve FortiGuard Labs s cílem zjištění jejich slabin.[12, 13]

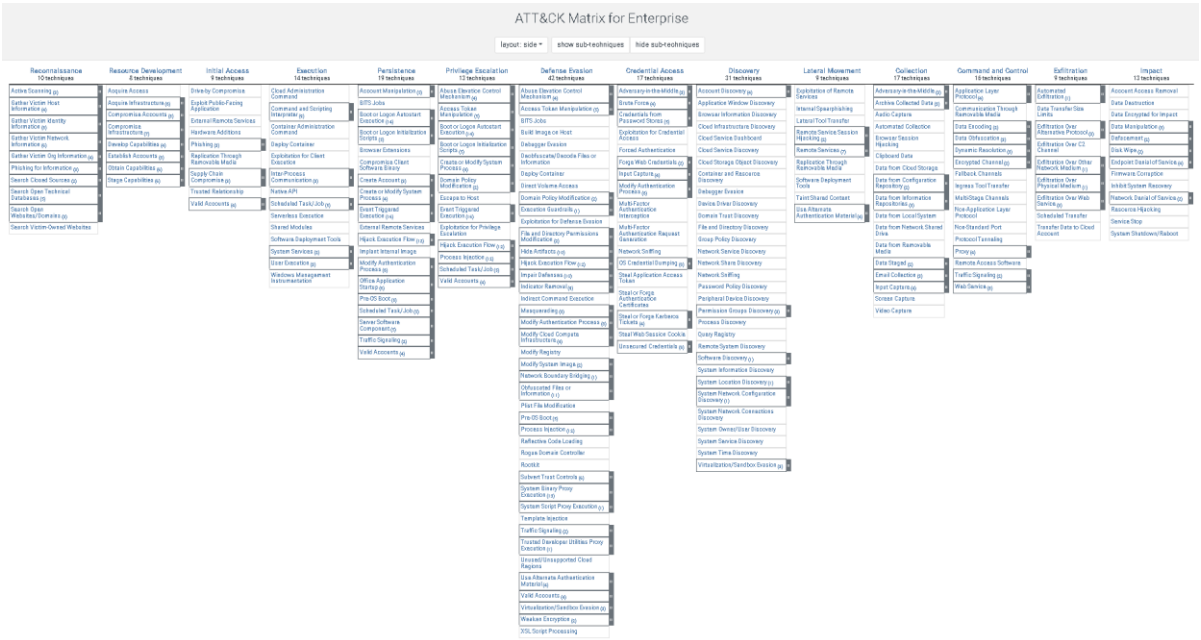
3.4. MITRE ATT&CK

ATT&CK je zkratkou pro „Adversarial Tactics, Techniques, and Common Knowledge“ což je znalostní databáze od společnosti MITRE. Je globálně přístupná a obsahuje podrobný popis taktik a technik používaných útočníky při útocích na počítačové sítě. Veškeré informace obsažené v této databázi jsou založeny na pozorování průběhů reálných kyberútoků.[14]

Databáze ATT&CK je široce využívána v oborech IT. Jedna ze skupin využívajících matice ATT&CK jsou takzvané červené týmy. To jsou skupiny, které zkouší provádět síťové útoky na počítačové sítě různých organizací s cílem odhalit jejich slabiny a následně zlepšit jejich zabezpečení. Konkrétně využívají ATT&CK ke zkoumání útoků, což vylepšuje efektivitu jimi prováděných testů. Další možné využití databáze, může být při detekci síťových útoků. Zařízení monitorující síť dokáže pomocí poskytnutých informací včas zjistit o jaký útok se jedná a zakročit. Také se ATT&CK používá při testování produktů, aby našel jejich případné slabiny, nebo otestoval, jak by se chovali při síťovém útoku.[15]

3.4.1. MITRE ATT&CK FRAMEWORK

MITRE ATT&CK Framework je repositář matic, které obsahují model chování kybernetických útoků a je zpravidla prezentován v podobě tabulky kde sloupce představují taktiky použité v průběhu útoku a v řádcích lze nalézt techniky použité k dosažení cílů útoku. Tento framework byl vytvořen s cílem umožnit simulaci jak útočníka, tak obránce a tím umožnit jednodušeji pochopit průběhy útoků a zároveň zefektivnit jejich detekci a následnou likvidaci.[15] Konkrétně tento framework využívá již výše zmíněný Fortinet FortiTester, jež pomocí něho provádí simulaci útoků na testovanou síť.[11]



Obrázek 2 - Ukázka matice Enterprise Zdroj: [14]

Matice ATT&CK Framework lze rozdělit na 3 základní typy:

- Enterprise ATT&CK – Jednou z kategorií, kterou lze v Enterprise ATT&CK nalézt je také PRE, jež popisuje aktivity, prováděné mimo počítačovou síť organizace a často předchází dalším útokům a většinou je složité tyto typy detekovat. Příkladem může být sběr veřejně dostupných informací z různých zdrojů. Další zde popsané techniky jsou již útočníkem prováděny přímo v počítačové síti na platformách Windows, Linux, macOS, Office 365, SaaS, IaaS a dalších v organizaci. Tyto matice mají umožnit lepe porozumět tomu, které části sítě by měli mít prioritu v zabezpečení.
- Mobile ATT&CK – Popisuje taktiky a techniky útoků na mobilní platformy iOS a Android. Vychází z katalogu mobilních hrozeb NIST, popisující právě hrozby mobilních zařízení.
- ICS ATT&CK – Tento typ popisuje útoky prováděné na industriální řídící systémy pro například továrny, elektrárny a další organizace pracující s technickými stroji.[14, 15]

3.5. Mitre Caldera

Caldera je framework od společnosti Mitre, využitelný pro testování síťového zabezpečení. Jednou z hlavních výhod tohoto frameworku je automatizace síťového testování. Caldera zastupuje práci takzvaného červeného, týmu, což je obvykle skupina, snažící se otestovat efektivitu zabezpečení sítě. Tento proces by měl být schopný zefektivnit a automatizovat

rutinní práci těchto týmů. Pro testování využívá Caldera již zmíněný MITRE ATT&CK framework pro co nejdůvěryhodnějšímu průběhu kyberútoku.[16, 17]

4. Kybernetické útoky

Útok na síť může mít několik různých podob a cílů. Může se snažit o napadení a poškození zařízení, nebo pouze dat v nich uložených, také může cílit na krádež uložených informací, anebo omezení funkčnosti zařízení, či celé sítě, jako je zamezení komunikace mezi zařízeními, čí znemožnění přístupu k některým datům. Tyto útoky lze rozdělit na několik základních typů.

4.1. Nejčastější typy kybernetických útoků

Tato kapitola se věnuje popisu několika nejčastěji se vyskytujících typů kybernetických útoků. Popisuje jejich základní principy a způsoby jejich provedení.

4.1.1. Neautorizovaný přístup

Zde se útočník snaží o získání přístupu do sítě a existuje několik způsobů které lze využit. Jednou z nejčastějších metod je zjišťování slabých hesel k účtům uvnitř sítě, která může útočník lehce odhadnout. Dalším způsobem může být sociální inženýrství, což znamená manipulovaní s lidmi s cílem krádeže citlivých informací, nebo přístupových údajů.

Tento útok může být proveden vzdáleným připojením útočníka k síti, kdy je využito slabých míst v zabezpečení. Avšak je zde i možnost, kdy se útočník dostane přímo k některému z fyzických síťových zařízení, díky kterému je schopný získat přístup do sítě.

4.1.2. Man-in-the-middle

Man-in-the-middle útok útočí na přenos dat mezi dvěma stranami, která spolu komunikují. Tuto komunikaci může pouze odposlouchávat s cílem zjištění citlivých informací, nebo tato data může upravovat, aniž by si toho obě strany komunikace byly vědomy.

4.1.3. SQL injekce

Tento typ útoku spočívá v napadení nezabezpečené části databázové vrstvy sítě, do které útočník vloží vlastní SQL kód, který je následně v databázi proveden. Cílem může být získání citlivých informací a přihlašovacích údajů, nebo poškození struktury databáze.

4.1.4. DDoS

Neboli útok typu odepření služby má za cíl přetížení cílového zařízení, nebo celé sítě. Útočník vysílá do sítě velké množství dat, které zahltí porty koncových zařízení a tím zpomalí, nebo dokonce znemožní komunikaci v síti. Pro tuto činnost jsou využívány takzvané botnety, což jsou infikovaná zařízení používaná pro generaci enormního množství dat.[18]

4.1.5. Malware

Malware je obecné označení pro software vytvořený s cílem ohrozit nějak bezpečnost zařízení, nebo celé sítě a může být následkem jiných útoků při kterých je vložen do zařízení. Existuje mnoho různých typů malwaru a mohou mít různé cíle. Některým jde o krádež dat, jiné se snaží síťová zařízení poškodit, další mohou sledovat provoz zařízení a napomáhat jako nástroj pro jiné útoky.

Konkrétními příklady mohou může být ransomware který zablokuje přistup k datům uvnitř zařízení a nabízí možnost zaplatit útočníkovi pro jejich odblokování. Spyware je typ malwaru, který pasivně monitoruje provoz uvnitř zařízení čímž získává data. Dalším příkladem může být botnet, což je infikované zařízení používané pro DDoS útoky.[19]

4.2. Hrozby síťových vrstev OSI

Každá počítačová síť je teoreticky vytvořena podle jedné z definovaných architektur, jednou možností může být model OSI, ale tou častěji využívanější je architektura TCP/IP, která je složena ze 4 vrstev a to aplikační, transportní, síťové a vrstvy síťového rozhraní. Tyto vrstvy jsou často cílem útoků využívajících některý z jejich protokolů.[20] Model OSI může být napaden identickými útoky, rozdílná by byla pouze vrstva, ve které by se odehrával. Tyto vrstvy a jejich části jsou velice častým cílem síťových útoků.

4.2.1. Aplikační vrstva

HTTP protokol slouží pro komunikaci uživatele v sítí s webovým serverem a neposkytuje žádnou ochranu, avšak při použití HTTPS jsou přenášená data šifrována. Tyto protokoly mohou být cílem mnoha typů útoků.

Jedním z nich je únos spojení, kde útočník používá program pro analýzu paketů, jako je například software Wireshark a používá jej k odchycení paketů. Z takto odchycené komunikace je schopný zjistit informace pomocí kterých je schopný převzít relaci a předstírat že je přihlášený uživatel.

Dalším možným příkladem je útok na vyrovnávací paměť cache, který může nastat poté, co útočník získá přístup do uživatelova zařízení. Zde se snaží získat přístup ke cookies, které si ukládají navštívené webové stránky a obsahují soukromé údaje uživatele. Získané cookies následně prohledává, či upravuje za účelem získání přístupových, nebo citlivých údajů uživatele.

Pro základní ochranu proti HTTP útokům je vhodné použít šifrovaný HTTPS protokolu namísto HTTP a firewall určený pro webové aplikace.[21]

DNS je protokol sloužící k překladu doménových jmen na odpovídající IP adresy a naopak. Otrávení cache je útok zaměřený na manipulaci obsahu DNS cache. Konkrétně se útočník snaží přepsat informace zde uložené. Následně může být přesměrování oběti na falešné webové stránky které se většinou snaží o získání citlivých údajů.[20]

4.2.2. Transportní vrstva

TCP a UDP slouží pro přenos dat, avšak TCP protokol nejprve naváže spojení s cílovým zařízením, poté kontroluje, zda nenastala chyba při přenosu a dodává data v pořadí, v jakém byla poslána pomocí segmentace. UDP je o něco jednodušší, a jeho hlavní výhodou je rychlost, avšak nenavazuje spojení mezi zařízeními a chyby při přenosu kontroluje pouze pomocí kontrolního součtu, který není vždy spolehlivý.

TCP může být cílem SYN DDoS útoku, který zneužívá takzvané třícestné potřesení rukou. Nejprve zdrojové zařízení vyšle synchronizační zprávu, která má za úkol synchronizaci s cílový zařízením. Následně cílové zařízení potvrdí synchronizaci a za běžných okolností by opět zdrojové zařízení mělo vyslat zprávu o potvrzení navázání spojení.[20] Avšak pokud je pod SYN útokem, tuto zprávu nevyšle. Místo toho jsou mu konstantně posílány SYN zprávy, na které odpovídá. Takže cílové zařízení bude čekat, než dostane potvrzení na jeho odpovědi, což vyčerpá jeho zdroje a může vést až ke zhroucení systému. Ochránit síť proti SYN útoku lze pomocí přidání SYN cookies to TCP paketů, to umožní zařízením dočasně

přerušit spojení při třícestném potřesení rukou, dokud neobdrží zprávu o navázání spojení od zdrojového zařízení.

Dalším častým DDoS útokem je UDP zaplavení, kdy útočník posílá velké množství UDP paketů po síti. Zařízení v síti musí přijaté pakety zpracovat a poslat odpověď což využívá veškerý dostupný výpočetní výkon a vede k velkému zpomalení, nebo až ke kolapsu zařízení. Zabezpečit síť proti UDP zaplavení lze pomocí filtrace přijatých paketů, kdy tyto filtrované pakety nejsou nadále zpracovávány a neposílají se odpovědi na ně.[22]

Mezi nejnovější DoS útoky na UDP patří takzvaný Loop DoS objevený v březnu roku 2024 institutem CISPA. Ten spočívá v navázání spojení mezi dvěma síťovými službami. Ty mezi sebou začnou vyměňovat informace, avšak každá z odeslaných informací požaduje další odpovědi, a tak je síť zahlcena daty, znemožňující další komunikaci. Takto navozená smyčka je prakticky nezastavitelná, ani samotný útočník již není schopný útok zastavit. Tento jev je unikátní oproti předchozím útokům využívajících smyčku, jelikož ty byli vždy omezeny konečným počtem opakování. Odhaduje se, že tento útok může ohrozit až 300 000 uživatelů využívající implementace protokolů TFTP, DNS a NTP, Echo, Chargen, nebo QOTD. Celkově se jedná velmi nebezpečný a inovativní útok, který je nutné řešit.[23]

4.2.3. Síťová vrstva

IP protokol je zodpovědný za routování paketů v síti do jejich cíle. Jelikož tyto přenášené pakety obsahují IP adresu zdrojového zařízení, mohou být využity pro takzvaný spoofing útok, který spočívá v zasílání dat s počáteční adresou jiného zařízení. Tato činnost může mít za cíl skrýt svou vlastní identitu, nebo se vydávat za jiného člena v síti a díky tomu získat přístup do dané sítě, kde může následně útočník navázat dalšími útoky.[20]

Hlavním úkolem protokolu ICMP je detekce chyb při přenosu dat. Vytváří takzvané tunely, což jsou cesty mezi klientem a serverem, které umožňují komunikaci mezi zařízeními bez kontroly firewallem. Některé funkce tohoto protokolu, konkrétně Echo Request a Echo Reply jsou využívány příkazem ping. ICMP je užitečným nástrojem pro tvorbu sítě, avšak může čelit několika útokům zneužívajících jeho vlastností.

Jedním z nich je ICMP tunelování, kde je mezi koncová zařízení ICMP tunelu připojen útočník, který sleduje Echo pakety a může do nich injektovat data. Takto je možné přenášet libovolná data po síti, aniž by byla detekována firewallem. Pro zamezení tomuto útoku je

možné zakázat některé funkce ICMP, avšak to může omezit funkčnost tohoto protokolu v síti. Dalším způsobem je omezení velikosti ICMP paketů, které budou propouštěny firewallem.

Dále lze uvést takzvaný DDoS Smurf útok, kdy útočník odesílá pomocí broadcast přenosu zdrojovou adresu ICMP paketu, což zaplaví veškerá zařízení v sítí a velice zpomalí, nebo znemožní přenos dat v síti. Bránit se proti němu lze pomocí zavedení filtrace paketů a firewallu do sítě.[24]

4.2.4. Vrstva síťového rozhraní

Tato vrstva je tvořena fyzickým hardwarem, tudíž útočník se pro provedení útoku musí dostat až k fyzickému přenosovému médiu, zařízení, nebo odchytit bezdrátový přenos.

Jednou cestou, jak na tuto vrstvu zaútočit, je odposlouchávání datového přenosu mezi zařízeními s cílem ukrást informace. Další typ útoku je o něco složitější na provedení, spočívá totiž v připojení nového zařízení do sítě, často jsou pro to využívány malé routery. Posledním způsobem, jak se dá na vrstvu síťového rozhraní útočit, je vandalizace, ta lze provést fyzickým poškození zařízení a přenosových médií, nebo pomocí rušičky signálu, která znemožní čtení přenášených dat. Ubránit se těmto útokům lze především pomocí fyzického zabezpečení sítě, což je například omezení přístupu k hardwarovým zařízením pomocí jejich umístění do zamčené místnosti.[25]

5. Zabezpečení sítě

Síťové zabezpečení má za cíl ochránit veškerá zařízení v počítačové síti proti krádeži dat, neautorizovanému přístupu do sítě, detekovat útoky na síť a zamezit jim. Sítě se neustále rozvíjí a zvětšují a tím se zároveň zvyšuje hrozba kybernetického útoku. Podle průzkumu společnosti IBM v roce 2022 čelilo alespoň jednomu úspěšnému útoku cíleného na krádež dat až 83 % organizací.[26]

Zabezpečení lze rozdělit na 3 základní typy fyzické, technické a administrativní. Fyzické spočívá v ochraně zařízení a sítě v reálném světě proti neautorizovanému přístupu k nim. Příkladem fyzického zabezpečení mohou být zařízení umístěná v zamčené místnosti. Technické má za úkol ochránit data uvnitř sítě, konkrétněji zabraňuje jejich krádeži a poškození. Posledním je administrativní zabezpečení, to je řešeno pomocí přístupových úrovní členů v síti, takže každá z úrovní omezuje či umožňuje přístup k některým datům, či funkcím v síti. Pro praktické zavedení těchto typů existuje několik nástrojů, které jsou běžně používány.[27]

5.1.1. Firewall

Firewall je bezpečnostní brána každé sítě, či samotného zařízení, která sleduje a filtruje veškerý síťový provoz. Filtrace dat probíhá pomocí předdefinovaných pravidel, pokud jsou některá porušena, firewall odepře datům přístup do zařízení. Tímto chováním tvoří první linii ochrany při jakémkoli pokusu o útok a je tak nezbytnou součástí každé dobře zabezpečené počítačové sítě. Existuje více typů firewallu, ty nejzákladnější a nejstarší pracují na principu filtrace paketů, avšak modernější jsou schopny rozeznat zdroj komunikace, filtrovat informace na všech síťových vrstvách což napomáhá detekci útoků.[28]

5.1.2. Antivirová ochrana

Dnešní podoba moderních antivirových programů se výrazně liší od té původní. Původně se tyto programy zabývaly spíše hledáním signatur malwaru a jejich následným odstraněním. Moderní software poskytující antivirovou ochranu kromě původní funkčností, nabízí další funkce pro co nejlepší zabezpečení proti virům. Hlavní rozdíl je snaha nakažení spíše předejít, což je prováděno pomocí emulace kódu, analýzou chování jednotlivých virů a

heuristikou, která dokáže otestovat podezřelé soubory ve virtuálním prostoru a předchází tak nakažení celého zařízení.[29]

5.1.3. Řízení přístupu k síti

Tento typ zabezpečení hlídá uživatele, kteří chtějí vstoupit do sítě a kontroluje, zda do ní mají přístup, popřípadě jaká mají uvnitř práva. Využívá takzvaného AAA protokolu, který provádí autentizaci, autorizaci a účtování. Autentizace ověřuje identitu vstupujícího uživatele, pokud se podaří identitu ověřit, proběhne autorizace, kdy je uživateli povolen vstup a následně účtování slouží k monitorování prováděných akcí uživatelů kterým byl přístup povolen. Některé provedení tohoto typu zabezpečení umí také zjistit, jak dobře je zabezpečené zařízení snažící získat přístup do sítě, pokud je zabezpečení nedostatečné a mohlo by zařízení být hrozbou pro ostatní členy sítě, je mu přístup zamítnut. Řízení přístupu je často používané pro administrativní zabezpečení pomocí uživatelských rolí.[26]

5.1.4. Segmentace sítě

Segmentace sítě znamená její rozdělení na několik menších podsíti, což napomáhá zabezpečení, výkonu a správě celé sítě. Jednotlivé podsítě mohou být rozdílně nastaveny a chovají se jako samostatné sítě. Takto rozdělená síť má lepší výkon, jelikož jednotlivé zařízení zatěžují svým chodem převážně svoji podsíť. Ohledně zabezpečení je segmentace užitečná v tom, že dokáže udržet útok od šíření mimo napadenou podsíť.[30]

5.1.5. Virtuální privátní síť

Virtuální privátní sítě, často známé pod zkratkou VPN, jsou nástrojem pro ochranu uživatelovy identity. Uživatel se místo přímému připojení k internetu připojí nejprve k zabezpečenému serveru, který před komunikací s internetem ochraňuje přenášená data pomocí šifrování, přičemž maskuje zdrojovou IP adresu a lokaci. Jednou z nevýhod použití VPN, může být zpomalení přenosu dat kvůli zmiňovanému připojení k serveru mezi zdrojovým zařízením a internetem.[26]

5.1.6. Detekce a prevence průniku

Systémy pro detekci průniku se používají pro sledování síťového provozu, který prohledávají s cílem nalezení podezřelých dat, které by mohli naznačovat pokus o ohrožení sítě. Pokud je nějaká hrozba detekována, nastupuje systém pro prevenci průniku, který má

za úkol podezřelá data zničit, popřípadě přerušit spojení se zařízením odkud byl přenos zahájen.[31]

6. Analýza možností Security Fabric

Fortinet je jednou z nejpopulárnějších společností zaměřených na kyberbezpečnost pro rok 2023.[32] Tato popularita byla jedním z důvodů pro výběr zařízení od této společnosti pro testování.

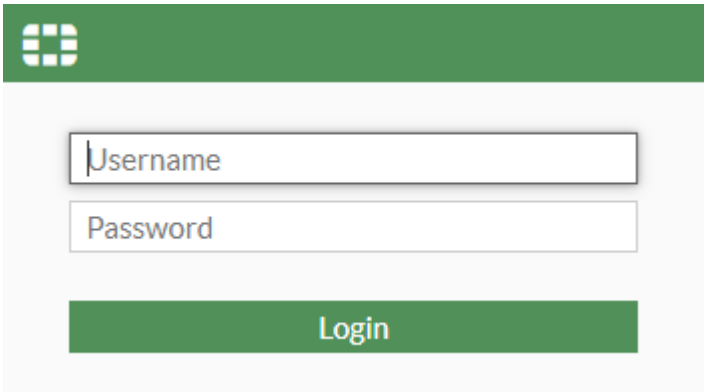
Cílem testování je prozkoumat možnosti a nástroje nabízené zařízeními od společnosti Fortinet a infrastruktury Security Fabric jimi tvořený. Pro testování jsou využity zařízení FortiGate firewall, FortiSwitch přepínač a FortiAP přístupový bod nabízející komplexní řešení pro testování. Testování by bylo možné provádět také způsobem simulace pomocí FortiGate VM, který nabízí stejné možnosti, jako fyzická zařízení. Pro získání informací potřebných pro konfiguraci a popis funkcí byla využita oficiální dokumentace Fortinet Document Library [33] a články na téma Fortinet z webu Samuraj-cz.com.[34]

6.1. Základní nastavení

Tato kapitola je zaměřena na základní nastavení potřebné, či doporučené pro navazující nastavení a celkové zabezpečení počítačové sítě využívající Security Fabric. Nejprve je shrnuto první přihlášení a počáteční nastavení firewallu FortiGate, poté je popsána aktualizace jednotlivých zařízení, a nakonec je zde uvedena změna jednotlivých portů pro administrativní přístup.

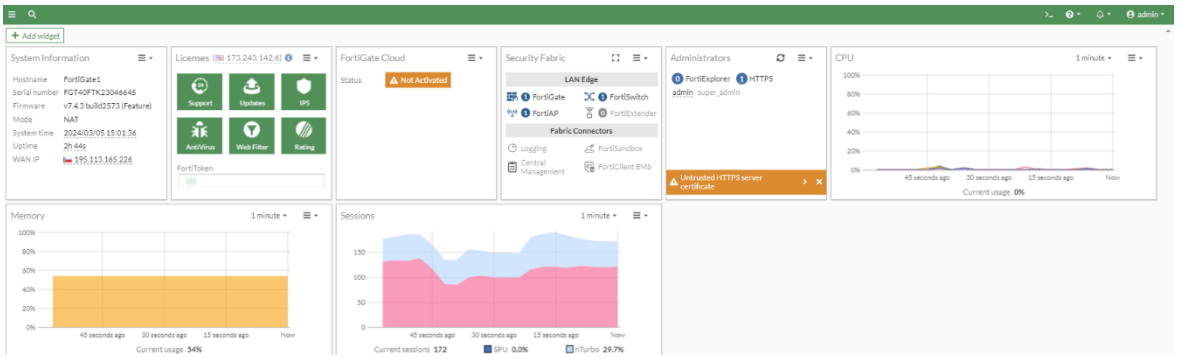
6.1.1. První přihlášení

Základním kamenem Fortinet Security Fabric je firewall FortiGate, který je schopný centrální správy a komplexní ochrany jednotlivých síťových zařízení. Pro testování byl použit model FortiGate 40F, který disponuje třemi RJ45 Ethernet porty, jedním RJ45 FortiLink portem, jedním RJ45 WAN portem, konzolovým portem a USB portem. Pro první přihlášení do Firewallu je třeba připojit zařízení pomocí WAN portu k internetu, dále existují tři možnosti připojení a to lokálně, pomocí cloud, nebo přístup dedikovaný pro iOS zařízení. Při testování bylo zvoleno lokální nastavení, při kterém se FortiGate propojí přes ethernet port 1 s počítačem na kterém je povoleno DHCP, nebo nastavena statická IP adresa 192.168.1.1 se síťovou maskou 255.255.255.0. Posledním krokem je v libovolném prohlížeči navštívit adresu 192.168.1.99 a zobrazí se stránka s přihlášením. Pro první přihlášení je nastaveno přihlašovací jméno admin a žádné heslo. Ihned poté je požadována změna hesla s minimálními požadavky osmi znaků bez jiných omezení.



Obrázek 3 – Přihlašovací obrazovka Zdroj: Vlastní

Po přihlášení je uživatel přivítán přehledným grafickým uživatelským rozhraním na záložce dashboard. Zde jsou zobrazeny různé informace o zařízení FortiGate jako název, sériové číslo, verze firmware, nainstalované licence, nebo stručný přehled Security Fabric. Dále se na levé straně nachází sloupec se záložkami, který slouží pro orientaci mezi jednotlivými možnostmi nastavení.



Obrázek 4 – Dashboard Zdroj: Vlastní

6.1.2. Aktualizace softwaru FortiGuard

Jeden z prvních řešených problémů může být právě zastaralý software FortiGuard na jednotlivých síťových zařízeních. Jelikož při využití Security Fabric je síť centrálně řízena, je firewall FortiGate schopný aktualizace nejen vlastního, ale i softwaru ostatních síťových zařízení. Nejprve je třeba navštívit záložku Systém kde se nachází položka Firmware & Registration a zde lze najít přehled jednotlivých zařízení se softwarem Fortinet. U každého lze najít momentálně nainstalovanou verzi a lze jej automaticky aktualizovat. Tato činnost zajistí možnost využití nejnovějších funkcí a zároveň poskytne nejnovější možnosti zabezpečení.

6.1.3. Změna portů pro administrativní přístup

Jedním z počátečních kroků bylo přenastavení portů používaných pro administrativní přístup jednotlivých protokolů. Pro tyto protokoly jsou přednastaveny obecně známé porty a jsou tedy jedny z prvních na které jsou vedeny pokusy o síťové útoky. Proto byli čísla portů přenastaveny u HTTPS protokolu z 80 na 1514, HTTPS z 443 na 1515, SSH z 22 na 1616 a Telnet na 1717. Zároveň byla povolena funkce přesměrování připojení přes HTTP na HTTPS a byla ponechána doba odhlášení při nečinnosti 5 minut.

6.2. Konfigurace portů FortiGate

Tato kapitola je zaměřena na konfiguraci a popis jednotlivých portů firewallu FortiGate, zajišťující správnou funkčnost, efektivitu a zabezpečení počítačové sítě a platformy Security Fabric. Popisovány budou role jednotlivých portů a jednotlivé možnosti jejich nastavení.

6.2.1. Ethernet porty

Jednou z prvních potřebných konfigurací je nastavení jednotlivých portů FortiGate, což lze provést v podzáložce Interfaces nacházející se v záložce Network.

Prvním nastavovaným portem je ethernetový port 1, pomocí kterého je připojen počítač určený pro správu firewallu. Nejprve je možné zvolit novou síťovou IP adresu na tomto portu, která bude zároveň novou adresou pro připojení do správy FortiGate. Nastavena byla adresa 192.168.100.99 a maska 255.255.255.0. Dalším nastavením je volba povolených způsobů pro administrativní přístup. Na výběr jsou možnosti HTTPS, HTTP, PING, FMG-Access, SSH, SNMP, FTM, RADIUS Autentizace a spoj Security Fabric. Při testování byl povolen protokol HTTPS, jež byl dostačující pro dané připojení, který zároveň aktivuje protokol HTTP, ten je v základu nastaven na přesměrování žádosti o připojení na HTTPS. Funkci PING je vhodné mít povolenou pouze v případě potřeby testování počítačové sítě, jelikož je častým cílem síťových útoků.[24] Možnost spoje Security Fabric je možné povolit pouze pokud již byl na FortiGate nakonfigurován Security Fabric. Další konfigurací pro tento port je DHCP server, který bude dynamicky přiřazovat IP adresy připojeným zařízením. Povolení této funkce automaticky vyplní rozsah možných přiřazovaných adres podle síťové adresy portu. Povolena byla také detekce a automatická autorizace zařízení na tomto portu.

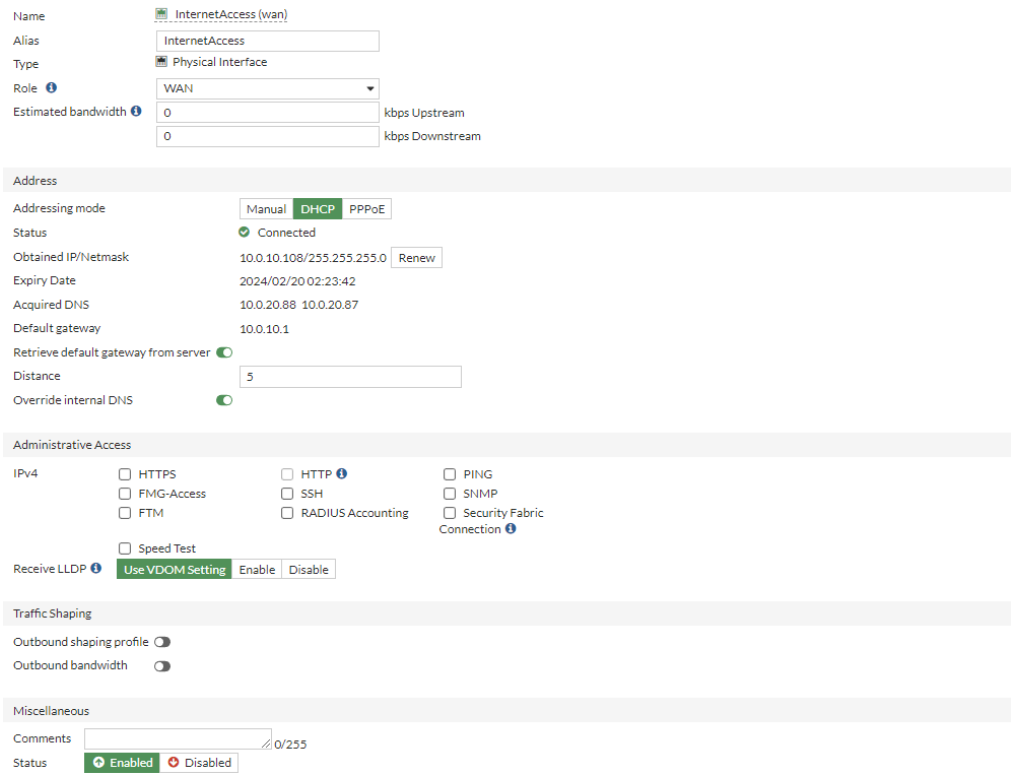
Ethernet port 3 je vhodné vypnout, jelikož v síti není využíván, tudíž nastavit je třeba pouze Ethernet port 2 ke kterému je připojen FortiSwitch port 3. Na tomto portu byla nastavena

síťová adresa 192.168.102.1 s maskou 255.255.255.0. Je povolen přístup HTTPS, k jemuž je přístup později omezen pomocí VLAN a po konfiguraci Security Fabric je povolena i možnost spoje Security Fabric. Povolena je také možnost DHCP serveru a automatická detekce nových zařízení.

6.2.2. WAN port

Přes WAN port na FortiGate je testovaná síť připojena k internetu. Pro nastavení lze nastavit statickou adresu poskytovatele internetu, dále je zde možnost PPPoE, nebo DHCP. V testované síti byla zvolena možnost DHCP. V sekci administrativní přístup není nutné povolit žádnou z možností, pokud není nutné připojovat se do sítě vzdáleně přes internet, což by mohlo vést k bezpečnostním rizikům.

Posledním krokem může být konfigurace výchozí brány pro dané rozhraní, ale pouze v případě, kdy je zvolena statická IP adresa WAN. Při použití DHCP existuje možnost získání výchozí brány od serveru a není tak nutné ji konfigurovat. Možnost ručního nastavení výchozí brány se provádí v konfiguraci statických cest.



Obrázek 5 – Konfigurace firewall WAN rozhraní Zdroj: Vlastní

6.2.3. FortiLink port

Posledním nastavovaným rozhraním je port A dedikovaný pro FortiLink. Což je speciální propojení určené pouze pro správu FortiSwitch.[35] Zde je nastaven režim adresování na Dedikováno pro FortiSwitch, konfigurována adresa 192.168.101.1 s maskou 255.255.255.0, povolena možnost uzamčení ISL, která by měla zamezit odstranění automaticky vytvořených ISL a byl zapnut DHCP server.

6.2.4. Vytvoření nového rozhraní

V záložce rozhraní se nachází také možnost vytvoření nového rozhraní, ta umožňuje konfiguraci virtuálních rozhraní, zón, virtuálních drátových párů, nebo Rozšíření WAN pomocí FortiExtender. Virtuální rozhraní se chová jako fyzická rozhraní a umožňuje stejná nastavení a může sloužit pro hromadnou konfiguraci několika fyzických rozhraní. Zóna pouze seskupí více rozhraní do jedné skupiny. Obě tyto možnosti mohou ulehčit například vytváření firewall politik tím, že lze pro veškerá obsažená rozhraní vytvořit pouze jedno pravidlo které se aplikuje na celou zónu. Virtuální drátový pár je využíván pouze ve specifických případech pro propojení dvou rozhraní bez IP adres a veškerá příchozí data mohou být odesílána pouze na druhé rozhraní.

Příkladem je vytvoření zóny VLAN_Zone do které byli zahrnuty VLAN rozhraní Office a Wifi. Obě tyto VLAN byli myšlené pro připojení případných zaměstnanců společnosti, a tak jsou požadavky na zabezpečení a přístup stejné. Avšak pokud by byla VLAN Wifi využívána pro veřejnost, bylo by vhodné separátní a přísnější zabezpečení.

6.3. FortiGate

Tato kapitola zmiňuje konkrétní funkce nabízené samotným zařízením FortiGate, které přispívají k zajištění efektivity a bezpečnosti zpravované počítačové sítě. Zmíněny jsou možnosti DNS, nastavení statických cest, firewall a DOS politiky

6.3.1. DNS

Konfigurace DNS lze nalézt v záložce Network. FortiGate má již přednastavené použití FortiGuard serverů s použitím TLS využívajícím TCP protokol, avšak při testování měla tato konfigurace poměrně časté problémy s vysokou odezvou, tudíž byla překonfigurována

na vlastní nastavení DNS serverů 8.8.8.8 pro primární server a 1.1.1.1 pro sekundární server s využitím UDP protokolu.

6.3.2. DNS server

Další možností je nakonfigurovat FortiGate jakožto DNS server, tato funkce se také nachází v záložce Network. Zapnutí DNS serveru využije FortiGate pro překlad mezi doménovými adresami a IP adresami pro síťová zařízení. Výhodou je také možnost využití DNS filtru, který umožní sledování a zakázání vybraných doménových adres.

Pro konfiguraci DNS serveru je nejprve třeba vybrat jednotlivé rozhraní na kterých bude FortiGate tuto službu poskytovat. Při vybírání rozhraní je třeba určit v jakém módu bude rozhraní poskytována služba DNS kde první možností je rekurzivní, nerekurzivní a předání systémové DNS. A druhým možným nastavením u rozhraní je, zda bude použit DNS filtr, popřípadě který konkrétní. Další součástí konfigurace DNS serveru je vytvoření DNS databáze. Zde je třeba určit typ DNS zóny z možností primární a sekundární a zda je zobrazení shadow, public, nebo proxy. Poté se určí jméno a doména DNS serveru. Dále zbývá pouze nastavit TTL a určit, zda bude DNS zóna autoritativní. Posledním krokem je přidání DNS vstupu, u kterého stačí nastavit typ pomocí výběru jedné z nabízených možností, vybrat libovolné jméno a nastavit IP adresu. Po vytvoření je ještě třeba vybrat rozhraní, pro která budou služby DNS serveru poskytována.

6.3.3. Statické cesty

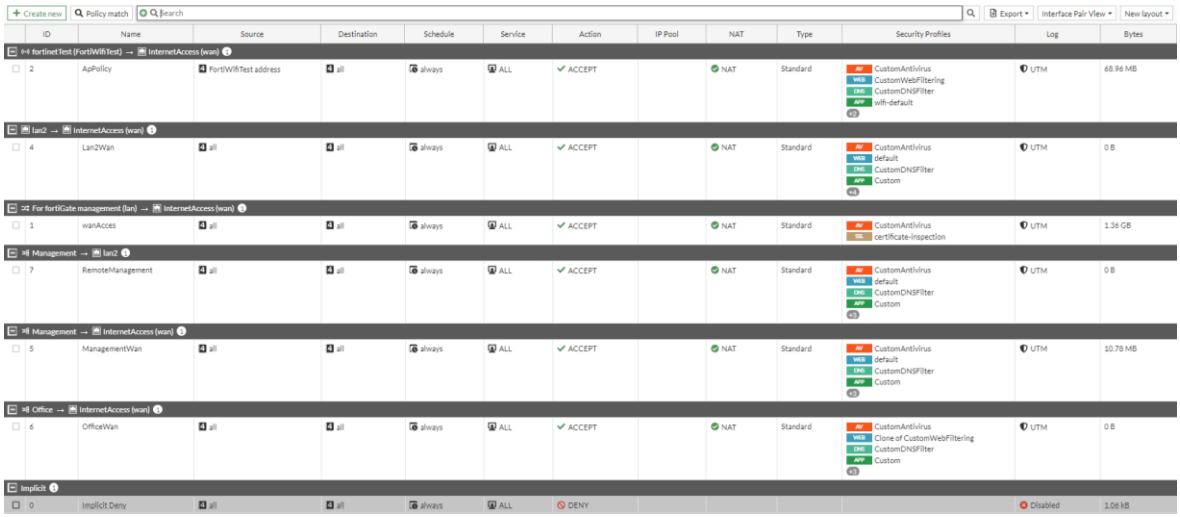
Statické cesty je nutné využít v případě využití statického směrování pro specifikaci jednotlivých cest v počítačové síti. Avšak lze je využít i v případě dynamického směrování například pro specifikaci záložních cest pro případ poruchy.

Nastavení statických cest na FortiGate se provádí v položce Static Routes a podzáložce Network. Při každém vytvoření nové statické cesty je třeba specifikovat jaká je destinace cesty pomocí výběru z možností. Dále je třeba vybrat, zda je výchozí brána manuálně specifikována, nebo dynamicky získána pomocí DHCP a posledním krokem je zvolit druhý konec statické cesty pomocí přidání rozhraní a nastavit administrativní vzdálenost.

Při testování byla konfigurována jedna statická cesta na WAN rozhraní s IP adresou 0.0.0.0/0 sloužící jako defaultní cesta pro veškerý provoz pro který nebyl v lokální síti nalezen vhodný cíl.

6.3.4. Firewall politiky

Firewall politiky jsou nástrojem, kterým lze pro konkrétní fyzická, či logická rozhraní řídit síťový provoz pomocí pravidel, která specifikují, zda je mezi zdrojovým a cílovým rozhraním povolena konkrétní služba, nebo zda je povolen celkový přenos dat mezi rozhraními.[36] Politiky jsou také jedním z míst, kde se dají aplikovat jednotlivé bezpečnostní profily, vysvětlené níže. Jedním z nejzákladnějších pravidel je přístup k internetu, kdy je zdrojovému rozhraní povolen přístup k WAN rozhraní.



Obrázek 6 – Přehled firewall politik Zdroj: Vlastní

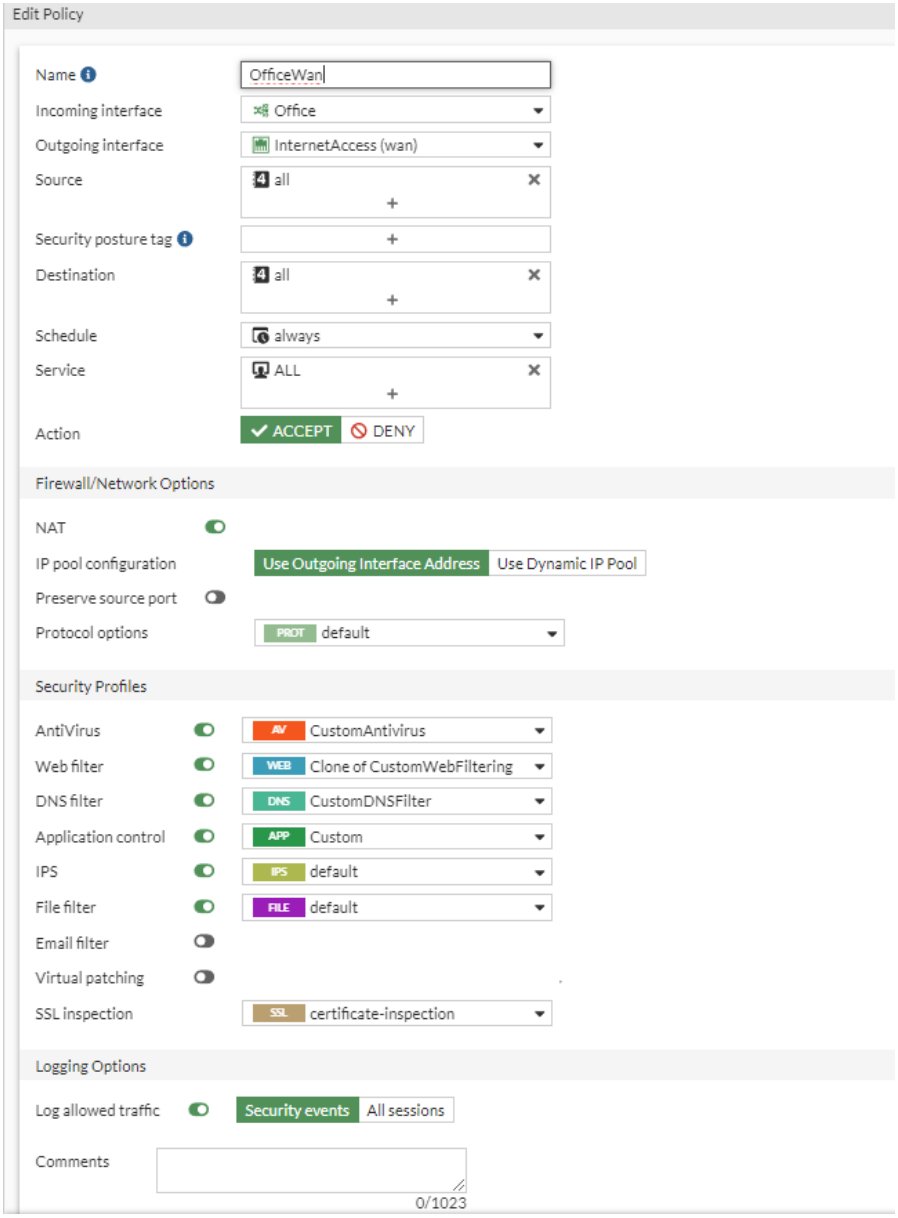
První konfigurovaná politika byla nastavena mezi WAN rozhraním a počítačem přes který probíhalo administrátorské připojení na firewall portu LAN 1 pojmenovaný WanAccess. Pomocí uložení MAC adresy počítače, se tato politika vztahuje pouze na konkrétní zařízení připojené pouze ke konkrétnímu rozhraní LAN1, tudíž při pokusu o připojení jakéhokoliv jiného zařízení by politika nebyla funkční a bylo by možné pro zajištění bezpečnosti vytvořit další politiku, která by mohla omezit práva jiných zařízení. Na tuto politiku byli aplikovány bezpečnostní profily zvyšující zabezpečení, což je antivirový profil sledující veškeré možné protokoly a blokující nalezené viry v přenášených souborech. Dalšími je emailový filtr pro blokaci spamu, profil pro prevenci průniku chránící síť proti útokům a profil pro prevenci ztráty dat ochraňující citlivá data. Posledním Aplikovaným je profil SSL/SSH kontroly povolující některým ostatním bezpečnostním profilům kontrolu šifrovaných dat.

Pro VLAN management byly nastaveny dvě politiky, první byla k WAN rozhraní a druhá byla k FortiGate LAN2 portu. Obě politiky mají nastaveny identické bezpečnostní profily jako firewall politika pro správu mezi LAN1 a WAN. Přístup k WAN rozhraní je zde pro

zajištění přístupu k internetu připojeného zařízení, avšak politika mezi rozhraním LAN2 a Management VLAN existuje pro umožnění správy FortiGate. To je umožněno díky povolení HTTP/HTTPS a SSH protokolů na obou rozhraních, avšak bez nastavení spojení mezi nimi není umožněna zařízením v Management VLAN správa FortiGate.

Další požívanou virtuální LAN byla OnboardingNAC, pro tuto VLAN byl povolen přístup k internetu, avšak veškerý provoz je zde pomocí bezpečnostních profilů monitorován. Je zde zakázán přístup k sociálním sítím a potenciálně nebezpečným webům pomocí DNS a web filtrace. Pomocí souborového filtru je zakázáno jakékoliv stahování. Použity jsou i ostatní bezpečností profily monitorující celkový provoz.

Zbylé VLAN Office a Wifi byli seskupeny do jedné skupiny rozhraní VLAN_Zone pro jednodušší aplikaci politik. VLAN_Zone má vytvořenou politiku pouze mezi rozhraním WAN pro přístup k internetu, avšak pokud by například ve společnosti existoval server se sdíleným uložištěm, bylo by třeba vytvořit politiku pro přístup k němu a totéž platí pro jakékoliv ostatní součásti sítě kam by byl nutný přístup. Aplikovány byli opět veškeré bezpečnostní profily jako u Onboarding VLAN, avšak zde jsou nastavena mírnější pravidla, které spíše monitorují síťový provoz a hledají hrozby. Například webová a DNS filtrace blokují přístup pouze k doménám nevhodným do pracovního prostředí jako jsou drogy, gambling, zbraně a další. Přenos a stahování je povoleno, ale je prováděna kontrola hledající potenciální nebezpečí.



Obrázek 7 – Konfigurace firewall politiky Zdroj: Vlastní

6.3.5. DOS politika

Tato politika je velmi důležitou vlastností firewallu FortiGate sloužící pro detekci a reakci na příchozí DoS útoky. Svoji činnost provádí na základě kontroly počtu požadavků za sekundu, pokud je překročen nastavený počet požadavků, je detekována takzvaná anomálie a firewall reaguje nastavenou reakcí.

Pro konfiguraci této politiky, je nejprve specifikovat rozhraní, na kterém budou detekována příchozí data. Dále je možné specifikovat konkrétní zdrojové a cílové adresy, nebo je možné zvolit možnost všech adres. Totéž platí pro výběr kontrolovaných služeb. Poté již zbývá v seznamů předdefinovaných anomálií třetí a čtvrté síťové vrstvy nastavit konkrétní pravidla.

Pro každou z nich lze zapnout logování, nastavit reakci z možností monitorování, blokování, nebo vypnutí sledování konkrétní anomálie. Poslední možnost je nastavení počtu výskytů konkrétní instance, kde po překročení je nahlášen výskyt anomálie.

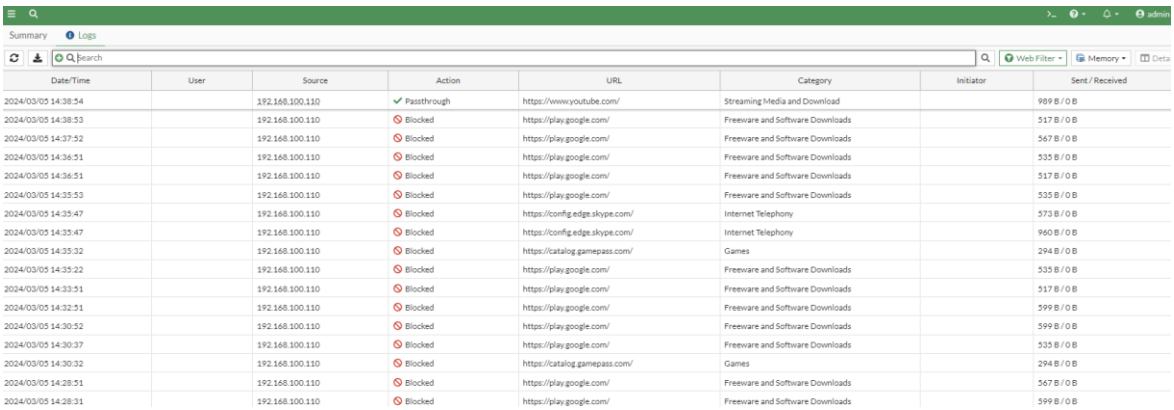
DoS politika byla vytvořena pro WAN rozhraní, které má z důvodu přímého připojení k internetu nejvyšší pravděpodobnost stát se cílem DoS útoku. Kontrolovány jsou veškeré zdrojové i cílové adresy u všech možných služeb. Logování bylo zapnuto pro veškeré nabízené anomálie. Jako reakce bylo všude nastaveno blokování a práh výskytů pro jednotlivé anomálie byl nastaven dle doporučených hodnot nalezených v oficiální dokumentaci Fortinet.[36]

6.3.6. Logování

Prostředí FortiGate nabízí záložku obsahující logy a zprávy, které jsou rozděleny do různých částí podle jejich významu. Dále zde lze najít konfigurace externího logování například s využitím FortiAnalyzer.

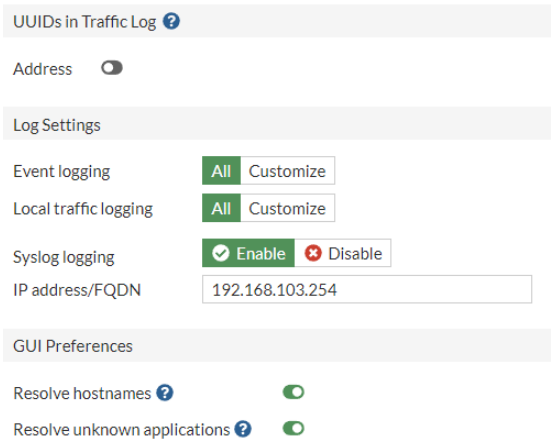
První stránkou je obecný přehled logů událostí, kde je vidět graf zobrazující množství jednotlivých událostí v systému rozdělených podle typu, či závažnosti. Dále je zde možnost zobrazení celkového seznamu logů.

Dalšími položkami v seznamu jsou stránky pro zobrazení systémových a bezpečnostních logů. Vzhled mají téměř identický, avšak liší se ve vypisovaném obsahu. Nachází se zde shrnutí, kde je zobrazen seznam pěti nejčastějších logů a obecné statistiky dané kategorie. Systémové logy zobrazují záznamy činností rozdělených do různých kategorií prováděných v systému jednotlivých zařízení zahrnutých v Security Fabric, mezi které patří například využití hardwaru jako procesor a další. Přehled bezpečnostních logů zobrazuje činnosti týkající se zabezpečení sítě a zařízení což mohou být například logy tvořené bezpečnostními profily.



Obrázek 8 – Výpis logů vytvořených profilem webové filtrace Zdroj: Vlastní

Také je možné nastavit zpracování vytvářených logů externími systémy jako je FortiAnalyzer, syslog server, nebo například systémy SIEM. V rámci testování proběhlo připojení dvou SIEM systémů AlienVault OSSIM a Wazuh. Ty byli virtuálně spuštěny na počítači připojeném přes firewall LAN 3 port. Pro základní funkčnost ze strany firewallu musela být nakonfigurována firewall politika pro umožnění přenosu dat mezi portem 3 a počítačem se spuštěným SIEM systémem. Dalším krokem je v záložce globálního nastavení logování, kde byla povolena možnost posílání všech logů událostí a lokálního síťového provozu, také bylo třeba povolit možnost syslog logování. Posledním krokem je specifikace IP adresy konkrétního SIEM systému. Výsledky logování SIEM systémů lze nalézt v bakalářské práci „Analýza řešení bezpečnostního dohledu v LAN sítích“.[37]



Obrázek 9 – Nastavení pro externí logování Zdroj: Vlastní

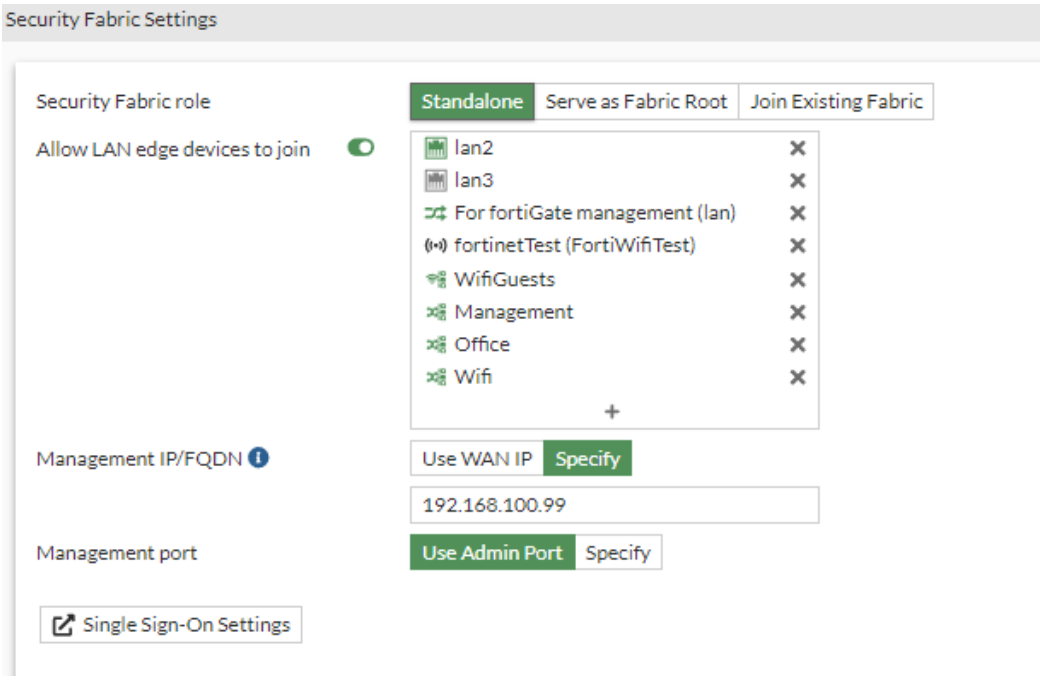
6.4. Security Fabric

V záložkách uživatelského rozhraní FortiGate se nachází také položka Security Fabric. Odtud je správce schopný samotný Security Fabric nastavit a využívat jeho funkce shrnuté v této kapitole.

6.4.1. Konfigurace

Základní konfigurace Security Fabric se provádí v záložce Fabric Connectors. Zde je možné nakonfigurovat firewall jako kořenový pro Security Fabric, připojení k existujícímu Security Fabric, nebo jako samostatná jednotka. Kořenový ve většinou firewall na nejvyšší úrovni v síti, umožňuje zobrazit celkovou topologii Security Fabric a poskytuje dalším firewallům získat nastavení pomocí připojení k existujícímu Security Fabric.[36]

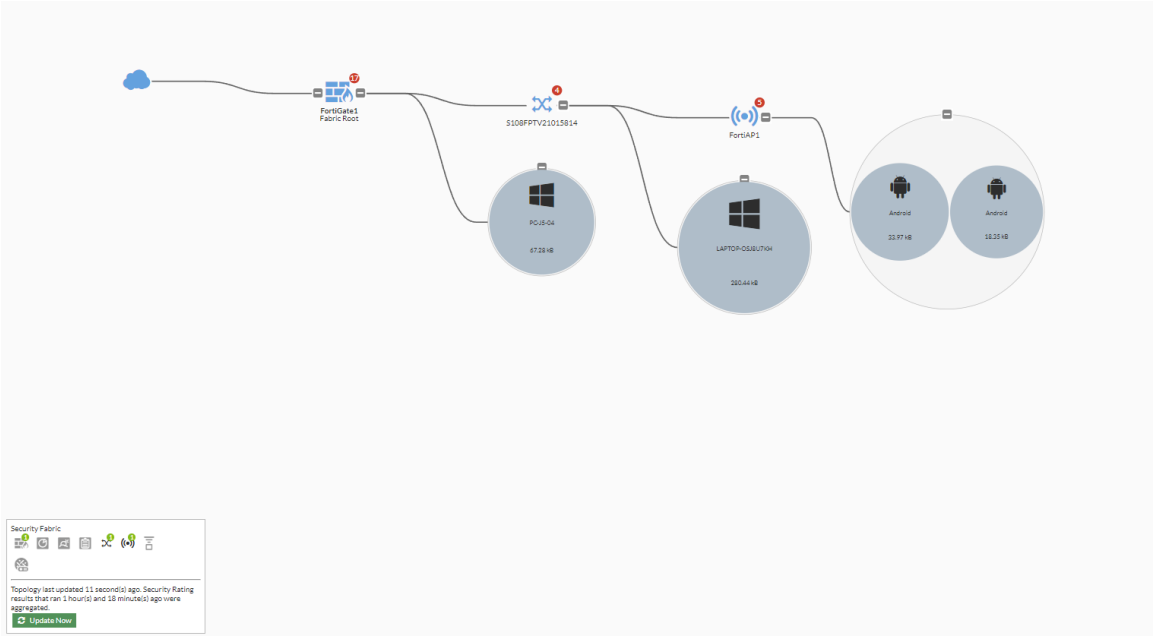
Jelikož v testované síti se nachází pouze jeden firewall, byl nastaven jako samostatný a poskytuje pro veškerá ostatní zařízení v síti veškeré výhody Security Fabric. Pro dokončení nastavení je třeba uvést na kterých rozhraních bude umožněno připojit zařízení k Security Fabric a specifikovat IP adresu a port pro správu, což je v tomto případě síťová adresa portu 1 na firewallu neboli 192.168.100.99.



Obrázek 10 – Nastavení Security Fabric firewallu Zdroj: Vlastní

6.4.2. Fyzická a logická topologie

Fyzická topologie umožňuje zobrazit síťová zařízení a koncová zařízení k nim připojená. Vzhled topologie lze měnit podle několika kategorií, a to síťového přenosu, počtu připojených zařízení, operačního systému, dodavatele hardwaru, jejich nebezpečnosti pro síť nebo bez koncových zařízení. Pokud by byla zvolena například možnost zobrazení podle síťového přenosu, byli by koncová zařízení rozdílné ve velikosti podle počtu přenesených dat. Na každé ze zařízení lze najet myší a zobrazit si o něm podrobnější informace.

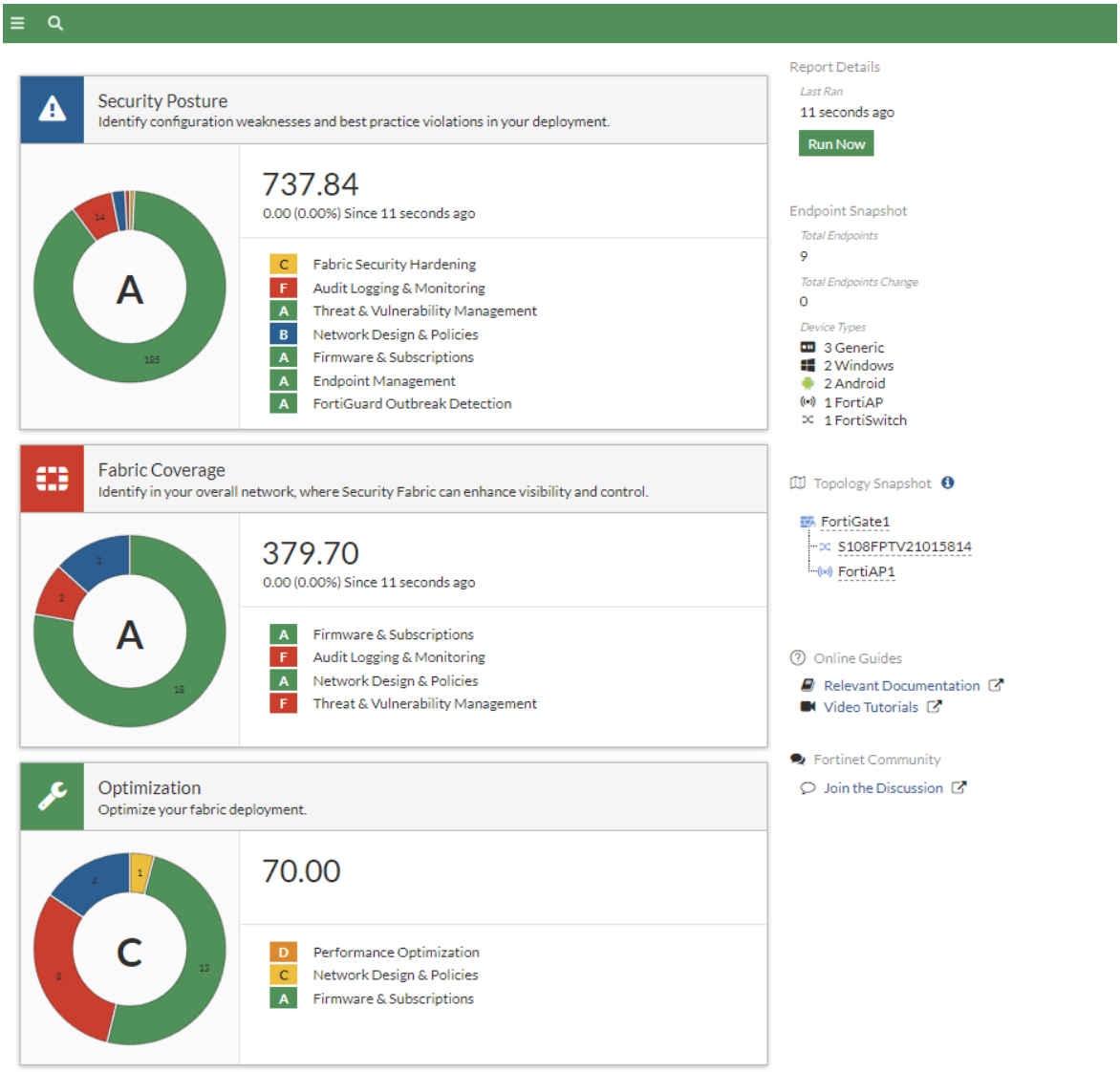


Obrázek 11 – Logická topologie Zdroj: Vlastní

Zobrazení logické topologie je velice podobné té fyzické, avšak místo zobrazení síťových zařízení vyobrazuje veškeré fyzické i logické síťové rozhraní ke kterým jsou koncová zařízení připojena.[36]

6.4.3. Hodnocení bezpečnosti

Security Fabric je schopný sledovat celkové nastavení síťových prvků a v záložce Security Rating hodnotí tři hlavní aspekty sítě, a to celkové zabezpečení, dosah Security Fabric v síti a optimalizace. Počítačová síť je podrobována mnoha testy, pomocí kterých je následně vypočítáno hodnocení mnoha podkategorií, ze kterých jsou složeny tří již zmíněné kategorie, kde F je nejhorší možné hodnocení a následují D, C, B a nejlepší možné A. Každý test má definovanou váhu pomocí čísla, při úspěšném testu je k celkovému hodnocení hodnota přičtena a při neúspěšném testu naopak odečtena.



Obrázek 12 – Hodnocení bezpečnosti Security Fabric Zdroj: Vlastní

6.5. FortiSwitch

Přepínač FortiSwitch zajišťuje komunikaci mezi zařízeními k němu připojenými. Nabízí funkce pro segmentaci, spravování a zabezpečení počítačové sítě.

6.5.1. VLAN

FortiSwitch nabízí možnost vytváření virtuálních LAN sítí. Ty napomáhají segmentaci sítě, což zvýší její celkové zabezpečení.

Vytvoření probíhá podobně jako konfigurace u obyčejných LAN portů. Pro vytvoření VLAN je nutné zadat její jméno, ID, síťovou IP adresu a její roli, což může být LAN, WAN, DMZ, nebo neurčené. Dále je možné zvolit povolené možnosti administrátorského připojení

stejně jako u LAN portů firewallu, nebo zvolit barevné označení vytvořené VLAN. Pro přidání VLAN do sítě, je třeba zajít do záložky portů směrovače kde lze pro každý port přidat nativní VLAN a další povolené VLAN.

Několik virtuálních LAN je vytvořeno automaticky pro účely některých funkcí. Například defaultFortilink1(default) byla vytvořena pro účely spravování spojení mezi FortiGate a FortiSwitch. Navíc byli vytvořeny další VLAN:

- Management – Zde jsou povoleny protokoly HTTP a HTTPS pro administrátorské připojení.
- Office a WiFi – Obě tyto VLAN jsou určeny pro připojení potenciálních zaměstnanců společnosti, WiFi VLAN není přístupná veřejnosti, tudíž jsou požadavky na zabezpečení podobné.
- OboardingNAC – Toto je speciální VLAN vytvořená pro protokol NAC.

6.5.2. Řízení přístupu k síťovým zdrojům (NAC)

Pro směrování na portech přepínače je možné využít protokolu NAC. Ten je schopný pomocí specifikovaných pravidel přiřazovat zařízení připojená k portům s aktivovaným NAC do specifických virtuálních LAN.[35]

Uživatelské rozhraní přepínače FortiSwitch nabízí vcelku rozmanitý výběr nastavení NAC pravidel. Nejprve je nutné vytvořit takzvanou onboarding VLAN, do které budou přiřazeny veškerá připojená zařízení, dokud nejsou pomocí pravidel přeřazena do jiné VLAN. Pro samotné pravidlo je nejprve třeba specifikovat, zda se tvořené pravidlo vztahuje na veškeré přepínače v síti, či pouze na některé. Dalším krokem je určení vzoru, podle kterého se bude NAC pravidlo řídit. Na výběr je přiřazování podle zařízení, uživatele, EMS štítku, nebo hrozby. U každého ze vzoru je možné řídit se podle širší skupiny až po konkrétní prvek. Například při přiřazování podle zařízení je možné řídit se například dle operačního systému připojeného zařízení, nebo konkrétně podle specifické MAC adresy a další, což umožňuje vytvořit pravidlo pro každou možnou situaci. Dále je třeba určit pouze jen do které VLAN bude zařízení přiřazeno, a to buď pomocí ovladače přepínače kde lze navíc zapnout funkci Bounce Port, nebo přiřazení zařízení do dynamické adresy. Druhou možností je přiřazení do VLAN pomocí akce bezdrátového ovladače, což je možnost určená pro bezdrátově připojená zařízení například přes přístupový bod.

V testované síti byl NAT protokol využit na všech portech přepínače, vyjma spojení FortiLink, které tuto možnost neumožňuje a bylo stanoveno několik pravidel. Nejprve byla vytvořena VLAN pojmenována OnboardingNAC, která byla nastavena jako onboarding pro NAC. Dále byli vytvořeny dvě další VLAN, Office a WiFi. Do Office VLAN jsou přiřazovány veškeré počítače připojené k fyzickým portům přepínače a poskytuje jim možnost komunikace mezi sebou a přístup k internetu. Druhá WiFi VLAN byla pomocí pravidla přiřazena k portům, ke kterým je připojen přístupový bod a má stejné vlastnosti jako Office VLAN. Takto byla síť rozdělena na dvě základní části oddělující fyzicky a bezdrátově oddělená zařízení. Také bylo vytvořeno bylo pravidlo, které přiřadí konkrétní zařízení určené MAC adresou notebooku do VLAN Management, která má povolená pravidla pro administrátorské připojení k firewallu FortiGate pomocí HTTP a SSH. Pokud je notebook připojen k jakémukoliv rozhraní se zapnutým NAC, je mu umožněno spravovat vzdáleně firewall FortiGate.

Obecně je NAC výborným nástrojem pro segmentaci sítě a prostředí FortiGuard umožňuje jeho poměrně jednoduchou a přehlednou konfiguraci.

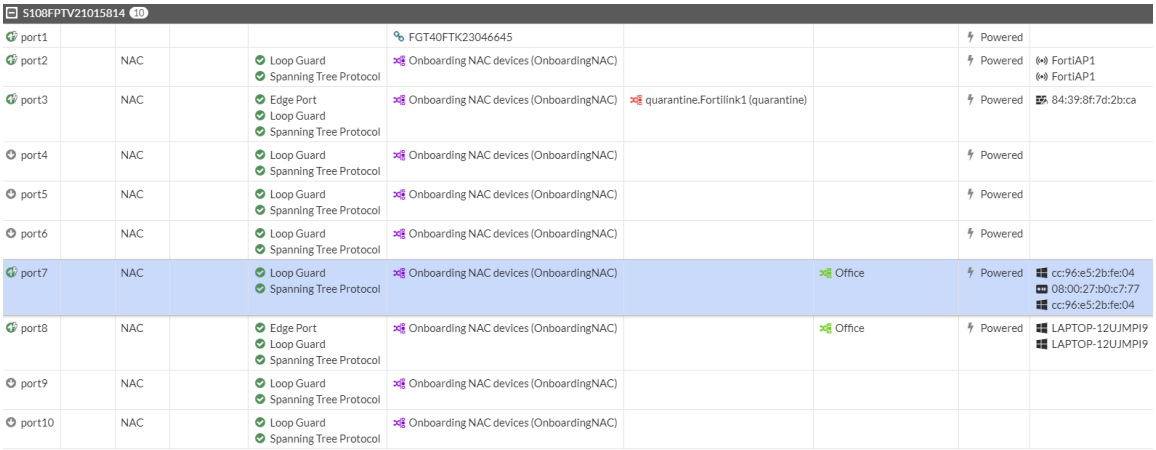
6.5.3. Nastavení portů

Prvním konfigurovaným portem je ten, který byl zvolen pro propojení pomocí FortiLink, v případě testované sítě, je to port 1 a byl již nakonfigurován na straně FortiGate firewallu. Nastavení lze provádět v okně otevřeném pomocí poklepání pravým tlačítkem myši na vybraný port. Zde lze zobrazit zařízení připojená na tento port, nastavit popisek, vyčištění čítačů portu, restartování napájení přes Ethernet a různá konkrétní nastavení portu.

Jednou z počátečních aktivit v testované síti bylo vypnutí všech nepoužívaných portů, což by v provozu zamezilo připojení neznámého zařízení, avšak všechny byli přednastaveny pro budoucí použití jako určené pro připojení koncové stanice jako počítač. Dále byla také u každého z portů vypnuta možnost napájení pomocí Ethernet, vyjma portu 2 který napájí FortiAP. Pro každý port je také možné vybrat jeden ze tří módů, statický, NAC, nebo vlastní politika.

Dále je nabízena možnost sledování DHCP, tuto možnost je dobré povolit na každém portu kde je možné připojení nových zařízení, jelikož zabraňuje tvorbě falešných DHCP serverů a DDOS útokům. Proto bylo sledování zapnuto na všech portech FortiSwitch vyjma FortiLink spojení.

FortiSwitch umožňuje na jednotlivých portech povolit protokol STP a funkce s ním spojené. Ten je vhodné mít zapnutý, pokud je v síti použito více přepínačů, které by mohli vytvořit smyčky, kterým je schopný tento protokol zamezit. Také je možné aktivovat dodatečnou ochranu proti zacyklení, která je určená jako doplnění STP protokolu. Tato pracuje na druhé síťové vrstvě a funguje na základě vysílání speciálních broadcast paketů do sítě, které pokud jsou detekovány portem, který je vyslal, znamená to, že síť je zacyklena a port je z důvodu zachování bezpečnosti vypnut. Také je možné nastavit port jako takzvaný Hraniční port, který je vhodný tehdy, kdy je k rozhraní přímo připojená koncová stanice jako je počítač. STP dále ještě nabízí funkci BPDU ochrany na druhé síťové vrstvě proti hrozbám spojeným s BPDU protokolem a druhou funkci root ochrany STP, což zabrání vytvoření takzvaného root bridge mezi dvěma přepínači. Jelikož byla testovaná síť malého rozsahu s pouze jedním přepínačem, nebyly funkce protokolu STP využity.



Obrázek 13 – Nastavení portů přepínače FortiSwitch Zdroj: Vlastní

6.6. FortiAP

V dnešní době, kdy se mobilní zařízení a notebooky stávají nezbytnými nástroji pro práci a komunikaci, je kvalitní a spolehlivé bezdrátové připojení důležitou součástí každé společnosti. V tomto kontextu se přístupový bod FortiAP stává nepostradatelnou součástí počítačové sítě s integrací Security Fabric.

6.6.1. SSID

Základním prvkem konfigurace FortiAP pro poskytování bezdrátového připojení je vytvoření identifikátoru SSID. Ten je poté přístupovým bodem bezdrátově vysílán do okolí, což umožňuje okolním zařízením detekci a následné připojení k bezdrátové síti.

Nejprve je třeba zvolit jméno pro tvořené SSID, přičemž v testované síti bylo zvoleno jméno FortiSSID. Prvním důležitým krokem je výběr jednoho ze tří režimů síťového provozu. Defaultně je nastaven režim Tunel, kdy jsou data posílána skrze WiFi ovladač. Další možností je Mesh, která je určena pro použití při zapojení více přístupových bodů v jedné počítačové síti. A poslední možností, která byla zároveň zvolena v testované síti, je možnost síťového mostu, kdy je vytvořeno přímé propojení mezi Ethernet a WiFi rozhraní přístupového bodu.[38]

Druhou částí SSID je nastavení WiFi, kde je opět třeba specifikovat jméno, avšak tento název bude zobrazován okolním zařízením, které budou detekovat WiFi signál. Defaultně je zde přednastaveno jméno fortinet, které bylo ponecháno. Dále lze specifikovat maximální počet připojených uživatelů, avšak tato možnost nebyla využita. Nastavení všesměrového vysílání SSID byla ponechána zapnutá, aby okolní zařízená byla schopná tuto síť detekovat, toto nastavení by bylo možné rozšířit o vysílání jména, modelu, nebo sériového čísla FortiAP. Poté už zbývá pouze výběr jednoho z několika módu zabezpečení, což byl v případě testování WPA2 Osobní. Výběr tohoto módu znamená, že je po uživateli pro připojení požadováno jedno, nebo více hesel, což lze nastavit v dalším kroku. V testované síti byla zvolena možnost pouze jednoho hesla. V tuto chvíli je již SSID schopné správně pracovat a zbývá jej pouze aplikovat v nastavení FortiAP. Ještě je dobré zapnutí možnosti aplikace bezpečnostních profilů, kde je možné nastavit konkrétní vytvořené profily. Je zde nabízeno několik dalších pokročilých nastavení, avšak ta nebyla v testované síti využita.

6.6.2. Nastavení

Nastavení samotného FortiAP probíhá pomocí vytvoření takzvaných FortiAP operačních profilů, které jsou pak aplikována na konkrétní připojené přístupové body. Pokud je pro přístupový bod přiřazen operační profil, ale je třeba provést malé úpravy na konkrétním zařízení, lze nastavení tohoto profilu přepsat bez jeho pozměnění. V nastavení samotného AP, se nacházejí možnosti identické jako při tvorbě FortiAP profilu, které lze libovolně nastavit a změní pouze část, která nebyla na profilu pro toto zařízení vhodná. Jelikož testovaná síť využívá pouze jeden přístupový bod, pro který byl vytvořen profil, byla funkčnost této možnosti vyzkoušena, avšak nebyla používána.

Při samotném vytváření profilu, byla vybrána možnost, kdy bude přístupový bod využívat jedno 5G pásmo, a to zbylé bude využito k monitorování, avšak ještě lze nastavit, aby obě pásma byla využívána k 5G přenosu. Přístupový bod má ještě třetí pásmo, ale to je vždy

využíváno pro přenos 2,4G. Dále je možné zapnout některé možnosti pro administrativní připojení z možností HTTPS, SSH a SNMP. Poté už zbývá pouze nastavit jednotlivá pásma, ta se od sebe v možnostech nastavení nijak neliší, vyjma využívaných technologií pro přenos 2,4G nebo 5G.

Samotné pásmo lze buď vypnout, nastavit na přístupový bod, nebo dedikovat pro monitorování. Také lze přiřadit bezpečnostní profil pro detekci vniknutí útočníka. Důležitým prvkem je výběr WiFi standardu 802.11 a přiřadit kanály které bude využívat, což ovlivní vlastností bezdrátového přenosu. Posledním krokem je přiřadit pásmu již dříve vytvořené SSID.

Testované FortiAP využívá jedno pásmo pro 2,4G, jedno pro 5G a poslední pro monitorování. Obě pásma určená pro přenos mají přiřazené již výše zmíněné SSID FortiSSID v režimu síťového mostu. Jediným rozdílem mezi pásmy je využití jiných WiFi technologií. Pásmo 2,4G využívá standardy 802.11 ax/n/g/b a pásmo 5G používá 802.11 ax/ac/n/a. Využití těchto kombinovaných standardu má za cíl podporu široké škály zařízení, která by nemusela podporovat některé konkrétní standardy.

6.7. Bezpečnostní profily

Bezpečnostní profily jsou nástroje, které umožňují definovat které typy síťového provozu má firewall sledovat a jak na ně reagovat. Jako reakci na sledovaný provoz lze vybrat blokace, povolení, nebo monitoring, dále existuje také možnost vytváření logů kontrolovaného provozu. FortiGate nabízí několik těchto bezpečnostních profilů a každý z nich má předdefinované nastavení, nebo lze vytvořit vlastní profily s unikátním jménem.

Použití jednotlivých profilů využívá prostředků firewallu což může mít za následek zpomalení síťového provozu. Je proto dobré aplikovat na jednotlivá rozhraní pouze takové profily, kde je kontrola konkrétního síťového provozu nutná.[39]

6.7.1. AntiVirus

Prvním z bezpečnostních profilů na seznamu, je antivirový profil. Jak již název napovídá, je určen pro hledání a blokování nakažených souborů, které se mohou v síti naskytnout. Lze nastavit které konkrétní protokoly pro přenos dat budou kontrolovány. Také je možné klasifikovat spustitelné soubory s příponou .exe v emailu jako vir, kontrola souborů pomocí

FortriSandbox, zahrnutí ochrany pro mobily, nebo například umístění nalezených virů do karantény.

6.7.2. Webový filtr

Profil webové filtrace představuje způsob blokování a monitorování webových stránek. V systému FortiGate je rozdělen na filtr kategorií FortiGuard a statickou filtraci.

Filtrace pomocí kategorií FortiGuard představuje možnost filtrovat pomocí předdefinovaných kategorií webového obsahu mezi které patří obsah pro dospělé, business, nebo bezpečnostní hrozby. Při nastavení je umožněno libovolně nastavit každou z těchto kategorií jako povolenou, sledovanou, blokovanou, s varováním, nebo uzamčenou za ověřením. Další možností je využít některý ze tří předdefinovaných filtrů:

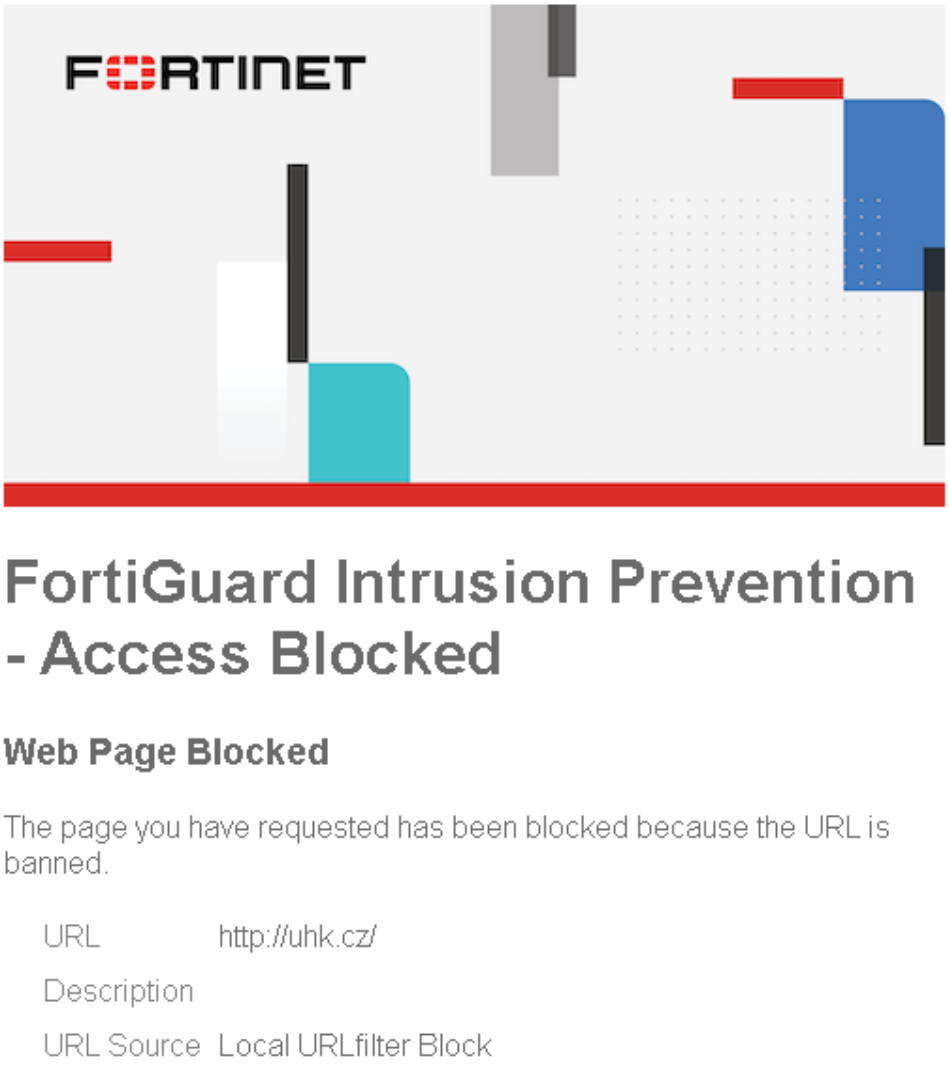
- G – Tento filtr je určen pro běžnou audienci každého věku, zakazuje přístup na weby které nejsou vhodné pro děti a mohli by urazit i dospělého.
- PG-13 – Povolí přístup na obsah označený jako přístupný od 13 let.
- R – Povolí i obsah určený pro dospělé.[36]

Pokud je zvolen některý ze zmíněných filtrů, je možné jej libovolně upravit dle potřeb sítě.

Další možností je statická filtrace definovaných URL adres. Při každém přidání nové položky do seznamu filtrace je nutné definovat URL adresu. Dále je třeba zvolit mód filtrace z možností jednoduchý, regulární výraz, nebo wildcard. Jednoduchá filtrace je aplikována pouze na přesnou shodu, tudíž pokud by filtrovaná URL adresa byla www.uhk.cz, adresa uhk.cz by filtrována nebyla.

Možnosti filtrace regulárních výrazů a wildcard jsou velice podobné a liší se především v syntaxi zadávaných URL adres. Wildcard umožní například filtraci pomocí speciálního znaku v URL jako je *.com který by filtroval jakékoliv URL adresy které mají na svém konci .com. Filtrace pomocí regulárních výrazů je o něco komplexnější, jelikož používá syntaxi Perl, která je schopna velice definovat velice specifické vzory. Obě tyto filtrace oproti jednoduché nehledají přesnou shodu, avšak jsou schopny zahrnout v jednom vzoru širší skupinu URL adres.[36]

Pro ukázku byl zablokován přístup na doménu uhk.cz. Při pokus o přístup na zablokovanou URL adresu z je uživateli zobrazena zpráva o zamezení přístupu z důvodu zablokování této adresy a je vytvořen záznam který lze zobrazit v záložce Log & Report.



Obrázek 14 – Blokace domény uhk.cz pomocí webové filtrace Zdroj: Vlastní

6.7.3. DNS filtr

DNS slouží ke stejnému účelu jako webový filtr, avšak ovládá přístup k webům pomocí DNS dotazů. Nabízí stejnou možnost filtrace pomocí kategorií FortiGuard včetně tří předdefinovaných možností G, PG13 a R, avšak chybí zde možnosti varování a ověření. Možnost statické filtrace je také stejná jako u webového filtru. Pokud je ve firewall politice používán webový filtr a DNS filtr současně, má DNS filtr přednost.[36]

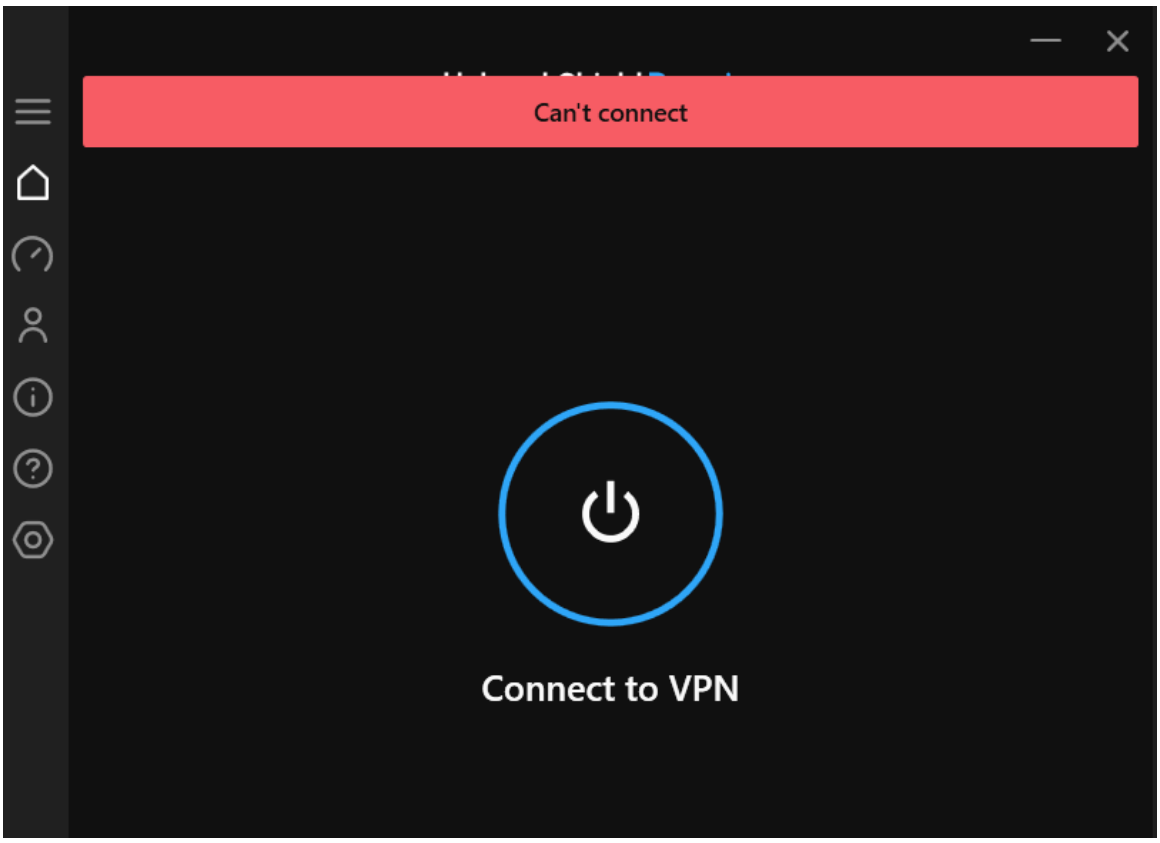
6.7.4. Kontrola Aplikací

Pomocí tohoto profilu je možné řídit síťový přístup různých aplikací. Dekodéry protokolu IPS jsou schopny analyzovat síťový provoz a najít data patřící aplikacím a tento bezpečnostní profil určí co bude s těmito daty provedeno.[36]

Při samotné konfiguraci je opět nabízena možnost filtrace pomocí předdefinovaných kategorií, u kterých lze zvolit co se s daty patřícími do této kategorie bude při detekci provede. Data lze blokovat, monitorovat, povolit, nebo přesouvat do karantény. K dispozici jsou tři přednastavení těchto kategorií a jsou jimi:

- Výchozí – Monitoruje veškeré kategorie.
- Výchozí pro WiFi – Podobná výchozí, avšak odlehčená pro urychlení WiFi provozu.
- Blokace vysoce riskantních aplikací – Zablokuje přenos aplikacím, u kterých je vysoká bezpečnostní hrozba.

V rámci testování proběhl pokus o blokaci služeb VPN. Důvodem je schopnost těchto nástrojů obejít některé typy zabezpečení jako přístup k blokovaným webovým stránkám. Jejich blokace proběhla pomocí zablokování certifikátů ISAKMP a IKE, které tyto služby většinou používají. Zde byly otestovány pokusy o připojení k VPN serverům u tří různých poskytovatelů VPN služeb na počítači i mobilním zařízení. Konkrétně byli testovány služby Touch VPN pro mobilní telefon, Nord VPN pro počítač a Shield VPN pro obojí z těchto zařízení. Všechny testované služby dosáhly jednotného výsledku, při pokusu o připojení k serveru po chvíli zobrazily chybu a nebyli schopny se připojit.



Obrázek 15 – Ukázka blokace VPN služby Hotspot Shield Zdroj: Vlastní

Také byli v předdefinovaných kategoriích zakázány hry a sociální sítě. Při pokusu o spuštění jakékoliv online hry byl odepřen přístup k serverům a hry nebyli schopné se spustit. Podobný výsledek byl i u sociálních sítí které nebyli schopné načíst nové příspěvky, tudíž není blokován přístup na tyto webové stránky jako u webového filtru, avšak je blokována komunikace se servery těchto služeb a aplikací.

6.7.5. Prevence průniku

Systém prevence průniku neboli IPS, je velmi důležitou součástí Firewallů nové generace. Pomocí různých technologií, jakými je porovnávání signatur, dekodéry protokolů, heuristiku, zpravodajství o hrozbách a další pokročilé způsoby detekce hrozeb pro detekci a prevenci známých i neznámých hrozeb. Systém prevence průniku FortiGate je také schopný hledat hrozby pomocí hloubkové inspekce paketů, a to i zašifrovaných.[36]

6.7.6. Souborový filtr

Tento bezpečnostní profil umožňuje kontrolu nad soubory procházející přes firewall FortiGate. Soubory jsou blokovány nebo povoleny pouze na základě jejich typu. Pro konfiguraci tohoto filtru je pouze nutné vybrat které protokoly používané pro přenos, budou

kontrolovány a zda budou prohlédány příchozí, odchozí, nebo oba směry toku dat. Druhým krokem je vybrat konkrétní typy souborů a zda budou monitorovány, nebo rovnou blokovány.

6.7.7. Emailový filtr

Filtr emailů slouží pro detekci nevyžádaných zpráv. Pro každý protokol používaný pro posílání pošty, lze nastavit co bude provedeno s nalezenými nevyžádanými zprávami. Tyto zprávy lze nechat projít, odstranit, nebo jim přiřadit štítek s libovolným označením. Existuje také možnost lokální filtrace, do které lze vložit libovolná slova, nebo například emailové adresy které bude FortiGate detekovat.

6.7.8. Prevence ztráty dat

Tento profil se stará o zabezpečení citlivých dat jako jsou čísla kreditních karet, údaje dokladů, nebo například finanční záznamy. Tato data jsou v síti detekována a je zabráněno jejich úniku, či naopak jejich vniknutí.

Pro konfiguraci tohoto profilu je třeba pouze přidávat pravidla ze kterých bude profil sestaven. Pro přidání nového pravidla je nutné specifikovat několik aspektů. Po pojmenování je vybrat senzor u kterého je na výběr ze tří předdefinovaných možností, nebo lze vytvořit vlastní. Tento senzor specifikuje, na které aktivity bude pravidlo reagovat. Dalším krokem je určit závažnost daného pravidla z pěti dostupných úrovní kterými jsou informační, nízká, střední, vysoká a kritická závažnost. Navazuje nastavení reakce na detekované pravidlo což může být povolit, zaznamenat, blokovat, nebo přesunutí IP adresy do karantény. Poté už zbývá pouze vybrat, zda je kontrolovaná zpráva anebo soubor, u kterého je dále ještě třeba specifikovat typ souboru. Posledním krokem je určit u kterých protokolů bude kontrola prováděna.

6.7.9. Virtual Patching

Virtual patching je technologie využívaná pro co nejdřívější detekci příchozího síťového útoku. Cílem je odvrátit útok dříve, než je schopný napadení citlivých zařízení.[36]

Konfigurace má podobný základ jako jiné profily. Je třeba specifikovat jméno, reakce v podobě povolit, nebo blokovat a zda má být po detekci vytvořen záznam. Je také nezbytné určit úrovně závažnosti, na které bude profil reagovat, prostřednictvím zaškrtnutí možností v nabídce, která nabízí úrovně závažnosti: nízká, střední, vysoká a kritická. V základní

konfiguraci jsou detekovány veškeré hrozby z vybraných úrovní a je možné pouze přidat výjimky, které nebudou při detekci řešeny. U tvořené výjimky lze specifikovat MAC adresa zařízení, na které bude výjimka platit a dále jsou přidávány buď vlastní, nebo předdefinované ID signatury konkrétních hrozeb.

6.7.10. SSL/SSH kontrola

Tento profil slouží spíše jako rozšíření funkčnosti webové, emailové filtrace a antivirovému profilu, kterým umožňuje zpracovávat i šifrovaná data.[36]

Prvním krokem při konfiguraci této politiky je určení, zda bude inspekce určena pro obecný síťový provoz, kde není určen cíl komunikace, nebo zda existuje v politice, na kterou bude tento profil aplikován, přesně specifikovaný cílový server, který bude tímto profilem ochraňován. Poté je vhodné zvolit, zda bude kontrola pouze ověřovat použitý certifikát, nebo zda bude inspekce probíhat i pro šifrovaná data. Dalším důležitým krokem je volba certifikátu pro inspekci jednotlivých paketů, kde je defaultně pouze možnost předinstalovaného Fortinet_CA_SSL, avšak lze importovat další. Následující kroky slouží pro nastavení reakce na některé situace. První z nich je možnost povolit, či zakázat potenciálně nebezpečné certifikáty, které lze zobrazit. Dále je možné nastavit reakci na nedůvěryhodné certifikáty v podobě povolit, blokovat, či ignorovat a je opět možné zobrazit list s informacemi o které certifikáty se jedná. Také je možné ověření serverového SNI certifikátu kdy, pokud je ověření povoleno může být server využít svůj URL filtr, nebo pomocí volby striktního režimu může být přerušeno spojení. Další možnosti jsou určeny pouze pro plnou SSL inspekci a mohou povolit některé specifické funkce.

Ve druhé sekci konfigurace se nachází seznam přenosových protokolů, přičemž je možné kontrolovat veškeré porty, nebo lze u každého z protokolů specifikovat konkrétní číslo používaného portu.

Mezi další možnosti patří možnost nastavení výjimek, kde lze specifikovat konkrétní skupiny obsahu, jako je například zdravotnictví, nebo je možné specifikovat adresy konkrétních služeb. Obě tyto možnosti je možné vybrat z předdefinovaného seznamu možností.

Poslední sekce slouží pro obecné nastavení a umožňuje nastavit reakci na certifikáty které jsou například prošlé, či zneplatněné.

Tento profil byl využit pro veškeré firewall politiky, na které byli aplikovány profily pro kontrolu spamu, webových adres či antiviru. Byli využity předdefinované profily, především profil pro hloubkovou inspekci paketů, jelikož se konfigurace těchto profilů zdála dostačující.

7. SHRNUTÍ

Analýza možností a nástrojů Security Fabric počala vytvořením malé testovací sítě složené z přístupového bodu FortiAP, přepínače FortiSwitch a firewallu FortiGate, který celý Security Fabric centrálně spravuje. V počátku je třeba zapnout a nastavit na firewallu možnost Security Fabric, aby byl schopný spravovat a poskytovat funkce ostatním zařízením. Prvním stěžejním bodem bylo uvést počítačovou síť do funkčního stavu, což zahrnovalo především konfiguraci jednotlivých portů zařízení, firewall politik mezi nimi a vytvoření SSID pro přístupový bod jež umožňuje bezdrátové připojení k síti.

Ve chvíli, kdy byla počítačová síť schopna komunikace mezi jednotlivými zařízeními započala fáze zabezpečení a zefektivnění vytvořené sítě. To zahrnuje aktualizaci softwaru jednotlivých zařízení do nejnovější verzí, bezpečnostní profily, segmentaci sítě, nebo nastavení DNS serveru. Na firewall politiky byli aplikovány některé předdefinované a některé vlastní bezpečnostní profily, které zajišťují bezpečnost v sítí a monitorují pomocí logů různé aktivity v síti. Segmentace sítě proběhla pomocí vytvoření VLAN na přepínači, které byly následně pomocí NAC dynamicky přiřazovány připojeným zařízením pomocí specifikovaných pravidel. Také byl firewall nakonfigurován jakožto DNS server poskytující ostatním připojeným zařízením DNS adresy s aplikovaným bezpečnostním profilem DNS filtrace.

V poslední fázi testování proběhla analýza prostředků pro logování a monitorování sítě. Mezi důležité nástroje patří zobrazení logické a fyzické topologie, které nabízejí mapu celé síťové topologie, která může měnit podobu podle specifikovaných pravidel. Zobrazením topologií lze zjistit, jak jsou mezi sebou jednotlivá zařízení v sítí propojena. Další analyzovanou funkcí bylo zobrazení logů. Ty jsou v Security Fabric rozděleny na dvě části, systémové a bezpečnostní a nabízí možnost sledovat efektivitu a zabezpečení počítačové sítě. V neposlední řadě proběhlo také připojení systému SIEM, který představuje nástroj pro sběr a analýzu dat v síti.

Infrastruktura Security Fabric nabízí nástroje pro efektivní správu a zabezpečení počítačové sítě. Díky své flexibilitě a škálovatelnosti umožňuje organizacím přizpůsobit správu a ochranu jejich sítě specifickým potřebám a požadavkům. Tyto vlastnosti dělají ze Security Fabric ideální nástroj využitelný pro síť s takřka libovolnými požadavky.

8. ZÁVĚR

Bakalářská práce se zabývá tématy spojenými s testováním a simulací počítačových sítí a jejich zabezpečení. V rámci teoretické části proběhlo seznámení s konkrétními nástroji určené pro simulaci, či testování efektivity provozu a bezpečnosti počítačových sítí, přičemž byli zmíněny jejich přednosti a praktické využití.

Další část byla věnována kybernetickým útokům. Nejprve byl zmíněn úvod do tématiky počítačových útoků v podobě představení několika nejčastěji se vyskytujících typů útoků společně s obecným popisem jejich provedení. Poté se práce zabývala konkrétními hrozbami síťových vrstev OSI a rozdělena byla do několika částí podle jednotlivých OSI vrstev. U každé z vrstev byli nejprve popsány protokoly a slabiny, které bývají častým cílem kybernetických útoků. Následně se práce zaměřila na konkrétní útoky, které cílí na identifikovaná slabá místa jednotlivých vrstev sítě. Tyto útoky byly detailně popsány včetně jejich metodiky, cílů, potenciálních dopadů a v neposlední řadě byli zmíněny způsoby, jak se proti daným útokům bránit.

Poslední kapitola teoretické části se zaměřila na zabezpečení počítačových sítí. Jsou zde uvedeny základní nástroje a osvědčené praktiky, které slouží pro efektivní ochranu sítě před kybernetickými útoky a dalšími hrozbami. V rámci popisu těchto nástrojů je vysvětleno, na jakém principu pracují a jak jsou využívány k eliminaci hrozeb.

Praktická část práce je zaměřena na analýzu možností Security Fabric v podobě popsání funkčnosti nabízených nástrojů a možnosti jejich konfigurace. Nejprve se zaměřila na základní nastavení důležité pro další postup jako je první přihlášení a aktualizace softwaru zařízení obsažených v Security Fabric. Dále byly prozkoumány prvky určené pro správné fungování síťové infrastruktury ze strany firewallu. To zahrnuje konfiguraci jednotlivých rozhraní a firewall politiky, nebo nastavení DNS. Následovala kapitola Security Fabric popisující nástroje pro centrální monitorování a správu počítačové sítě pomocí firewallu FortiGate. Navazují kapitoly FortiSwitch a FortiAP zaměřené na možnosti nabízené těmito zařízeními v rámci Security Fabric. Přepínač FortiSwitch testované síti nabízel především možnost segmentace pomocí VLAN a NAC, zatímco přístupový bod FortiAP poskytl možnost bezpečného bezdrátového připojení k počítačové síti. Posledním probíraným tématem bylo důkladné popsání bezpečnostních profilů poskytujících testované počítačové sítí co nejlepší možné zabezpečení.

Celkově lze konstatovat, že práce poskytuje ucelený pohled na problematiku kyberbezpečnosti, simulačních a testovacích nástrojů počítačových sítí a jejich zabezpečení. Zahrnuje důkladné seznámení s teoretickými základy těchto oblastí, včetně konkrétních nástrojů, detailního popisu kybernetických útoků a možností obrany proti nim. Nabízí také detailní pohled na možnosti Security Fabric. Důkladně zkoumá funkčnost a možnosti konfigurace poskytovaných nástrojů s důrazem na efektivní zabezpečení počítačové sítě.

9. SEZNAM POUŽITÉ LITERATURY

9.1. Internetové zdroje

[1] Products, Solutions, and Services. *Cisco* [online]. [vid. 2023-10-22]. Dostupné z: https://www.cisco.com/c/en/us/products/index.html

[2] NEDBAL, Jaroslav. Jak si nasimulovat provoz datové sítě? S tím vám pomůže Cisco Packet Tracer. *Jaroslav Nedbal* [online]. 9. únor 2021 [vid. 2023-10-20]. Dostupné z: https://www.jaroslavnedbal.cz/jak-si-rychle-navrhnout-a-otestovat-datovou-sit-s-tim-vam-pomuze-cisco-packet-tracer/

[3] JAVID, SHEIKH. Role of Packet Tracer in learning Computer Networks. *International Journal of Advanced Research in Computer and Communication Engineering*. 2014, 3, 2278–1021.

[4] CLARKE, Joe. Cisco Modeling Labs: Labbing Made Easy. *Cisco Blogs* [online]. 29. červenec 2022 [vid. 2023-10-21]. Dostupné z: https://blogs.cisco.com/learning/cisco-modeling-labs-labbing-made-easy

[5] Cisco Modeling Labs. *Cisco* [online]. [vid. 2023-10-21]. Dostupné z: https://www.cisco.com/c/en/us/products/cloud-systems-management/modeling-labs/index.html

[6] *What is Fortinet?* [online]. [vid. 2023-10-22]. Dostupné z: https://www.cbtnuggets.com/blog/certifications/security/what-is-fortinet

[7] Fortinet Security Fabric for Securing Digital Innovations. *Fortinet* [online]. [vid. 2023-10-21]. Dostupné z: https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric

[8] Fortinet Security Fabric zajišťuje bezpečnost virtuálního prostředí. *Lupa.cz* [online]. [vid. 2023-10-21]. Dostupné z: https://www.lupa.cz/pr-clanky/fortinet-security-fabric-zajistuje-bezpecnost-virtualniho-prostredi/

[9] Network Device Testing - FortiTester. *Fortinet* [online]. [vid. 2023-10-22]. Dostupné z: https://www.fortinet.com/de/products/fortitester.html

[10] *FortiTester Data Sheet* [online]. B.m.: Fortinet. 23. květen 2023. Dostupné z: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiTester.pdf

[11] *MITRE ATT&CK Breach simulation cookbook | Administration Guide* [online]. [vid. 2023-10-22]. Dostupné z: https://docs.fortinet.com/document/fortitester/7.3.0/administration-guide/897191/docs.fortinet.com/document/fortitester/7.3.0/administration-guide/897191/mitre-att-ck-breach-simulation-cookbook

[12] FortiGuard AI-powered Security Services. *Fortinet* [online]. [vid. 2023-10-22]. Dostupné z: https://www.fortinet.com/solutions/enterprise-midsize-business/security-as-a-service/fortiguard-subscriptions

[13] HARMON, Andrew. What Is FortiGuard? See the Security Services Available for your FortiGate. *Firewalls.com* [online]. 31. říjen 2018 [vid. 2023-10-22]. Dostupné z: https://www.firewalls.com/blog/what-is-fortiguard/

[14] *MITRE ATT&CK®* [online]. [vid. 2023-10-30]. Dostupné z: https://attack.mitre.org/#

[15] What Is MITRE ATT&CK - Definition | VMware Glossary. *VMware* [online]. [vid. 2023-10-30]. Dostupné z: https://www.vmware.com/topics/glossary/content/mitre-attack.html

[16] *Caldera* [online]. [vid. 2023-12-19]. Dostupné z: https://caldera.mitre.org/

[17] *CALDERA™ | MITRE* [online]. [vid. 2023-12-19]. Dostupné z: https://www.mitre.org/ourimpact/intellectual-property/caldera

[18] OOTEGHEM, Karel Van. Threats to network security and network attacks. *Parallels Remote Application Server Blog - Application virtualization, mobility and VDI* [online]. 7. únor 2023 [vid. 2023-10-20]. Dostupné z: https://www.parallels.com/blogs/ras/network-attacks/

[19] BAKER, Kurt. 10 Most Common Types of Cyber Attacks Today. *CrowdStrike* [online]. 13. únor 2023 [vid. 2023-10-20]. Dostupné z: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/#10.%20IoT-Based%20Attacks

[20] ALOTAIBI, Albandari, Bedour ALRASHIDI, Samina NAZ a Zahida PARVEEN. Security issues in Protocols of TCP/IP Model at Layers Level. 2017.

[21] ROZEN, Lior. HTTP Attacks. *Radware* [online]. 15. listopad 2017 [vid. 2023-10-20]. Dostupné z: https://www.radware.com/blog/security/2017/11/http-attacks/

[22] HANÁK, Jiří. Nejčastějšími DDoS útoky jsou SYN a UDP záplavy. *MasterDC* [online]. 22. říjen 2015 [vid. 2023-10-20]. Dostupné z: https://www.master.cz/blog/jak-funguji-ddos-utoky-typy-ddos-syn-udp-zaplavy/

[23] *Loop DoS: New Denial-of-Service attack targets application-layer protocols* [online]. [vid. 2024-04-10]. Dostupné z: https://cispa.de/en/loop-dos

[24] MAZERIK, Ryan. ICMP attacks. *Infosec* [online]. 12. březen 2018 [vid. 2023-10-20]. Dostupné z: https://resources.infosecinstitute.com/topics/hacking/icmp-attacks/

[25] S, David E. Lares. Common TCP/IP OSI layer attacks. *Medium* [online]. 13. prosinec 2021 [vid. 2023-10-20]. Dostupné z: https://systemweakness.com/common-tcp-ip-osi-layer-attacks-51e4b9f99fb1

[26] What is Network Security? *IBM* [online]. [vid. 2023-10-20]. Dostupné z: https://www.ibm.com/topics/network-security

[27] What Is Network Security? Definition and Types. *Fortinet* [online]. [vid. 2023-10-20]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/what-is-network-security

[28] Firewall. *ESET* [online]. [vid. 2023-10-20]. Dostupné z: https://www.eset.com/cz/firewall/

[29] *Co je antivirus | ESET* [online]. [vid. 2024-04-16]. Dostupné z: https://www.eset.com/cz/antivirus-software/

[30] What Is Network Segmentation? *Cisco* [online]. [vid. 2023-10-20]. Dostupné z: https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

[31] What is IDS and IPS? *Juniper Networks US* [online]. [vid. 2023-10-20]. Dostupné z: https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html

[32] SHAH, Nirav a Alexandra MEHAT. Fortinet Named a 2023 Gartner® Peer Insights™ Customers' Choice for Security Service Edge (SSE). *Fortinet Blog* [online]. 6. říjen 2023 [vid. 2024-03-29]. Dostupné z: https://www.fortinet.com/blog/business-and-technology/fortinet-2023-gartner-peer-insights-security-service-edge

[33] FORTINET. *Fortinet Document Library | Home* [online]. [vid. 2024-04-04]. Dostupné z: https://docs.fortinet.com/

[34] BOUSKAP@SAMURAJ-CZ.COM, Petr Bouška-Samuraj; e-mail: SAMURAJ-cz.com - administrace, počítačové sítě, Cisco, Microsoft, Fortinet, NetApp, Veeam, VMware. *SAMURAJ-cz.com* [online]. [vid. 2024-04-04]. Dostupné z: https://www.samuraj-cz.com/

[35] *FortiOS 7.4.2 | FortiLink Guide* [online]. [vid. 2024-04-16]. Dostupné z: https://docs.fortinet.com/document/fortiswitch/7.4.2/fortilink-guide/950458/docs.fortinet.com/document/fortiswitch/7.4.2/fortilink-guide/950458/what-s-new-in-fortios-7-4-2

[36] FORTINET. *FortiGate | FortiOS 7.4.3 | Getting started | Administration Guide* [online]. [vid. 2024-04-10]. Dostupné z: https://docs.fortinet.com/document/fortigate/7.4.3/administration-guide/954635/docs.fortinet.com/document/fortigate/7.4.3/administration-guide/954635/getting-started

[37] BÍLÝ, Aleš. *Analýza řešení bezpečnostního dohledu v LAN sítích*. Hradec Králové, 2024. Bakalářská práce. Fakulta informatiky a managementu Univerzity Hradec Králové.

[38] FORTINET. *FortiWiFi and FortiAP Configuration Guide* [online]. [vid. 2024-04-16]. Dostupné z: https://docs.fortinet.com/document/fortiap/7.4.2/fortiwifi-and-

fortiap-configuration-guide/13665/docs.fortinet.com/document/fortiap/7.4.2/fortiwifi-and-fortiap-configuration-guide/13665/whats-new-in-this-release

[39] *Security profiles | Best Practices* [online]. [vid. 2024-03-07]. Dostupné z: https://docs.fortinet.com/document/fortigate/7.4.0/best-practices/889496/docs.fortinet.com/document/fortigate/7.4.0/best-practices/889496/security-profiles

10. Seznam obrázků

11. ZADÁNÍ PRÁCE Z IS (eVŠKP)

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání bakalářské práce

Autor:	**Martin Mičkech**
Studium:	I2100246
Studijní program:	B1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název bakalářské práce:	**Analýza využitelnosti simulačních nástrojů pro síťovou bezpečnost**
Název bakalářské práce AJ:	Analysis of the usability of simulation tools for network security

Cíl, metody, literatura, předpoklady:

Cílem práce je zmapovat možnosti využitelnosti simulačních nástrojů pro testování síťové bezpečnosti a na vybraných řešeních navrhnout a realizovat sadu laboratoních úloh zaměřených na síťovou bezpečnost.

Osnova:

1. Úvod
2. Popis Packet Tracer
3. Popis Mitre Att&ck
4. Popis Fortinet nástrojů
5. Zabezpečení sítí
6. Praktické testování v laboratoři
7. Výsledky testování
8. Závěr

Zadávající pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	doc. Mgr. Josef Horálek, Ph.D.
Datum zadání závěrečné práce:	20.1.2023