Krycí list dokumentu	
Název:	BC107882 – Projekt redesign infrastruktury WAN/LAN
Typ:	**Prováděcí projekt „Redesign infrastruktury WAN/LAN“**
Určení:	IT
Adresát:	Povodí Labe, státní podnik, Víta Nejedlého 951/8, 500 03 Hradec Králové
Verze:	2.1
Datum vydání:	2.11.2022
Autoři:	Richard Vodička, richard.vodicka@autocont.cz Michal Havlíček, michal.havlicek@autocont.cz
Správce:	Petr Křivka, petr.krivka@autocont.cz

Pozor dokument obsahuje důvěrné informace!
Tato verze neobsahuje hesla!

Společnost AUTOCONT a.s. tímto uděluje oprávnění pro Povodí Labe, státní podnik k reprodukování, uchovávání nebo přenášení jakýmkoli způsobem včetně elektronického, magnetického, fotografického či jiného záznamu dokumentu Prováděcí projekt „Redesign infrastruktury WAN/LAN“.

_____

Bc. Petr Křivka, Manažer realizačních týmů, AUTOCONT a.s.

Obsah

1. Cíl projektu

Cílem projektu je snížení rizik bezpečnostních incidentů v podnikové síti prostřednictvím její segmentace na menší části (různé typy technologických sítí, administrativní sít apod.) s řízenou vzájemnou komunikací. Projekt obsahuje návrh architektury LAN v koncových lokalitách (61) a v centrální lokalitě, včetně návrhu IP adresace.

1.1 Obecné požadavky na projekt

Projekt mimo návrhu cílového stavu nastiňuje i cestu (návrh postupu, doporučení), jak se k tomuto cílovému stavu dobrat:

- návrh postupu upgradu redesignu všech lokalit včetně centra v HK, stanovení časové náročnosti, s ohledem na minimalizaci doby výpadků při výměně, konfiguraci a zprovoznění
- návrh eventuálního rozdělení celé akce do postupných etap, zhodnocení důsledků rozdělení této akce do jednotlivých etap
- odhad celkové ceny nového řešení i jednotlivých etap při postupné realizaci
- preferovat řešení od jednoho výrobce (jednotná správa aktívních prvků, udržitelné nároky na rozsah a spektrum znalostí administrátorů)
- stanovení všech parametrů pro výběr HW i SW tak, aby bylo příslušnou část projektu možné použít jako podklad pro výběrové řízení na HW a kompletní službu montáže, konfigurace a zprovoznění
- zhodnocení náročnosti správy navrženého řešení, návrh školení zainteresovaných správců a doporučení jejich počtu s ohledem na počet lokalit a jejich rozptýlenost

2. Stávající stav

Síťová infrastruktura Povodí Labe, s.p. (dále jen PLA) je rozlehlá síť provozovaná v lokalitách v oblasti povodí horního a středního Labe. Aktuální infrastruktura je tvořena LAN a WAN prvky různých výrobců, převážně staršími modely zařízení, většinou již s ukončenou podporou výrobce.

Dotčená síťová technika je umístěna v následujících lokalitách:

Lokalita PLA	Zkratka
Bedřichov	
Brandýs nad Labem	
Čelákovice	
České Kopisty	
Dolní Beřkovice	
Fojtka, Fojtecká	
Hamry, Studnice	
Harcov, Liberec	
Hradišťko	
Hučák, Hradec Králové	
Hvězda (rybník), Opatov	
Josefův Důl	
Klavary - Veltruby	
Kolín	
Kostelec nad Labem	
Kostomlátky	
Křižanovice	
Labská	
Les Království - Bílá Třemešná	
Lobkovice, Mlékojedy	
Lovosice	
Lysá nad Labem	
Mšeno - Jablonec nad Nisou	
Nymburk	
Obříství	
Pařížov - Běstvina	
Pastviny	
Poděbrady	
Pracoviště Náchod	
Předměřice	
Přelouč, Břehy	
Rozkoš	
Rudolfov (MVE)	
ŘSP	
Seč	
Smiřice	

Souš - Desná	[redacted]	
Srnojedy		
Středisko Čáslav		
Středisko Děčín		
Středisko Dvůr Králové		
Středisko Hradec Králové		
Středisko Jičín		
Středisko Kostomlaty		
Středisko Litoměřice		
Středisko Mladá Boleslav		
Středisko Turnov		
Středisko Vaňov - Ústí		
Středisko Vysoké Mýto		
Středisko Žamberk		
Střekov		
Štětí, Račice		
Týnec		
Veletov		
Velký Osek		
Vrchlice - Miskovice		
Závod Jablonec nad Nisou		
Závod Pardubice		
Závod Roudnice nad Labem		
Závod Střední Labe		
Zlíč (rozd. Objekt)		

Tabulka 1 - Lokality PLA

2.1.1 WAN síť

Propojení lokalit je realizováno pronajatými datovými trasami připojujícími jednotlivé koncové lokality k centrální lokalitě Generálního ředitelství v Hradci Králové (HK9).
V době vzniku tohoto projektu je realizována postupná náhrada dosluhující WAN sítě postavené na bezdrátových spojích za technologii MPLS sítě společnosti České Radiokomunikace a.s. (ČRa). Nad touto MPLS sítí ČRa je budována vlastní WAN síť PLA, postavená na prvcích společnosti Fortinet využívající technologii softwarově definované sítě (SD-WAN).

2.1.2 Centrální lokalita

Centrální lokalita Generálního ředitelství s.p. v Hradci Králové je fyzicky rozdělena do 3 budov (A, B, C), kde v budovách A a B jsou umístěny serverovny s centrálními prvky sítě PLA. LAN síť je tvořena staršími modely přepínačů Cisco Catalyst, v síti je provozováno oddělení sítí technologií VLAN.
V samostatném rozvaděči serverovny v 1. patře B budovy jsou zakončeny přípojky ISP providerů. Primární připojení CESNET je zajištěno optickou linkou zakončenou optickým singlemodovým 1GB SFP modulem. Sekundární připojení COMA je zajištěno metalickým kabelem zakončeným 1GB RJ45 konektorem. Obě linky jsou fyzicky zakončeny v hraničním

prvku sítě [redacted] Do stejného prvku na perimetru sítě je zakončena i MPLS síť ČRa. Ve stejném rozvaděči je umístěn i druhý firewall [redacted] v režimu studené zálohy.

IP adresace v síti PLA používá privátní IPv4 rozsahy dle standardů daných normou RFC 1918. Základní koncept rozdělení sítě do jednotlivých zón a jejich IP adresace jsou realizovány na perimetru sítě. Logicky lze infrastrukturu PLA rozdělit do následujících zón:

- [redacted] – zóna v transparentním VDOM připojující oba ISP
- [redacted] – demilitarizovaná zóna, servery pro externí DNS, mailproxy a antispam
- [redacted] – zóna pro externí přístup na dohledový systém Alcoma a dispečink
- [redacted] – reverzní proxy pro WWW zónu
- [redacted] – webové servery publikované do internetu, dostupné přes zónu EXTRANET
- [redacted] – zóna pro přístup hostů přes WiFi
- [redacted] – zóna interní LAN sítě PLA zahrnující lokální počítače a servery
- [redacted] – rozsáhlá WAN síť PLA přes privátní radiové spoje a SD-WAN
- [redacted] – zóna pro zakončení vzdáleného přístupu pro externí organizace

Z hlediska L2/L3 vrstvy můžeme rozdělit centrální lokalitu na dvě samostatné lokality, jedna v budovách A a C, druhá v budově B. Vzájemné propojení mezi serverovnami v budovách A a B je zajištěno pomocí optického páteřního spoje.

Lokalita	Rozvaděče	Typ vlákna	Počet vláken	Délka (m)
ŘSP Hradec Králové	Budova A – Budova B	MM 50/125	24	65

Tabulka 2 - GŘ HK optika

Obrázek 1 - GŘ HK – propojeni A a B

Provozované oddělené sítě VLAN a jejich adresace v budovách A a C:

VLAN ID	Jméno VLAN	IP subnet	Router
1	default	[redacted]	
2	segm003		
3	segm005		
4	segm006		
5	segm010		
11	segm008-032		
12	segm008-064		
23	segm008-008(hk9sw-02_WAN)		
99	voice		

Tabulka 3 - VLAN HK budova A a C

Provozované oddělené sítě VLAN a jejich adresace v budově B:

VLAN ID	Jméno VLAN	IP subnet	Router
1	[redacted]	[redacted]	
2			
3			
4			
5			
11			
12			
22			
23			
71			
72			
73			
99		[redacted]	
200			
201			
901			
902			
903			
904			
905			

Tabulka 4 - VLAN HK budova B

Jednotlivé datové rozvaděče s koncovými přepínači Cisco Catalyst jsou do datového centra v serverovnách budovy A a B připojeny pomocí portchannelu 2x1GE ethernet v závislosti na délce buď metalickým, nebo optickým přípojem. Z jednotlivých rozvaděčů jsou pak horizontálními rozvody strukturované kabeláže (Cat5E) připojována jednotlivá koncová zařízení.

Obrázek 2 - GŘ HK - budova A a C

Obrázek 3 - GŘ HK - budova B

V serverovně budovy A jsou umístěny tři servery VMware ( ), v serverovně budovy B jsou umístěny další tři servery VMware ( ). Tyto servery jsou pomocí samostatné neroutované VLAN spojeny do HA. Jelikož VMware infrastruktura neumožňuje distribuovaný vSwitch napříč jednotlivými servery, je každý z těchto serverů připojen do infrastruktury PLA samostatnými linkami do přístupových přepínačů v dané serverovně.

Obrázek 4 - GŘ HK - VMware infratruktura

V síťové infrastruktuře je provozována Microsoft doména pla.cz, síťové služby DNS, DHCP, NTP apod. Není žádným pokročilým způsobem řízeno připojování koncových zařízení do sítě, jejich kontrola a prostupy mezi jednotlivými interními sítěmi.

2.1.3 Koncové lokality

V koncových lokalitách sítě PLA je většinou provozována administrativní VLAN a VOIP. Veškeré síťové služby jsou poskytovány z centrální lokality [redacted].

Provozované oddělené sítě VLAN a jejich adresace v lokalitách:

VLAN ID	Jméno VLAN	IP subnet	Router
[redacted]			

Tabulka 5 - VLAN lokalita

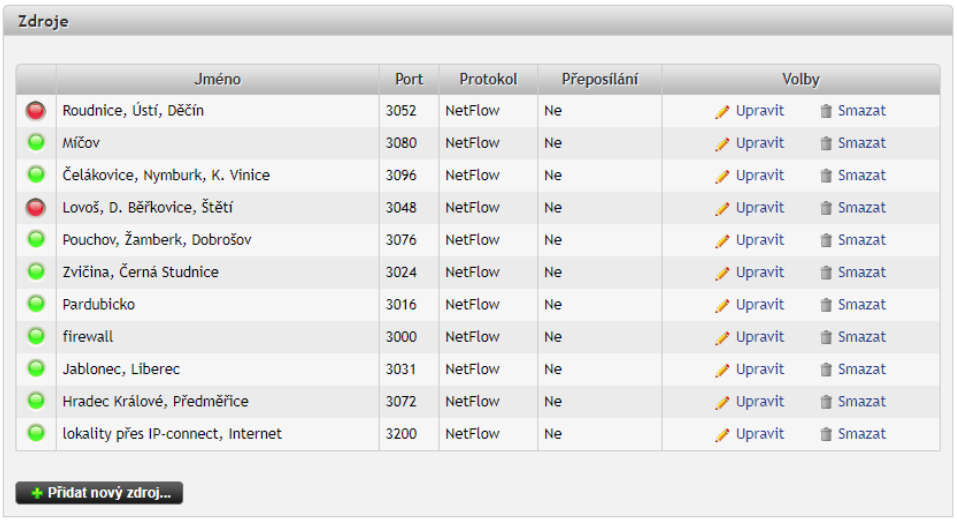
Z jednotlivých rozvaděčů v lokalitách jsou horizontálními rozvody strukturované kabeláže (Cat5E) připojována jednotlivá koncová zařízení.

2.1.4 Bezdrátová síť

V centrální lokalitě sítě PLA je provozována bezdrátová síť pro uživatele PLA a pro hosty, řízená bezdrátovým kontrolérem Cisco ([redacted]. Samostatné SSID pro hosty je směrováno na firewallu [redacted] bez přístupu do interní sítě PLA.
Na lokalitách sítě PLA není bezdrátová síť provozována.

2.1.5 FlowMon

Stávající FlowMon řešení reprezentuje Invea Flowmon Collector 1000VA, nainstalovaný jako virtuální apliance v prostředí VMWare s přidělenou diskovou kvótou 1TB. Kolektor naslouchá na různých portech, na které zasílají páteřní směrovače WAN sítě informace Netflow.v5 o datových tocích na svých rozhraních směrem k jednotlivým lokalitám.

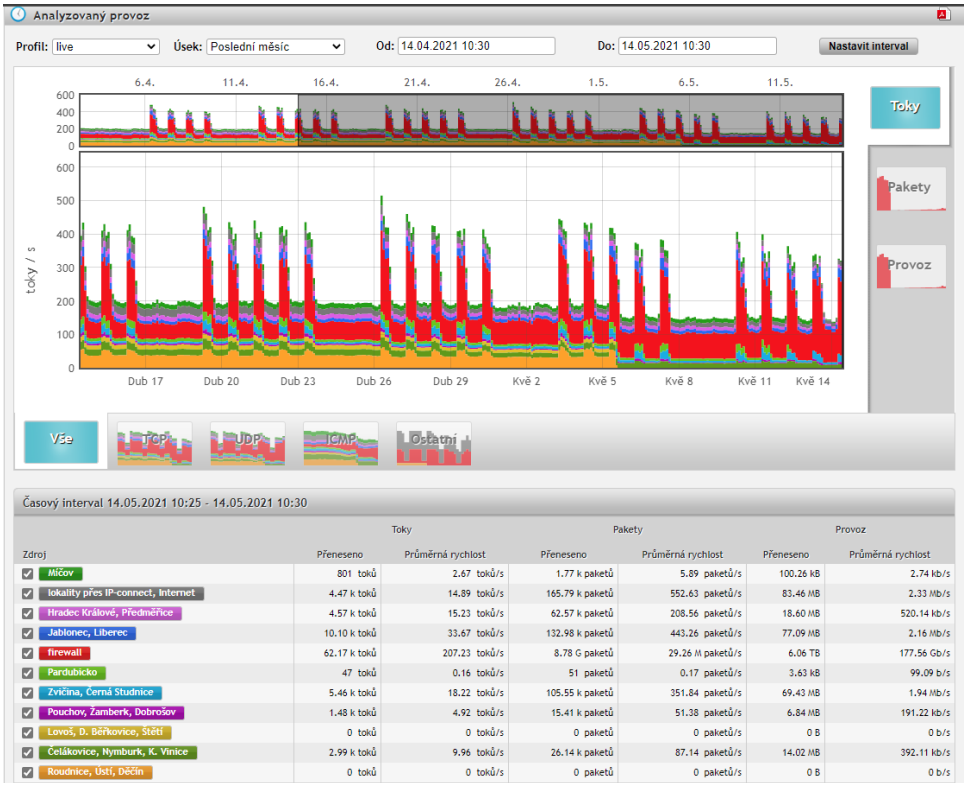

Zdroje

	Jméno	Port	Protokol	Přeposílání	Volby
	Roudnice, Ústí, Děčín	3052	NetFlow	Ne	Upravit Smazat
	Míčov	3080	NetFlow	Ne	Upravit Smazat
	Čelákovice, Nymburk, K. Vinice	3096	NetFlow	Ne	Upravit Smazat
	Lovoš, D. Běřkovice, Štětí	3048	NetFlow	Ne	Upravit Smazat
	Pouchov, Žamberk, Dobrošov	3076	NetFlow	Ne	Upravit Smazat
	Zvičina, Černá Studnice	3024	NetFlow	Ne	Upravit Smazat
	Pardubicko	3016	NetFlow	Ne	Upravit Smazat
	firewall	3000	NetFlow	Ne	Upravit Smazat
	Jablonec, Liberec	3031	NetFlow	Ne	Upravit Smazat
	Hradec Králové, Předměřice	3072	NetFlow	Ne	Upravit Smazat
	lokality přes IP-connect, Internet	3200	NetFlow	Ne	Upravit Smazat

+ Přidat nový zdroj...

Obrázek 5 - FlowMon zdroje

FlowMon řešení zobrazuje statistiky provozu založené na datech obsažených v použitém protokolu Netflow 5, tedy zdrojové a cílové IP adresy a zdrojové a cílové porty.



Zdroj	Toky Přeneseno	Toky Průměrná rychlost	Pakety Přeneseno	Pakety Průměrná rychlost	Provoz Přeneseno	Provoz Průměrná rychlost
Míčov	801 toků	2.67 toků/s	1.77 k paketů	5.89 paketů/s	100.26 kB	2.74 kb/s
lokality přes IP-connect, Internet	4.47 k toků	14.89 toků/s	165.79 k paketů	552.63 paketů/s	83.46 MB	2.33 Mb/s
Hradec Králové, Předměřice	4.57 k toků	15.23 toků/s	62.57 k paketů	208.56 paketů/s	18.60 MB	520.14 kb/s
Jablonec, Liberec	10.10 k toků	33.67 toků/s	132.98 k paketů	443.26 paketů/s	77.09 MB	2.16 Mb/s
firewall	62.17 k toků	207.23 toků/s	8.78 G paketů	29.26 M paketů/s	6.06 TB	177.56 Gb/s
Pardubicko	47 toků	0.16 toků/s	51 paketů	0.17 paketů/s	3.63 kB	99.09 b/s
Zvičina, Černá Studnice	5.46 k toků	18.22 toků/s	105.55 k paketů	351.84 paketů/s	69.43 MB	1.94 Mb/s
Pouchov, Zamberk, Dobrošov	1.48 k toků	4.92 toků/s	15.41 k paketů	51.38 paketů/s	6.84 MB	191.22 kb/s
Lovoš, D. Beřkovice, Stětí	0 toků	0 toků/s	0 paketů	0 paketů/s	0 B	0 b/s
Čelákovice, Nymburk, K. Vinice	2.99 k toků	9.96 toků/s	26.14 k paketů	87.14 paketů/s	14.02 MB	392.11 kb/s
Roudnice, Ústí, Děčín	0 toků	0 toků/s	0 paketů	0 paketů/s	0 B	0 b/s

Obrázek 6 - FlowMon statistiky

3. Návrh technického řešení

Sítě v současné době prochází zásadnějšími změnami než kdykoli za posledních 30 let. Podniky a organizace se zároveň potýkají s problémy jako BYOD, IoT, virtualizace, SDN, cloud, nekontrolované šíření aplikací, velká data včetně změn v chování zaměstnanců, kteří chtějí sdílet jedno zařízení jak pro soukromé, tak i pro pracovní účely bez ohledu na to, kde se připojí. Tím se exponenciálně zvětšuje prostor pro potenciální útoky, kterým by se podniky měly zabývat. Například:

- IoT a cloudová řešení s sebou nesou nutnost zabezpečit tuto komunikaci proti potenciálním útokům, které nejsou na první pohled viditelné.
- Mnoho IoT zařízení nemá centrální správu pro definici bezpečnostních pravidel, a tudíž nedokáže čelit moderním hrozbám v rámci užívaných aplikací.
- Kriticky důležitá a důvěrná obchodní data se přesouvají do cloudu, který spravují třetí strany. To pak znamená, že mnoho organizací nemá přehled o tom, kde se jejich data právě nachází nebo jaká bezpečnostní politika je aktuálně chrání.
- Přechod na digitální obchodní model rozšiřuje síť za hranici firewallu, což znamená, že dnešní sítě jdou za hranice standardního modelu zabezpečení.
- Privátní zařízení využívaná zaměstnanci k pracovním účelům jsou převážně mobilní a spojují tak soukromé a pracovní záležitosti, čímž představují reálné riziko z hlediska úniku dat.

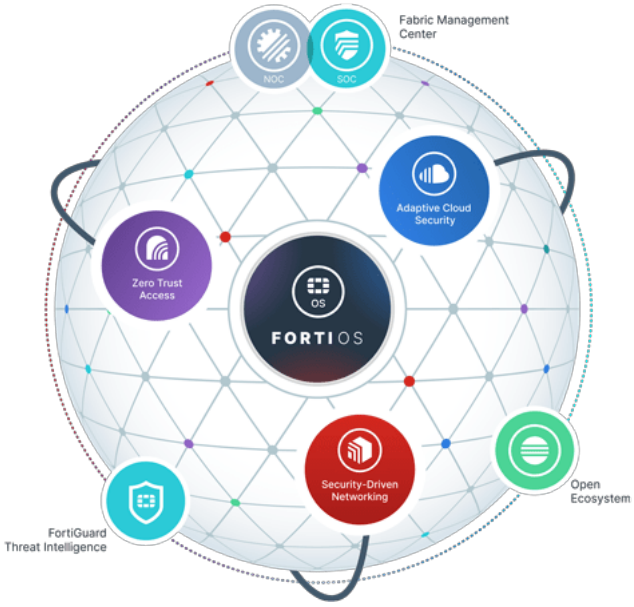
Problémy dále narůstají integrací bezpečnostních modulů v rámci ochrany sítě a následnou nepřehledností v rámci sítě. Izolované bezpečnostní moduly s vlastním rozhraním pro správu pak neumožňují shromažďovat informace o hrozbách nebo incidentech a sdílet je s dalšími zařízeními v síti, co značně eliminuje jejich přínos. Nasazení mnoha nových zařízení pak alokuje příliš mnoho času, jenž následně chybí pro optimalizaci a aktualizaci stávajících zařízení. Odpovědí na tyto otázky je určitě zjednodušení. Tato integrace vyžaduje tři věci:

- **Segmentace** – sítě je nutné inteligentně segmentovat do funkčních zabezpečených zón. Segmentace celé sítě od externího připojení po koncová zařízení, od IoT po cloud, včetně fyzických i virtuálních prostředí pak přináší podrobný přehled o provozu, který probíhá horizontálně v distribuovaných sítích, eliminuje šíření malwaru a umožňuje následně odhalovat a izolovat infikovaná zařízení.
- **Sdílení informací** – mezi bezpečnostními zařízeními je nutné sdílet jak lokální, tak globální informace o hrozbách a centrálně koordinovat následnou reakci.
- **Univerzální pravidla** – centrální bezpečnostní politika, jenž určuje míru důvěry mezi segmenty sítě, shromažďuje informace o hrozbách v reálném čase, zavádí jednotná bezpečnostní pravidla a následně koordinuje jejich uplatňování.

Návrh technického řešení vychází z dostupných informací o síťové infrastruktuře PLA, požadavků administrátorů sítě PLA a snaží se v co největší míře také využít stávající a nově budovanou infrastrukturu SD-WAN na prvcích výrobce Fortinet.

3.1 Fortinet Security Fabric

Fortinet Security Fabric je nejvýkonnější platforma pro kybernetickou bezpečnost v oboru, založená na FortiOS, s bohatým otevřeným ekosystémem. Architektura integruje technologie pro koncové body, síť, aplikace, datové centrum, obsah a cloud do jediného provázaného bezpečnostního řešení, kterým lze řídit a definovat politiku z jednoho rozhraní.



Obrázek 7 - Fortinet Security Fabric

Tato architektura je založená na třech klíčových atributech:

- **Broad** – široké portfolio umožňuje koordinovanou detekci hrozeb a vynucování zásad v celém životním cyklu s konvergovanou sítí a zabezpečením přes edge, cloud, koncové body až po uživatele.
- **Integrated** – integrované a sjednocené zabezpečení napříč různými technologiemi, lokalitami a nasazením umožňují úplnou viditelnost. Rovněž umožňuje zabezpečení všech typů zařízení, včetně hardwarových zařízení, virtuálních strojů, cloudových služeb a služeb jako servis (X-as-a-Service).
- **Automated** – automatizovaná, kontextově orientovaná síť a bezpečnostní pozice s využitím pokročilé AI pro automatické poskytování koordinované ochrany téměř v reálném čase od uživatele až k aplikaci.

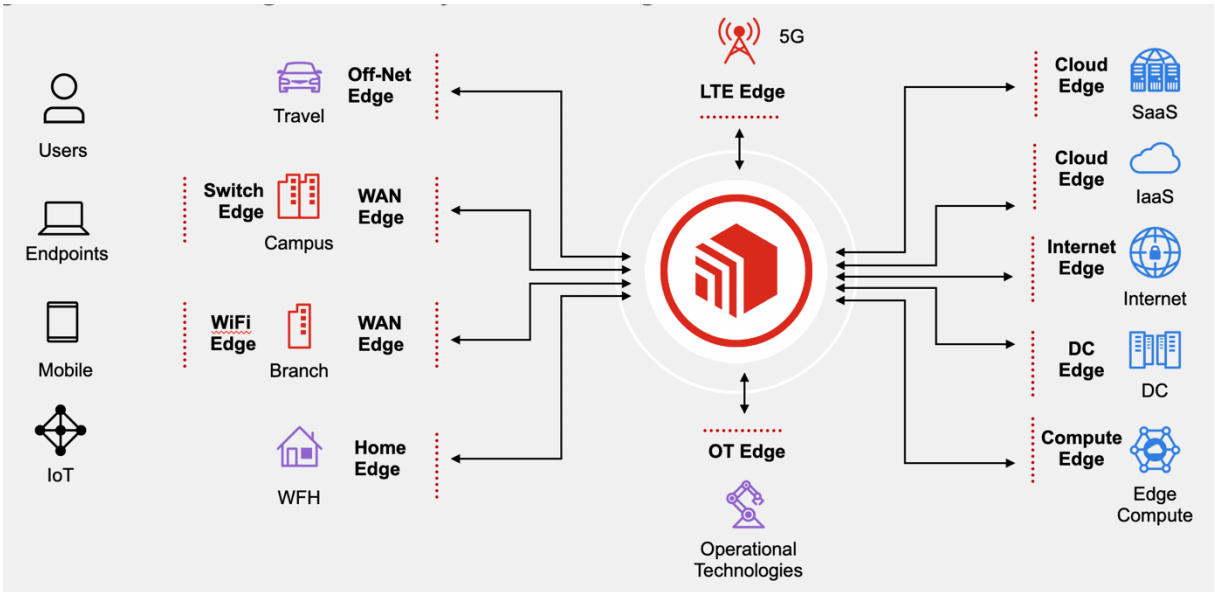
3.1.1 Klíčové pilíře Fortinet Security Fabric

Jeden operační systém (FortiOS) pohání Fortinet Security Fabric, který podporuje více modelů nasazení než jakékoli jiné řešení. Patří mezi ně fyzická, virtuální, cloudová a X-as-a-Service prostředí. Zahrnuje také nejširší portfolio systémů a produktů zahrnující koncové body, sítě a cloudy.

3.1.1.1 Security-Driven Networking

Zabezpečení sítí umožňuje digitální inovace sbližováním sítí a zabezpečení do jediného integrovaného systému, který lze rozšířit na jakékoli místo. Síťová strategie společnosti Fortinet úzce integruje síťovou infrastrukturu a architekturu zabezpečení do jednoho celku, což umožňuje škálování a změnu sítě bez ohrožení zabezpečení.
Velmi důležitou součástí zabezpečení sítě je firewall nové generace (NGFW). Ale pro skutečnou ochranu sítě jsou zapotřebí další technologie a efektivní zabezpečení sítě vyžaduje

holistický přístup, který integruje bránu firewallu s dalšími důležitými funkcemi. Abychom ochránili celou infrastrukturu organizace, musí vrstvený přístup s bezpečnostními řešeními pro všechny oblasti sítě spolupracovat jako integrovaná a kolaborativní bezpečnostní struktura.



Obrázek 8 - Fortinet Security Driven

Typy řešení, zařízení a nástrojů pro sjednocené zabezpečení sítě jsou následující:

- Next-generation firewall (NGFW)
- WAN and Branch Protection (SD-WAN)
- Intrusion Prevention System (IPS)
- Secure Web Gateway
- SSL Inspection
- Application Optimization
- Cloud On-ramp
- Virtual private networks (VPNs)
- Perimeter Security
- Hyperscale Applications
- Network Automation
- Compliance
- Secure Ethernet Switching
- Secure Wireless LAN

3.1.1.2 Zero Trust Network Access

Fortinet Zero Trust Network Access (ZTNA) podporuje přijetí přístupu nulové důvěryhodnosti, který ověřuje, kdo a co je v síti. S využitím agenta FortiClient Agent lze využívat možnosti nulového důvěryhodného přístupu k síti (ZTNA). Správa je zjednodušena pomocí stejné adaptivní zásady přístupu k aplikacím, ať už jsou uživatelé v síti nebo mimo ni.

Dnešní sítě mají obrovské, dynamické a v některých případech i dočasné okraje. Skutečnost, že mnoho zařízení je často offline, ztěžuje průběžné hodnocení rizika a důvěry. Protože neexistuje způsob, jak ověřit, že uživatelům nebo zařízením v síti nebo mimo ni lze důvěřovat, lze z hlediska zabezpečení předpokládat, že každé zařízení v síti je potenciálně infikováno. Kromě toho je každý uživatel schopen úmyslně nebo neúmyslně ohrozit kritické zdroje.

Efektivní strategie ZTNA řeší jak síťové připojení, tak přístup k aplikacím na základě základního předpokladu, že žádný uživatel nebo zařízení není ze své podstaty důvěryhodný. Žádná důvěra se neuděluje žádné transakci, aniž byste nejprve ověřili, že uživatel a zařízení mají oprávnění k přístupu.
Implementace modelu ZTNA vyžaduje zaměření na tři klíčové prvky:

- **Znát všechna zařízení, která jsou v síti** – z důvodu rozšíření hranice sítě, nárůstu aplikací a zařízení je nyní nutné spravovat a chránit potenciálně miliardy hran. Nástroje pro řízení přístupu k síti (NAC) poskytují viditelnost do síťového prostředí.
- **Poznat každého uživatele, který přistupuje k síti** – k vytvoření efektivní strategie ZTNA je důležité určit, kdo je každý uživatel a jakou roli v organizaci hraje. Model nulové důvěryhodnosti se zaměřuje na „zásadu nejmenšího přístupu“, která uživateli poskytuje pouze přístup k prostředkům, které jsou nezbytné pro jeho roli nebo práci.
- **Vědět, jak chránit aktiva v síti i mimo ni** – efektivní strategie ZTNA řeší výzvu ochrany zařízení mimo síť zlepšením viditelnosti koncových bodů. Kvůli zvýšené mobilitě a práci na dálku mohou uživatelé nechtěně vystavit svá zařízení a zdroje společnosti hrozbám. Poté, co budou online kdekoli jinde, mohou se tito uživatelé nechtěně vystavit prostředkům společnosti virům a malwaru.

3.1.1.2.1 Fortinet ZTNA Framework

Fortinet ZTNA využívá úzce integrovanou kolekci bezpečnostních řešení, která pomáhají identifikovat a klasifikovat všechny uživatele a zařízení, která usilují o přístup k síti a aplikacím. Mohou posoudit jejich stav souladu s interními zásadami zabezpečení, automaticky je přiřadit k zónám kontroly a průběžně je sledovat, ať už v síti, nebo mimo ni.

- **Řízení přístupu ke koncovému bodu** – koncové body jsou často terčem počátečního kompromisu nebo útoků. Fortinet posiluje zabezpečení koncových bodů prostřednictvím integrované viditelnosti, kontroly a proaktivní obrany. Schopnost objevovat, sledovat a hodnotit rizika koncových bodů pomáhá zajistit shodu koncových bodů, zmírnit rizika a snížit expozici. Řešení Fortinet FortiClient pro přístup ke koncovým bodům:
    - Podporujte zabezpečená, šifrovaná připojení napříč nebezpečnými sítěmi s podporou služeb split tunneling and secure access service edge (SASE) oprav a stavu zabezpečení.
    - Poskytujte nepřetržitá telemetrická data zabezpečení koncových bodů, včetně operačního systému zařízení (OS) a aplikací, známých chyb zabezpečení, oprav a stavu zabezpečení.
- **Správa přístupu k identitě** – prostředí podnikové identity jsou tvořena různými systémy záznamu, které mohou zahrnovat síťová zařízení, servery, adresářové služby a cloudové aplikace. Bezpečná a efektivní správa ověřování a autorizace identity pro všechny systémy a aplikace je zásadní pro minimalizaci narušení zabezpečení. Řešení pro správu identit a přístupu Fortinet (IAM) se používají k:
    - Vytvoření identity prostřednictvím přihlášení, vícefaktorové autentizace (MFA) a certifikátů, které se mohou vyvíjet a přidávat nepřetržité kontextové ověřování.
    - Poskytovat informace založené na rolích ze zdroje autentizace v privilegovaném přístupu.
    - Zavést a prosazovat zásady nejmenšího přístupu založené na rolích.
    - Poskytnout větší zabezpečení s podporou jednotného přihlášení (SSO).

- **Řízení přístupu k síti** – poskytuje viditelnost do síťového prostředí pro vynucování a dynamickou kontrolu zásad. Ať už se zařízení připojují zevnitř nebo vně sítě, FortiNAC může automaticky reagovat na napadená zařízení nebo s neobvyklou aktivitu. S FortiNAC mohou organizace:
    - Identifikovat, profilovat a skenovat všechna zařízení na chyby zabezpečení.
    - Zavést a zajistit průběžné řízení sítě.
    - Zavést a prosazovat zásady, které omezují přístup k síti pouze na to, co je pro dané zařízení nutné.
- **Řízení přístupu k aplikacím** – v modelu nulové důvěryhodnosti by měl být přístup k aplikacím řízen na základě relace a každý uživatel a zařízení by mělo být ověřeno, zda se připojují vzdáleně nebo z vlastní sítě. Přístup k aplikacím by měl být mapován na roli jednotlivce, aby byly k dispozici pouze ty aplikace, které jsou relevantní pro uživatele. S řešeními Fortinet ZTNA lze řízení přístupu k aplikacím použít v různých scénářích nasazení, včetně služeb SASE. Tato řešení poskytují:
    - Ověření uživatelů a zařízení pro každou relaci aplikace.
    - Kontrolu přístupu uživatelů k aplikacím na základě zásad.
    - Vynucení zásady přístupu k aplikacím bez ohledu na to, kde se uživatel nachází.
    - Vytvoření bezpečného, automatického spojení mezi uživatelem a proxy bodem ZTNA.

Řešení Fortinet ZTNA se skládá z:

- **FortiGate NGFW** – tyto síťové brány fungují jako proxy bod ZTNA a jako bod pro vynucování zásad. FortiGate poskytuje šifrované ukončení tunelu a vynucení přístupu aplikace. FortiOS také spustí ověření uživatele a posouzení rizik zařízení pro každou relaci aplikace.
- **Centralizovaná správa FortiManager** – řešení pro správu zabezpečení umožňuje použít konfiguraci pro všechny FortiGate zařízení v síti současně.
- **FortiClient agent** – funguje jako agent ZTNA a je nainstalován na koncovém zařízení. Vytváří automatické šifrované tunely ZTNA do bodu vynucování ZTNA (FortiGate).
- **FortiClient Enterprise Management Server (EMS)** - hraje rozhodující roli při konfiguraci agentů ZTNA pro správu řešení ZTNA. Umožňuje jim zjistit, ke kterému proxy bodu FortiOS by se měli připojit.
- **Správa identity a přístupu Fortinet (IAM)** - poskytuje služby nezbytné k bezpečnému potvrzení totožnosti uživatelů a zařízení při jejich vstupu do sítě. Zahrnuje:
    - **FortiAuthenticator** k poskytování centralizovaných autentizačních služeb, včetně jednotného přihlášení (SSO).
    - **FortiToken** k potvrzení identity uživatelů přidáním druhého faktoru (dvoufaktorové ověřování).
- **FortiNAC** – řešení pro řízení přístupu k síti s viditelností, kontrolou a automatickou odpovědí na vše, co se připojuje k síti.

3.1.1.3 Adaptive Cloud Security

Konzistentní nativní zabezpečení s automatickým škálováním je poskytováno i v prostředí cloudů. Adaptivní cloudové zabezpečení umožňuje efektivní využití zdrojů s automatickým škálováním, dynamickým vyvažováním zátěže a viditelností až do aplikací. Kromě toho je kontextová politika rozšířena i do těchto prostředí a poskytuje koordinovanou reakci na hrozby prostřednictvím integrace s bezpečnostními službami využívajícími FortiGuard AI.

3.1.1.4 Fortinet Fabric Management Center

Fabric Management Center umožňuje centralizovanou správu, automatizaci a orchestraci sítě a analýzu zabezpečení. Sjednocená konzola napříč sítěmi, koncovými body a cloudy zvyšuje efektivitu, snižuje riziko a snižuje celkové náklady na vlastnictví.

3.1.1.5 FortiGuard Security Services

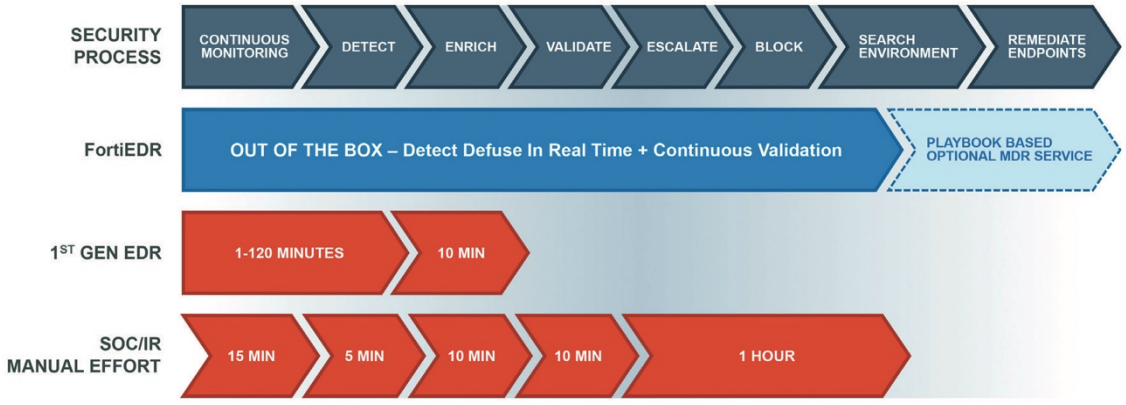
Portfolio bezpečnostních služeb FortiGuard zahrnuje komplexní a pokročilé funkce zabezpečení pro sítě, obsah, uživatele, zařízení, přístup a aplikace. Služby FortiGuard poskytují ochranu téměř v reálném čase neustálou analýzou dat o hrozbách v reálném světě z více než 5,6 milionu senzorů rozmístěných po celém světě. Pokročilá AI se používá k identifikaci abnormalit a podezřelých vzorů a také ke generování nových ochran, které se automaticky distribuují do Fortinet Security Fabric. Tím je zajištěna včasná a koordinovaná ochrana v celém životním cyklu útoku.

3.1.1.6 Open Ecosystem

Otevřený ekosystém Fortinet Security Fabric lze rozšířit napříč organizacemi prostřednictvím bezproblémové integrace s různými řešeními Fabric-Ready Partner řešení. Povolení širokého ekosystému minimalizuje mezery v podnikových bezpečnostních architekturách a maximalizuje návratnost investic (ROI). A vše lze spravovat pomocí jediné konzole pro správu.

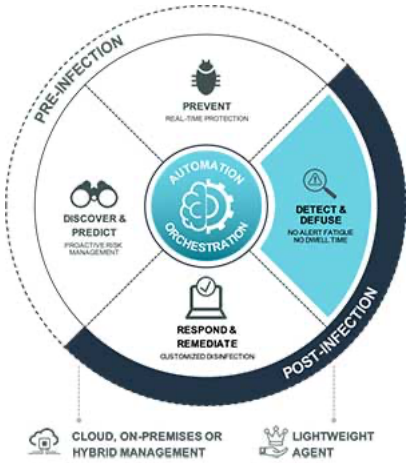
3.1.1.7 Endpoint Detection & Response (EDR)

Pokročilé útoky mohou kompromitovat koncové body pouze za několik minut, ne-li během pár sekund. Nástroje pro detekci a odezvu koncových bodů první generace (EDR) prostě nemohou držet krok. Vyžadují manuální třídění a reakce, které jsou nejen příliš pomalé pro rychle se pohybující hrozby, ale také generují obrovské množství indikátorů, které zatěžují již přetížené bezpečnostní týmy.



Obrázek 9 - FortiEDR Benefits

FortiEDR poskytuje pokročilou ochranu před hrozbami v reálném čase před i po infekci. Proaktivně snižuje dosah útoků, předchází infekci malwarem, detekuje a eliminuje potenciální hrozby v reálném čase a může automatizovat postupy odezvy a nápravy pomocí přizpůsobitelných příruček. FortiEDR pomáhá zastavit narušení v reálném čase automaticky a efektivně, aniž by zahltil bezpečnostní týmy pomocí falešných poplachů.



Obrázek 10 – FortiEDR Security Platform

3.2 Centrální lokalita

3.2.1 Datové centrum sítě

Datové centrum sítě je geograficky rozmístěno ve dvou budovách A a B. Datové rozvaděče v serverovnách dotčených budov jsou vzájemně propojeny optickým kabelem, viz. Tabulka 2 - GŘ HK optika. Použitý typ vlákna multimode OM2 50/125 neumožňuje na uvedenou vzdálenost použít vyšší rychlosti přenosu, než 10GB a může být limitujícím faktorem dalšího rozvoje datového centra.
Navrhujeme realizovat propojení budov A a B na nové optické trase s použitím Singlemode 9/125 v počtu min. 48 vláken.

3.2.1.1 Páteřní prvky sítě

Páteřní prvky sítě musí poskytovat bezpečné, jednoduché, škálovatelné ethernetové řešení s vynikající propustností, odolností a škálovatelností. Virtualizace a cloud computing vytvořily požadavky na ethernetové sítě s velkou šířkou pásma. Přepínače FortiSwitch řady Data Center splňují tyto výzvy poskytováním vysoce výkonné přepínací platformy pro rychlosti 10 GB, 40 GB nebo 100 GB.
Navrhované typy páteřních prvků:

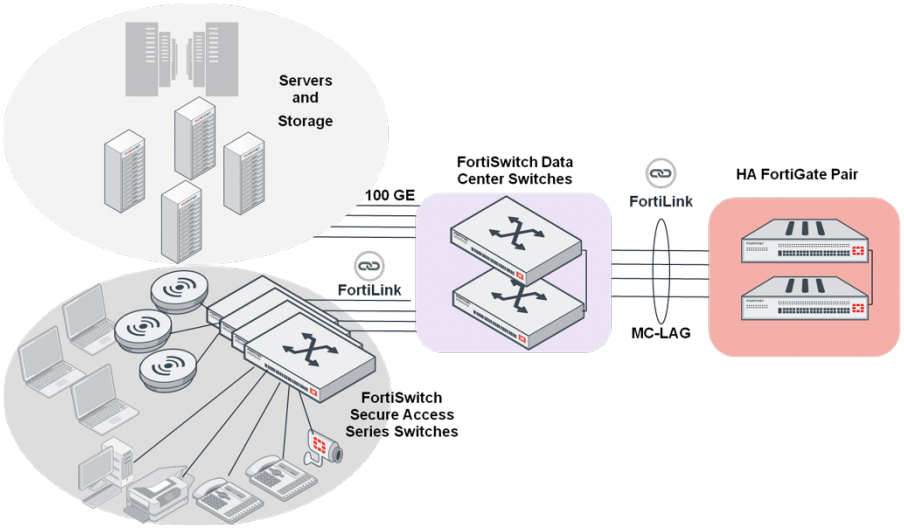
Typ prvku	Produkt	Popis
Přepínač typ A	FS-1048E	Layer 2/3 FortiGate switch controller compatible switch with 48 x GE/10GE SFP/SFP+ slots and 6 x 40GE QSFP+ or 4 x 100GE QSFP28. Dual AC power supplies
Přepínač typ B	FS-1024E	Layer 2/3 FortiGate switch controller compatible switch with 24 x GE/10GE SFP/SFP+ slots and 2 x 100GE QSFP28. Dual AC power supplies

Tabulka 6 - Typy páteřních prvků

3.2.1.1.1 Integrace Fortinet Security Fabric

FortiSwitch Data Center podporují FortiGate management prostřednictvím FortiLink a zajišťují tak rozšíření výše uvedeného zabezpečení sítě Fortinet Security Fabric až na úroveň

ethernetového portu. Díky aktivaci a správě funkcí zabezpečení sítě a přístupové vrstvy prostřednictvím jediné konzoly lze centralizovanou správu zásad, včetně přístupu a řízení na základě rolí, snadno implementovat a spravovat. Uživatele nebo zařízení lze ověřit proti stejné databázi a použít stejné zásady zabezpečení bez ohledu na to, jak a kde se k síti připojují.
FortiLink je inovativní proprietární protokol pro správu, který umožňuje bezpečnostnímu zařízení FortiGate bezproblémově spravovat jakýkoli FortiSwitch. FortiLink umožňuje, aby se FortiSwitch stal logickým rozšířením FortiGate a integroval jej přímo do Fortinet Security Fabric.

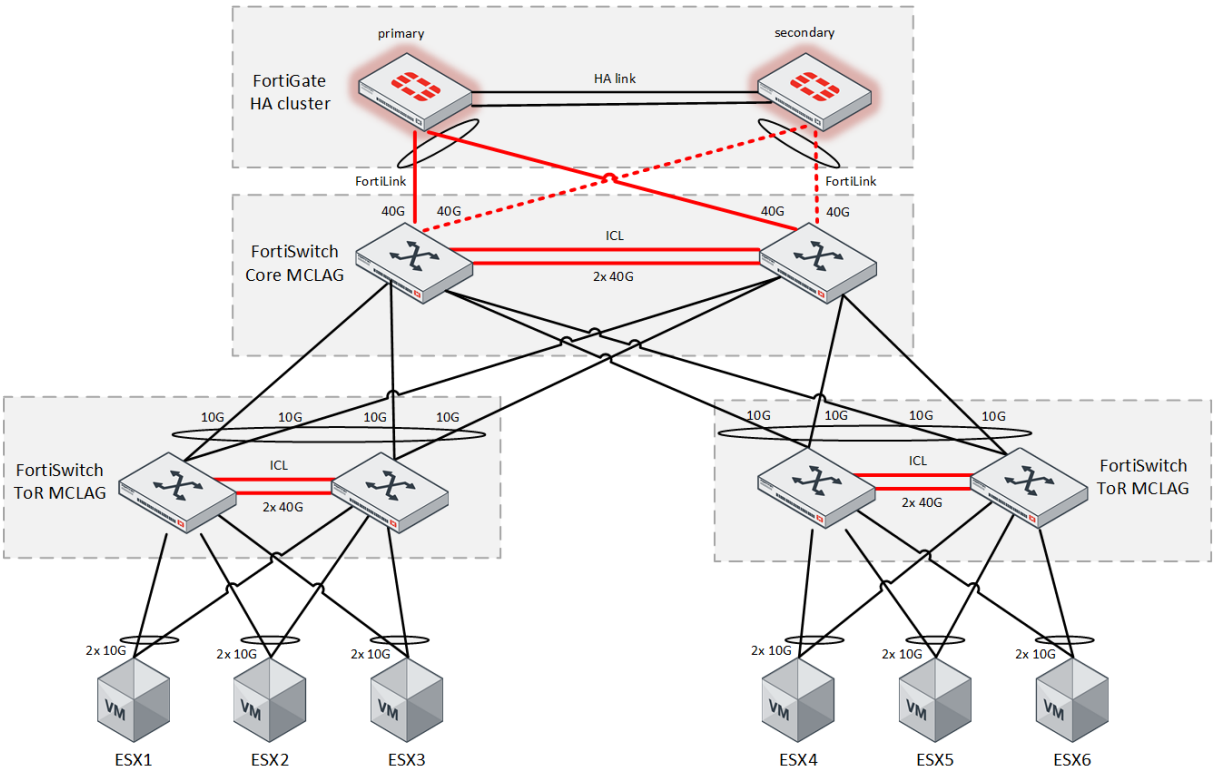


Obrázek 11 – FortiLink koncept

Páteřní prvky sítě (přepínač typ A) budou tvořit core vrstvu, která bude geograficky rozmístěna do dvou serveroven v budově A a B. Do tohoto centra sítě budou propojeny jednotlivé přístupové prvky LAN sítě vždy alespoň dvěma linkami s využitím protokolu LACP tak, aby případný výpadek jedné z linek, nebo jednoho z centrálních prvků neznamenal celkový výpadek, ale aby došlo případně pouze ke snížení max. přenosové rychlosti na polovinu.

3.2.1.2 VMware servery

Virtualizační infrastruktura je geograficky rozmístěna do dvou serveroven v budově A a B. V každé ze serveroven v budovách A a B je vždy trojice ESX hostů. Každý z hostů bude připojen do páteřní infrastruktury pomocí dvojice Top of Rack datacentrových přepínačů (přepínač typ B) vždy alespoň dvěma 10GB linkami tak, aby případný výpadek jedné z linek, nebo jednoho z centrálních prvků neznamenal celkový výpadek, ale aby došlo případně pouze ke snížení max. přenosové rychlosti na polovinu. Navrhovaná optimální varianta topologie páteřní vrstvy a datacentra je zřejmá z následujícího obrázku:

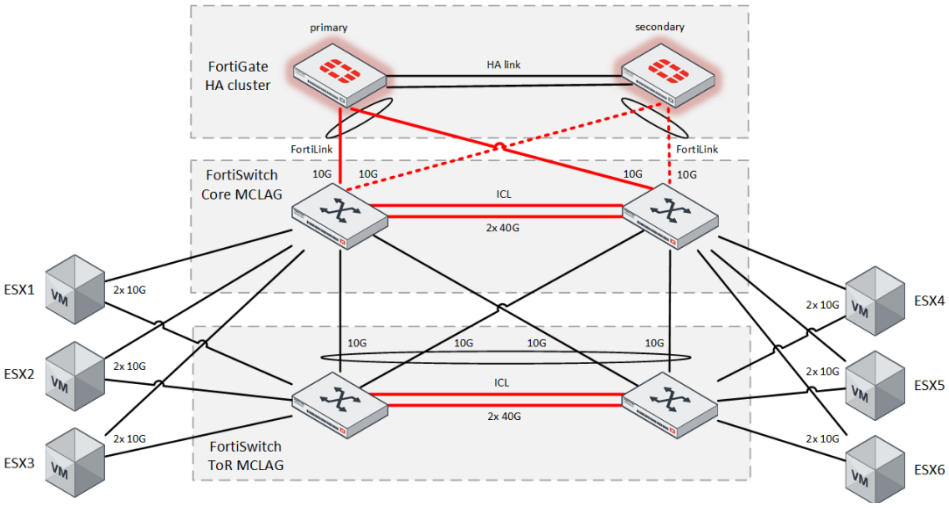


Obrázek 12 – Optimální varianta topologie datacentra

Vybudování této topologie vyžaduje dostatečnou kapacitu optické sítě s parametry pro přenos 40GB rychlosti. Dalším limitujícím faktorem je stávající firewal[redacted] který má pouze 2x SFP+ porty a neumožňuje další rozšíření. Také aktuální použití druhého boxu [redacted] v režimu studené zálohy z důvodu absence potřebných podpor neumožní vybudování plnohodnotné topologie.
Na zařízení[redacted] je již ohlášen konec podpory ze strany výrobce (14. říjen 2024), navrhujeme tak zvážit nákup dvojice nových zařízení s podporou 40GB interface a vybudování plnohodnotného HA clusteru napříč serverovnami v budovách A a B.

3.2.1.3 Ekonomická varianta DC

Ekonomická varianta datového centra umožňuje částečné sloučení CORE a ToR vrstvy se zachováním geografického rozdělení virtualizační infrastruktury. Každý z hostů bude připojen do páteřní infrastruktury pomocí core přepínače (přepínač typ A) a Top of Rack přepínače (přepínač typ B) vždy alespoň dvěma 10GB linkami tak, aby případný výpadek jedné z linek, nebo jednoho z centrálních prvků neznamenal celkový výpadek a nedostupnost poskytovaných služeb. Navrhovaná ekonomická varianta topologie páteřní vrstvy a datacentra je zřejmá z následujícího obrázku:



Obrázek 13 – Ekonomická varianta topologie datacentra

Vybudování této topologie vyžaduje dostatečnou kapacitu optické sítě s parametry pro přenos 10GB a případně 40GB rychlosti.

3.2.2 LAN

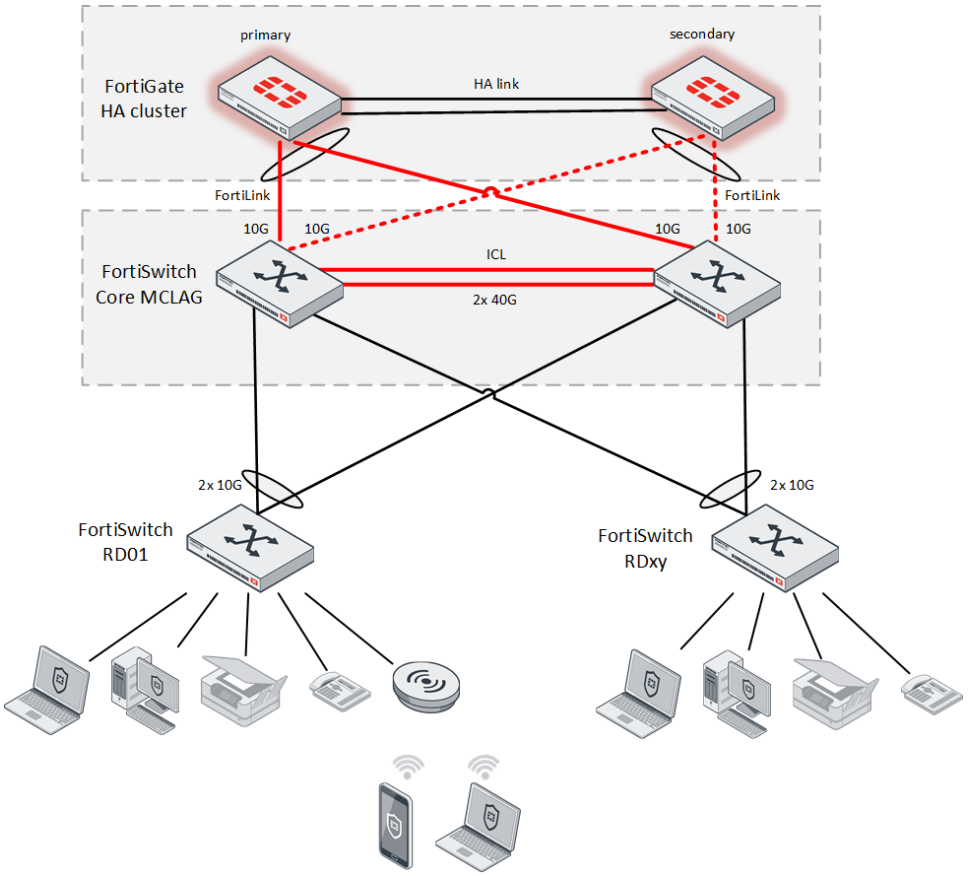
Lokální síť PLA je rozvedena po budovách A, B a C do datových rozvaděčů. Z jednotlivých rozvaděčů jsou pak horizontálními rozvody strukturované kabeláže (Cat5E) připojována jednotlivá koncová zařízení.

Rozvaděč	Připojení
Budova A - RD-LAN/WAN	[redacted]
Budova A - RD-SERVERY	
Budova A - RD3 (6.patro)	
Budova A - RD (4.patro dispečink)	
Budova A - RD5 (přízemí)	
Budova A - ústředna	
Budova B - RD-LAN	
Budova B - RD2 (2.patro)	
Budova B - RD6 (recepce)	
Budova C - RD4	

Tabulka 7 - GŘ HK rozvaděče

Z výše uvedené tabulky vyplývá, že propojení pomocí metalické kabeláže Cat5E jednotlivých rozvaděčů je limitujícím faktorem pro použití vyšších rychlostí než 1GB. Navrhujeme propojení jednotlivých datových rozvaděčů s horizontálními rozvody realizovat do každé z centrálních serveroven v budovách A a B pomocí Singlemode vlákna 9/125.
Do distribuovaného centra sítě budou propojeny jednotlivé přístupové přepínače LAN sítě vždy alespoň dvěma 10GB linkami s využitím protokolu LACP. Navrhované aktivní prvky sítě budou podporovat Power over Ethernet (PoE) pro připojení bezdrátových přístupových bodů a dalších zařízení bez nutnosti použít dedikovaný napájecí zdroj.

Přístupové přepínače FortiSwitch podporují FortiGate management prostřednictvím FortiLink a zajišťují tak rozšíření zabezpečení sítě Fortinet Security Fabric až na úroveň ethernetového portu. Navrhovaná topologie přístupové vrstvy je zřejmá z následujícího obrázku:



Obrázek 14 - Topologie přístupové vrstvy

Vybudování této topologie vyžaduje dostatečnou kapacitu optické sítě s parametry pro přenos 10GB rychlosti mezi jednotlivými datovými rozvaděči a distribuovaným centrem sítě v serverovnách budovy A a B.
Navrhované typy přístupových přepínačů:

Typ prvku	Produkt	Popis
Přepínač typ C	FS-108F-POE	Layer 2 FortiGate switch controller compatible PoE+ switch with 8 x GE RJ45 ports, 2 x GE SFP, Fanless with automatic Max 65W POE output limit
Přepínač typ D	FS-124F-POE	L2+ managed POE switch with 24GE + 4SFP+, 24port POE with max 185W limit and smart fan temperature control
Přepínač typ E	FS-148F-POE	L2+ management switch with 48GE + 4SFP+ 1x RJ45 console. Port 1- 24 are POE ports with automatic Max 370W POE output limit (24 port 802.3af or 12 port 802.3at)

Tabulka 8 - Typy přístupových přepínačů

3.2.2.1 IP adresace LAN

Stávající oddělení sítí pomocí technologie VLAN bude doplněno o potřebné technologické sítě, sítě pro dodavatele a karanténní oddělené sítě pro zařízení nesplňující potřebné zabezpečení.

Dvě směrovací domény pro budovu A a C a pro budovu B budou sloučeny do jednoho centra. Z důvodu bezproblémového přechodu bude zachován stávající koncept IP adres pro jednotlivé subnety interní sítě, bude nutné změnit VLAN id pro subnety přenesené ze směrovače v budově A ([redacted] . Seznam IP subnetů a VLAN je zřejmý z následující tabulky:

VLAN ID	Jméno VLAN	IP subnet	Router	Popis
1	[redacted]	[redacted]	[redacted]	[redacted]
101				
102				
103				
104				
105				
106				
109				
110				
732				
764				
832				
864				
71				
72				
73				
40				
48				
997				
998				
200				
201				
208				
52				
601				
724				
728				
54				
53				
901				
902				
903				
904				
905				
N/A				
4090				
4091				
4092				

4093	[redacted]	[redacted]	[redacted]	[redacted]

Tabulka 9 - GŘ HK seznam VLAN

Všechny navrhované aktivní prvky disponují požadovanými funkcionalitami jako je ARP Poison Routing, ARP spoofing, DHCP spoofing, MAC flooding a dalšími.

3.2.3 Bezdrátová síť

Pro obnovu bezdrátové infrastruktury sítě PLA byly zvoleny přístupové body FortiAP, které jsou komponentou Fortinet Security Fabric. Přístupové body budou řízeny kontroléry integrovanými přímo v jednotlivých firewallech FortiGate. Každý přístupový bod bude mít vytvořen zabezpečený tunel ke kontroléru. Každá z nakonfigurovaných Wi-Fi sítí bude zároveň virtuálním firewallovým rozhraním, na které je možné aplikovat bezpečnostní a směrovací pravidla dle potřeby.

Navrhované modely přístupových bodů:

Typ prvku	Produkt	Popis
Přístupový bod A	FAP-231F-E	pro pokrytí vnitřních prostor (montáž na strop nebo zeď)
Přístupový bod B	FAP-234F-E	pro pokrytí venkovních prostor (montáž na stožár nebo zeď)
Přístupový bod C	FAP-23JF-E	pro pokrytí vnitřních prostor (montáž na el. parapet nebo volně na stůl)

Tabulka 10 - Typy přístupových bodů

Tabulka znázorňující maximální počet tunelem připojených přístupových bodů dle modelu kontroléru:

Typ FortiGate	Max. FortiAP	Max. FortiSwitch
[redacted]	512	64
[redacted]	48	16
[redacted]	32	8
[redacted]	8	8

Tabulka 11 - Max. počet AP

Vysílaná SSID:

SSID [redacted] bude sloužit pro připojení firemních zařízení. Na SSID bude aplikován protokol pro zabezpečení fyzického přístupu do sítě 802.1x. Klient bude připojen do bezdrátové sítě pouze tehdy, pokud se prokáže platným certifikátem počítače, vydaným certifikační autoritou zadavatele, uživatelským jménem a heslem. Tato ověření bude provádět autentizační server zadavatele, který nahlíží do uživatelské databáze. Klientem RADIUS serveru bude bezdrátový kontrolér.
Jako typ zabezpečení bude nastaveno WPA2 – podnikové se šifrováním AES. Ověřovací metodu bude plnit protokol EAP-TLS.

SSID [redacted] bude sloužit pro připojení soukromých zařízení zaměstnanců. Na SSID bude aplikován protokol pro zabezpečení fyzického přístupu do sítě 802.1x. Klient

bude připojen do bezdrátové sítě pouze tehdy, pokud se prokáže platným uživatelským jménem a heslem. Tato ověření bude provádět autentizační server zadavatele, který nahlíží do uživatelské databáze. Klientem RADIUS serveru bude bezdrátový kontrolér. Jako typ zabezpečení bude nastaveno WPA2 – podnikové se šifrováním AES. Ověřovací metodu bude plnit protokol PEAP-MSCHAPv2.

SSID [redacted] bude sloužit pro připojení návštěvníků. Jako typ zabezpečení bude nastaveno OPEN (žádné ověřování) bez šifrování.
Na SSID bude aplikován portálový přístup (webová autentizace). Klientovi se po připojení povolí pouze DHCP protokol a veškerý webový provoz bude přesměrovaný na https přihlašovací stránku (ostatní provoz je zakázán).
Klient se autentizuje přidělenými přístupovými údaji a tím je povolena jeho session. K ukončení komunikace dojde při odhlášení nebo po vypršení session timeout.
Přístupové údaje pro návštěvy bude generovat pověřená osoba. Vygenerované údaje bude možné vytisknout a předložit uživateli – návštěvě. Vzhled přihlašovací stránky lze upravit dle požadavku zadavatele.

3.2.4 FlowMon

Stávající FlowMon řešení poskytuje statistiky provozu založené pouze na hlavičkách L4, tedy zdrojová a cílová IP adresa a zdrojový a cílový port. Místem sběru statistik jsou rozhraní páteřních směrovačů na WAN síti, tedy nejsou informace o datových tocích konkrétně pro jednotlivé lokality.

Instalovaný Invea Flowmon Collector 1000VA je ve verzi 5.8 a je bez jakékoliv podpory a služby výrobce. Vzhledem k tomu, že používané statistiky založené na informacích z Netflow v5 neposkytují v porovnání s informacemi poskytovanými firewally FortiGate s centralizovaným pohledem přes FortiAnalyzer žádnou přidanou hodnotu, doporučujeme stávající Flowmon řešení ponechat bez změny a v první etapě implementace vyřešit Fortinet SecurityFabric, který je z pohledu bezpečnosti klíčový.
V dalších etapách doporučujeme doplnění bezpečnostního řešení o Flowmon systém, rozšířený o hardwarové flowmon sondy s odpovídajícím počtem portů 1GE/10GE, připojených do klíčových míst v síti. Tímto místem bývají nejčastěji SPAN porty páteřních přepínačů, na kterých se objevuje většina komunikace klient/server a klient/internet. Jádrem nového řešení by byl hardwarový kolektor s velikostí diskového subsytému vyhovující pro množství dat a požadované retenci těchto dat. Hardwarové sondy Flowmon poskytují kromě dat standardů Netflow/IPFIX ještě další dodatečné informace, které jsou využitelné pro měření tzv. Network Performance charakteristik a pro behaviorální bezpečnostní analýzu, které je vhodným doplňkem, ne konkurentem, pro instalované UTM firewally. Pro automatizovanou behaviorální analýzu doporučujeme použít plugin pro Flowmon kolektor Flowmon Anomaly Detection System (ADS), který dokáže odhalit hrozby na základě detekce anomálií v síťovém provozu a vytvoří tak v kombinaci se stávajícími standardními bezpečnostními technologiemi ucelený vícevrstvý systém ochrany podnikových dat.

Řešení monitorování datových toků a jeho využití pro behaviorální bezpečnostní analýzy je natolik rozsáhlé, že doporučujeme zpracovat pro toto řešení samostatný projekt, který by vycházel za stavu implementace Security Fabric popisované tímto projektem. Zejména se jedná o skutečné fyzické zapojení, ze kterého by se dal určit počet a umístění SPAN portů, a

tím počet a typy hardwarových sond. Z toho se pak odvíjí množství dat na kolektor, a tedy velikost tohoto kolektoru a výkon pluginu pro behaviorální analýzu.

3.2.5 Řízení přístupů

Řízení přístupu k síti neboli Network Access Control (NAC), je řešení pro přístup k síti s nulovou důvěrou, které poskytuje přehled o všech zařízeních v podnikových sítích. Tato technologie pomáhá organizacím držet krok s dnešním stále se rozšiřujícím počtem útoků a přináší nejen viditelnost síťového prostředí, ale také vynucování a dynamickou kontrolu zásad. Ať už se zařízení připojují zevnitř nebo vně sítě, může automaticky reagovat na napadená zařízení nebo neobvyklou aktivitu. NAC je důležitou součástí modelu Zero Trust Network Access (ZTNA).
NAC poskytuje přehled o všem, co je připojeno k síti, stejně jako schopnost ovládat tato zařízení a uživatele, včetně dynamických, automatických odpovědí. Hraje roli při posilování celkového zabezpečení infrastruktury sítě.
Správně fungující řešení může odepřít přístup nevyhovujícím uživatelům nebo zařízením, umístit je do karantény nebo omezit přístup k malému počtu síťových prostředků oddělených od zbytku sítě. NAC obecně podporuje následující:

- Ověřování a autorizace uživatelů a zařízení
- Profilování uživatelů a zařízení
- Odmítnutí nezabezpečených zařízení
- Karanténu nezabezpečených zařízení
- Omezení přístupu k nezabezpečeným zařízením
- Reakci na incidenty prostřednictvím prosazování zásad
- Řízení síťového přístupu pro hosty

3.2.5.1 FortiNAC

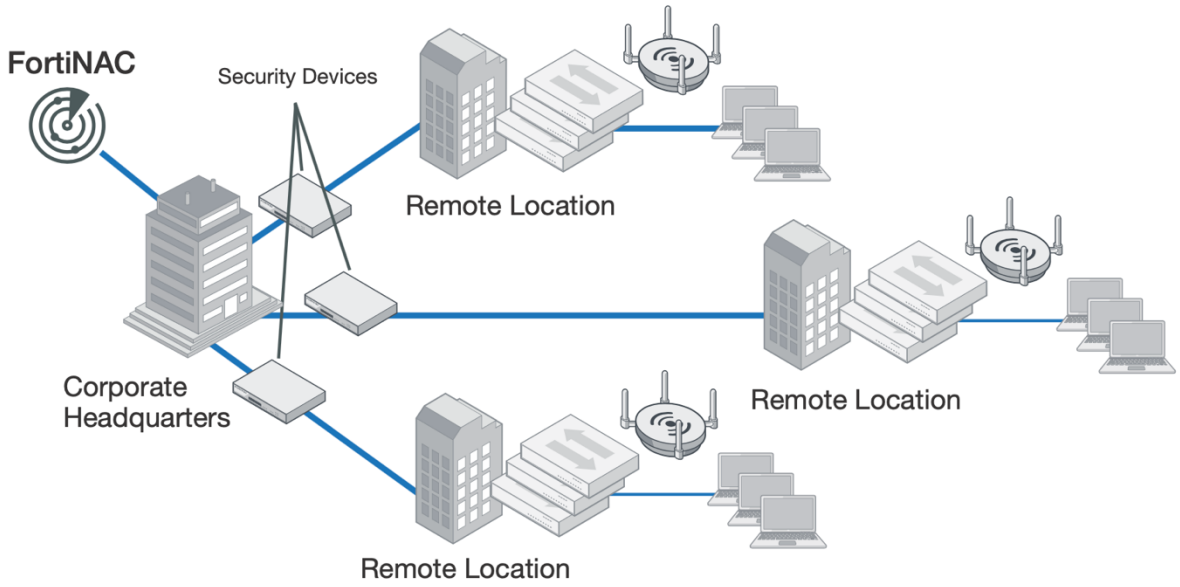
FortiNAC je řešení společnosti Fortinet pro řízení přístupu k síti, které vylepšuje Fortinet Security Fabric o viditelnost, kontrolou a automatickou odpověď na vše, co se připojuje k síti. FortiNAC poskytuje ochranu před hrozbami IoT, rozšiřuje kontrolu na zařízení třetích stran a organizuje automatické odpovědi na širokou škálu síťových událostí. Řešení FortiNAC chrání bezdrátové i drátové sítě pomocí centralizované architektury, která umožňuje distribuované nasazení s automatickou odezvou. Tři základní pilíře FortiNAC poskytují:

- **Device Visibility** – FortiNAC prohledá síť a najde každého uživatele, aplikaci a zařízení. S až 20 různými technikami pak může FortiNAC profilovat každý prvek na základě pozorovaných charakteristik a odpovědí.
- **Dynamic Network Control** – Jakmile jsou zařízení klasifikována a uživatelé jsou známí, umožňuje FortiNAC podrobnou segmentaci sítě, aby umožnila zařízením a uživatelům přístup k požadovaným a povoleným prostředkům sítě. FortiNAC používá dynamické řízení přístupu k síti založené na rolích k logickému vytváření síťových segmentů seskupováním aplikací a podobných dat k omezení přístupu k určité skupině uživatelů nebo zařízení.
- **Automated Response** – FortiNAC síť průběžně sleduje a vyhodnocuje koncové body, aby se ujistil, že odpovídají jejich profilu. FortiNAC znovu prohledá zařízení ke zjištění, že např. spoofing MAC adres nebude obcházet zabezpečení přístupu k síti.

FortiNAC je flexibilní a škálovatelné řešení. Řešení FortiNAC má tři prvky:

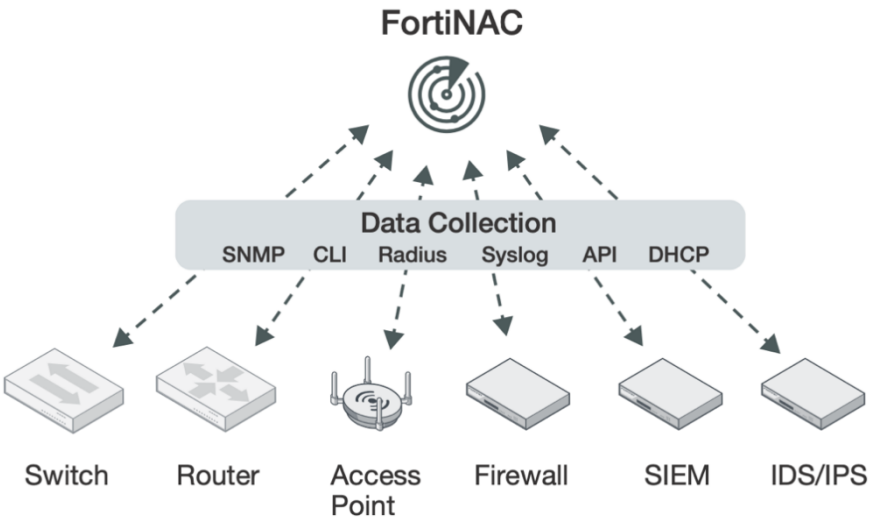
- **Aplikace a řízení** (povinné) - Aplikace poskytuje viditelnost, řízení poskytuje konfigurační funkce a funkce automatické odezvy.
- **Správa** (volitelné) - Správa umožňuje sdílení informací v rámci nasazení na více serverech.
- **FortiAnalyzer pro reporty** (volitelné) - FortiAnalyzer poskytuje zprávy a analýzy založené na informacích shromážděných ze sítě prostřednictvím FortiNAC.

FortiNAC je „out of band“ řešení, což znamená, že není v in-line provozu uživatele. Tato architektura umožňuje, aby byl FortiNAC nasazen centrálně a spravoval mnoho vzdálených míst. FortiNAC je tak ideální pro podporu distribuovaných architektur, včetně SD-WAN.



Obrázek 15 - FortiNAC deploy

Sběr dat se shromažďuje z různých zdrojů pomocí různých metod. K dosažení podrobné end-to-end viditelnosti potřebné k vytvoření skutečně bezpečného prostředí lze použít protokoly a metody SNMP, CLI, RADIUS, SYSLOG, API a DHCP.



Obrázek 16 - FortiNAC Data Collection

FortiNAC nabízí flexibilní možnosti nasazení na základě požadované úrovně pokrytí a funkčnosti:

- **BASE License** – Úroveň licence BASE poskytuje snadné řešení zabezpečení IoT a koncových bodů zobrazením všech koncových zařízení v síti, automatizací autorizace, povolením mikrosegmentace a uzamčení sítě.
- **PLUS License** – Zahrnuje všechny funkce BASE s vylepšenou viditelností a pokročilejšími kontrolami přístupu k síti a automatizovaným zajišťováním pro uživatele, hosty a zařízení, jakož i hlášení a analýzy.
- **PRO License** – Úroveň licence PRO poskytuje maximální viditelnost, kontrolu a odpověď. Licence PRO nabízí viditelnost koncových bodů v reálném čase, komplexní řízení přístupu a automatickou reakci na hrozby a poskytuje kontextové informace s tříděnými výstrahami.

		FORTINAC LICENSE TYPES	BASE	PLUS	PRO
Visibility	Network	Network Discovery	✓	✓	✓
		Rogue Identification	✓	✓	✓
		Device Profiling & Classification	✓	✓	✓
	Endpoint	Enhanced Visiblity	✓	✓	✓
		Anomaly Detection	✓	✓	✓
		MDM Integration	✓	✓	✓
		Persistent Agent		✓	✓
	User	Authentication		✓	✓
		Captive Portal		✓	✓
Automation / Control		Network Access Policies	✓	✓	✓
		IoT Onboarding with Sponsor	✓	✓	✓
		Rogue Device Detection & Restriction	✓	✓	✓
		Firewall Segmentation	✓	✓	✓
		MAC Address Bypass (MAB)	✓	✓	✓
		Full RADIUS (EAP)		✓	✓
		BYOD / Onboarding		✓	✓
		Guest Management		✓	✓
		Endpoint Compliance		✓	✓
		Web & Firewall Single Sign-on		✓	✓
Incident Response		Event Correlation			✓
		Extensible Actions & Audit Trail			✓
		Alert Criticality & Routing			✓
		Guided Triage Workflows			✓
Integrations		Inbound Security Events			✓
		Outbound Security Events		✓	✓
		REST API	✓	✓	✓
Reporting		Customizable Reports	✓	✓	✓

Obrázek 17 - FortiNAC licence

FortiNAC je plně integrovatelný v rámci Fortinet Security Fabric s dalšími nabízenými a již provozovanými produkty Fortinet, jak je zřejmé z následující tabulky:

Fabric produkt	**Integrace**	**Popis**
FortiGate	FortiSwitch řízený FortiGate	FortiNAC poskytuje viditelnost v síti (kde se připojují koncové body) a spravuje přiřazení VLAN pro koncový bod. Toho lze dosáhnout odesláním příslušných konfiguračních příkazů do zařízení.
	FortiAP řízené FortiGate	FortiNAC poskytuje viditelnost v síti (kde se připojují koncové body) a spravuje přiřazení VLAN pro koncový bod. Toho lze dosáhnout odesláním příslušných konfiguračních příkazů do zařízení.

	FortiNAC/FortiGate Fortinet Single Sign-On (FSSO)	FortiNAC poskytuje automatické použití firewall politiky na FortiGate na hostitele připojující se k síti. Toho je dosaženo použitím RADIUS accounting informací odeslaných z FortiNAC do SSO agenta na FortiGate.
	FortiGate VPN kontrolované FortiNAC	ForitNAC řídí přístup k síti využitím FSSO na FortiGate. Když se uživatelé připojují, je přístup pro uživatele z VPN k síti ve výchozím nastavení omezen. Přístup je upraven, pouze pokud se uživatel úspěšně autentizuje prostřednictvím FortiNAC, spustí příslušného agenta FortiNAC a projde všemi požadovanými kontrolami.
FortiClient EMS	Řešení MDM jako připojení důvěryhodných zařízení	Tato integrace zrychluje proces registrace zařízení, která byla zaregistrována pomocí EMS. Zařízení připojená k síti lze zaregistrovat ve FortiNAC pomocí dat z EMS.
FortiAnalyzer	Reportování	FortiAnalyzer poskytuje centralizované logování, analýzu a reporty napříč Fortinet Security Fabric. Integrace s FortiNAC umožňuje FortiAnalzyeru rozšířit informace o: • Eventy • FortiNAC alarmy • Endpoint data, včetně reportů o inventarizaci • Data o síťové infrastruktuře
FortiEDR	Reakce na incidenty	Syslog integrace umožňuje FortiNAC reagovat na základě zpráv odeslaných z FortiEDR. Tyto zprávy poskytují informace, které FortiNAC může použít k odesílání upozornění (například e-mail) nebo k akci proti přidruženému hostiteli, například deaktivaci hostitele nebo jeho označení „za rizikové“.

Tabulka 12 - FortiNAC integrace

3.3 Koncové lokality

Koncové lokality jsou identifikovány podle třetího byte v IP adrese a tento je pak použit ve všech sítích pro jednotlivou koncovou lokalitu. Seznam identifikátorů (Síť ID) je zřejmý z následující tabulky:

Lokalita PLA	**Zkratka**	**Síť ID**	**Název firewallu**
Bedřichov	[redacted]	[redacted]	[redacted]
Brandýs nad Labem			
Čelákovice			
České Kopisty			
Dolní Beřkovice			
Fojtka, Fojtecká			
Hamry, Studnice			
Harcov, Liberec			
Hradišťko			
Hučák, Hradec Králové			
Hvězda (rybník), Opatov			
Josefův Důl			

Klavary - Veltruby	[redacted]	[redacted]	[redacted]
Kolín			
Kostelec nad Labem			
Kostomlátky			
Křižanovice			
Labská			
Les Království - Bílá Třemešná			
Lobkovice, Mlékojedy			
Lovosice			
Lysá nad Labem			
Mšeno - Jablonec nad Nisou			
Nymburk			
Obříství			
Pařížov - Běstvina			
Pastviny			
Poděbrady			
Pracoviště Náchod			
Předměřice			
Přelouč, Břehy			
Rozkoš			
Rudolfov (MVE)			
Seč			
Smiřice			
Souš - Desná			
Srnojedy			
Středisko Čáslav			
Středisko Děčín			
Středisko Dvůr Králové			
Středisko Hradec Králové			
Středisko Jičín			
Středisko Kostomlaty			
Středisko Litoměřice			
Středisko Mladá Boleslav			
Středisko Turnov			
Středisko Vaňov - Ústí			
Středisko Vysoké Mýto			
Středisko Žamberk			
Střekov			
Štětí, Račice			
Týnec			
Veletov			
Velký Osek			
Vrchlice - Miskovice			
Závod Jablonec nad Nisou			
Závod Pardubice			

Závod Roudnice nad Labem	[redacted]	[redacted]	[redacted]
Závod Střední Labe			
Zlíč (rozd. Objekt)			

Tabulka 13 - ID sítě lokality

Seznam navrhovaných IP subnetů a VLAN pro koncovou lokalitu je pak zřejmý z následující tabulky:

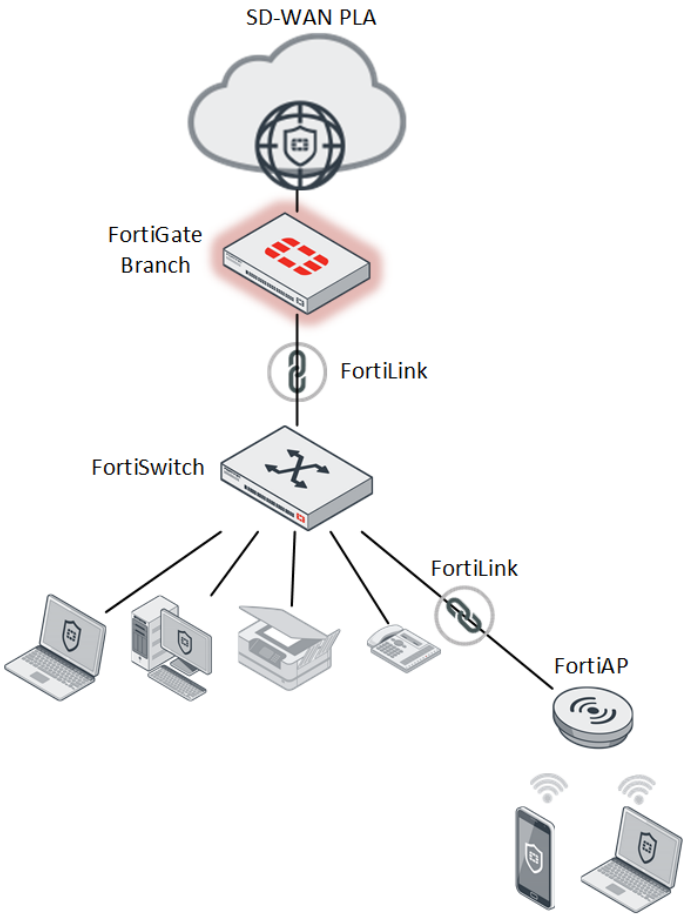
VLAN ID	Jméno VLAN	IP subnet	Router	Popis
1	[redacted]	[redacted]	[redacted]	[redacted]
40				
48				
99				
201				
208				
724				
728				
N/A				
4090				
4091				
4092				
4093				

Tabulka 14 - Lokalita seznam VLAN

Navrhované FortiSwitch přepínače podporují FortiGate management prostřednictvím FortiLink a zajišťují tak rozšíření výše uvedeného zabezpečení sítě Fortinet Security Fabric až na úroveň ethernetového portu. FortiLink umožňuje, aby se FortiSwitch stal logickým rozšířením FortiGate a integroval jej přímo do Fortinet Security Fabric. Požadované prostupy mezi jednotlivými VLAN jsou poté řízeny v konfiguraci bezpečnostních pravidel na FortiGate v koncové lokalitě.

Díky aktivaci a správě funkcí zabezpečení sítě a přístupové vrstvy prostřednictvím jediné konzoly FortiManager lze centralizovanou správu zásad, včetně přístupu a řízení na základě rolí, snadno implementovat a spravovat. Uživatele nebo zařízení lze ověřit proti stejné databázi a použít stejné zásady zabezpečení bez ohledu na to, jak a kde se k síti připojují.

Všechny navrhované aktivní prvky disponují požadovanými funkcionalitami jako je ARP Poison Routing, ARP spoofing, DHCP spoofing, MAC flooding a dalšími. Budou také podporovat Power over Ethernet (PoE) pro připojení bezdrátových přístupových bodů a dalších zařízení bez nutnosti použít dedikovaný napájecí zdroj. Navrhovaná topologie přístupové vrstvy koncové lokality je zřejmá z následujícího obrázku:



Obrázek 18 - Topologie koncové lokality

Na jednotlivých koncových lokalitách budou nasazeny přístupové přepínače typů C, D a E podle výše uvedené tabulky č. 8:

Název lokality	**Počet portů**	**Typ C**	**Typ D**	**Typ E**
Bedřichov	8	1		
Brandýs nad Labem	16	2		
Čelákovice	16	2		
České Kopisty	16	2		
Dolní Beřkovice	16	2		
Fojtka, Fojtecká	8	1		
Hamry, Studnice	16	2		
Harcov, Liberec	24		1	
Hradišťko	8	1		
Hučák, Hradec Králové	8	1		
Hvězda (rybník), Opatov	4	1		
Josefův Důl	8	1		
Klavary - Veltruby	8	1		
Kolín	20	1	1	
Kostelec nad Labem	8	1		
Kostomlátky	16	2		
Křižanovice	32	4		
Labská	8	1		

Les Království - Bílá Třemešná	24		1	
Lobkovice, Mlékojedy	16	2		
Lovosice	16	2		
Lysá nad Labem	8	1		
Mšeno - Jablonec nad Nisou	8	1		
Nymburk	8	1		
Obříství	24	4		
Pařížov - Běstvina	8	1		
Pastviny	8	1		
Poděbrady	8	1		
Pracoviště Náchod	8	1		
Předměřice	8	1		
Přelouč, Břehy	8	1		
Rozkoš	24		1	
Rudolfov (MVE)	8	1		
ŘSP	928	2	2	18
Seč	16	2		
Smiřice	8	1		
Souš - Desná	24		1	
Srnojedy	8	1		
Středisko Čáslav	24		1	
Středisko Děčín	24		1	
Středisko Dvůr Králové	24		1	
Středisko Hradec Králové	56	1	2	
Středisko Jičín	24		1	
Středisko Kostomlaty	24		1	
Středisko Litoměřice	24		1	
Středisko Mladá Boleslav	24		1	
Středisko Turnov	24		1	
Středisko Vaňov - Ústí	48			1
Středisko Vysoké Mýto	24		1	
Středisko Žamberk	24		1	
Střekov	72	3	2	
Štětí, Račice	16	2		
Týnec	32	1	1	
Veletov	32	1		
Velký Osek	24		1	
Vrchlice - Miskovice	8	1		
Závod Jablonec nad Nisou	96			2
Závod Pardubice PU2	128	1	1	2
Závod Roudnice nad Labem	128	4	2	1
Závod Střední Labe PU4	96			2
Zlíč (rozd. Objekt)	8	1		

Tabulka 15 - Přístupové přepínače

Z dostupné dokumentace stávající strukturované kabeláže vyplývá, že bude možné využít rychlost 1GB pro připojení jednotlivých koncových zařízení a přístupového přepínače umístěného v datovém rozvaděči koncové lokality. Propojení datových rozvaděčů pomocí optické linky je limitováno délkou a použitým multimode optickým kabelem dle následující tabulky:

Typ	Core/Cladding Diameter (µm)	FastEthernet 100Base-FX	GigabitEthernet 1000Base-SX	GigabitEthernet 1000Base-LX
Multimode OM1	62,5/125	2km	220m	550m s mode condition cable
Multimode OM2	50/125	2km	500m	550m s mode condition cable

Tabulka 16 - Multimode vzdálenosti

Optické linky v přístupové vrstvě sítě PLA jsou použity v následujících koncových lokalitách:

Lokalita	Rozvaděče	Typ vlákna	Počet vláken	Délka (m)
Brandýs nad Labem				
České Kopisty	Velin komory - provozni budova	MM 50/125	4	
	Velin komory - velín jezu	MM 50/125	8	
Dolní Beřkovice	Velin komory - vedouci jezu	MM 50/125	4	100
Kostomlátky				
Lysá nad Labem	Velin komory - velín jezu	MM 50/125	4	90
Nymburk	pilíř RB - kancelář			
Obříství	Velin komory - velín jezu			
Seč	domek hrazneho - prehradni hraz			
Smiřice	pilíř RB - kancelář	MM 50/125	4	220
Srnojedy	pilíř RB - kancelář			
Středisko Hradec Králové				
Střekov	Velín komory RD01 - Jezové pole RD04	MM 50/125	8	350
	Velín komory RD01 - Dílny RD02	MM 50/125	4	220
	Velín jezu RD03 - Jezové pole RD04	MM 50/125	4	70
Štětí, Račice	Velin komory - provozni budova	MM 50/125	4	100
Závod Pardubice PU2	Budova závodu 2 - budova dílen	MM 62,5/125	4	100
	Velín komory - budova dílen	MM 50/125	4	210
	Kancelář jezného - budova dílen	MM 50/125	4	90
Závod Roudnice nad Labem	Budova Ředitelství RD01 - Provozní budova č. 305 RD04	MM 62,5/125	8	120
	Velín Jezu RD05 - Provozní budova č. 305 RD04	MM 50/125	8	230
	Budova Ekonomové RD03 - Provozní budova č. 305 RD04	MM 62,5/125	8	90
	Budova Ředitelství RD01 - Budova mlýna RD02	MM 62,5/125	8	300
	Velín Jezu RD05 - Velín komory	MM 62,5/125	8	1.300

	Velín komory - provozní budova RD06	MM 62,5/125	4	250

Tabulka 17 - Optické spoje LAN

Z výše uvedené tabulky vyplývá, že použitý typ vlákna je limitujícím faktorem zejména v lokalitě Závod Roudnice nad Labem a Střekov. Zde doporučujeme nahrazení Multimode tras za Singlemode vlákna 9/125.

V lokalitě Obříství je pro připojení objektu dílen Kly použito modemové spojení přes telefonní linku, neumožňující dosažení vyšších přenosových rychlostí než řádově kbps. Vybudování optické trasy se jeví jako neekonomické, bezdrátový spoj mezi těmito lokalitami nelze vybudovat z důvodu nepřímé dohlednosti. Z tohoto důvodu navrhujeme nahradit tuto modemovou linkou vybudováním objektu Dílny Kly jako samostatný přístupový bod SD-WAN sítě PLA s využitím LTE konektivity některého z místně dostupných providerů.

V lokalitách Čelákovice, Kolín, Křižanovice, Lovosice, Střekov a Týnec jsou nyní provozovány bezdrátové spoje bod-bod pro propojení místních provozoven. Stávající spoje jsou různých typů, parametrů a konfigurací, mnohdy se zastaralými možnostmi zabezpečení a nízkou přenosovou rychlostí. Z tohoto důvodu navrhujeme nahradit tyto spoje moderním spojem RBLHGG-60adkit. Jedná se o gigabitový spoj v bezlicenčním pásmu 60GHz s šifrováním AES.

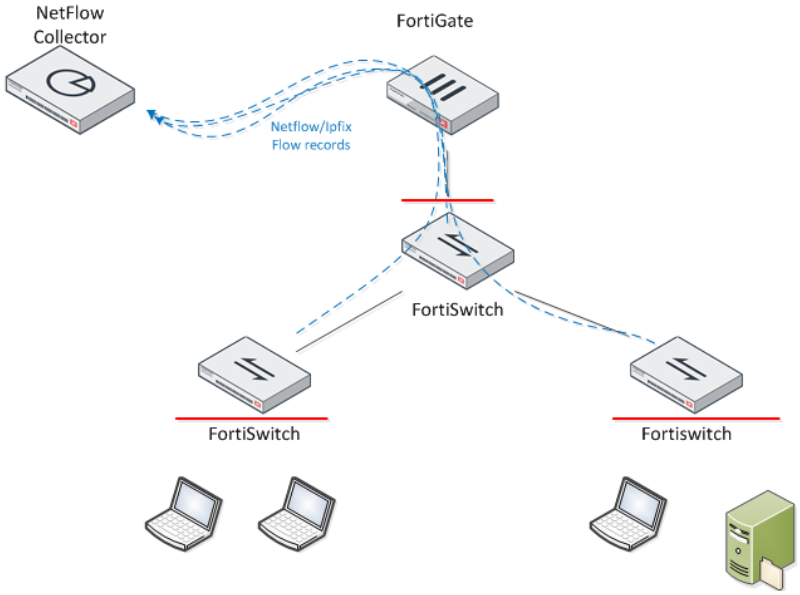
Umístění a přibližné vzdálenosti bezdrátových spojů:

Bezdrátové spoje			
Název lokality	**Směr**	**Vzdálenost**	**Typ spoje**
Čelákovice	Velín komory – Domek jezného	100 m	RBLHGG-60adkit
Kolín	Přes komoru	70 m	RBLHGG-60adkit
Křižanovice	Dolní Provozní budova – Dílny	70 m	RBLHGG-60adkit
Křižanovice	Dílny – Přehradní hráz	150 m	RBLHGG-60adkit
Lovosice	Velín komory – Provozní budova	50 m	RBLHGG-60adkit
Lovosice	Velín komory – Velín jezu	160 m	RBLHGG-60adkit
Střekov	Jezové pole u velínu jezu – Budova střediska	250 m	RBLHGG-60adkit
Týnec	Velín komory – Provozní budova	130 m	RBLHGG-60adkit

Tabulka 18 - Bezdrátové spoje LAN

Veškeré navrhované aktivní prvky umožňují monitoring pomocí SNMP dotazů, konfigurací lze omezit nebo vypnout zasílání trapů a jsou k dispozici MIB definice jednotlivých OID.

FortiGate a FortiSwitch podporují zasílání informací o provozu Netflow (v1, v5, v9) a IPFIX.



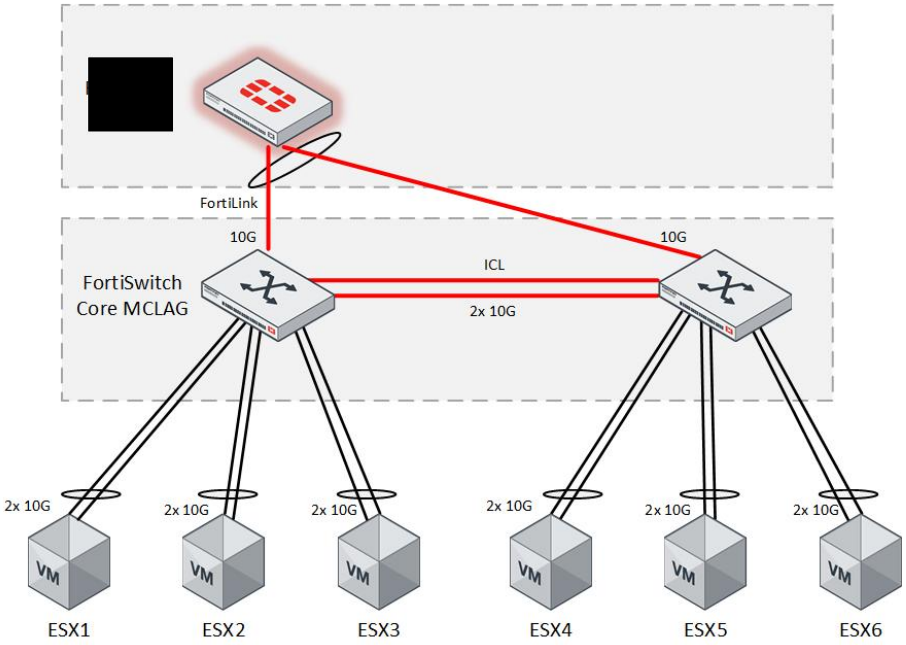
Obrázek 19 - Netflow

4. Doporučený postup migrace

Navrhované technické řešení se snaží v co největší míře využít stávající a nově budovanou infrastrukturu SD-WAN na prvcích výrobce Fortinet a ochránit tak již vložené investice. Řešení zároveň integruje síťovou infrastrukturu a architekturu zabezpečení do jednoho celku, což umožňuje škálování a změnu sítě bez ohrožení zabezpečení.

4.1 Centrální lokalita

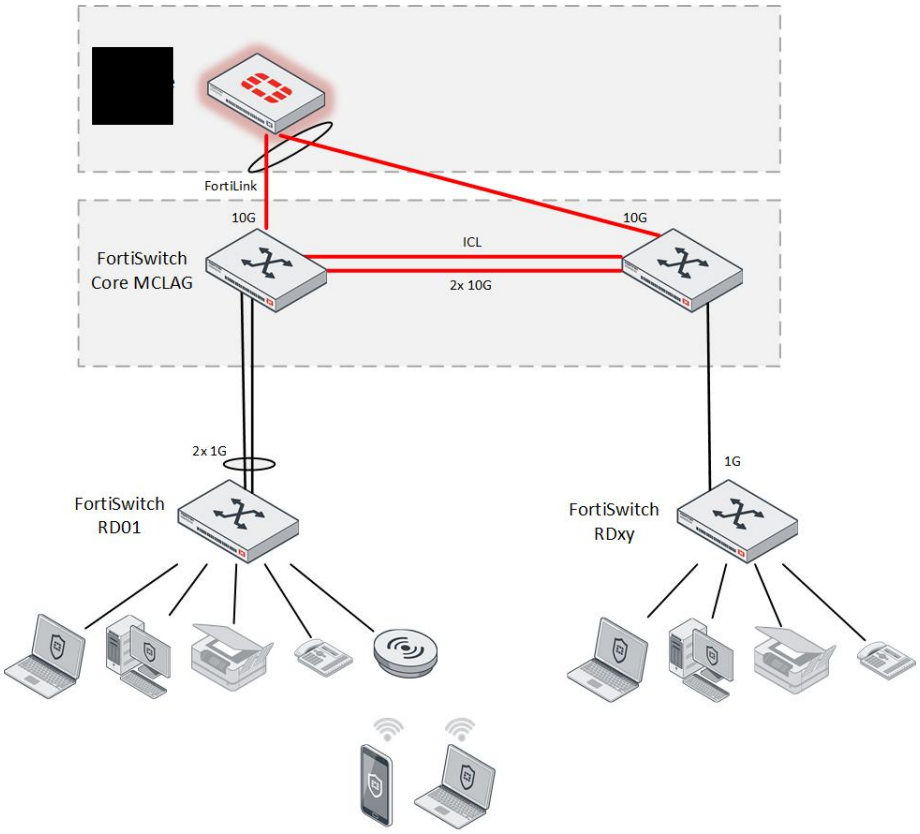
Jak je uvedeno výše v kapitole 3.2.1 je pro vybudování dostatečně robustního a redundantního centra sítě vhodné vytvořit páteřní vrstvu, která bude geograficky rozmístěna do dvou serveroven v budově A a B. Do tohoto centra sítě pak propojit ToR přepínače a jednotlivé přístupové prvky LAN sítě vždy alespoň dvěma linkami s využitím protokolu LACP.
Vybudování této topologie vyžaduje mít vybudovanou dostatečnou kapacitu optické sítě mezi serverovnami A a B a také k jednotlivým datovým rozvaděčům s horizontálními rozvody strukturované kabeláže.
Limitujícím faktorem pro vybudování plnohodnotné redundantní infrastruktury je také stávající firewall [redacted] nepodporující 40GB interface a bez licencovaného druhého boxu. Na zařízení [redacted] je již výrobcem ohlášen konec podpory [redacted], navrhujeme tedy nahradit tyto boxy dvojicí nových FortiGate s podporou dostatečného počtu 25GB a 10GB SFP+ interface, např. FortiGate 600F. Nicméně do doby, než skončí již předplacená podpora na [redacted] (expirace 15. 3. 2023) lze tento prvek s omezením použít a zakomponovat do nové infrastruktury LAN/WAN.
Topologie páteřní vrstvy a datacentra bez redundance FortiGate a optické sítě s použitím Singlemode mezi serverovnami A a B je zřejmá z následujícího obrázku:



Obrázek 20 - Topologie datacentra bez redundance

Topologie páteřní vrstvy a datacentra redundantní infrastruktury po nahrazení [redacted] a vybudování optické sítě s použitím Singlemode mezi serverovnami A a B je zřejmá z výše uvedeného obrázku č. 13 – Ekonomická varianta topologie datacentra.

Topologie přístupové vrstvy bez redundance FortiGate a optické sítě s použitím Singlemode mezi serverovnami A a B a jednotlivými datovými rozvaděči je zřejmá z následujícího obrázku:



Obrázek 21 - Topologie přístupové vrstvy bez redundance

Topologie přístupové vrstvy po nahrazení [redacted] a vybudování optické sítě s použitím Singlemode mezi serverovnami A a B a jednotlivými datovými rozvaděči je zřejmá z výše uvedeného obrázku č. 14 – Topologie přístupové vrstvy.

4.1.1 Realizace projektu – etapa 1

V první etapě realizace projektu bude vytvořena nová páteřní infrastruktura, a to variantně v závislosti na vybudování nové optické sítě v centrální lokalitě.

4.1.1.1 Páteřní infrastruktura

4.1.1.1.1 Varianta bez redundance

Bez nové optické sítě bude do každé ze serveroven v budovách A a B nainstalován nový páteřní přepínač typu A, který bude ke stávajícímu firewallu [redacted] připojen pomocí FortiLink 1x 10GB linkou a vzájemně propojen 2x 10GB ICL linkou. Do tohoto páteřního centra sítě pak budou připojeny jednotlivé přístupové přepínače z datových rozvaděčů s horizontálními rozvody strukturované kabeláže pomocí SFP 1GB modulů.

Stávající VMware servery budou doplněny o 10GB interface a zapojeny do páteřního centra sítě vždy alespoň 2x 10GB linkou v rámci dané serverovny v budovách A a B pomocí SFP+ 10GB modulů.

4.1.1.1.2 Varianta s redundancí

V případě realizace projektu až po vybudování nové optické sítě v centrální lokalitě bude možné vybudovat redundantní topologii páteřní infrastruktury a datového centra. Tato varianta předpokládá také náhradu stávajícího firewallu [redacted] za dvojici nových firewallů s podporou dostatečného počtu 10GB SFP+ interface (např. FortiGate 600F).

Do každé ze serveroven v budovách A a B bude nainstalován nový páteřní přepínač typu A, který bude ke každému z dvojice firewallů připojen pomocí alespoň FortiLink 1x 10GB linkou s využitím linkové agregace a vzájemně propojen 2x 40GB ICL linkou. Dvojice páteřních přepínačů bude technologií multichassis LAG (MCLAG) spojena do jednoho logického celku.

Do každého páteřního přepínače pak budou připojeny jednotlivé přístupové přepínače z datových rozvaděčů s horizontálními rozvody strukturované kabeláže pomocí 2x SFP+ 10GB modulů s využitím linkové agregace, jak je uvedeno výše v obrázku č. 14 - Topologie přístupové vrstvy.

4.1.1.1.2.1 Optimální varianta topologie DC

Do každé ze serveroven v budovách A a B bude nainstalována dvojice Top of Rack přepínačů typu B, která bude k distribuovanému páteřnímu přepínači připojena pomocí FortiLink 4x 10GB linkou a vzájemně propojena 2x 40GB ICL linkou. Každá z dvojice Top of Rack přepínačů bude technologií multichassis LAG (MCLAG) spojena do jednoho logického celku.

VMware servery budou připojeny k ToR přepínačům vždy alespoň 2x 10GB linkou v rámci dané serverovny v budovách A a B pomocí SFP+ 10GB modulů s využitím linkové agregace.

4.1.1.1.2.2 Ekonomická varianta topologie DC

Do každé ze serveroven v budovách A a B bude nainstalován jeden Top of Rack přepínač typ B, který bude k distribuovanému páteřnímu přepínači připojen pomocí FortiLink 2x 10GB linkou a vzájemně propojeny 2x 40GB ICL linkou. Dvojice Top of Rack přepínačů bude technologií multichassis LAG (MCLAG) spojena do jednoho logického celku.

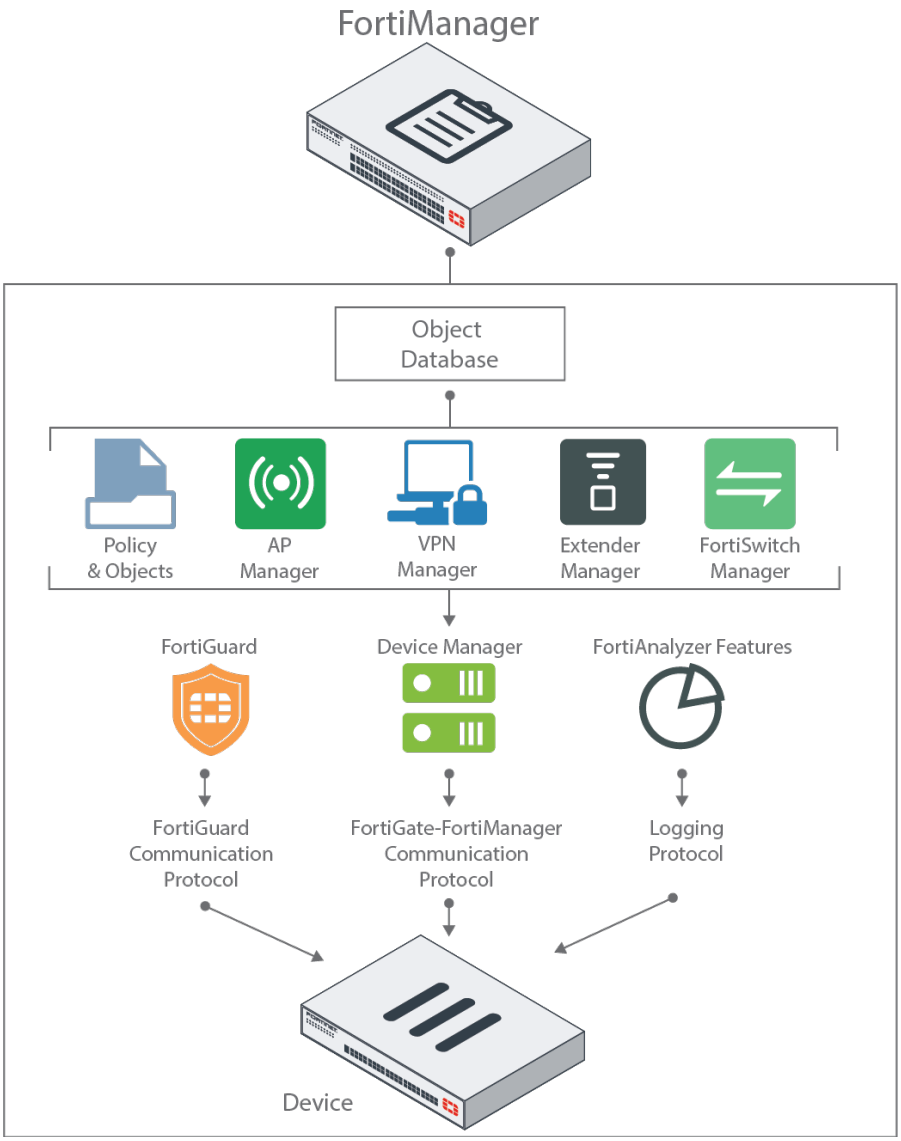
VMware servery budou připojeny k ToR přepínači v rámci dané serverovny vždy alespoň 1x 10GB linkou a zároveň budou připojeny k páteřnímu přepínači v rámci dané serverovny vždy alespoň 1x 10GB linkou pomocí SFP+ 10GB modulů bez možnosti využití linkové agregace.

4.1.1.2 FortiManager

Do virtuálního prostředí PLA bude nainstalována centrální management konzole FortiManager, která umožní centralizovanou správu nainstalovaných přepínačů v datovém centru sítě a přístupové vrstvy centrální lokality. FortiManager bude zalicencován na dostatečný počet registrovaných zařízení a bude také použit pro centralizovanou správu nainstalovaných FortiGate koncových lokalit ve WAN síti PLA. V době vzniku projektu předpokládáme licenci pro 100 registrovaných zařízení. Licenční model FortiManager je definován takto:

- VDOM disabled: 1 FortiGate = 1 licence
- VDOM enabled: 1 VDOM = 1 licence
- FortiGate v HA: Žádná licence pro sekundární FortiGate
- FortiAP, FortiSwitch a FortiExtender není licencován, tzn. že max. počet spravovatelných zařízení je limitován dle modelu kontroléru uvedeného výše v tabulce č. 11 - Max. počet AP.

Uvnitř FortiManageru je databáze objektů, která je sdílena jednotlivými moduly Policies & Objects, AP Manager, VPN Manager a FortiSwitch Manager, které budou poté využity k zavedení přístupových politik a sdíleny napříč všemi zaregistrovanými FortiGate.



Obrázek 22 - FortiManager

4.1.1.2.1 Device Manager

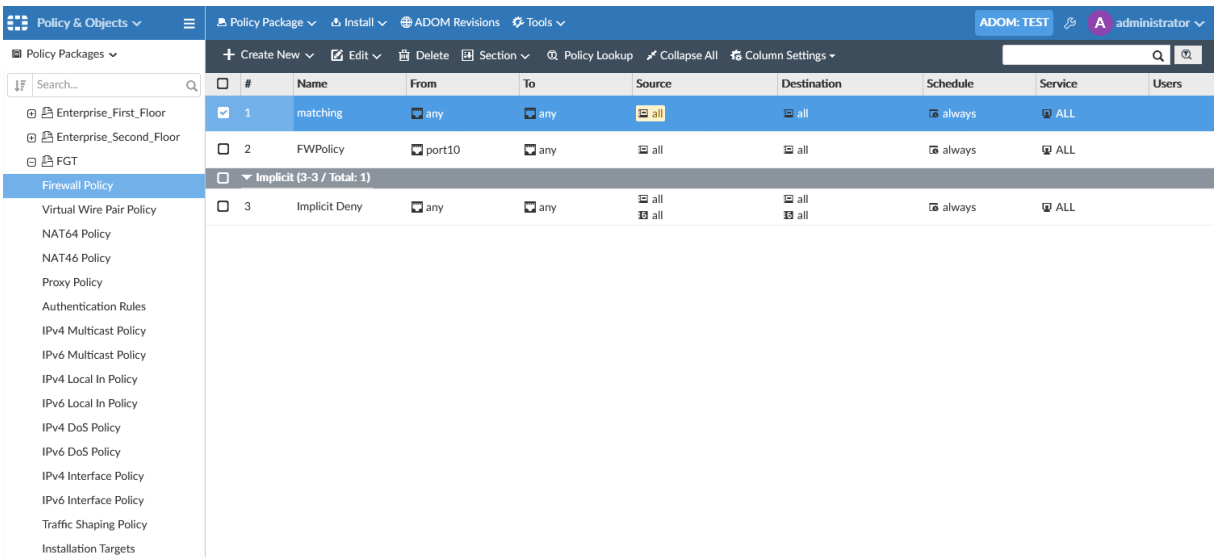
Pomocí podokna Device Manager lze přidávat a autorizovat zařízení, která budou řízena pomocí FortiManageru. Lze také vytvořit změny konfigurace zařízení a nainstalovat tyto změny do spravovaných zařízení. Podokno obsahuje ve stromové nabídce následující položky:

- **Device & Groups** – použito pro přidání, konfiguraci a zobrazení zařízení. Lze také spustit průvodce instalací.
- **Scripts** – pro vytvoření, nebo import skriptů.
- **Provisioning Templates** – konfigurace template pro zjednodušení konfigurace nových zařízení a hromadných úprav konfigurace.
- **Firmware Templates** – konfigurace template pro upgrade firmware na FortiGate a dalších zařízení, jako jsou FortiAP a FortiSwitch.
- **Monitors** – sledování provozu všech SD-WAN sítí a VPN.

4.1.1.2.2 Policy & Objects

Podokno Policy & Objects umožňuje centrálně spravovat a konfigurovat zařízení, která jsou spravována jednotkou FortiManager. To zahrnuje základní nastavení sítě pro připojení zařízení k síti, firewallová pravidla přístupu do jednotlivých definovaných zón a také definice bezpečnostních profilů a jejich přiřazení do pravidel. Všechny změny týkající se politik a objektů by pak měly být prováděny pouze pomocí FortiManageru, nikoli na jednotlivých spravovaných zařízeních.

Po přidání stávajícího firewallu [redacted] do FortiManageru budou naimportována veškerá pravidla a objekty do jednotlivých bezpečnostních balíčků dle příslušnosti do jednotlivých VDOM, které jsou již na FortiGate vytvořeny.



Obrázek 23 - FortiManager Policy

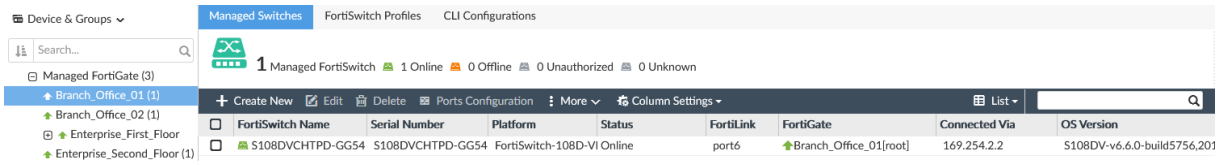
Všechny importované objekty budou spravovány jedinou databází jedinečnou pro FortiManager ADOM. Objekty uvnitř této databáze mohou zahrnovat položky, jako jsou adresy, síťové služby, definice IPS, definice antiviru, profily filtrování webu atd.
Mnoho objektů obsahuje možnost povolit dynamické mapování. Dynamické objekty se poté používají k mapování jednoho logického objektu na jedinečnou definici pro každý řízený FortiGate, což umožní vytvoření společného bezpečnostního balíčku pro více FortiGate v síti PLA. Stávající firewalová IPv4 pravidla budou doplněna o požadované prostupy mezi jednotlivými segmenty LAN sítě PLA, dle zadané komunikační matice.

4.1.1.2.3 FortiSwitch Manager

FortiSwitch Manager bude použit ke správě instalovaných FortiSwitchů, které jsou řízeny zařízeními FortiGate pod správou FortiManageru. FortiSwitch Manager lze použít ve dvou režimech správy:

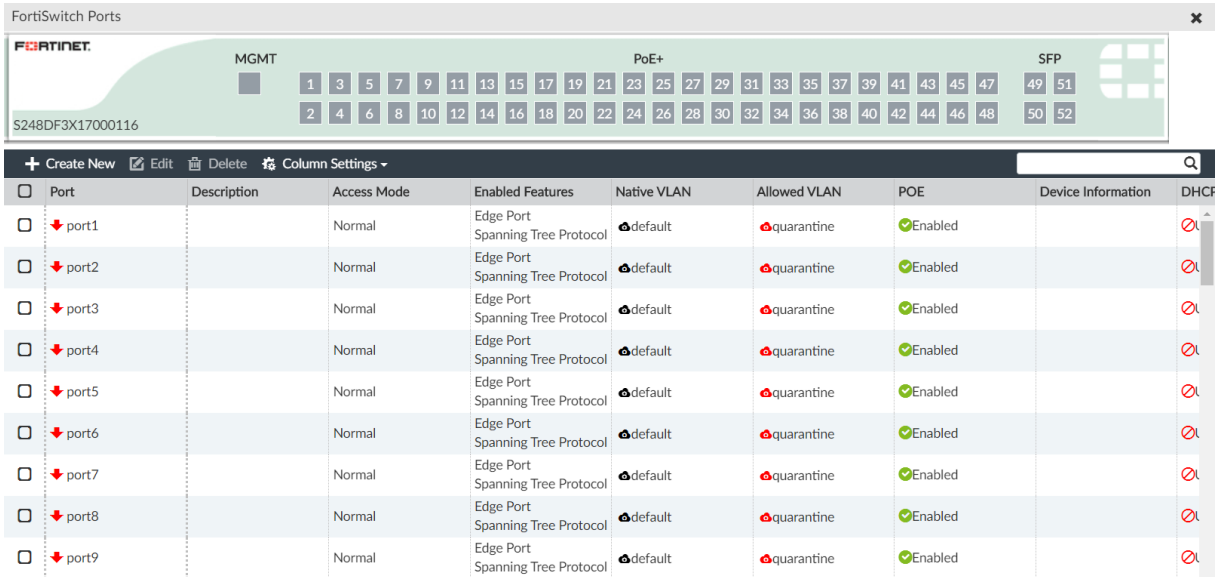
- Centrální správa přepínačů – lze vytvořit šablony pro různé konfigurace přepínačů a přiřadit šablony více spravovaným přepínačům.
- Per-device správa přepínačů – lze konfigurovat změny na každém spravovaném přepínači.

V centrální lokalitě sítě PLA předpokládáme použití per-device správu přepínačů, což umožní v menu FortiSwitch Profile vytvořit a spravovat profily pro definice VLAN, NAC politiky, politiky pro zabezpečení, LLDP profily, QoS profily a vlastní příkazy, které lze přiřadit jednotlivým přepínačům.



Obrázek 24 - Managed Switches

V režimu správy podle zařízení bude pak možné nakonfigurovat jednotlivé porty pro každý spravovaný přepínač.



Obrázek 25 - FortiSwitch porty

Více informací a kompletní administrační průvodce je volně dostupný na stránkách výrobce, viz.: https://docs.fortinet.com/document/fortimanager/7.0.0/administration-guide/512210/setting-up-fortimanager.

4.1.1.3 Komunikační matice

Prostupy mezi jednotlivými segmenty LAN sítě v centrální lokalitě a na koncové lokality sítě PLA budou definovány pomocí centrální management konzole FortiManager a distribuovány

do jednotlivých VDOM vytvořených na stávajícím [redacted] dle komunikační matice uvedené v příloze tohoto projektu PLA-WAN-komunikacni-matice.xlsx.
V době vzniku tohoto projektu nejsou zřejmé vazby potřebných prostupů na úroveň TCP/UDP portů, zejména pro technologickou část sítě. Bez profilování připojovaných zařízení pomocí FortiNAC a proaktivní ochrany Fortinet Zero Trust Network Access tak budou pravidla definována na základě IP adresy a v případě uživatele a zařízení připojeného do Microsoft domény také na základě znalosti přihlášeného uživatele do domény PLA.CZ pomocí Fortinet SSO tak, jak je již v síti PLA implementováno.

4.1.2 Realizace projektu – etapa 2

V této etapě bude, nad již vybudovanou infrastrukturou z etapy 1 zavedeno řízení přístupu k síti.

4.1.2.1 FortiNAC

Do virtuálního prostředí PLA bude nainstalována konzole FortiNAC, která umožní centralizovanou správu pro řízení přístupu k síti v centrální lokalitě a také koncových lokalit sítě PLA. FortiNAC bude zalicencován na celkový počet portů přístupových přepínačů s rezervou pro online zařízení v bezdrátové síti PLA. V době vzniku tohoto projektu je počítáno s licencí pro 2400 koncových zařízení.
FortiNAC bude integrován v rámci Fortinet Security Fabric s dalšími nabízenými a již provozovanými produkty Fortinet, jak je zřejmé z tabulky č. 12 – FortiNAC integrace.

4.1.2.1.1 Device profiler

Profilování zařízení je mechanizmus k automatické kategorizaci a kontrole zřízení která se připojují do sítě. Tento proces běží kontinuálně, skenuje host databázi s IP adresami, pro neznámá zařízení přiřadí typ na základě profilů nebo pravidel nastavených ve FortiNAC.
Device profiler pravidla používají informace jako je operační systém, vendor OUI apod. Po kategorizaci zařízení je k tomuto zařízení přidruženo pravidlo použité k jeho profilování. Pokud se zařízení odpojí od sítě a později se znovu připojí, profiler zařízení potvrdí, že zařízení stále odpovídá pravidlu. Pokud zařízení neodpovídá jeho přidruženému pravidlu, profiler zařízení může zařízení deaktivovat nebo upozornit správce pomocí událostí a alarmů.

Pokud se nová, neznámá zařízení připojují k síti Device profiler zařízení kategorizuje a umisťuje je do FortiNAC na základě pravidel profilování. Proces je následující:

1. Zařízení nebo host se připojí k síti.
2. FortiNAC zjistí, že se něco připojilo.
3. Funkce Device Identity kontroluje MAC adresu. Pokud je MAC adresa k dispozici, identita zařízení ji porovná se známými MAC adresami.
4. Pokud MAC adresa není známa, zařízení se umístí do host databáze jako rogue s dalšími dostupnými informacemi, jako je IP adresa nebo operační systém.
5. Pokud má zařízení IP adresu, profiler zařízení porovná dostupné informace o zařízení s pravidly profilování zařízení.
6. Shoda je určena kombinací typu zařízení a jedné nebo více metod detekce zařízení. Pokud je například vybraným typem zařízení Mobilní zařízení a vybranou metodou je DHCP fingerprinting, pak by toto pravidlo odpovídalo zařízení se systémem Windows

CE. DHCP fingerprintining by určil, že zařízení používá Windows CE, což je operační systém, který odpovídá mobilnímu zařízení. Metody identifikace založené na fingerprinting používají databázi na FortiNAC, kterou uživatel nemůže upravit.

7. Pokud je povolena funkce Upozornit sponzora, FortiNAC nebo řídicí server odešle e-mail všem správcům zařízení, kteří mají oprávnění pro zařízení spojená s tímto pravidlem.
8. Zařízení je přiřazen typ zařízení obsažený v pravidle. Pokud to však není pravidlo Catch All, které nemá žádný typ.
9. Zařízení je přiřazena role obsažená v pravidle. Pokud není vybrána žádná role, je zařízení přiřazena výchozí NAC role.
10. Zařízení lze registrovat automaticky nebo ručně. Pokud je pravidlo nastaveno na ruční registraci, musí se v menu Profiled Devices zaregistrovat.
11. Pokud je v pravidle povoleno Zaregistrovat jako, lze zařízení umístit do zobrazení Host View, nebo do Inventory, nebo do obou.
12. Pokud je zvoleno Host View, může být zařízení přidáno do konkrétní skupiny uvedené v Host View.
13. Pokud je zvoleno Inventory, zařízení se přidá do kontejneru určeného uživatelem.
14. Pokud byla možnost přístupu nastavena na omezený čas, je přístup k síti u zařízení umístěných v Host View omezen na nakonfigurované časy. Aby zařízení nemohla přistupovat k síti mimo nakonfigurovaný časový rámec, jsou označena jako „At Risk“ pro hosta bez přístupu.
15. Pokud zařízení prošlo celým procesem a bylo zaregistrováno automaticky nebo ručně, již se nebude zobrazovat jako rogue.
16. Pokud zařízení neodpovídá žádnému pravidlu, je přidruženo k výchozímu pravidlu Catch All. V závislosti na nastavení nakonfigurovaném v rámci tohoto pravidla může být zařízení přidruženo k pravidlu, ale stále zůstává jako rogue.
17. Zařízení, která jsou registrována a přidružena k uživateli, jsou umístěna do zobrazení Host View a odebrána z okna Profiled Devices. Zařízení, která jsou umístěna pouze v Inventory, jsou odebrána z profilovaných zařízení. Všechna ostatní zařízení zpracovaná profilem zařízení zůstávají v okně Profiled Devices a v zobrazení Host View.

4.1.2.1.2 Monitor zařízení

FortiNAC poskytuje visibilitu do sítě. Umožňuje zaregistrovat známá zařízení, izolovat neznámá zařízení a zjistit, kde jsou zařízení připojena k síti. Zařízení lze spravovat nebo ovládat na základě rolí zařízení.

Zobrazit a zaregistrovat známá zařízení lze provést několika způsoby. Je vhodné však začít s přepínači, směrovači a řadiči, protože tato zařízení ovládají síť a poskytují FortiNAC informace o dalších zařízeních připojených k síti. Způsoby registrace zařízení:

- **Import zařízení** – CSV soubory obsahující informace o zařízení, lze je využít k importu zařízení do FortiNAC. Každý typ zařízení musí být v samostatném souboru. Lze importovat SNMP zařízení i zařízení, která nejsou dostupná přes SNMP (nebo pingovatelná).
- **Discovery** – automatizovaný proces spuštěný správcem FortiNAC. FortiNAC prohledává rozsahy IP adres zařízení, která lze spravovat pomocí protokolu SNMP. Jak je objeveno a ve FortiNACu je vytvořen model každého zařízení, lze jej zobrazit v pohledu Network Devices. Každé zařízení pak musí být nakonfigurováno, aby bylo zajištěno, že FortiNAC má správná hesla do CLI a konfigurace VLAN.

- **Registrace non-SNMP zařízení** – zařízení, která nelze spravovat pomocí protokolu SNMP, jako jsou tiskárny, bezpečnostní kamery nebo poplašné systémy. Tento typ zařízení se označuje jako pingovatelné zařízení. Zařízení, která nejsou SNMP, lze importovat do databáze, jak je uvedeno výše, lze je zaregistrovat ručně nebo je lze automaticky zaregistrovat pomocí Device profiler.
- **Registrace PC** – PC jako zařízení lze provést ručně připojením PC k síti. Když FortiNAC detekuje připojení, počítač se zobrazí v Host View jako rogue. Lze poté vybrat jedno nebo více PC a zaregistrovat je jako zařízení, jak je uvedeno výše.

Registraci PC lze do určité míry automatizovat. Vyžaduje to instalaci agenta na PC. Persistent Agent lze poté nakonfigurovat tak, aby registroval počítače podle hostname. Agent se připojí k serveru FortiNAC, zaregistruje počítač podle názvu hostitele a odešle informace jako je IP adresa a MAC adresa, zpět do databáze. Protože agent se používá pouze jako mechanismus registrace počítačů, není vyžadována žádná bezpečnostní politika.

Když se jakékoli zařízení připojí k síti, FortiNAC zkontroluje, zda je zaregistrováno nebo ne. Registrovaným zařízením je povolen přístup do produkční sítě. Neregistrovaná, nebo neznámá zařízení jsou umístěna v izolační VLAN.

4.1.2.1.3 Integrace s FortiSwitch

FortiNAC se naučí kde jsou koncové body připojeny na základě následujících metod:

- SNMP Link State trap odeslaný přepínačem
- Syslog zprávou o přidání/odebrání MAC adresy
- RADIUS komunikací
- L2 Polling – získáním MAC adres z CAM tabulky přepínače
- L3 Polling – získáním ARP cache ze směrovače

FortiSwitche ve FortiLink módu jsou řízeny pomocí FortiGate. FortiNAC poskytuje viditelnost v síti (kde se koncové body připojují) a spravuje přiřazení patřičné VLANy pro koncové body. Toho je dosaženo odesláním příslušného konfiguračního příkazu do zařízení. Když FortiNAC provede jakékoli změny ve FortiGate nebo FortiSwitchi, Fortigate/FortiSwitch následně aktualizuje FortiManager, který je díky tomu synchronizován.

4.1.2.1.4 Integrace Fortinet Security Fabric

Fortinet Single Sign-On (FSSO) je protokol pro transparentní autentikaci uživatele na FortiGate. FortiNAC vystupuje v roli Collector Agent, který získává informace o připojení uživatele do sítě PLA. Tyto informace poté přes TCP port 8000 zasílá na FortiGate. Tyto události obsahují:

- Device Information: IP adresu
- User information: User ID nebo MAC adresu (pokud není User ID)
- User Group Filter: FortiNAC User Group, Host Group nebo Firewall Tag

Když online zaregistrované zařízení vyhoví nakonfigurované politice FortiNAC Network Access Policy tak, FortiNAC odešle FortiGate jednu z následujících možností:

- Firewall Tag
- User nebo Administrator Group
- Host Group

FortiGate použije tyto informace k uplatnění příslušných IPv4 politik na zařízení. Host status

má přednost před nakonfigurovanou politikou. FortiNAC například nepoužije politku pro přístup k síti, pokud je zaregistrované zařízení označeno jako ohrožené, ale zařízení označené jako At-Risk přesune do VLAN definované jako „Karanténa“ s omezeným přístupem do sítě PLA.

4.1.2.1.5 Integrace SD-WAN

FortiNAC poskytuje nejen kontrolu souladu a kontrolu přístupu, ale také poskytuje komplexní viditelnost připojených zařízení. FortiGate v koncových lokalitách ve WAN síti PLA můžou získat tyto informace z FortiNAC pomocí metody Fortinet SSO a používat je v těchto třech hlavních oblastech:

- Firewall politiky, které umožňují určitým zařízením komunikovat pouze k zamýšleným cílům, jako je např. IP kamera, která může komunikovat pouze s DNS serverem a serverem s řízením IP kamery.
- QoS politiky k definování různých zařízení ve stejné podsíti které získají požadované QoS bez ohledu na jejich IP adresy. Zařízení PoS a PC s Windows mohou být ve stejné podsíti, ale mohou vyžadovat různé QoS politiky.
- SD-WAN, kdy lze používat různé politiky pro různá zařízení na základě jejich značky nebo typu zařízení identifikovaného pomocí FortiNAC a řídit provoz přes některu z linek vybudované SD-WAN sítě PLA.

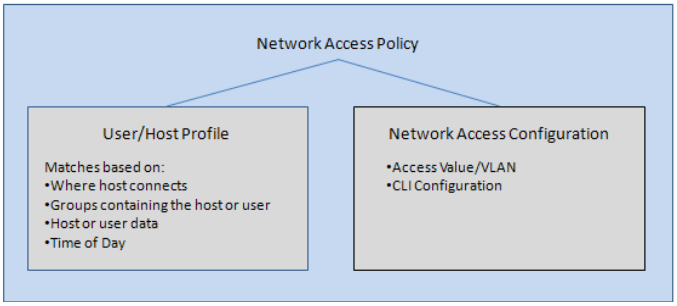
4.1.2.1.6 Profily uživatelů

Profily uživatelů/hostů se používají k mapování sad hostů a uživatelů na politiky přístupu k síti, zásady dodržování koncových bodů, Supplicant EasyConnect politiky, pravidla portálu nebo pravidla zabezpečení. Stejné profily lze znovu použít v mnoha různých politikách.
Profily uživatelů/hostů jsou kombinací údajů uživatel/host. Profil hosta nebo uživatele není pevný, ale může se změnit na základě přesunutí uživatele do jiné skupiny, použití nového atributu, připojení k síti na jiném místě nebo aktuální denní doby. Uživatelé/hosté jsou klasifikováni pouze v době, kdy potřebují službu, například politiku pro přístup k síti. Když FortiNAC vyhodnotí připojení, jsou data pro uživatele a hosta upřednostněna následovně:

- Přihlášený uživatel a host
- Registrovaný uživatel a host
- Registrovaný host

4.1.2.1.7 Network access policies

Politiky přístupu k síti se skládají z profilu uživatele a konfigurace přístupu k síti. Profil uživatele/host se používá k určení uživatelů a hostů, na které se tato politika může vztahovat. Konfigurace přístupu k síti přiřazuje zacházení, které uživatelé a hosté obdrží při připojení k síti.



Obrázek 26 - FortiNAC Network Access Policy

Veškerá zařízení přistupující k síti PLA budou identifikována, profilována a na základě znalosti zařízení budou zavedeny a prosazovány politiky, které omezí přístup k síti pouze na to, co je pro dané zařízení požadováno, dle zadané komunikační matice uvedené v příloze tohoto projektu PLA-WAN-komunikacni-matice.xlsx.

Více informací a kompletní administrační průvodce je volně dostupný na stránkách výrobce, viz.: https://docs.fortinet.com/document/fortinac/9.1.0/administration-guide/659283/fortinac.

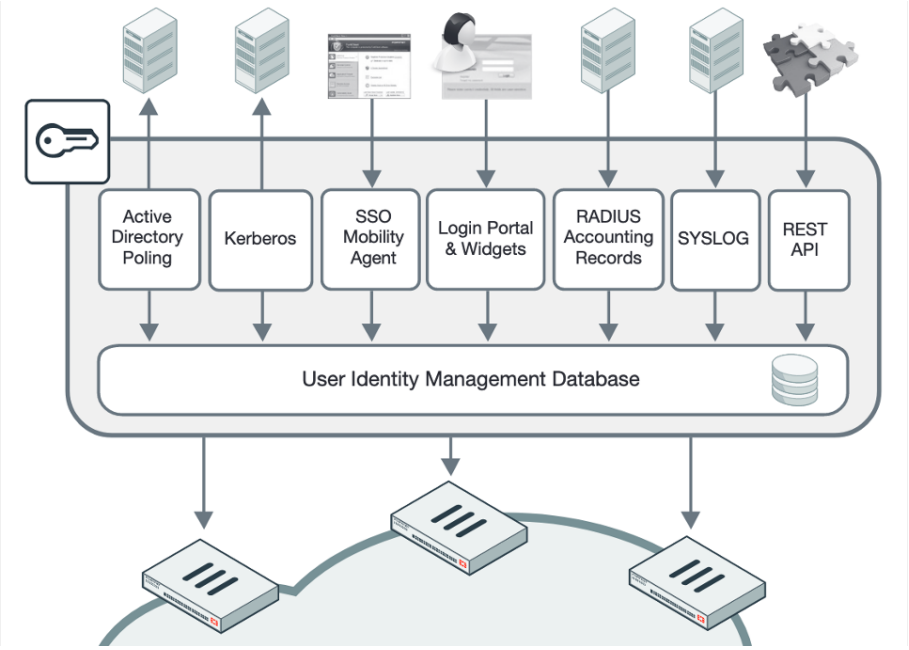
4.1.2.2 FortiAuthenticator

Do virtuálního prostředí PLA bude nainstalována centrální autentizační konzole FortiAuthenticator, která umožní centralizovanou správu pro řízení přístupu k síti v centrální lokalitě a také koncových lokalit sítě PLA. FortiAuthenticator bude zalicencován na celkový počet on-line uživatelů v síti PLA. V době vzniku tohoto projektu je počítáno s licencí pro 1100 uživatelů.
FortiAuthenticator poskytuje služby identity uživatelů nejen pro produktovou řadu Fortinet, ale i pro zařízení třetích stran. FortiAuthenticator poskytuje několik funkcí, včetně:

- Ověřování – FortiAuthenticator zahrnuje podporu standardního protokolu RADIUS, metody ověřování serveru pomocí protokolu LDAP (Lightweight Directory Access Protocol) a SAML (Security Assertion Markup Language), který se používá k výměně údajů o ověřování a autorizaci mezi poskytovatelem identity (IDP) a poskytovatel služeb (SP).
- Dvoufaktorové ověřování – FortiAuthenticator může fungovat jako dvoufaktorový ověřovací server s podporou jednorázových hesel (OTP) pomocí FortiToken Hardware, FortiToken Mobile, SMS (Short Message Service) nebo e-mailu. Dvoufaktorové ověřování FortiAuthenticator je kompatibilní s jakýmkoli systémem, který podporuje RADIUS.
- Podpora IEEE802.1x – FortiAuthenticator podporuje standard 802.1X pro použití v bezdrátových a kabelových sítích FortiGate.
- Identifikace uživatele – FortiAuthenticator může identifikovat uživatele prostřednictvím více zdrojů dat, včetně služby Active Directory (AD), klientského počítače, přihlášení k portálu pro hosty, RADIUS accounting, Kerberos a rozhraní REST API.
- Správa certifikátů – FortiAuthenticator může vytvářet a podepisovat digitální certifikáty pro použití například ve FortiGate VPN a úložiště certifikátů USB FortiToken 300.

- Integrace – FortiAuthenticator se může integrovat s ověřovacími systémy RADIUS, LDAP a SAML jiných výrobců, což umožní znovu použít stávající zdroje informací. Rozhraní REST API lze také použít k integraci s externími provision systémy.

Dostupné metody identifikace uživatele jsou naznačeny na následujícím obrázku:



Obrázek 27 - FortiAuthenticator User Identity

4.1.2.2.1 Identifikace uživatele

FortiAuthenticator může identifikovat uživatele prostřednictvím více zdrojů dat, včetně služby Active Directory (AD), klientského počítače, přihlášení k portálu pro hosty, RADIUS accounting, Kerberos a rozhraní REST API.

Uživatelská databáze FortiAuthenticator má tu výhodu, že může s každým uživatelem spojovat rozsáhlé informace, jak je očekávané od serverů RADIUS a LDAP. Tyto informace zahrnují, zda je uživatel administrátorem, používá ověření RADIUS nebo používá dvoufaktorové ověření, a zahrnují osobní informace, jako je celé jméno, adresa, možnosti obnovení hesla a skupiny, ke kterým uživatel patří.

FortiAuthenticator podporuje získání uživatelské identity z následujících externích zdrojů:

- **LDAP** – Vzdálení uživatelé LDAP mohou být importováni do databáze uživatelů FortiAuthenticator z LDAP serverů, zahrnující službu Microsoft Active Directory (AD). Podobně jako u lokálních uživatelů lze pak u uživatelů přiřadit token pro dvoufaktorové ověření.
- **RADIUS** – Vzdálené uživatele protokolu RADIUS lze vytvářet, migrovat na uživatele LDAP, upravovat a mazat. Některé služby mohou přijímat informace o ověřeném uživateli prostřednictvím vendor RADIUS specifických atributů. Skupiny uživatelů a uživatelské účty FortiAuthenticator pak mohou zahrnovat atributy RADIUS pro Fortinet a další dodavatele.

  Atributy ve skupinách uživatelů mohou specifikovat obecnější informace vztahující se na celou skupinu. Například zadání atributů dodavatele jiného výrobce do přepínače

může umožnit přihlášení na úrovni správy všem členům skupiny Network Admins nebo autorizovat uživatele na správnou úroveň oprávnění v systému.

- **SAML** – Vzdálení uživatelé z externího systému typu SAML (Security Assertion Markup Language).

FortiAuthenticator bude integrován na stávající doménové řadiče v doméně PLA.CZ pomocí vzdáleného LDAP serveru a pomocí protokolu RADIUS na další požadované bezpečnostní řešení implementované ve 2. a 3. etapě tohoto projektu.
FortiAuthenticator bude poskytovat centralizované autentizační služby, včetně jednotného přihlášení (SSO). FortiAuthenticator také bude poskytovat portálovou službu pro hosty přistupující k drátové i bezdrátové síti PLA jak v centrální lokalitě, tak i v koncových lokalitách WAN sítě PLA.

4.1.2.3 Bezdrátová síť

V této etapě lze také vybudovat bezdrátovou síť jak v centrální lokalitě, tak i v koncových lokalitách WAN sítě PLA. Jednotlivé přístupové body bezdrátové sítě budou do Fortinet Security Fabric integrovány pomocí FortiLink, jak je uvedeno v kapitole 3.2.3.

4.1.2.3.1 FortiManager AP Manager

Centrální management konzole FortiManager umožňuje spravovat přístupové body FortiAP, které jsou ovládány zařízeními FortiGate a jsou spravovány FortiManagerem. AP Manager lze použít pro následující režimy správy:

- Centrální správa spravovaných přístupových bodů – lze prohlížet, vytvářet, upravovat a importovat profily. Profily WiFi sdílejí společnou databázi. Profily se použijí na jakékoli zařízení bez ohledu na to, ke kterému kontroleru FortiGate je přístupový bod připojen.
- Per-device management řízených přístupových bodů – lze změnit nastavení pro každý spravovaný přístupový bod. Všechna zařízení FortiAP a profily WiFi jsou spravovány na úrovni zařízení bez sdílených objektů.

V centrální lokalitě i koncových lokalitách sítě PLA předpokládáme použití centrální správy FortiAP, což umožní vytvořit jednotné prostředí bezdrátové sítě napříč lokalitami sítě PLA.

	#	Access Point	Connected Via	SSIDs	Channel	Clients	OS Version	AP Profile
☐	1	FP320B3X00000000	192.168.100.116	Radio 1: Radio 2:	Radio 1: 0 Radio 2: 0	Radio 1:2 Radio 2:2	FP320B-v5.4-build0371	
☐	2	FP320B3X00000000		Radio 1: Radio 2:	Radio 1: 0 Radio 2: 0	Radio 1:0 Radio 2:0		
☐	3	FP320C3X00000000	192.168.100.112	Radio 1: Radio 2:	Radio 1: 6 Radio 2: 132	Radio 1:1 Radio 2:0	FP320C-v5.6-build0476	
☐	4	FP320C3X00000000	192.168.100.111	Radio 1: Radio 2:	Radio 1: 6 Radio 2: 136	Radio 1:0 Radio 2:2	FP320C-v5.6-build0476	
☐	6	PS223E3X00000000	192.168.1.122	Radio 1: Radio 2:	Radio 1: 6 Radio 2: 36	Radio 1:0 Radio 2:0	PS223E-v5.4-build4137	
☐	7	PS311C3U00000000	192.168.1.123	Radio 1: Radio 2:	Radio 1: 165 Radio 2: 0	Radio 1:2 Radio 2:0	PS311C-v5.4-build0155	
☐	5	PU421E3X00000000	192.168.100.113	Radio 1: Radio 2:	Radio 1: 0 Radio 2: 0	Radio 1:0 Radio 2:0	PU421E-v5.4-build0035	

Obrázek 28 - FortiManager AP Manager

Přesný počet a umístění jednotlivých přístupových bodů v centrální lokalitě a koncových lokalit sítě PLA není v tomto projektu stanoven. Doporučujeme zpracovat pro toto řešení samostatný projekt, který by vycházel za stavu implementace Security Fabric popisované tímto projektem.

Zejména se jedná o skutečné požadavky na pokrytí signálem bezdrátové sítě, ze kterého by se dal určit počet a umístění.

4.1.3 Realizace projektu – etapa 3

V další etapě projektu bude zavedeno řízení přístupu ke koncovému bodu prostřednictvím integrované viditelnosti, kontroly a proaktivní ochrany Fortinet Zero Trust Network Access (ZTNA), jak uvedeno v kapitole 3.1.1.2.

FortiClient agent funguje jako agent ZTNA, bude nainstalován na koncová zařízení v síti PLA a bude poskytovat nepřetržitá telemetrická data zabezpečení koncových bodů, včetně zranitelností operačního systému zařízení a aplikací. V závislosti na expiraci podpory stávajícího řešení antivirové ochrany stanic a serverů v síti PLA může být FortiClient agent použit jako adekvátní náhrada tohoto řešení.

FortiClient Enterprise Management Server (EMS) bude nainstalován do virtuálního prostředí PLA. Tato centrální konzole bude nedílnou součástí při konfiguraci a správě řešení ZTNA.

4.1.4 Další rozvoj Fortinet Security Fabric

Jak je uvedeno výše, stávající firewall [redacted] je limitujícím faktorem pro další rozvoj zabezpečení sítě PLA. Vybudování plně redundantní infrastruktury datového centra sítě PLA vyžaduje nahrazení [redacted] za nové bezpečnostní prvky Fortinet zapojené v režimu vysoké dostupnosti v serverovnách A a B.

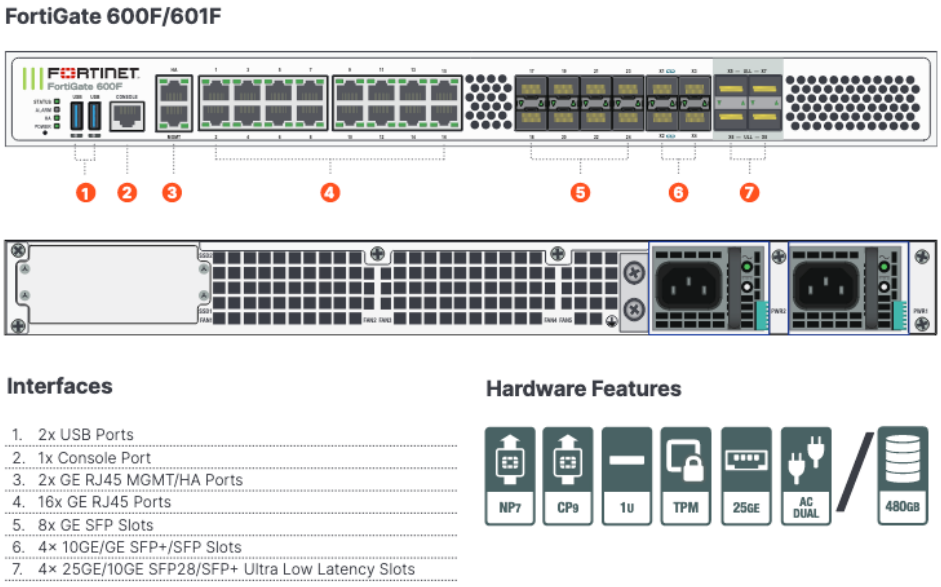
4.1.4.1 FortiGate 600F

Řada FortiGate 600F poskytuje vysoce výkonné funkce firewallu nové generace (NGFW) pro velké podniky a poskytovatele služeb. S vysokorychlostními rozhraními, vysokou hustotou portů a vysokou propustností jsou ideální pro nasazení na perimetr sítě, v jádru hybridního datového centra a také napříč interními segmenty. Využívá nejnovější SPU NP7 network procesor, špičkové IPS, kontrolu SSL a pokročilou ochranu před hrozbami k optimalizaci výkonu sítě.

Klíčové parametry navrhované řady FortiGate jsou tyto:

Firewall	IPS	NGFW	Threat Protection	Interfaces
139 Gbps	14 Gbps	11,5 Gbps	10,5 Gbps	16x 1GE RJ45, 8x 1GE SFP, 4x 10GE SFP+, 4x 25GE SFP28

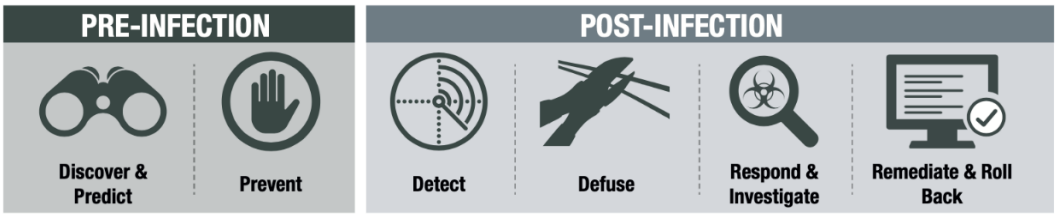
Tabulka 19 - FortiGate 600F



Obrázek 29 - FortiGate 600F

4.1.4.2 *Endpoint Detection & Response (EDR)*

FortiEDR poskytuje pokročilou ochranu před hrozbami v reálném čase před i po infekci. FortiEDR využívá architekturu Fortinet Security Fabric a integruje se s mnoha komponentami Security Fabric včetně FortiGate, FortiNAC, FortiSandbox a FortiSIEM. Řešení pro zabezpečení koncových bodů je postavené od základu k detekci pokročilých hrozeb a zastavení narušení a poškození ransomwarem v reálném čase i na již kompromitovaném zařízení, což umožňuje automaticky reagovat a napravovat incidenty k ochraně dat, včetně zajištění provozuschopnosti systému a zachování kontinuity.



Obrázek 30 - FortiEDR funkce

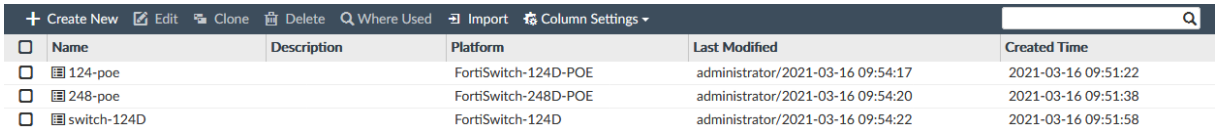
4.2 Koncové lokality

V době vzniku tohoto projektu jsou ve výše uvedených koncových lokalitách WAN sítě PLA instalovány firewally FortiGate, jako součást SD-WAN technologie. Jde vesměs o FortiGate řady FG40F, FG60F a FG80F které podporují veškeré uvedené funkce Fortinet Security Fabric.

4.2.1 Realizace projektu – etapa 1

V první etapě realizace projektu pro koncové lokality budou nahrazeny dosluhující přepínače v jednotlivých lokalitách. Navrhované přepínače dle tabulky č. 18 - Přístupové přepínače, budou k jednotlivým nainstalovaným FortiGate v SD-WAN připojeny pomocí FortiLink a integrovány do Fortinet Security Fabric tak, jak je popsáno v kapitole 3.3 - Koncové lokality.

Pro centralizovanou správu přepínačů a FortiGate bude použit FortiManager, viz. kapitola 4.1.1.2 – FortiManager.
Pro identické lokality jako jsou např. jezy bude možné použít správu přepínačů v režimu centrálního managementu. Budou vytvořeny FortiSwitch Template, které budou obsahovat definice VLAN, bezpečnostní profily, profily LLDP a QoS politiky. Tyto template jsou pak přiřazeny k jednotlivým spravovaným typům přepínačů.



Obrázek 31 - FortiSwitch Template

V lokalitách, kde je požadováno specifikovat vlastní pravidla, nebo přiřazení jednotlivých portů přepínače k těmto pravidlům bude použita správa přepínačů v režimu per-device správy.

4.2.1.1 Komunikační matice

Prostupy mezi jednotlivými segmenty LAN sítě v koncových lokalitách sítě PLA budou definovány pomocí centrální management konzole FortiManager a distribuovány do jednotlivých FortiGate, instalovaných v rámci vybudování SD-WAN sítě PLA, dle komunikační matice uvedené v příloze tohoto projektu PLA-WAN-komunikacni-matice.xlsx.
V době vzniku tohoto projektu nejsou zřejmé vazby potřebných prostupů na úroveň TCP/UDP portů, zejména pro technologickou část sítě. Bez profilování připojovaných zařízení pomocí FortiNAC a proaktivní ochrany Fortinet Zero Trust Network Access tak budou pravidla definována na základě IP adresy a v případě uživatele a zařízení připojeného do Microsoft domény také na základě znalosti přihlášeného uživatele do domény PLA.CZ pomocí Fortinet SSO tak, jak je již v síti PLA implementováno.
Součástí standardní licence FortiCare jsou signatury Application Control, Device & OS Identification a definice Internet Service Database. Tyto bezpečnostní definice pak lze použít pro požadované politiky.

4.2.1.2 Monitoring provozu sítě v koncových lokalitách

Všechny zařízení FortiGate v koncových lokalitách budou v rámci Fortinet Security Fabric integrovány s již nainstalovaným centrálním logovacím nástrojem FortiAnalyzer. Ve všech firewallových politikách bude zapnuto logování provozu a logy automaticky v reálném čase odesílány na tento nástroj.

4.2.1.2.1 One-arm sniffer

FortiGate umožňuje použít fyzické rozhraní jako systém detekce narušení (IDS). Provoz odeslaný na toto rozhraní je zkoumán na shodu s nakonfigurovaným profilem zabezpečení, potencionální hrozby se zaprotokolují a poté se zruší veškerý přijatý provoz.
One-arm sniffer lze také použít v konfiguraci FortiGate tak, aby fungoval jako zařízení IDS bez skutečného zpracování paketů. Fyzické rozhraní v režimu sniffer je připojeno k portu SPAN přepínače nebo vyhrazené síťové kartě, která může replikovat provoz na FortiGate.
Pro plnohodnotné využití IDS systému je nutné použít profily s bezpečnostními definicemi Antiviru, Aplikační kontroly, WebFilteru a IPS. Tyto definice vyžadují mít platnou licenci pro tyto služby na FortiGate v koncové lokalitě a být připojen k FortiGuard Distribution Network (FDN), nebo k FortiManageru v roli built-in FDS.

Provoz skenovaný na rozhraní One-arm sniffer je zpracováván v CPU, i když je na FortiGate k dispozici hardware SPU (NPU nebo CP). Může tak způsobit vyšší využití procesoru a pracovat na nižší úrovni než tradiční inline skenování, které používá NTurbo nebo CP k urychlení provozu, které je k dispozici na FortiGate. Z tohoto důvodu doporučujeme využít tuto funkcionalitu pouze v nejnutnějším případě a pouze po nezbytně dlouhou dobu. V dalších etapách realizace projektu je řízení a monitoring provozu v koncových lokalitách vyřešen na úrovni znalosti a chování jednotlivého koncového bodu, včetně zařízení typu IoT.

4.2.2 Realizace projektu – etapa 2 a 3

V těchto etapách bude zavedeno řízení přístupu k síti pomocí FortiNAC a řízení přístupu ke koncovému bodu prostřednictvím integrované viditelnosti, kontroly a proaktivní ochrany Fortinet Zero Trust Network Access (ZTNA). Realizace je stejná pro centrální i koncové lokality.

5. Doporučené zaškolení správců

Fortinet NSE Training Institute poskytuje certifikaci a školení v rostoucí oblasti kybernetické bezpečnosti. Program zahrnuje širokou škálu samoobslužných školení, vedených instruktorem a praktických cvičení, která prokazují zvládnutí komplexních konceptů zabezpečení sítě. Z nabízené škály školení doporučujeme účast požadovaného počtu administrátorů na těchto školeních:

Název	**Rozsah (MD)**	**Forma**	**Popis**
FortiGate Security	3	Self-paced online Instructor-led	Základní funkce FortiGate, včetně bezpečnostních profilů
FortiGate Infrastructure	2	Self-paced online Instructor-led	Jak používat pokročilé sítě a zabezpečení FortiGate
FortiManager	2	Self-paced online Instructor-led	Základy používání FortiManageru pro centralizovanou správu sítě mnoha zařízení FortiGate
FortiAnalyzer	1	Self-paced online Instructor-led	Základy používání FortiAnalyzer pro centralizované protokolování a reportování
FortiClient EMS	1	Self-paced online Instructor-led	Jak používat FortiClient a spravovat FortiClient pomocí FortiClient EMS
Secure Wireless LAN	1	Self-paced online Instructor-led	Jak nasadit, konfigurovat a řešit problémy se zabezpečenou bezdrátovou sítí LAN pomocí integrovaného bezdrátového řešení zahrnující FortiGate, FortiAP, FortiWiFi, FortiAP Cloud, FortiPlanner a FortiPresence
FortiAuthenticator	2	Self-paced online Instructor-led	Jak konfigurovat a nasadit FortiAutheticator, používat FortiAuthenticator pro správu certifikátů a dvoufaktorovou autentizaci, ověřovat uživatele pomocí serverů LDAP a RADIUS a SAML SSO a jak může FortiAuthenticator fungovat jako poskytovatel identity a poskytovatel služeb SAML
FortiNAC	3	Self-paced online Instructor-led	Jak využít výkonné a rozmanité schopnosti FortiNAC pomocí osvědčených postupů pro dosažení viditelnosti, kontroly a reakce
FortiEDR	2	Self-paced online Instructor-led	Jak používat FortiEDR k ochraně koncových bodů proti pokročilým útokům pomocí funkce reakce na incidenty v reálném čase
Secure Access	3	Self-paced online	Jak FortiGate, FortiAP, FortiSwitch a FortiAuthenticator umožňují

		Instructor-led	zabezpečené připojení přes drátové a bezdrátové sítě, jak udržet síť zabezpečenou využitím integrace Fortinet Security Fabric mezi FortiGate, FortiSwitch, FortiAP a FortiAnalyzer k automatické karanténě rizikových a kompromitovaných zařízení pomocí spouštěčů IOC
Enterprise Firewall	3	Self-paced online Instructor-led	Jak implementovat, řešit problémy a centrálně spravovat infrastrukturu podnikového zabezpečení složenou z více zařízení FortiGate

Tabulka 20 - Školení NSE Institute

Odhadovaná náročnost na správu navrženého řešení záleží, které všechny etapy (technologie), navržené v tomto projektu bude v konečném důsledku realizovány.
V případě, že budou realizovány všechny níže zmíněné technologie:
Fortigate Firewall Security a infrastructure, Fortimanager, Fortianalyzer, FortiClient EMS, FortiAuthenticator, FortiNAC a FortiEDR. Je nutné počítat pro ŘSP (generální ředitelství) s orientační časovou náročností 252h na kalendářní měsíc. Pro závod je nutné počítat s orientační časovou náročností 8h tzn. 32h celkem na kalendářní měsíc (celkem 4 závody v organizaci). Pro lokalitu je nutné počítat s orientační časovou náročností 2h tzn. celkem 112h na kalendářní měsíc (celkem 56 lokalit v organizaci).
Z výše uvedeného vychází celková časová náročnost na 2,4 pracovníka na 1 měsíc (za předpokladu jeho 100% pracovní utilizace (168h pracovních hodin / 1 měsíc).

Variantně uvádíme i možnost, že bude realizován pouze FortiGate Firewall. V takovém případě činí orientační náročnost celkem 210h pro všechny organizační jednotky (1x ŘSP, 4x závod, 56x lokalita).
Z výše uvedeného vychází celková časová náročnost 1,5 pracovníka na 1 měsíc za předpokladu jeho 100% pracovní utilizace (168h pracovních hodin / 1 měsíc).

Doporučení reálného fyzického počtu správců s ohledem na počet lokalit a jejich rozptýlenost nelze definovat. Tento fakt vychází z personální politiky organizace – aktuální utilizace pracovníků IT, jejich pracovní náplně apod.

6. Parametry pro výběr HW a SW

Detailní parametry hardware, software pro vypsání výběrového řízení jsou přiloženy v samostatné příloze „PLA-WAN-Technicka-specifikace.xlsx“, která je nedílnou součástí tohoto dokumentu.