Síťová bezpečnost a řízení přístupu

Bc. Petr Liška

Diplomová práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Petr Liška**
Osobní číslo:	**A21485**
Studijní program:	**N1032A020003 Bezpečnostní technologie, systémy a management**
Specializace:	**Bezpečnostní technologie**
Forma studia:	**Kombinovaná**
Téma práce:	**Síťová bezpečnost a řízení přístupu**
Téma práce anglicky:	**Network Security and Access Control**

Zásady pro vypracování

1. Popište možné hrozby narušení síťové bezpečnosti a navrhněte vhodná opatření pro jejich mitigaci.
2. Identifikujte a popište opatření k zajištění síťové bezpečnosti v rámci systému řízení informační bezpečnosti (ISMS – Information Security Management Systém).
3. Porovnejte metody řízení přístupu k síťovým prostředkům a popište jejich výhody.
4. Navrhněte systém řízení síťového přístupu na základě identity uživatele.
5. Vytvořte korelační pravidla pro detekci pokusu o překonání navrženého systému řízení.
6. Vyhodnoťte navržené řešení.

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

Seznam doporučené literatury:

1. STALLINGS, William. Cryptography and network security: principles and practice. Seventh edition. Boston: Pearson, 2017. Global edition. ISBN 978-1-292-15858-7.
2. DIOGENES, Yuri a Erdal OZKAYA. Cybersecurity – Attack and Defense Strategies. Birmingham: Packt Publishing, 2018. ISBN 78-1-78847-529-7
3. STALLINGS, William a Lawrie BROWN. Computer Security: Principles and Practice. Fourth Edition. Upper Saddle River: Pearson Education, 2018. ISBN 978-0-13-479410-5
4. RAWAL, Bharat S., Gunasekaran MANOGARAN a Alexender PETER. Cybersecurity and Identity Access Management. Singapore: Springer Nature, 2022. ISBN 978-981-19-2657-0
5. KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-34-8

Vedoucí diplomové práce: **prof. Mgr. Roman Jašek, Ph.D., DBA**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **2. prosince 2022**
Termín odevzdání diplomové práce: **1. června 2023**

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

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 8. prosince 2022

Prohlašuji, že

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

Prohlašuji,

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

V Brně, dne 19. 5. 2023

Bc. Petr Liška v.r.
podpis studenta

ABSTRAKT

Práce se zabývá využitím identity uživatele v procesu řízení přístupu k síťovým prostředkům v rámci zajištění informační bezpečnosti. Práce zkoumá rizika narušení síťové bezpečnosti na jednotlivých vrstvách dle referenčního modelu ISO/OSI a navrhuje odpovídající opatření k jejich minimalizaci. V praktické části práce je navržen automatizovaný systém řízení přístupu k síťovým prostředkům vázaný na identitu uživatele, za využití řízení přístupu na základě rolí (RBAC – Role Based Access Control) systémem pro správu identit (IAM – identity and access management) a aplikace firewall politik na základě identit. V závěru práce jsou vytvořeny korelační pravidla v systému SIEM (Security Information and Event Management) pro detekci pokusu o překonání navrženého způsobu řízení přístupu.

Klíčová slova: síťová bezpečnost, řízení přístupu, správa identit, firewall politiky, IAM, IdM, RBAC, SIEM.

ABSTRACT

The thesis deals with the use of user identity in the process of network resource access control as part of the information security. The thesis analyses the risks of network security breaches at individual layers according to the ISO/OSI reference model and suggests appropriate mitigation measures. In the practical part of the thesis, an automated user identity-based network resource access control system is designed using Role Based Access Control (RBAC) by identity and access management (IAM) system and application of identity-based firewall policies. At the end of the thesis, correlation rules are created in the Security Information and Event Management (SIEM) system to detect an attempt to bypass the designed access control method.

Keywords: network security, access control, identity management, firewall policy, IAM, IdM, RBAC, SIEM.

Rád bych poděkoval vedoucímu mé diplomové práce prof. Mgr. Romanu Jaškovi, Ph.D., DBA za rady a čas, který mi věnoval, mému kolegovi Ing. Jiřímu Malečkovi za přínosné odborné připomínky, a především mé rodině za trpělivost a nepolevující podporu při studiu.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Již na startu svého profesionálního života, který započal v dobách ranného internetu v České republice, jsem byl vrhnut do problematiky počítačových sítí a dostal tak jedinečnou možnost sledovat vývoj v této oblasti. V těchto dobách (90. léta) si počítačové stanice v komerčních firmách vystačily s jedním nebo několika málo fyzickými servery v lokální síti a k internetu byl připojen analogovým modemem jeden z počítačů, u kterého se ze zvědavosti střídalo pár nadšenců. Bezpečnost počítačové sítě byla v lepším případě řešena jejím administrátorem a rozhodně to nebyla jeho nejdůležitější činnost. Následoval prudký rozvoj výpočetní a komunikační techniky (ICT), ruku v ruce s rozvojem internetu, a s každým dalším dosaženým milníkem stoupal význam síťové bezpečnosti v rámci kybernetické bezpečnosti jako celku. Dnes už snad ani neexistuje elektronické zařízení, které by nebylo nebo se nedalo připojit do některé z počítačových sítí, ať už kabelem, nebo čím dál častěji bezdrátově. Dalo by se přeneseně říct, že naše životy jsou z velké části odkázány na počítačové sítě a jejich kolaps by znamenal ohrožení lidské existence. V takové chvíli je zajištění bezpečnosti sítě kriticky důležitá disciplína, které je potřeba věnovat nemalé úsilí a prostředky.

Důležitou součástí síťové bezpečnosti je řízení přístupu k prostředkům, které síť poskytuje jejím uživatelům. Cílem této práce je navrhnout automatizovaný systém řízení přístupu k síťovým prostředkům, orientovaný na identitu uživatele a jeho pracovní charakteristiku. Součástí návrhu je i vytvoření korelačních pravidel v nástroji pro management bezpečnostních informací a událostí (SIEM) pro identifikaci pokusu o jeho překonání. Čtenář má být také seznámen s hlavními aspekty řízení přístupu, síťové bezpečnosti a ochraně proti jejímu narušení.

Motivací pro výběr zvoleného tématu diplomové práce mi byla snaha zužitkovat své mnoholeté zkušenosti z oblasti bezpečnosti sítí, které jsem získal jako specialista IT bezpečnosti ve finančních a pojišťovacích institucích a dříve jako systémový administrátor ve společnosti poskytující ICT služby. Informace uvedené v této práci by mohly najít uplatnění při návrhu obdobných systémů řízení přístupu a pomoci kolegům v oboru s jejich implementací.

V praktické části jsou se souhlasem manažera IT bezpečnosti použity anonymizované výstupy ze systémů, za jejichž správu spoluzodpovídám.

I. TEORETICKÁ ČÁST

1 ZÁKLADY SÍŤOVÉ BEZPEČNOSTI

Síťová bezpečnost je nedílnou a nepochybně významnou součástí informační bezpečnosti. Cílem následující kapitoly je popsat základní principy informační a síťové bezpečnosti a jednotlivé jejich aspekty z pohledu technických i organizačních opatření.

1.1 Bezpečnost informací

Úkolem informační bezpečnosti je ochrana informací z pohledu **důvěrnosti**, **integrity** a **dostupnosti** (viz kapitola *1.1.2 CIA triáda*), bez ohledu na jejich formu. Informace mohou být uloženy digitálně na datovém nosiči, ale mohou být přítomny i fyzicky, např. vytištěné na papíře. Informační bezpečnost je množina opatření, které jsou tvořeny technickými prostředky, procesy a lidmi. Jako podmnožinu můžeme vnímat kybernetickou bezpečnost, která je více zaměřena na ochranu informací v kyberprostoru a klade větší důraz na technické prostředky a opatření. Cíl jmenovaných bezpečností je však shodný a síťová bezpečnost je základním stavebním kamenem u obou. [1] [2]

1.1.1 Základní pojmy

Na úvod je třeba vymezit několik pojmů, které se budou vyskytovat v průběhu celé práce.

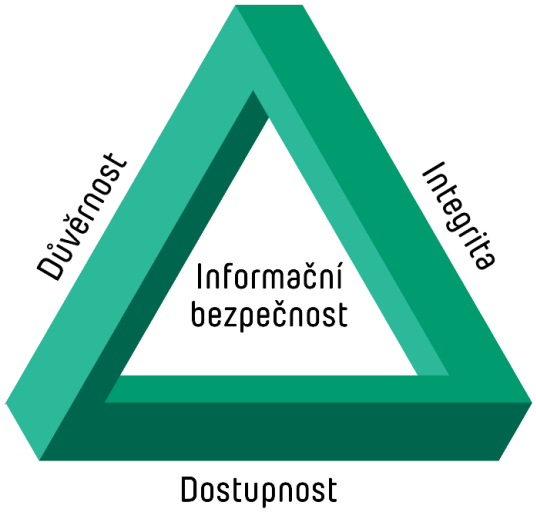
- **informace**: existuje mnoho definic pro tento výraz. Nejvýstižnější pro potřebu této práce a zároveň velice univerzální je: *„jsou údaje, které byly zpracovány do podoby užitečné pro příjemce“* [3],
- **kyberprostor**: dle zákona o kybernetické bezpečnosti, *„kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“* [4],
- **bezpečnost**: na bezpečnost můžeme nahlížet různými způsoby. Každý obor definuje bezpečnost dle vlastí potřeby. Pro **informační bezpečnost** je nejpříhodnější: *„Vlastnost prvku (např. informační systém), který je na určité úrovni chráněn proti ztrátám, nebo také stav ochrany (na určité úrovni) proti ztrátám.“* [5],
- **kybernetická bezpečnost**: v souvislosti s předchozími pojmy odpovídá definice Výkladového slovníku kybernetické bezpečnosti: *„souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.“* [5],
- **aktivum**: je *„vše, co má pro společnost jakoukoliv hodnotu a co je třeba chránit“* [1]. V případě síťové bezpečností jsou to všechny prvky sítě, připojené systémy

a zařízení (všechny hardwarové i softwarové komponenty, data a jejich úložiště, ale i procesy a lidská obsluha),

- **hrozba**: je jakákoliv událost, s potenciálem narušení důvěrnosti, integrity nebo dostupnosti aktiva,
- **zranitelnost**: je slabina aktiva, která může být zneužita hrozbou. [1]

1.1.2 CIA triáda

CIA je zkratkou pro anglické výrazy Confidentiality (důvěrnost), Integrity (integrita), a Availability (dostupnost) (Obr. 1). Jedná se o základní pilíře informační bezpečnosti, které jsou natolik významné, že kdykoliv dojde k nějaké bezpečnostní události, můžeme si být jisti narušením minimálně jednoho z nich. Úkolem pracovníků oddělení IT bezpečnosti je hodnocení hrozeb a zranitelností, působících negativně na aktiva organizace a implementace odpovídajících opatření k minimalizaci jejich dopadu na důvěrnost, integritu a dostupnost informací.



Obrázek 1. Základ informační bezpečnosti,
upraveno z: [6]

Význam uvedených tří pilířů informační bezpečnosti je následující:

- **důvěrnost**: každé aktivum musí být zabezpečeno tak, aby k němu měly přístup pouze oprávněné osoby. Ať už se jedná o informace nebo technologie, které je přenáší, zpracovávají a ukládají. Toho je docíleno např. řízením přístupu, klasifikací dat, šifrováním atp.,

- **integrita**: je třeba zajistit, aby aktivum bylo správné a autentické, aby nebylo nikým neoprávněně změněno a bylo spolehlivé. Pro zajištění integrity je využíváno především digitálního podpisu, šifrování, „hashování“ atd.,
- **dostupnost**: aby aktivum neztratilo svoji hodnotu, musí být dostupné vždy, když je to potřeba. Informace není užitečná, pokud k ní nemáme přístup. Jedná se tedy o zajištění spolehlivého provozu všech systémů. K tomu jsou využívána opatření pro zajištění vysoké dostupnosti, jako např. zdvojování technických zařízení, datových linek, systémy nepřerušovaného napájení atd. [6]

Často se setkáváme s názorem, že CIA triáda již není zcela dostačující a bývá doplněna dalšími principy. Příkladem je Parkerian hexad bezpečnostní model (Obr. 2), který doplňuje CIA triádu o další tři principy:

Obrázek 2. Parkerian Hexad model,
upraveno z: [7]

- **držení / kontrola** (Possession/Control): tento princip má zajistit udržení kontroly nad aktivem oprávněným držitelem. V případě převzetí kontroly neoprávněným subjektem se nemusí jednat o porušení principu důvěrnosti. Neoprávněný držitel sice ovládá aktivum, ale nijak jej nevyzrazuje. Obava před vyzrazením však existuje. Zamezení ztráty kontroly lze zabránit např. důsledným řízením přístupu,
- **autentičnost:** (Authenticity): označuje se také pojmy nepopiratelnost nebo neodmítnutelnost. Účelem je zajistit nepochybnost, že informace pochází ze zdroje, ze kterého pochází, byla vytvořena osobou, která tvrdí, že ji vytvořila, a nikoli

útočníkem. Autenticita zahrnuje důkaz totožnosti. K doložení autentičnosti je využíván např. digitální podpis nebo vícefaktorová autentizace,

- **užitečnost** (Utility): aktivum musí být nejen dostupné, ale i použitelné. Příkladem, kdy není princip užitečnosti dodržen, jsou zašifrovaná data, ke kterým byl ztracen dešifrovací klíč. I když jsou taková data v úložišti dostupná, nejsou nikomu užitečná. Zachování užitečnosti lze docílit např. procesními opatřeními. [8] [7]

1.2 Legislativa

V úvodu práce byl vyzdvihnut existenční význam informační bezpečnosti. Důležitosti ochrany ICT systémů a vlivu narušení jejich bezpečnosti jsou si samozřejmě vědomi i veřejní činitelé. V dnešní době existuje v naši národní i evropské legislativě mnoho zákonů a nařízení zaměřených na kybernetickou bezpečnost a ochranu informací. S vývojem a proměnou kyberprostoru je nutné reagovat na nové hrozby a legislativu průběžně aktualizovat a doplňovat. Následující kapitola shrnuje nejvýznamnější stávající i připravované normativy v našem společenském prostoru.

1.2.1 Zákon o kybernetické bezpečnosti a NIS

V roce 2000 vznikla v gesci Ministerstva vnitra ČR *Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření* [9] se zaměřením na potírání trestné činnosti v oblasti informačních technologií. V průběhu dalších let bylo představeno několik dalších konceptů, strategií a akčních plánů v oblasti informační a kybernetické bezpečnosti, což vyústilo dne 28. června 2013 k předložení návrhu zákona o kybernetické bezpečnosti Národním bezpečnostním úřadem (NBÚ), Vládě České republiky. *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [4] vstoupil v platnost dne 29. srpna 2014 s účinností od 1. ledna 2015 a to včetně prováděcích právních předpisů. V roce 2017 byl zákon o kybernetické bezpečnosti dvakrát novelizován, kdy zákonem č. 205/2017 Sb. byla implementována *Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii* (NIS) [10]. Na základě této novelizace byl rovněž zřízen Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), který po NBÚ převzal veškeré činnosti v oblasti kybernetické bezpečnosti a ochrany utajovaných informací

v oblasti ICT. Každým následujícím rokem proběhly další novelizace, přičemž aktuální znění zákona je účinné od 6. srpna 2022 (novelizace zákonem č. 226/2022 Sb.). [11] [12]

Zákon o kybernetické bezpečnosti si klade za cíl:

- nastavit opatření pro ochranu kritické informační infrastruktury a významných informačních systémů tak, aby byly ochráněny zájmy České republiky,
- zavést detekci kybernetických bezpečnostních událostí a hlášení incidentů,
- vytvořit systém pro zvládání kybernetických bezpečnostních incidentů,
- vymezit činnosti dohledových center. [12] [1]

1.2.2 Zákon o zpracování osobních údajů, GDPR a ePrivacy

Ochrana osobních údajů je úzce propojena s informační bezpečností, bez které by nemohl být naplněn její účel. Mezi lety 2000–2019 byl v české legislativě v platnosti *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů* [13], který implementoval *Směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů* [14]. Cílem zákona bylo zajistit ochranu osobních údajů fyzických osob, což je jedním ze základních práv daných Ústavou České republiky, zejména čl. 10, Listiny základních práv a svobod:

„(1) Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.

(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“ [15].

Zákon č. 101/2000 Sb. byl s účinností od dne 24. 04. 2019 plně nahrazen *Zákonem č. 110/2019 Sb., o zpracování osobních údajů* [16], který přejímá do české legislativy *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)* [17] (GDPR).

GDPR nepřinesl žádné převratné změny v oblasti ochrany osobních údajů. Cílem GDPR zůstává ochrana fyzických osob v souvislosti se zpracováním osobních údajů, avšak posiluje práva subjektu údajů a sjednocuje právní rámce ve všech zemích, pro které nařízení platí.

Upravuje některé povinnosti správců a zpracovatelů tak, aby byly přizpůsobeny dnešní době. Stanovuje sankce za porušení nařízení nebo např. zavádí statut pověřence pro ochranu osobních údajů (DPO) a povinnost vypracování posouzení vlivu na ochranu osobních údajů (DPIA). [18] [1]

V lednu 2017 začala Evropská komise připravovat návrh nařízení o soukromí a elektronických komunikacích – **ePrivacy Regulation**, které mělo doplnit obecné nařízení GDPR. ePrivacy rozšiřuje opatření na ochranu soukromí v elektronických komunikacích, vč. dat a metadat multimediálních souborů přenášených po internetu, má se vztahovat i na tzv. over-the-top (OTT) služby, které poskytují provozovatelé služeb typu Skype, WhatsApp nebo volání přes internet (VoIP) a které jsou provozovány nad službami tradičních poskytovatelů internetu. Evropská komise měla původně v plánu ePrivacy vydat v platnost současně s GDPR, ale vlivem četných připomínek je nařízení stále pouze ve formě návrhu a jeho přijetí je stále odkládáno. [19]

1.2.3 Nová směrnice EU o kybernetické bezpečnosti – NIS2

Od roku 2020 pracovala EU na návrhu nové směrnice – NIS2. Finální znění směrnice bylo dne 27. prosince 2022 zveřejněno v Úředním věstníku Evropské unie a vstoupilo v platnost dne 16. ledna 2023. Do 16. října 2024 by měla mít Česká republika ve svém právním řádu implementovány její požadavky. Původní směrnice NIS stanovovala některé oblasti pro zajištění kybernetické bezpečnosti pouze obecně. NIS2 rozšiřuje původní směrnici NIS jak z pohledu obsahového, tak i z pohledu účinnosti na nové odvětví:

- nejvýznamnější změnou je rozsah povinných osob, který se zvětší ze současných cca 400 na 6 000,
- nově směrnice dělí organizace a požadavky na ně podle jejich velikosti na dva režimy: „essential“ a „important“. Na organizace v režimu „essential“ se budou vztahovat přísnější požadavky,
- NIS2 stanovuje detailněji opatření, které musí povinné osoby zajistit k ošetření rizik a zabránění incidentům,
- směrnice více rozpracovává způsob hlášení incidentů pro CERT (Computer Emergency Response Team) a zavádí možnost dobrovolného hlášení pro nepovinné osoby. Hlášení by mělo být jednodušší, více automatizované a jednotnější v rámci každého členského státu,

- regulační úřady budou mít větší pravomoci v oblasti dohledu nad povinnými osobami, lepší možnosti vymáhat povinnosti a sankcionovat zjištěné nedostatky. Organizace v režimu „essential“ můžou obdržet pokutu až do výše 10 miliónů EUR nebo 2 % ze světového obratu,
- NIS2 také klade větší důraz na vzájemnou spolupráci, jak mezi jednotlivými regulovanými organizacemi, tak mezi regulačními úřady, a to na národní úrovni i v rámci EU. [20]

1.2.4 Nařízení o digitální provozní odolnosti – DORA

Dne 16.01.2023 vstoupilo v platnost *Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti pro finanční sektor* [21] (DORA), jimž se dotčené instituce musejí v praxi začít řídit do 24 měsíců od uvedeného data. Cílem nařízení je zavést pravidla zajišťující vyšší provozní odolnost ICT a normalizovat je napříč celým finančním sektorem v EU. Společná opatření by měla vést ke zmírnění kybernetických útoků a dalších rizik v dlouhodobém horizontu. Jedním z úkolů DORA je také zavedení rámce dohledu nad kritickými poskytovateli třetích stran, jako jsou poskytovatelé outsourcingu nebo cloudových služeb. [22]

1.3 Základní principy v informační bezpečnosti

Principy zde uvedené jsou obecnými zásadami, které se ustálily mezi odbornou veřejností při implementaci bezpečnostních mechanismů.

1.3.1 Princip nejnižších oprávnění

Každý uživatel nebo proces by měl mít pouze takovou sadou oprávnění, která je nezbytná k provedení svěřeného úkolu. Každé oprávnění povoluje přístup pouze k určitému prostředku, např. oprávnění k provedení určité operace v konkrétním systému. Pokud není oprávnění výslovně uděleno, uživatel nebo proces nesmí mít k chráněnému prostředku přístup. Pro zajištění tohoto principu je využíváno řízení přístupu na základě přidělených rolí (RBAC). Uživatel by měl mít přístup k prostředku pouze po dobu, kdy je to nezbytné. Např. administrátor systému s privilegovaným oprávněním by měl mít toto oprávnění pouze v případě potřeby, kdy systém spravuje. Při běžné činnosti by měl mít vysoká oprávnění odebrána. Pro časové přidělení privilegovaných oprávnění se využívá systému Privileged Access Management (PAM). [23]

1.3.2 Princip neslučitelnosti roli

Jde o techniku, při níž je provedení nějakého úkolu rozděleno na části, kde každá část vyžaduje specifické oprávnění. Např. jeden uživatel nemůže projít celým procesem od přidělení privilegovaného oprávnění pro danou operaci, až po její vykonání. Tato technika se používá ke zmírnění potenciálních škod způsobených útokem na bezpečnost ICT. [23]

1.3.3 Princip nesdílných přístupů

Všechny přístupy musejí být uděleny jmenovitě konkrétnímu uživateli nebo procesu. Skupinové, sdílené či generické účty, hesla nebo jiné autentizační metody, znemožňující identifikovat původce operace v systému, by neměly být použity. Každý uživatel a proces musí mít vlastní autentizační prvky, kterými lze jednoznačně identifikovat jeho přístup. [23]

1.3.4 Princip jednoduchosti a modularity

Při navrhování bezpečnostních opatření je třeba dbát na jednoduchost a minimalizaci. Složité a rozsáhlé návrhy zabezpečení jsou nepřehledné na údržbu, ověřování funkčnosti a testování zranitelností. Ve složitém mechanismu najde potenciální útočník daleko snadněji zranitelnost, která zůstala skryta před odhalením. Jednoduché mechanismy mají obecně méně zneužitelných chyb a jejich konfigurace, aktualizace nebo výměna je méně náročný proces. Návrh zabezpečení by měl také splňovat požadavek na modularitu. Pokud jsou v systému zabezpečení funkce využitelné pro více jeho částí, není dobré je implementovat odděleně v každé z nich. Je vhodnější vyvinout speciální modul, který bude funkci poskytovat všem částem systému. Při použití modulární architektury bezpečnostního systému, lze jednodušeji provádět upgrade nebo výměnu jeho jednotlivých částí. [23]

1.3.5 Princip explicitního povolení

Dle tohoto principu musejí být všechny přístupy do systémů ve výchozím stavu zakázány a povolují se pouze na základě přiděleného oprávnění. Princip explicitního povolení je méně náchylný na chybu. Pokud je někomu chybně zamezen přístup, přijde se na to ihned. V systému, kde je aplikován opačný princip, nemusí být chyba (nezakázaný přístup) odhalena nikdy. [23]

1.3.6 Princip úplného řízení přístupů

Dodržení principu úplného řízení přístupu vyžaduje, aby bylo oprávnění k přístupu ověřeno při každé operaci s kontrolovaným prostředkem. Běžně není tento princip, náročný na

prostředky, využíván. V praxi bývá oprávnění přístupu ověřeno vůči zprostředkovateli při začátku komunikace a nadále je udržováno v mezipaměti systému. Dobu uložení pověření v mezipaměti a způsob kontroly změny pověření je potřeba smysluplně nastavit. [23]

1.3.7 Princip psychologické přijatelnosti a přívětivost

Psychologická přijatelnost znamená, že bezpečnostní opatření by neměla nepřiměřeně zasahovat do práce uživatelů, bránit použitelnosti nebo znepřístupňovat zdroje. Zároveň však musí být zachována funkčnost opatření. Pokud není tento princip dodržen, uživatelé se mohou snažit tyto mechanismy obcházet nebo vypnout. Uživateli musejí bezpečnostní opatření dávat smysl a musejí být pro něj transparentní. [23]

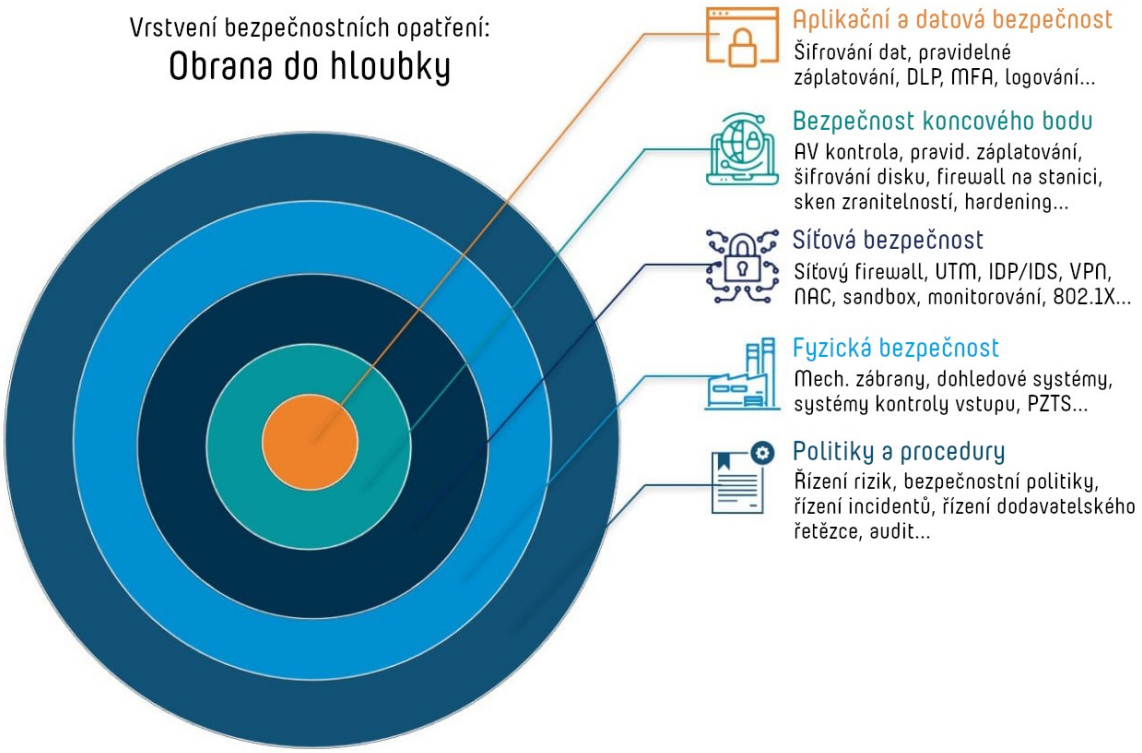
1.3.8 Princip izolace informačních prostředí

Princip izolace má tři kontexty:

- **oddělení kritických systémů od veřejných**: systémy poskytující kritické služby nebo citlivá data, musejí být fyzicky nebo logicky odděleny od systémů s veřejným přístupem, aby se zamezilo jejich kompromitaci. V případě logického oddělení je potřeba zvolit takový systém zabezpečení, aby nemohlo dojít k narušení bezpečnosti kritického systému,
- **oddělení dat uživatelů**: data nebo procesy uživatelů by měli být vzájemně odděleny, kromě případů, kdy je jejich sdílení vyžadováno,
- **oddělení přístupu k bezpečnostním mechanismům**: přístup k bezpečnostním systémům musí být omezen pouze na osoby oprávněné k jejich správě nebo procesy, které je využívají. [23]

1.3.9 Princip vrstvení bezpečnostních opatření

Pro zamezení selhání bezpečnostního mechanismu je využíváno principu vrstvení (Obr. 3). Pokud je ochrana vícevrstvá – jednotlivé bezpečnostní opatření se při ochraně prostředku překrývají a při selhání jedné z vrstev ochrany není bezpečnost systému narušena. Přístup založený na vrstvení, který mezi protivníka a chráněné aktivum staví více bariér, se často označuje jako obrana do hloubky. [23]



Obrázek 3. Vrstvení bezpečnostních opatření, upraveno z: [24]

1.4 Referenční model ISO/OSI

Návrh mechanismů pro zabezpečení sítě vyžaduje od bezpečnostního architekta komplexní znalosti ve více odvětvích ICT. Nezbytným předpokladem je úplná znalost principů fungování sítě – síťové architektury a souvisejících technologií. Řízení komunikace mezi systémy v síti je velice složitý proces, sestávající z mnoha navazujících úkonů. Pro efektivnější práci se sítěmi byl navržen komunikační model sestávající z jednotlivých vrstev. Každá z vrstev odpovídá určité činnosti při řízení komunikace, což má více výhod. Nejpodstatnější je záměna různých protokolů v rámci jedné vrstvy, bez vlivu na funkčnost jiné vrstvy. Např. změna technologie přenosu signálu na první vrstvě nemá žádný vliv na fungování komunikace na ostatních vrstvách. Každá vrstva poskytuje určitou službu vrstvě sousední a sama vykonává funkce dané jednotlivými protokoly. Univerzálnost „vrstvového“ komunikačního modelu mezi výrobci komunikačních zařízení zajišťuje referenční model architektury otevřených systémů (OSI) (Tab. 1). [25]

Tabulka 1. 7 vrstvý ISO / OSI model, data čerpána z: [26]

Č.	Název vrstvy	Funkce	Aplikace	Zařízení	Technologie / protokol
L7	Aplikační	Zpřístupňuje procesům aplikací komunikační systém	Uživatelská aplikace	UTM / NGFW	HTTP, DNS, SMTP, LDAP, NFS, SMB
L6	Prezentační	Reprezentace dat, formátování, dohoda a transformace syntaxe	Komprese, šifrování		
L5	Relační	Vytváření, řízení a ukončování relací, synchronizace a řízení výměny dat mezi dvěma hostiteli	Relace		RPC, SOCKS, L2TP, PPTP
L4	Transportní	Koncové řízení spojení, multiplex. spojení, segmentace a fragment. zpráv, řízení chyb, řízení toku - koncové spojení (porty)	TCP	Firewally	TCP, UDP
L3	Síťová	Směrování a zprostředkování přenosu, navázání a ukončení síťových spojení - logické adresování (IP adresy)	Packety	Routery, firewally, L3 switche	IPv4, ICMP, IPsec
L2	Spojová	Řízení logického spoje (LLC), řízení přístupu k přenosovému prostředku (MAC) - fyzické adresování (MAC adresy)	Rámce	Switche	ARP, Ethernet, IEEE 802.11
L1	Fyzická	Zajišťuje přenos bitů přes fyzické medium, aktivaci / deaktivaci fyzických spojení, dat. okruhů…	Fyzická struktura	Síťové karty, huby	1000Base-T, DSL, GSM

Referenční model OSI byl navržen Mezinárodní normalizační organizací (ISO) – IS 7498 v roce 1984 a zapracován Mezinárodní telekomunikační unií (ITU-T) do doporučení X.200. Norma neupřesňuje, jak by měla být implementována do systémů, ale pouze definuje všeobecné principy v rámci 7 vrstvého modelu. Pro účely kontinuity informací v následujících kapitolách, je potřeba uvést stručný popis funkcí jednotlivých vrstev a služeb, které poskytují. [26] [27]

1.4.1 Aplikační vrstva (L7)

Poskytuje procesům aplikací komunikační rozhraní, tedy přístup ke službám v nižších vrstvách modelu ISO/ OSI. Na úrovni aplikace stanovuje syntaxi dat, pravidla protokolu, vyjednává dohodu o zajištění integrity a důvěrnosti přenášených dat, zjišťuje informace o identifikaci komunikujících stran a jejich dostupnosti, synchronizaci atd. Funkce aplikační vrstvy využívají nejen softwarové prostředky, ale i lidé. [26] [27]

1.4.2 Prezentační vrstva (L6)

Zajišťuje, aby byla data čitelná pro aplikaci příjemce. Zabývá se pouze strukturou dat, jejich formátem, syntaxí. Při příjmu provádí případnou dekompresi dat, dešifrování, transformaci syntaxe do vhodné formy. Při šifrování / dešifrování dat dochází na této vrstvě k výměně šifrovacích metod a klíčů. [26] [27]

1.4.3 Relační vrstva (L5)

Řídí a synchronizuje komunikaci mezi dvěma body. Vytváří relační spojení, udržuje ho a ukončuje. Za vlastní přenos dat odpovídají protokoly nižší úrovně, které vytváří přenosy kratšího trvání. Relace udržuje spojení po delší dobu a může být tvořena více transportními spojeními. Relační spojení jsou jednosměrné (simplexní), střídavě obousměrné (polo duplexní) nebo současně obousměrné (plně duplexní). [26] [27]

1.4.4 Transportní vrstva (L4)

Zajišťuje spolehlivý přenos zpráv v požadované kvalitě. Optimalizuje síťové služby a poskytuje mechanismy kontroly chyb a řízení toku dat. Komunikace na transportní vrstvě probíhá mezi koncovými systémy, nikoliv procesy. Díky tomu jsou transportní služby poskytované vyšším vrstvám síťově neutrální. Poskytuje služby přenosu v režimu se spojením a bez spojení. V režimu se spojením (TCP) je navazováno, udržováno a ukončováno spojení. V režimu bez spojení (UDP) jsou pouze přenášeny bloky dat. Rozdíly mezi TCP a UDP přenosem jsou popsány v Tab. 2. [26] [27]

Tabulka 2. Porovnání přenosových protokolů, upraveno z: [28]

Funkce	TCP	UDP
Velikost hlavičky packetu	20 Bytů	8 Bytů
Entita packetu	Segment	Datagram
Kontrola chyb	Ano	Ano
Číslování portu	Ano	Ano
Orientace na spojení	Ano	Ne
Požadavek na automatické opakování	Ano	Ne
Číslování segmentu	Ano	Ne
Řízení toku	Ano	Ne

Funkce	TCP	UDP
Zamezení přetížení	Ano	Ne

Při přenosu je každému spojení přiřazena dvojice čísel portů, kterými je komunikace identifikována. Transportní vrstva poskytuje funkce adresování, sdružování a rozvětvování spojení, detekce a řízení chyb, řízení toku, rozkládání nebo skládání zpráv (formátování) a další. [26] [27]

1.4.5 Síťová vrstva (L3)

Umožňuje vytvořit síťové spojení mezi systémy na libovolnou vzdálenost a přenášet data mezi zdrojem a cílem. Směrování a přenos datových částí (packetů) v jedné síti i mezi různými sítěmi je realizováno na základě síťové adresace. Komunikující prostředky v síti jsou identifikovány tzv. IP adresou. Hlavní funkcí síťové vrstvy je umožnit propojení různých sítí a podsítí, prostřednictvím směrování. Síťové směrovače (routery) předávají packety na základě algoritmů určujících nejvýhodnější cestu – virtuální okruh. Další služby poskytované síťovou vrstvou jsou dohodnutí kvality, řízení síťových spojení, identifikace koncových bodů, oznamování chyb, řízení datového toku a další. Síťová vrstva je koncipována tak, že je nezávislá na použité přenosové technologii. [26] [27]

1.4.6 Spojová vrstva (L2)

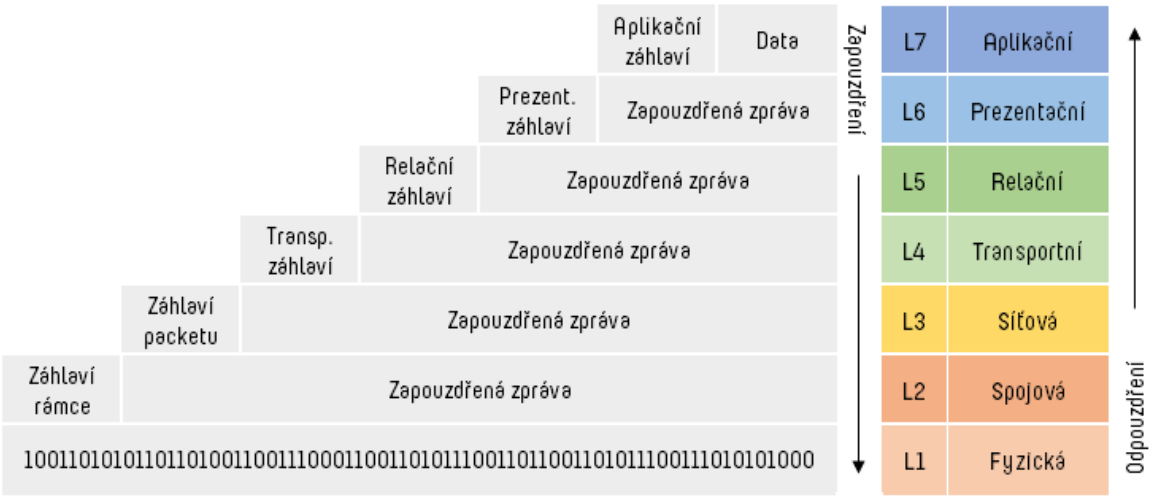
Zajišťuje přenos dat vždy jen mezi dvěma přímo sousedícími systémy, tj. v rámci jedné sítě, přes jeden spoj – fyzický okruh. Spojová vrstva poskytuje funkce zahájení, řízení a ukončení přenosu dat po fyzickém okruhu, synchronizaci, řízení toku, určování pořadí rámců, detekci a opravu chyb, fyzickou adresaci a další. Spojová vrstva má dvě podvrstvy: podvrstvu řízení logického spoje (LLC) a podvrstvu řízení přístupu k médiu (MAC). LLC poskytuje rozhraní mezi komunikujícím prostředkem a síťovou vrstvou, MAC naopak poskytuje služby přenosovému prostředku na fyzické vrstvě. Každé fyzické zařízení v síti je identifikováno jednoznačným označením – MAC adresou (složena z kódu výrobce a fyzického rozhraní síťové karty). [26] [27]

1.4.7 Fyzická vrstva (L1)

Nejnižší vrstva referenčního modelu ISO/OSI je jediná vrstva, která zajišťuje fyzický přenos dat mezi systémy. Spojení je vytvořeno propojením datových okruhů po fyzických médiích

a přenos dat je realizován posloupností bitů. Poskytuje funkce aktivace a deaktivace fyzických spojení, přenosu a řízení bitů po datovém okruhu, oznamování chyb přenosu a další. Na rozhraní mezi fyzickou vrstvou a přenosovým prostředkem jsou definovány charakteristiky přenosových veličin (v závislosti na přenosovém mediu – elektrické, optické, bezdrátové). [26] [27]

Některé funkce a služby, jako jsou řízení toku nebo detekce chyb, se v jednotlivých vrstvách opakují. Jedná se o funkce, které se vzájemně doplňují, nikoliv duplikují. V každé verzi fungují zcela samostatně a jsou relevantní právě pro určitou vrstvu. Spojení je vytvářeno postupně od vyšší vrstvy až k nejnižší. Spojení na vyšší vrstvě nemůže existovat, pokud není vytvořeno spojení na nižší sousedící vrstvě a na všech dalších nižších vrstvách. Při požadavku na spojení se v každé vrstvě ke zprávě přidá záhlaví. S předáním dat na nižší vrstvu dojde k zapouzdření původní zprávy a přidání záhlaví nižší vrstvy. Průchodem jednotlivými vrstvami směrem k nejnižší se tak původní zpráva postupně zvětšuje o záhlaví každé předchozí vrstvy. V opačném směru, při příjmu zprávy, opět dochází v každé vrstvě směrem nahoru k „odpouzdření“ a zahození záhlaví nižší vrstvy (Obr. 4). Znalosti tohoto principu se využívá při diagnostice síťového provozu a hledání chyb spojení. [25]



Obrázek 4. Zapouzdření protokolových datových jednotek, upraveno z: [25]

1.5 Síťová bezpečnost v rámci ISMS

Bez ohledu na velikost, potřebuje každá organizace provozující ICT implementovat bezpečnostní opatření k ochraně proti kybernetickým hrozbám. Úsilí a množství investovaných prostředků je odvislé od velikosti a významu společnosti. [1]

Při návrhu konceptu informační bezpečnosti musí organizace postihnout všechny oblasti bezpečnosti informací, vč. zajištění ochrany informací přenášených prostřednictvím počítačové sítě. Z praxe prověřeným způsobem je implementace systému řízení bezpečnosti informací (ISMS) a bezpečnostních politik dle mezinárodní normy ISO/IEC 27001. Soubor norem ISO/IEC 27xxx čítá padesátku norem zabývajících se bezpečnostními technikami v informačních technologiích. Síťová bezpečnost má dopad na mnoho oblastí ošetřených v tomto souboru norem, avšak pro potřeby této práce budou stěžejní:

- soubor postupů pro opatření bezpečnosti informací ISO/IEC 27002,
- specifické postupy pro síťovou bezpečnost v normách řady ISO/IEC 27033. [29]

1.5.1 ISO/IEC 27002

Zatímco norma ISO/IEC 27001 definuje systém řízení informační bezpečnosti a stanovuje rámec k identifikaci, vyhodnocení a ošetření informačních rizik v organizaci [30], ISO/IEC 27002 v obecné rovině nabízí osvědčené postupy kontrol k minimalizaci hrozeb narušení informační bezpečnosti. Nejedná se o formální specifikaci, ale doporučující dokument, z nějž si organizace mohou vybrat postupy vhodné k ošetření identifikovaných rizik. Síťová bezpečnost je podmnožinou informační bezpečnosti a v ISO/IEC 27002 se prolíná v mnoha kapitolách. ISO/IEC 27002 byla v roce 2022 kompletně přepracována ve svém třetím vydání. Následující odstavce budou odkazovat na kapitoly dle nového číslování. Postupy uvedené v ISO/IEC 27002 postihují celou informační bezpečnost bez ohledu na formu informace a způsob nakládání. Informace uvedené v každém odstavci nejsou kompletním výčtem, ale pouze volně interpretovaným výběrem, vztahujícím se k tématu síťové bezpečnosti a doplněné vlastním komentářem:

- **přenos informací** (5.14): v části věnované elektronickému přenosu informací je doporučeno stanovit pravidla a procesy mimo jiné pro:
    - detekci malware v přenášených informacích a ochraně proti němu,
    - ochranu citlivých informací přenášených v přílohách,
    - prevenci zasílání informací nesprávnému příjemci,
    - zamezení zasílání informací za použití veřejných služeb typu „instant messaging“, sociální sítě, sdílení souborů nebo cloudová úložiště, a to bez souhlasu,
    - zajištění silnějšího ověření při přenosu informací prostřednictvím veřejně přístupných sítí,

jedná se o hrubý rámec opatření, které jsou detailněji rozpracovány v dalších kapitolách normy,

- **řízení přístupů** (5.15): řízení přístupu je v síťové bezpečnosti zásadní. Politika řízení přístupů by měla obsahovat pravidla a postupy pro zajištění přístupu k informacím pouze oprávněným entitám (uživatel, proces, technický prostředek), pouze k těm informacím, které nezbytně potřebují a pouze tehdy, kdy to potřebují. Jde tedy o aplikaci základních bezpečnostních principů – nejnižších oprávnění, explicitního povolení, případně principu úplného řízení přístupů (viz *1.3.6 Princip úplného řízení přístupů*). Další doporučená pravidla mají zajistit:
    - omezení privilegovaného přístupu,
    - oddělení povinností obecně, i při řízení přístupu (princip neslučitelnosti rolí),
    - správu přístupových práv, vč. formálních žádostí o přístup,

  detailněji se přidělováním práv zabývají kapitoly normy *Přístupová práva* (5.18) a *Privilegovaná přístupová práva* (8.2),
- **řízení identit** (5.16): úzce souvisí s předchozím bodem. Doporučuje se zajistit řízení kompletního životního cyklu identit. Každá entita přistupující k informacím organizace musí mít jedinečnou identifikaci (aplikace principu nesdílných přístupů),
- **autentizační informace** (5.17): každá identita disponuje autentizačními informacemi. V souvislosti se síťovou bezpečností jsou důležitá doporučení, jako je změna výchozí autentizace přednastavené výrobcem systému, bezprostředně po jeho instalaci (výchozí autentizační prvky v aktivních síťových prvcích…) nebo přenášet hesla v chráněné podobě (šifrování, hashování). Bezpečné autentizaci se podrobně věnuje kapitola 8.5 normy,
- **bezpečnost informací ve vztahu k dodavatelům a cloudu** (5.19, 5.20, 5.21, 5.22, 5.23): je třeba poznamenat, že doporučení popsaná v předchozích odstavcích je potřeba vztahovat i na externí dodavatele služeb, včetně poskytovatele cloudu. V souvisejících kapitolách normy najdeme doporučené postupy např. pro přístup dodavatelů k informačním systémům organizace, udělování oprávnění k informacím, řízení dodavatelského řetězce ICT nebo pravidla pro použití cloudových služeb,
- **připravenost ICT na zajištění kontinuity provozu** (5.30): doporučení pro zajištění kontinuity provozu ICT při mimořádné událostí (narušení dostupnosti informací) se vztahují i na všechny síťové prvky a další systémy zajišťující síťové služby. Účelem

doporučení je vytvořit strategii pro vypracování, implementaci a testování plánů, které zajistí v požadovaných časech dostatečnou úroveň dostupnosti ICT služeb po přerušení nebo selhání kritických procesů. S kontinuitou provozu úzce souvisí postupy popsané v kapitole normy *Redundance zařízení pro zpracování informací* (8.14),

- **práce na dálku** (6.7): přenos informací při práci na dálku (při práci s informacemi organizace mimo její provozovnu) musí být prováděn tak, aby nedošlo k narušení jejich bezpečnosti. Doporučené postupy zahrnují:
    - vytvoření požadavků na bezpečnost komunikace s ohledem na citlivost informací, k nimž se má přistupovat a které se mají přenášet,
    - použití vzdáleného přístupu, jako je přístup k virtuálním plochám, který umožní uchovat informace uvnitř organizace,
    - omezení nebo nastavení podmínek při používání domácích a veřejných sítí,
    - používání bezpečnostních opatření, jako jsou firewally a ochrana proti malware,
    - navržení bezpečných mechanismů pro ověřování a povolování přístupových oprávnění (vícefaktorová autentizace) v případech, kdy je povolen vzdálený přístup do sítě organizace,
- **zabezpečení kanceláří, místností a zařízení** (7.3) a **umístění a ochrana zařízení** (7.8): ve vztahu k fyzické bezpečnosti existují postupy, které mají bezprostřední vliv na síťovou bezpečnost, konkrétně na zajištění ochrany proti fyzickému narušení bezpečnosti síťových zařízení. Doporučeno je zajistit:
    - umístění kritických zařízení tak, aby k nim neměla přístup veřejnost,
    - konfiguraci zařízení tak, aby důvěrné informace nebyly viditelné a slyšitelné zvenčí,
    - přijetí kontrolních opatření k minimalizaci rizika možných fyzických a přírodních hrozeb (např. krádeže, požáru, prachu, přerušení elektrického napájení, rušení komunikací, elektromagnetického záření…) – např. umístění aktivních prvků sítě do serveroven,
    - monitorování podmínek prostředí, které mohou nepříznivě ovlivnit provoz zařízení, jako je teplota a vlhkost,
    - použití ochrany před bleskem, vybavení všech přívodních elektrických a komunikačních vedení ochranou před bleskem,

  - fyzické oddělení zařízení, které zpracovává informace organizací od zařízení jiných subjektů,

  navazující doporučení jsou uvedené v kapitole *Práce v zabezpečených oblastech* (7.6). V kapitole normy Ochrana *před fyzickými a přírodními hrozbami* (7.5) je relevantní doporučení pro zajištění ochrany proti elektrickému přepětí (např. UPS). V kapitole *Zabezpečení majetku mimo provozovnu* (7.9) je doporučeno poskytnout dostatečnou fyzickou ochranu i zařízením umístěným např. na střeše (antény datových spojů),
- **zabezpečení kabeláže** (7.12): kabeláži je právem věnována zvláštní kapitola. Doporučení jsou:
  - silové a telekomunikační vedení určené pro zařízení zpracovávající informace by mělo být pod zemí nebo v chráničce pod podlahou a zároveň chráněno proti náhodnému přerušení,
  - silové a telekomunikační kabely musí být odděleny nebo elektromagneticky odstíněny kvůli rušení,
  - u citlivých nebo kritických systémů by měly být provedeny dodatečné opatření, jako je použití pancéřovaných kabelů, uzamčených skříní na koncových nebo průběžných bodech, kontrolovaný přístup do kabelových místností, provádění pravidelných kontrol (zda není ke kabelům připojené cizí zařízení), použití optických kabelů a označování kabelů pro jejich rychlou identifikaci,
- **uživatelská koncová zařízení** (8.1): doporučené postupy zde uvedené nesouvisí primárně se zabezpečením sítě, ale jsou pro její bezpečnost podstatné. Nezřídka je koncové zařízení (a jeho uživatel) nejslabším bodem zabezpečení a vstupním bodem pro vedení útoku na organizaci skrze počítačovou síť. Tato obsáhlá kapitola je tedy ve vztahu k síťové bezpečnosti důležitá jako celek. Zvláštní odstavce jsou věnovány bezdrátovému připojení a použití soukromého zařízení pro pracovní účely (BYOD),
- **řízení kapacity** (8.6): z pohledu zajištění dostupnosti informací, a to i v rámci bezpečnosti sítě, je nutné plánovat potřebné kapacity. Měla by být zvážena doporučení pro zajištění dostatečné kapacity, jako jsou:
  - určení požadavků na kapacitu zařízení (např. výkon firewallu při zapnutých UTM funkcích musí být dobře dimenzován),
  - zavedení monitoringu a ladění systémů pro zlepšení jejich efektivity,

  - zavedení detekčních kontrol, které včas upozorní na nedostatečnou kapacitu nebo problémy,
  - pořízení výkonnějších zařízení v případě nedostatečné kapacity,
  - omezení šířky pásma pro služby náročné na zdroje, pokud nejsou důležité,
- **ochrana proti malware** (8.7): doporučené postupy v této kapitole jsou vztažené na veškeré technologie umožňující ochranu vůči malware, včetně síťových prvků, některé postupy se týkají sítí bezprostředně:
  - zavedení mechanismů, které brání přístupu na známé nebo podezřelé škodlivé webové stránky,
  - zavedení kontroly všech dat přijatých prostřednictvím sítí,
  - skenování příloh a stažených souborů e-mailů, zda neobsahují malware, na různých místech a při vstupu do sítě organizace,
  - při přístupu na webové stránky, jejich skenování, zda neobsahují malware,
  - využití zásady obrany do hloubky – detekci malware v síťové bráně (v různých aplikačních protokolech) a dále v koncových zařízeních a serverech,
  - zavedení detekce krycích technik útočníka (např. použití šifrování při doručení malware),
- **správa technických zranitelností** (8.8): technické zranitelnosti se často vyskytují i v operačních systémech síťových prvků, proto je potřeba doporučené postupy pro celý cyklus řízení zranitelností aplikovat i na ně. Ve stručnosti jde o zavedení detekce zranitelností, procesu testování a aplikace záplat zranitelností, případně vytvoření opatření pro znemožnění zneužití zranitelnosti (pokud záplata neexistuje),
- **správa konfigurací** (8.9): účelem postupů v této kapitole je zajistit, aby konfigurace veškerého hardware (HW), software (SW), služeb i sítí byly provedeny optimálně, s ohledem na funkčnost i bezpečnost. Následně nesmí být konfigurace nekontrolovaně měněny:
  - pravidla pro konfigurace by měly být určeny dle osvědčených postupů, politiky organizace a s ohledem na požadovanou úroveň ochrany. Pravidla by měla být pravidelně revidována a aktualizována,
  - mezi zásady konfigurace patří např. omezení privilegovaných uživatelů, zakázaní nepotřebných funkcí, služeb, přístupových identit, změna výchozích

autentizačních údajů, synchronizace hodin (podrobně v kapitole normy 8.17), a další,

- všechny změny konfigurace by měly podléhat řízení změn (rozpracováno v kapitole normy 8.32), měly by být monitorovány a evidovány. Konfigurace je nezbytné zálohovat (detaily v kapitole normy *Informační záloha* 8.13),

- **redundance zařízení pro zpracování informací** (8.14): další důležitá opatření pro zabezpečení dostupnosti informací, která jsou v bezpečnosti síti široce uplatňována. Veškeré komponenty kritické pro plynulý chod procesů v organizaci by měly být zdvojené a dle potřeb zajišťovat vysokou dostupnost. Síťové bezpečnosti se věnují doporučení:
  - uzavření smlouvy s minimálně dvěma dodavateli síťových služeb, jako jsou poskytovatelé internetových služeb (ISP),
  - použití redundantních sítí,
  - použití redundantních zdrojů napájení,
  - použití vyrovnávání zátěže (např. algoritmy pro zajištění vysoké dostupnosti),
  - použití zdvojených zařízení v sítích (např. firewally, směrovače, přepínače),
  - testování funkčnosti navrženého řešení při výpadku jedné z komponent,
- **logování** (8.15): je rozsáhlé téma a postupy doporučené normou zasahují kompletně všechny oblasti ICT. Zajištění logování událostí síťových prvků, jejich ukládání, vyhodnocování a korelování s ostatními událostmi (v nástroji SIEM) je nenahraditelné pro podporu síťové bezpečnosti (investigace bezpečnostních a provozních událostí v síti) i pro celou informační bezpečnost. Veškeré doporučené postupy ohledně logování uvedené v normě mají význam pro síťovou bezpečnost, některé jsou však konkrétní:
  - zajistit detekci událostí na bráně firewall, systému detekce narušení (IDS) nebo malwaru,
  - provádět přezkoumání úspěšných a neúspěšných pokusů o přístup k chráněným zdrojům,
  - kontrolovat DNS požadavky v odchozích síťových připojení ke škodlivým serverům, jako např. řídicí servery botnetů (C&C servery),

  - prověřovat zprávy a reporty o využívání služeb od jejich poskytovatelů, zda nedochází k neobvyklým aktivitám (např. reporty o vytížení datových linek, o přístupech do hostovaných systémů…),
- **monitorovací činnosti** (8.16): přímo navazuje na kapitolu normy *Logování* (8.15) a doplňuje ji o návrh monitorování konkrétních událostí v systémech a sítích:
  - přístup k systémům, serverům, síťovému vybavení… a k jejich konfiguracím, logy o jejich činnosti,
  - události z bezpečnostních nástrojů (firewally, antivir, IDS / IPS, webové filtry…) a o činnostech spojených s malware nebo provozem pocházejícím ze známých škodlivých IP adres a domén,
  - vytížení zdrojů v systémech (u sítových prvků se může jednat o procesor, paměť nebo vytížení síťových portů),
  - známé charakteristiky útoku (např. odepření služby nebo přetečení bufferu),
  - neobvyklé chování systému (např. odchylky v používání standardních protokolů), síťové anomálie (např. „retransmise“, zvýšená latence a „jitter“),
  - nedovolené skenování v síti, úspěšné a neúspěšné pokusy o přístup k chráněným zdrojům, neobvyklé chování uživatelů,
- **zabezpečení sítí** (8.20): následující čtyři kapitoly normy jsou výhradně věnované bezpečnosti sítí. První z nich (8.20), nabízí obecné postupy, které se víceméně odkazují na předchozí kapitoly v kontextu sítí. Doporučuje se například:
  - dokumentovat síťovou architekturu, včetně schémat a konfigurací síťových prvků,
  - zavést mechanismy, které zajistí bezpečnost informací přenášených přes veřejné a bezdrátové sítě,
  - provádět logování a monitorování sítí k odhalení pokusů o narušení informační bezpečnosti,
  - filtrovat provoz v síti (firewall), autentizovat systémy v síti, řídit připojování zařízení do sítě, zakázat používání zranitelných síťových protokolů,
  - provádět „hardening“ síťových zařízení, oddělit jejich správu od provozní části sítě, oddělit jejich správu od správy ostatního ICT,
  - doporučuje se využívat virtuální sítě, včetně softwarově definovaných sítí (SD-WAN),

  závěrem je odkázáno na související normy řady ISO/IEC 27033,

- **bezpečnost síťových služeb** (8.21): síťovými službami je myšleno vše, od poskytování připojení, privátních sítí (VPN), služeb bezpečnostních systémů (firewall, IDS…), až po komplexní správu. Je doporučeno zavést taková pravidla, která budou přesně vymezovat požadavky na poskytované služby, jejich monitoring a kontrolu, provozní postupy, pravidla pro autentizaci, autorizaci, řízení přístupů, šifrování, použité prostředky, technické parametry zařízení, a další,
- **segregace sítí** (8.22): je další z fundamentálních opatření pro zajištění síťové bezpečnosti. Organizace by měly rozdělit síť na více oddělených domén, především veřejnou síť od vnitřní firemní. Ve vnitřní síti vybudovat oddělená prostředí, dle citlivosti a kritičnosti přenášených dat (vice také v kapitole normy 8.31 – *Oddělení vývojového, testovacího a produkčního prostředí*), dle důležitosti zařízení připojených v síti (servery, zabezpečovací zařízení, uživatelské stanice…) a dále dle potřeby a stanovených bezpečnostních politik. Sítě mohou být odděleny fyziky nebo logicky, ale vždy musí být jasně definovány jejich hranice. Pokud je potřeba mezi nimi komunikovat, musí být využito zařízení typu firewall pro řízení a omezování síťových prostupů. Zvláštní pozornost je věnována bezdrátovým sítím, které jsou ze své podstaty více náročné na zajištění bezpečnosti a oddělení bezdrátových sítí pro hosty,
- **filtrování webových stránek** (8.23): kapitola se detailně věnuje filtrováním přístupu na webové stránky. Doporučuje zavést mechanismy, které nedovolí zaměstnancům organizace přistupovat na stránky se škodlivým či nelegálním obsahem (phishing, malware, C&C servery) nebo nežádoucími funkcemi (ukládání a sdílení informací mimo kontrolu organizace),
- **využití kryptografie** (8.24): je důležité pro zajištění důvěrnosti a integrity informací přenášených sítí a ukládaných na datových médiích. Je doporučeno na základě klasifikace informací stanovit které informace je nutné chránit kryptografií a jaké použít algoritmy. Doporučení zahrnují i detailní postupy pro správu šifrovacích klíčů, organizační opatření nebo poukazují na možná technologická či legislativní omezení. Výstižně je popsáno použití kryptografie v informační bezpečnosti: *„Kryptografie může být použita k dosažení různých cílů informační bezpečnosti, např:*

  a) důvěrnost: použití šifrování informací k ochraně citlivých nebo kritických informací, ať už uložených nebo přenášených;

b) integrita nebo autenticita: použití digitálních podpisů nebo autentizačních kódů pro ověření pravosti nebo integrity uložených nebo přenášených citlivých nebo kritických informací. Použití algoritmů pro účely kontroly integrity souborů;

c) nepopiratelnost: použití kryptografických technik k poskytnutí důkazu o (ne)výskytu události nebo akce;

d) autentizace: použití kryptografických technik k autentizaci uživatelů a jiných systémových entit, které žádají o přístup k uživatelům, entitám a zdrojům systému nebo s nimi provádějí transakce.“ [1] [31]

Opatření s dopadem na síťovou bezpečnost se prolínají téměř všemi kapitolami normy ISO/IEC 27002 a jejich kompletní výčet by v podstatě znamenal její celý přepis.

1.5.2 ISO/IEC 27033

ISO/IEC 27033 je série šesti norem, které detailně rozvádí postupy pro provádění kontrol síťové bezpečnosti, stanovených v ISO/IEC 27002. Obsahují rozsáhlé a velice hodnotné informace, od základních principů a terminologie, až po konkrétní bezpečnostní techniky, postupy pro tvorbu bezpečnostních opatření v síti a způsoby provádění kontrol. Text je doplněný názornými blokovými i síťovými diagramy, příklady dokumentace nebo např. technickými popisy hrozeb s protiopatřeními. Následující odstavce přibližují obsah každé z šesti částí normy ISO/IEC 27033:

- **ISO/IEC 27033-1:2015 – Část 1: Přehled a pojmy bezpečnosti sítě**: jedná se o úvodní dokument k celé sérii norem ISO/IEC 27033. Vysvětluje základní pojmy a zkratky, popisuje koncepty síťové bezpečnosti, návody, jak řídit bezpečnostní rizika nebo charakterizuje různé kontrolní mechanismy. Součástí jsou i vybrané síťové scénáře se stručným popisem rizik a vhodných technik k jejich ošetření.

[1] Cryptography can be used to achieve different information security objectives, for example:
a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;
b) integrity or authenticity: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information. Using algorithms for the purpose of file integrity checking;
c) non-repudiation: using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action;
d) authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.

Doporučení obecnějšího rázu v ISO/IEC 27002 převádí na specifické postupy technických kontrol a tvoří rozcestník pro navazující normy ISO/IEC 27033-(2-6), [32] [33]

- **ISO/IEC 27033-2:2012 – Část 2: Pokyny pro návrh a implementaci zabezpečení sítě**: jak je patrné z názvu, norma popisuje krok po kroku, jak navrhnout zabezpečení sítě a následně jej implementovat. Kromě úvodních definic a příloh, obsahuje norma tři hlavní části – příprava návrhu síťové bezpečnosti, samotný návrh a implementace. Každá část je soupisem činností, kterými by měl projít každý proces návrhu zabezpečení sítě. V přípravě jsou to činnosti, jako identifikace aktiv a zjištění požadavků (legislativní, obchodní, technické…), v části návrhu je za základě požadavků a bezpečnostních principů navrhnuta architektura a v implementační části jsou popsány činnosti spojené s realizací návrhu (kritéria pro výběr komponent, dodavatele, zajištění správy, logování, dokumentace…), [34]
- **ISO/IEC 27033-3:2010 – Část 3: Vzorové síťové scénáře – hrozby, techniky návrhu a problematika kontroly**: jedná se o soupis devíti reálných scénářů s dopadem na bezpečnost sítě. Každý scénář zahrnuje detailní popis situace, plynoucích rizik, způsobu jejich ošetření a kontroly. Pro příklad můžeme jmenovat scénáře zabývající se poskytování připojení k internetu zaměstnancům, používání služeb pro vzájemnou spolupráci nebo síťovou segmentaci, [35]
- **ISO/IEC 27033-4:2014 – Část 4: Zabezpečení komunikace mezi sítěmi pomocí bezpečnostních bran**: účelem čtvrté části souboru norem ISO/IEC 27033 je poskytnout návody na zabezpečení sítě ve vztahu k síťovým bezpečnostním branám (firewallům) a to pro všechny osoby podílející se na návrhu a správě sítě. Téma bezpečnosti firewallů je rozčleněno do šesti částí:
    - přehled, k čemu se využívají firewally,
    - bezpečnostní hrozby, které mohou na firewally působit,
    - požadavky na funkce firewallu, v souvislosti s ošetřením bezpečnostních hrozeb,
    - bezpečnostní kontroly prováděné firewallem (způsoby filtrování komunikace, kontroly na vyšších vrstvách ISO/OSI modelu…),
    - techniky návrhu (komponenty návrhu, nasazení kontrol…),
    - pokyny pro výběr firewallu dle jeho funkcí a schopností, [36]

- **ISO/IEC 27033-5:2013 – Část 5: Zabezpečení komunikace v sítích pomocí virtuálních privátních sítí (VPN)**: je obdobně koncipována, jako ISO/IEC 27033-4, se zaměřením na plánování, návrh a implementaci VPN. Po vysvětlení principu VPN a přehledu jejich typů, následují kapitoly popisující bezpečnostní hrozby spojené s poskytováním VPN, bezpečnostní požadavky, kontroly… Detailně jsou rozpracovány různé technické i obecné aspekty při návrhu VPN, [37]
- **ISO/IEC 27033-6:2016 – Část 6: Zabezpečení přístupu k bezdrátové IP síti**: jedná se o obecnou normu pro zabezpečení bezdrátových sítí, jako je Wi-Fi, Bluetooth nebo mobilní datové sítě. Popis bezpečnostních hrozeb je zaměřen hlavně na techniky působící na bezdrátový přenos dat. Techniky a aspekty návrhu zabezpečení jsou dělené dle druhu bezdrátové technologie. [38]

Ve fázi návrhu je další, již sedmá část, **ISO/IEC 27033-7 – Část 7: Pokyny pro bezpečnost síťové virtualizace**. Její zveřejnění se předpokládá nejdříve v roce 2024. Dokument se snaží reagovat na rychlý rozvoj technologií založených na virtualizaci a nabídnout postupy pro identifikaci bezpečnostních rizik, pro návrh a implementaci bezpečnostních opatření v této oblasti. Virtualizace nabízí nesporné výhody oproti tradičním technologiím, především větší flexibilitu a škálovatelnost při nižších provozních nákladech. Virtualizace ale přináší i nová rizika, jejichž ošetření vyžaduje změnu v přístupu při návrhu bezpečnostních opatření. [32] [39]

Normy, jako je soubor ISO/IEC 27xxx, mohou sloužit jako dobrá předloha k vytvoření pravidel v organizaci pro naplnění požadavků daných legislativou, ale i praktickým průvodcem při návrhu zabezpečení ICT. Pochopení a osvojení si principů informační bezpečnosti je společně se znalostí síťových technologií dobrým základem a zároveň nutným předpokladem pro schopnost navrhovat zabezpečení sítě.

2 VRSTVENÍ SÍŤOVÉ BEZPEČNOSTI

Jeden z obecných principů budování bezpečnosti informací je obrana do hloubky (viz *1.3.9 Princip vrstvení bezpečnostních opatření*). Obrana do hloubky, jinak řečeno vrstvení bezpečnostních opatření, se rovněž uplatňuje specificky v oblastech informační bezpečnosti, jako je bezpečnost síťová. Cílem kapitoly je popsat vrstvy síťové bezpečnosti, jejich účel a používané technologie.

2.1 Bezpečnostní strategie

Navrhnutá opatření k zajištění síťové bezpečnosti musejí vycházet z předem vytvořené a schválené bezpečnostní strategie, která definuje, jak budou ITC prostředky a uživatelé chráněni před kybernetickými hrozbami. Strategie se opírá o tři základní pilíře:

- **znalost obchodních požadavku**: pokud chceme něco chránit, musíme dobře vědět co. Musíme mít detailní představu o tom, co je pro organizaci důležité, jaké má obchodní plány, jaké jsou její aktiva a jaká rizika je ochotna podstoupit pro dosažení svých cílů,
- **znalost hrozeb a rizik**: řízení rizik v organizaci je důležité pro pochopení, jaké zranitelnosti mají aktiva, jaké hrozby na ně působí, jaká je pravděpodobnost, že budou hrozby zneužity a jaký to bude mít dopad. Postupy pro řízení rizik jsou popsány např. v normě ISO/IEC 27001. Na základě výsledku analýzy rizik lze navrhnout odpovídající bezpečnostní opatření, která jsou v souladu s obchodními požadavky organizace,
- **odpovídající dokumentace**: dokumentace je zásadním aspektem bezpečnostní strategie. Dokumentace umožňuje standardizovat činnosti v organizaci tak, aby všichni zúčastnění pracovali způsobem, kterým budou cíle bezpečnostní strategie naplněny. [40]

Stanovená bezpečnostní opatření musejí být v souladu se základními principy informační bezpečnosti, nesmějí znemožňovat výkon činností k dosažení obchodních cílů organizace a náklady na jejích zavedení a provoz nesmí být vyšší než hodnota chráněných aktiv. Ani precizně implementovaná bezpečnostní opatření nemusí zaručit jejich nepřekonatelnost. Z toho důvodu je potřeba do strategie zahrnout i kontrolní mechanismy k detekci narušení bezpečnosti, postupy, jak na útoky reagovat a plány na obnovení činnosti. [41]

Bezpečnostní strategií může být dokument – *Bezpečnostní politika informací*, jehož náplň obsahově vychází z norem ISO/IEC 27001 a ISO/IEC 27002, jak je popsáno v kapitole *1.5 Síťová bezpečnost v rámci ISMS*.

2.2 Fyzická bezpečnost

Účelem fyzické bezpečnosti je zamezení neoprávněného přístupu k prvkům ICT, jejich poškození, neoprávněné manipulace nebo zneužití. Při nekontrolovaném fyzickém přístupu k síťovým prvkům může dojít k narušení dostupnosti informací (krádež, zničení zařízení nebo kabeláže), důvěrnosti i integrity (instalace zařízení k odposlechu nebo pozměnění komunikace). Prvky síťové infrastruktury musí být umístěny v zabezpečeném perimetru (např. objekt organizace), kritické prvky sítě v zabezpečených oblastech (např. serverovna, hostingové centrum). K ochraně perimetru a zabezpečených oblastí je využíváno prostředků fyzické bezpečnosti:

- mechanické zábranné systémy (MZS) fyzicky omezují přístup k chráněnému aktivu, např. pomocí zámků, dveřních systémů a dalších stavebních a konstrukčních prvků,
- systémy kontroly vstupu (SKV) umožňují elektronicky řízenou kontrolu vstupu do objektu nebo zabezpečené oblasti, pomocí identifikačního prvku (čip, PIN, biometrie…),
- poplachové zabezpečovací a tísňové systémy (PZTS) poskytují elektronickou ochranu zabezpečených oblastí – vyhlášením poplachu při neoprávněném vniknutí,
- dohledové videosystémy (VSS) umožňují přenášet, zobrazovat, vyhodnocovat a ukládat obraz a zvuk ze zabezpečených oblastí a tím reagovat na neoprávněné vniknutí,
- elektronická požární signalizace (EPS) detekuje a vyhodnocuje projevy hoření (plamen, kouř, teplo) a spouští procesy vedoucí k uhašení (např. vyvolání poplachu, spuštění samočinného hašení, předání poplachové informace na dohledové centrum…). [42]

Do oblasti fyzické bezpečnosti můžeme zařadit i systémy zajišťující vhodné prostředí pro plynulý chod aktivních prvků v zabezpečených oblastech, jako je klimatizace, zdroj nepřerušovaného napájení (UPS) nebo záložní zdroje napájení při déle trvajícím výpadku (diesel agregát). [42]

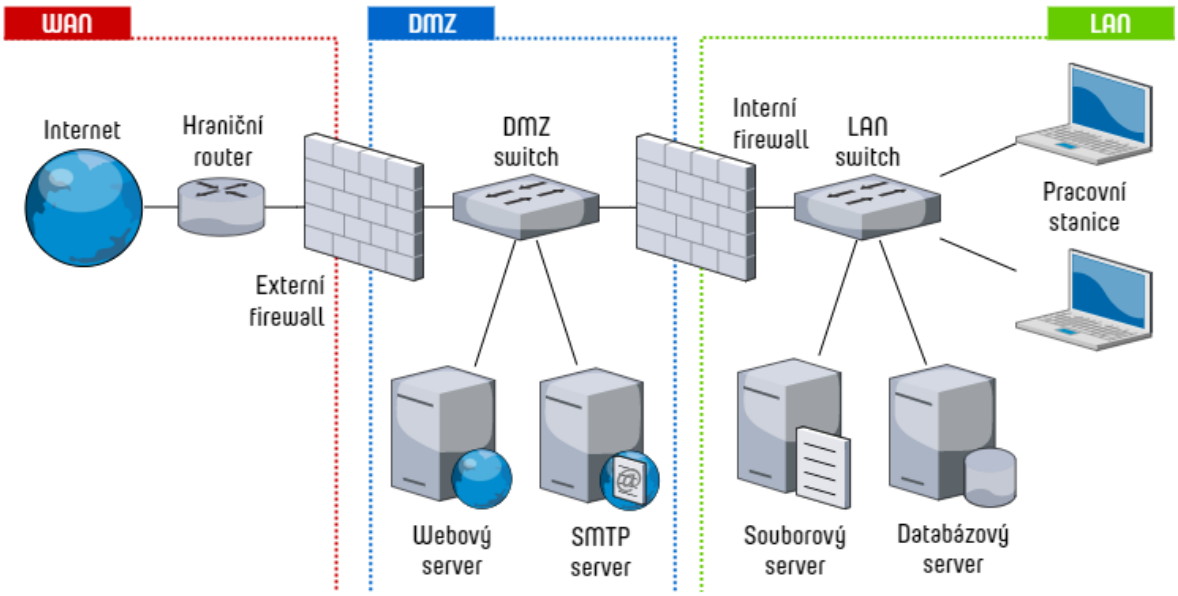
Pokyny a doporučení k fyzickému zabezpečení aktiv, včetně síťových prvků a kabelových tras, jsou součástí normy ISO/IEC 27002, viz kapitola *1.5 Síťová bezpečnost v rámci ISMS*.

2.3 Segmentace sítě

Základním stavebním prvkem v návrhu bezpečné síťové architektury je segmentace sítě na více funkčních celků. Účelem rozdělení sítě je oddělení informací anebo systémů podle jejich kritičnosti. Při průniku útočníka do systému v méně kritické nebo veřejné části sítě nedojde ke kompromitaci systémů ve více chráněném segmentu sítě. Další důvody rozdělení sítě mohou vyplývat z provozních požadavků. [43]

2.3.1 Zóny

Prvním stupněm je rozdělení sítí na zóny (Obr. 5). Zónami jsou odděleny veřejné sítě (WAN), jako je internet od sítě lokální (LAN), uvnitř organizace. Organizace mají běžně potřebu vystavovat některé informace nebo služby veřejně. Pokud k tomu nevyužívají cloudové služby, umisťují část svých systémů do sítě označované jako demilitarizovaná zóna (DMZ) aby neohrozili ostatní ICT v lokální síti. Síťový provoz mezi zónami kontroluje firewall s jednoznačně definovanými pravidly. DMZ by neměly být z bezpečnostních důvodů tvořeny pouze logicky oddělenou sítí (viz následující podkapitola), ale fyzicky odděleným HW, což zvýší odolnost vnitřní sítě např. proti útoku typu odepření služby (DoS). [43] [44]



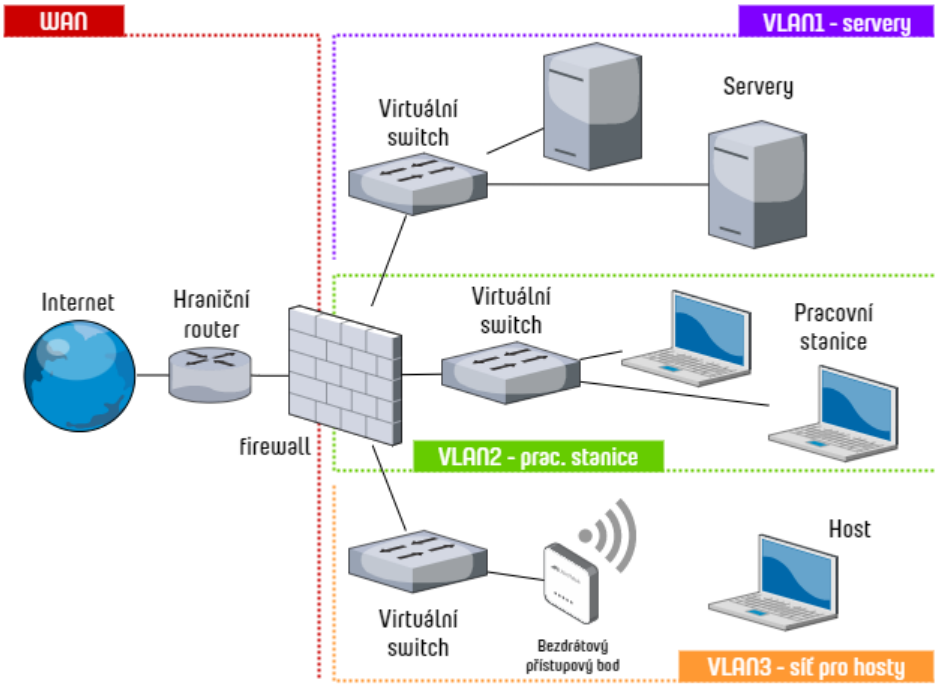
Obrázek 5. Příklad oddělení síťových zón, upraveno z: [44]

2.3.2 Logické sítě (VLAN)

Další stupeň ochrany sítí jejich dělením se uplatňuje uvnitř organizace. Záměrem dalšího dělení je:

- oddělit koncová zařízení uživatelů od kritických částí infrastruktury. Při napadení koncového zařízení uživatele je útočníkovi zamezeno nebo ztíženo útočit na další, významnější systémy v síti (servery, síťové prvky…),
- oddělit správu síťových prvků a serverů od ostatního síťového provozu. Do sítě určené ke právě ICT by neměl mít přístup nikdo jiný než systémoví administrátoři. Jedná se o další bezpečnostní opatření s cílem znemožnit útočníkovi získání významné kontroly nad celým systémem,
- seskupit uživatele a jim přidělené zdroje dle jejich pracovního zařazení. Např. oddělení financí, personální, call centrum a další. Využívá se spíše v menších organizacích za účelem zpřehlednění správy koncových zařízení a poskytnutých zdrojů,
- oddělit lokality organizace. Organizace působící ve více geografických oblastech mají rozděleny sítě dle jejich fyzického umístění. V závislosti na použité technologii propojení geograficky oddělených sítí to může být nezbytné, ale zároveň rozdělení poskytuje provozní výhody,
- optimalizovat provoz na síti. Rozdělení sítě na menší „broadcastové“ domény má pozitivní vliv na její výkon. Zároveň je tím omezen prostor pro některé typy útoků,
- oddělit síť pro hosty nebo pro soukromá zařízení zaměstnanců (BYOD) od ostatních sítí. Koncová zařízení návštěvníků nebo uživatelů, která nejsou pod plnou správou organizace, ale je žádoucí je připojit např. k internetu, musejí být oddělena od ostatního síťového provozu organizace. Riziko útoku prostřednictvím „cizího“ zařízení na ICT organizace je nezanedbatelné. [43] [45]

Výsledné dělení sítě na VLAN je kombinací výše uvedeného. Zařízení a systémy v rámci jedné VLAN nedokážou většinou fungovat izolovaně a potřebují přistupovat na zdroje v dalších VLAN. Z tohoto důvodu je každá VLAN zakončena na firewallu, který pomocí definovaných pravidel povoluje nezbytně nutnou komunikaci mezi nimi a případně do jiné zóny (WAN, DMZ) (Obr. 6). [45]



Obrázek 6. Příklad segmentace sítě pomocí VLAN, upraveno z: [45]

2.3.3 Prostředí

V souvislosti s rozdělením sítě uvažujeme také o různých prostředích. Malá obchodní organizace, která ke svému chodu potřebuje pouze pár systémů a připojení k internetu, si vystačí s jediným provozním prostředím. Jinak tomu bude např. u technologické organizace, která vyvíjí vlastní produkt pro své klienty, nebo u banky poskytující internetové bankovnictví. Jediné provozní prostředí už není dostačující a v rámci sítě je potřeba odděleně provozovat prostředí další. Rozdělení dle prostředí může vypadat následovně:

- **provozní prostředí**: slouží pro běžný chod organizace, nabízí všechny podpůrné funkce pro uživatele všech oddělení organizace. Dále je děleno na různí síťové segmenty, s různou mírou kritičnosti, jak bylo popsáno dříve,
- **vývojové prostředí**: slouží pro vývoj produktu, který organizace poskytuje svým klientům. Do tohoto prostředí mají přístup především uživatelé, podílející se na vývoji produktu,
- **testovací prostředí**: během vývoje produktu probíhá testování jeho částí i finálního sestavení, pro ověření jeho funkčnosti. Při testování se používají anonymizovaná nebo syntetická data. Testovacích prostředí může být více, dle potřeb, způsobu vývoje nebo druhu testu. Do testovacího prostředí mají přístup např. vývojáři, testeři nebo třeba produktový tým, podle požadavků organizace,

- **před-produkční prostředí**: slouží k ověření, že nová verze produktu funguje správně s kopií reálných produkčních dat a že je možné ji uvolnit k produkčnímu využití, tzn. poskytnout klientům organizace. Vzhledem k tomu, že produkční prostředí obsahuje klientská data, má do něj přístup pouze omezená skupina uživatelů, kteří jsou zodpovědní za finální testování a nasazení nové verze do produkce,
- **produkční prostředí**: jedná se o prostředí, které slouží k poskytování produktu zákazníkům organizace. Produkční prostředí je pro organizaci nejkritičtější a zajištění jeho bezpečnosti z pohledu důvěrnosti, integrity i dostupnosti je naprosto klíčové. Přístup do tohoto prostředí je omezen pouze na osoby, poskytující přímou technickou podporu prostředí a produktu. [31]

Prostředí mohou být od sebe oddělená logicky použitím VLAN, ale i fyzicky a geograficky, dle požadavků organizace.

2.3.4 Datacentra

Rozdělení sítí (a veškerých systémů ICT) na dvě nezávislá datacentra, se provádí z důvodu zajištění kontinuity podnikání v případě mimořádné události, kdy organizace požaduje vysokou dostupnost (HA) poskytovaných služeb. Mimořádnou událostí může být prosté selhání dodávky elektrické energie pro datacentrum, ale i poškození datacentra požárem, zemětřesením nebo jinou živelní pohromou. Spíše než o rozdělení sítě, se jedná o kopii primárního datacentra (PDC) do vzdáleného, geograficky odděleného datacentra (v jiném regionu, státu, na jiném kontinentu – podle požadované ochrany), které slouží jako záložní pro potřeby zotavení po havárii (DRC). [31]

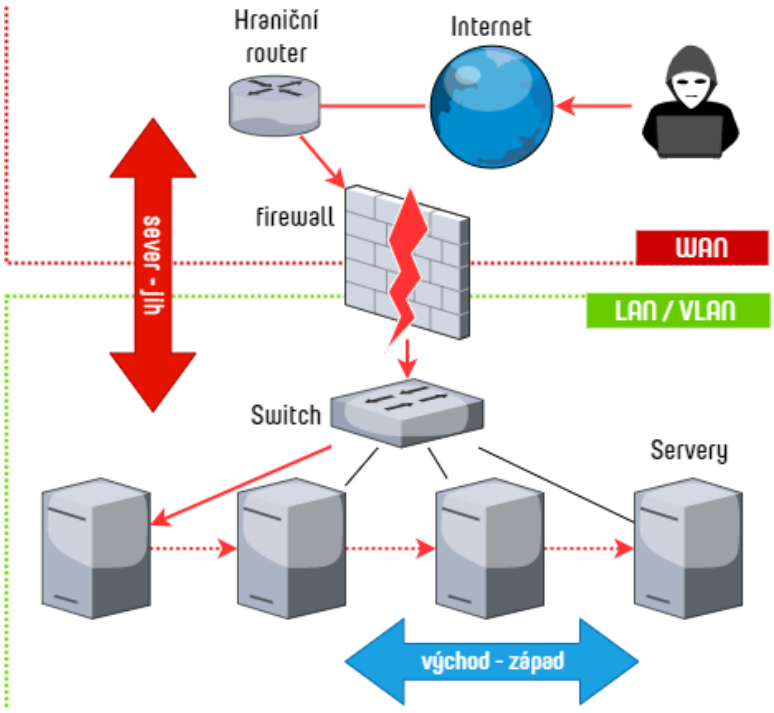
2.3.5 Mikrosegmentace

Při klasické síťové segmentaci je prostup řízen mezi většími segmenty, typicky mezi VLAN, na hardwarové úrovni prostřednictvím firewallu. Řízení prostupů mezi síťovými segmenty je vertikální, severo-jižní (klient-server), zatímco komunikace horizontální, východo-západní (server-server) není nijak zabezpečena (Obr. 7). V případě, kdy útočník překoná ochranu perimetru, dokáže se následně pohybovat horizontálně a může napadat všechny systémy v rámci celého síťového segmentu. Tento nedostatek odstraňuje bezpečnostní metoda zvaná mikrosegmentace, která umožňuje větší granularitu v řízení síťových přístupů. Politiky mikrosegmentace nedefinují prostupy pouze mezi síťovými segmenty, ale i mezi

pracovní zátěží (prostředek, potřebný pro běh aplikace, např. virtuální server nebo kontejner). Mikrosegmentace může být plně SW řešení, nezávislé na použitém síťovém HW, je tak vhodná pro řízení přístupu napříč veřejnými i privátními cloudovými službami. Existuje několik základních přístupů použití mikrosegmentace:

- **na základě agentů**: na každý koncový bod je instalován SW agent, který je centrálně spravován. Výhodou je výborná škálovatelnost řízení a viditelnost do síťové komunikace všech procesů,
- **na síťovém základu**: je velice podobná klasické segmentaci, kdy je provoz řízen mezi síťovými prostředky. Využívá se např. v softwarově definovaných sítích (SDN),
- **na základě hypervizoru**: při tomto způsobu mikrosegmentace je kontrolován veškerý provoz procházející přes hypervizor. Výhodou je možnost přesouvat politiky mezi hypervizory vzájemně,
- **nativní podpora cloudových služeb**: využívá se služeb řízení přístupů zabudovaných přímo v produktech poskytovatelů cloudu (např. Amazon security group, Azure firewall, Google Cloud firewall). [46]

Mikrosegmentace je základní předpoklad pro Zero Trust koncept.



Obrázek 7. Severo-jižní a východo-západní provoz, upraveno z: [46]

2.3.6 Zero Trust koncept

Dříve se za důvěryhodnou považovala síť umístěná na vnitřní straně perimetru, chráněná firewallem. Bezpečnost byla zaměřena na ochranu perimetru s cílem zabránit útočníkovi proniknout do vnitřní sítě. Zero Trust (nulová důvěryhodnost) je konceptem bezpečnosti založeném na myšlence, že neexistuje žádná důvěryhodná síť a je potřeba řídit a prověřovat veškeré digitální interakce ve všech sítích a systémech. Předpokládá, že útočník se již ve vnitřní síti nachází a může škodit a že jakýkoliv pokus o síťový přístup je hrozbou. Zero Trust koncept je plně ve shodě s principem nejnižších oprávnění (viz kapitola *1.3.1 Princip nejnižších oprávnění*), přenáší pozornost z ochrany perimetru na ochranu zdrojů a identit. Implementace nulové důvěryhodnosti vyžaduje přísné ověření identity každé osoby nebo zařízení přistupujícího k síti nebo aplikaci, ověření oprávněnosti přístupu ke zdroji, minimalizaci prostoru, ke kterému je udělen přístup, zabezpečení přístupu a maximální viditelnost na všechny provedené operace. Jedná se tedy o integraci technologií a postupů, jako jsou vícefaktorové ověření (MFA) uživatele, prověření zařízení uživatele (kontrola koncového bodu), mikrosegmentace, správa identit a přístupů (IAM), kryptografie, Next-Generation Firewall, SIEM a další. [47]

2.4 Kontrola síťového provozu

Při kontrole síťového provozu dochází k technickému uplatnění stanovených zásad přístupu k prostředkům organizace prostřednictvím sítě.

2.4.1 Firewall

Firewall je hlavní součástí síťového zabezpečení. Jeho účelem je na základě stanovených politik povolovat síťový přístup k prostředkům ICT. Síťový firewall prověřuje příchozí a odchozí provoz, brání nežádoucímu průniku do vnitřní sítě, kontroluje provoz mezi síťovými segmenty, směruje komunikaci do dalších sítí, poskytuje záznamy o síťovém provozu a poskytuje další služby v závislosti na typu firewallu. Personální firewally jsou instalovány na koncová zařízení uživatelů pro poskytnutí další vrstvy ochrany. Existují různé druhy firewallů, dle způsobu filtrace packetů:

- **paketový filtr**: nejjednodušší způsob filtrování packetů založený na kontrole čísla zdrojové / cílové adresy a zdrojového / cílového portu (pracuje na vrstvách L3-4 modelu ISO/OSI). Každý packet je prověřován samostatně, zda vyhovuje nastavené

politice. Výhodou je rychlost zpracování, nevýhodou omezené nastavení kontroly a nutnost povolovat komunikaci v obou směrech,

- **stavový firewall**: funguje podobně jako paketový filtr, ale navíc si uchovává tabulku s informacemi o navázaných spojeních (relacích). Výhodou je rychlejší zpracování packetů spadajících do otevřené relace, více možností nastavení kontroly provozu a potřeba nastavovat politiku pouze ve směru z kterého dochází k navázání relace,
- **aplikační firewall**: nebo také proxy firewall pracuje na 7. vrstvě modelu ISO/OSI a může tak nahlížet do obsahu komunikace. Aplikační firewall přijme požadavek na komunikaci, případně jej i dešifruje (pokud má k dispozici privátní klíč), prověří obsah a sestaví novou komunikaci, kterou zašle na cílový server. To umožňuje v komunikaci detekovat chyby a pokusy o útok,
- **UTM / NGFW**: systém jednotné správy hrozeb (UTM) a firewall nové generace (NGFW) jsou zařízení pro zabezpečení sítě, kombinující několik bezpečnostních nástrojů. Kontrolují provoz na všech vrstvách modelu ISO/OSI a z každého integrovaného nástroje přebírají ty nejlepší schopnosti detekovat a blokovat kybernetické bezpečnostní hrozby. NGFW i UTM kromě stavového firewallu integrují aplikační firewall, IPS, antivirovou kontrolu, webový filtr, VPN služby, SSL (Secure Sockets Layer) inspekci a další funkcionality. UTM oproti NGFW může zahrnovat i další funkce, jako je správa koncového bodu, ochranu proti úniku dat (DLP) a další. Poskytuje jednotnou správu všech nástrojů s předpřipravenými politikami a umožňuje snadnější a rychlejší nasazení. UTM je vhodné pro nasazení v menších organizacích. NGFW je více škálovatelný a poskytuje větší výkon. Pořizují jej velké organizace, které disponují týmem odborníků s odpovídajícími znalostmi, a kteří využijí možnosti lepšího přizpůsobení potřebám organizace,
    - **aplikační kontrola**: většina aplikací komunikuje v síti rozpoznatelným způsobem. Zařízení typu UTM / NGFW disponují signaturami chování mnoha aplikací. Správci tak mohou nastavit politiky blokování síťového provozu zvolených aplikací nebo jejich kategorií (např. torrent, peer to peer aplikace, VPN klienti…),
    - **webový filtr**: v organizaci je více než vhodné omezovat přístup uživatelů na webové stránky v internetu, které jsou nebezpečné svým obsahem (stránky s malware, nevhodným obsahem, phishingové stránky a jiné podvodné stránky…). UTM / NGFW mohou každý požadavek o přístup na webovou

stránku porovnat s on-line databází hodnocení obsahu stránek a přístup zamítnout nebo povolit. Lze také blokovat přístup na IP adresy v internetu na základě jejich geografické lokace nebo jejich umístění v některém z veřejných „blacklistů“,

- **antivirová kontrola**: součástí systémů UTM / NGFW je i modul pro antivirovou kontrolu dat přenášených v síti. Stejně jako na koncové stanici, vyhledává antivirová kontrola v síti části kódu, které porovnává s databází signatur známého malware,
- **SSL inspekce**: v současné době je většina komunikace v síti šifrována. Tento stav je příznivý pro zajištění důvěrnosti přenášených informací, ale ztěžuje využití nástrojů pro detekci hrozeb, které jsou popsány výše. SSL inspekce funguje podobně jako aplikační firewall. Komunikace, která prochází přes UTM / NGFW je nejdříve přijata, dešifrována a následně prochází všemi kontrolami. Následně je opět zašifrována a odeslána koncovému příjemci. SSL inspekce vyžaduje, aby stanice v síti důvěřovali certifikátu bezpečnostního zařízení, což může být v některých případech problém. [48] [49]

2.4.2 IDS / IPS

Systém detekce průniku (IDS) je bezpečnostní systém, který sleduje síťový provoz a na základě signatur známých praktik útočníků detekují pokus o narušení síťové bezpečnosti. Informace o narušení jsou následně zasílány např. do systému SIEM k dalšímu zpracování. Systémy prevence průniku (IPS) používají stejné metody detekce, jako systémy IDS, ale navíc dokážou závadnou komunikaci automaticky blokovat. Systémy IDS mohou být instalovány na koncovém systému (HIDS), kde mohou sledovat kromě komunikace na síti i chování aplikací, procesů nebo změny v operačním systému (OS), nebo jsou součástí síťového zařízení (NDIS), kde kontrolující síťový provoz. [49]

2.5 Vzdálené připojení

Většina organizací řeší potřebu bezpečného připojení uživatelů pracujících na dálku do interní sítě. Tato potřeba byla navíc umocněna v době pandemie, kdy organizace omezovali přítomnost zaměstnanců na pracovišti a preferovali práci z domova. Vystavit firemní prostředky v interní síti tak, aby byly přístupné z internetu, lze otevřením příslušného portu

služby (např. RDP, SSH…) na firewallu, ale tento přístup je z bezpečnostního hlediska nepřijatelný. Další potřebou organizací je propojení více interních sítí, které jsou od sebe geograficky vzdálené (typicky pobočky organizace v různých regionech). Obě potřeby lze uspokojit použitím privátního propojení sítí, prostřednictvím vlastních nebo pronajatých okruhů. Další možností je použití technologií virtuálních privátních síti (VPN). VPN poskytuje oproti privátním okruhům levnější a flexibilnější možnost, proto ji organizace ve velké míře využívají. VPN využívá pro přenos dat existující internetové připojení. Komunikace mezi koncovými body je zabezpečena kryptografickými prostředky, což zabezpečí důvěrnost i integritu přenášených informací. Nejpoužívanějšími VPN technologiemi jsou:

- **Internet Protocol Security (IPsec VPN)**: je sada protokolů a algoritmů, kterými je zajištěno šifrování dat mezi dvěma koncovými body VPN. IPsec pracuje na síťové vrstvě ISO/OSI modelu a používá se především k propojení celých sítí (site-to-site VPN), ale i k připojování vzdálených pracovníků do interní sítě (především dříve, v současnosti spíše SSL VPN). IPsec VPN je zpravidla zakončena na firewallu nebo VPN koncentrátoru, na kterých je definována konfigurace pro vytvoření VPN tunelu a politiky pro řízení přístupu. Na vzdáleném koncovém bodu v případě připojení zařízení uživatele je použit speciální SW – VPN klient,
- **Secure Sockets Layer VPN (SSL VPN)**: dnes již nevyužívá zastaralý SSL protokol, ale protokol TLS (Transport Layer Security). SSL VPN pracuje na transportní a vyšších vrstvách ISO/OSI modelu a používá se k vytvoření šifrované komunikace mezi vzdáleným koncovým bodem (uživatel pracující na dálku) a interní síti. SSL VPN lze konfigurovat i pro vytvoření zabezpečeného spojení mezi aplikacemi či službami. Oproti IPsec není u SSL VPN nutné na koncovém bodu použít speciální SW. SSL VPN tunel lze vytvořit z jakékoliv aplikace umožňující TLS (SSL) komunikaci, např. z webového prohlížeče. [50]

Zda zvolit IPsec nebo SSL VPN záleží na účelu použití, potřebách a preferencích organizace. Hlavní rozdíly jsou popsány v tabulce (Tab. 3).

Tabulka 3. Porovnání IPsec a SSL VPN, upraveno z: [50]

Funkce	**IPsec VPN**	**SSL VPN**
Síťové vrstvy	Funguje na L3	Funguje na L4-7

Funkce	IPsec VPN	SSL VPN
Konektivita	Propojuje vzdálené stanice s celou sítí	Připojuje uživatele ke konkrétním aplikacím a službám
Aplikace	Může podporovat všechny aplikace založené na IP	Nejlepší pro e-mail, sdílení souborů, a webové aplikace
Umístění brány	Brána obvykle implementována do firewallu	Brána nasazena typicky za firewallem (může být také implementována – NGFW)
Bezpečnost / řízení	Široký přístup vytváří obavy o bezpečnost	Více granulární řízení vyžaduje více správy
Použití na koncových bodech	Vyžaduje klienta na stanici	Funguje ve webovém prohlížeči nebo v tenkém klientovi

2.6 Řízení přístupů

Řízení přístupu je základním předpokladem pro celou informační bezpečnost. Vzhledem k šíři a obsáhlosti tohoto tématu je kapitola zaměřena na uvedení základních pojmů a specifičtěji na řízení přístupu k síti. Obecně řízení přístupu definuje kdo, nebo co (**subjekt** řízení) může mít přístup k jakým prostředkům organizace (**objekt** řízení), jaký typ přístupu je udělen (přístupové **oprávnění**) a případně na jakou dobu. [51]

2.6.1 AAA

Za zkratkou AAA se skrývají tři základní prvky v řízení přístupu: authentication, authorization, a accounting. Pro úplnost je doplněna identifikace, která AAA v některých případech předchází:

- **identifikace**: v případě, kdy je subjektem řízení přístupu fyzická osoba, je někdy potřeba tuto osobu ztotožnit. Typickým příkladem je nový zaměstnanec organizace. Ověření totožnosti provádí pracovník osobního oddělení v organizaci, na základě předložení identifikačních dokladů (průkaz totožnosti, rodný list, pas…). Po ztotožnění je novému zaměstnanci vytvořena identita v personálním systému a je zahájen proces vytvoření unikátní identity a ověřovacího faktoru (pověření) uživatele pro použití v ICT systémech organizace. Vhodným nástrojem pro zajištění životního cyklu identity uživatele je Identity and Access Management (IAM),
- **autentizace**: je proces ověření platnosti pověření subjektu. Při autentizaci dochází k porovnání jednoho nebo více ověřovacích faktorů vůči databázi platných identit.

Příkladem je identifikace subjektu uživatelským jménem a autentizace ověřením jeho hesla. Pro udělení přístupu ke kritickým systémům je využíváno autentizace s ověřením více faktorů současně (vícefaktorová autentizace – MFA). Faktory ověřeni jsou obecně:

- **něco co vím**: příkladem je heslo, PIN, fráze,
- **něco co mám**: čip, HW token, mobilní telefon,
- **něco jsem**: fyzická charakteristika člověka (biometrie), např. otisk prstu, hlasu, duhovky, sítnice, dynamika podpisu, chůze…,

- **autorizace**: *„Autorizace je proces udělování přístupu subjektům na základě prokázané identity. Uvádí, kdo smí provádět určité operace. Pokud je činnost povolena, je subjekt autorizován; pokud je zakázána, subjekt není autorizován… Proces autorizace zajišťuje, že požadovaná činnost nebo přístup k objektu je možný na základě oprávnění přidělených danému subjektu.“*[2] [52]. Autorizace neznamená pouze ověření, jestli má subjekt přístup k objektu řízení, ale určuje také jeho oprávnění, tzn. jaké činnosti může s objektem provádět,
- **audit** (nebo také accounting či accountability, dle zaměření řízení přístupu): po identifikaci a autentizaci, začne systém zapisovat do logu činnosti, které subjekt provádí. Zaznamenává se kdo, kdy, kde a jakou akci provedl – vzniká auditní stopa pohybu subjektu v systému. Vytváření auditní stopy je nezbytné pro detekci či šetření bezpečnostních incidentů a jejich prokazování. [53]

  V souvislosti s řízením síťových přístupů je používán výraz **accounting** (účtování), místo audit. Význam je podobný, hlavním účelem je však zaznamenávání statistických informací o spotřebě prostředků během připojení, např. zaznamenávání doby připojení nebo počet přenesených dat pro následné vyúčtování či plánování kapacity.

[2] Authorization is the process of granting access to subjects based on proven identities.
It indicates who is allowed to perform certain operations. If the action is allowed, the subject is authorized; if disallowed, the subject is not authorized… The process of authorization ensures that the requested activity or object access is possible based on the privileges assigned to the subject.

2.6.2 Autorizační mechanismy

V navazující praktické části práce bude využit autorizační mechanismus řízení přístupu na základě rolí (RBAC), patřící mezi několik základních mechanismů:

- **diskreční řízení přístupu (DAC)**: jinak řečeno řízení přístupu podle vlastního uvážení. Řízení přístupu k objektu provádí jeho vlastník nebo správce, dle vlastního uvážení. Na každém jednotlivém objektu může jeho vlastník nastavit přístup a oprávnění pro vybraného uživatele (nebo skupinu uživatelů), který je v systému identifikován vlastní identitou. Příkladem DAC řízení jsou seznamy řízení přístupů (ACL). Každý objekt má přiřazen vlastní ACL, který popisuje pravidla přístupu. Výhodou DAC je flexibilita při nastavování přístupu, nevýhodou je nemožnost provádět správu DAC centralizovaně. Ostatní popsané mechanismy řízení přístupu jsou nediskrečního typu,
- **povinné řízení přístupu (MaAC)**: všechny objekty v systému musí mít předem přiřazen bezpečnostní štítek. Ten u každého objektu stanovuje stupeň utajení (přísně tajné, tajné, důvěrné…) a kategorii (úroveň řízení, oddělení nebo projekt, pro které je objekt dostupný). Bezpečnostní štítek s klasifikací a kategorií mají i všechny subjekty v systému. Při pokusu o přístup, systém zkontroluje bezpečnostní štítek uživatele (subjektu) a porovná, zda se klasifikace a kategorie shoduje s bezpečnostním štítkem objektu. V případě shody je přístup povolen. MaAC je nejbezpečnějším způsobem řízení přístupu, což je jeho výhodou. Nevýhodou je náročná správa. Správce systému musí na počátku nastavit všechny štítky objektům i subjektům a následně kontinuálně provádět jejich aktualizaci při každé změně,
- **řízení přístupu na základě rolí (RBAC)**: k objektu je řízen přístup na základě přiřazených rolí. Role je skupina uživatelů, kteří mají společné vlastnosti. Členství v roli je přiřazeno uživateli na základě jeho pracovní pozice nebo umístění na oddělení. Přiřazení uživatele do role provádí správce např. na základě organizační struktury. Uživateli není nikdy přiřazen přístup přímo k objektu. Ve chvíli, kdy nastoupí do organizace nový zaměstnanec, např. na pozici „účetní“, je mu přiřazena role pro všechny účetní a tím získá přístup ke všem objektům, na kterých je nastavena skupina odpovídající roli. Uživatel může mít samozřejmě rolí více. RBAC přináší hned několik výhod. Při změně pracovní pozice (např. z účetního na pokladníka) stačí uživateli odebrat původní roli pro účetní a přiřadit mu novou roli pro pokladníky. Tím dojde k zneplatnění všech přístupů, které již k práci nepotřebuje

a získání rolí nových. Kromě efektivní správy je výhodou i zamezení hromadění přístupů. Nevýhodou je nutnost použití více rolí při požadavku na větší granularitu oprávnění. RBAC bývá spojován s řízením přístupů na základě úkolu (TBAC). Účetní může být zařazen do role na základě své pracovní pozice, a navíc i do role zaměřené na určitý pracovní úkon, např. „vyplácení mezd“, která mu zpřístupní další potřebné prostředky organizace,

- **řízení přístupu založené na pravidlech (RuBAC)**: základem řízení je sada pravidel, přidělena objektu, která platí globálně pro všechny přistupující subjekty. Subjektu je udělen přístup, pokud splní alespoň jednu podmínku v sadě pravidel. Příkladem RuBAC řízení je firewall. Při požadavku na komunikaci je procházen seznam pravidel jedno po druhém a při první shodě podmínek s vlastnostmi komunikace je udělen přístup. Pokud žádné z pravidel vlastnostem komunikace nevyhovuje, přístup je odepřen posledním pravidlem, který komunikaci implicitně zakazuje. Výhodou RuBAC je možnost přesněji definovat podmínky přístupu, než je tomu u RBAC, nevýhodou je náročnější správa sady pravidel pro každý objekt,
- **řízení přístupu založený na atributech (ABAC)**: je pokročilá implementace mechanismus řízení přístupu RuBAC. Zatímco princip RuBAC je založen na sadě pravidel, která platí globálně pro všechny uživatele, ABAC používá pro řízení pravidel řadu různých atributů, kterými lze přesně specifikovat podmínky přístupu. Kontrolované atributy se mohou vztahovat k subjektu (pracovní pozice, oddělení, role…), objektu (vlastník, typ, citlivost…), požadované akci (čtení, zápis, smazání…) a prostředí / kontext (čas, lokace, komunikační protokol, síla autentizace…). Výhodou ABAC je vysoká granularita nastavení podmínek řízení přístupu a snadné udělení přístupu novým subjektům na základě přiřazení atributů. Nevýhodou je náročnost prvotní implementace. [54]

2.6.3 Centralizované řízení přístupu k prostředkům v síti

Centralizované řízení přístupu je proces autentizace a případně i autorizace v jediném bodě, společný pro více systémů. Centrální prostředek spravuje omezená skupina lidí na jednom místě, místo na každém systému jednotlivě. To zvyšuje efektivitu i bezpečnost správy. Příklady protokolů využívaných pro centralizované řízení přístupů jsou:

- **Lightweight Directory Access Protocol (LDAP) a adresářové služby**: LDAP je otevřený protokol, používaný pro zabezpečený přístup k adresářovým službám

a jejich správě. I přes jeho dlouhou historii se stále jedná o velice rozšířený a využívaný protokol. LDAP je optimalizován pro velice rychlé vyhledávání i ve velkých databázích a je nezávislý na platformě. Byl původně vyvinut pro OS UNIX, ale díky jeho univerzálnosti se stal standardem pro dotazování adresářových služeb ve většině OS, SW i HW, které podporují centralizované řízení přístupu. Adresářová služba poskytuje databázi údajů identifikující subjekty v síti (např. uživatele, skupiny, zařízení…) a další služby potřebné pro autentizaci a autorizaci. Mezi nejrozšířenější adresářové služby patří Active Directory (AD), proprietární služba vyvinuta firmou Microsoft, [55]

- **Security Assertion Markup Language (SAML) a jednotné přihlášení (SSO)**: SAML je otevřený protokol zajišťující zabezpečenou komunikaci mezi uživatelem, zprostředkovatelem identity (IdP) a zprostředkovatelem služby (SP), pro účely autentizace a autorizace. Na rozdíl od protokolu LDAP, který je využíván ve vnitřní síti organizace, SAML je určen pro použití v internetu. Uživatel se nepřihlašuje přímo do webové aplikace (SP), ale prostřednictvím IdP, na nějž je přesměrován. Po úspěšném ověření, IdP vygeneruje token (SAML tvrzení – zašifrovaný a podepsaný XML dokument), který je předán přes webový prohlížeč k SP a ten po validaci zpřístupní požadované prostředky. SAML je nejrozšířenějším standardem pro SSO. Uživatel je ověřen vůči IdP pouze jednou a získané SAML tvrzení je následně předáno jakémukoliv SP, registrovanému ke stejnému IdP. SAML SSO může být použito pro webové aplikace v internetu i v místní síti,
- **Open Authorization (OAuth)**: je autorizační protokol a samotný nezajišťuje autentizaci. Pro účely autentizace je nad OAuth vybudována autentizační vrstva Open ID Connect (OIDC). OAuth umožňuje klientské aplikaci (klient) získat delegovaný, časově omezený, autorizovaný přístup k chráněným prostředkům uživatele (vlastník zdrojů) na jiném serveru (server zdrojů), aniž by jí byly předány přihlašovací informace uživatele. Při požadavku klienta na přístup k datům na serveru zdrojů je uživatel, tedy vlastník zdrojů přesměrován na autorizační server. Uživatel autorizuje požadovaný přístup a autorizační server předá klientovi přístupový token k serveru zdrojů. Výhodou OAuth je jeho jednoduchá implementace ve webových, desktopových i mobilních aplikacích. Je častěji používán pro sdílení dat uživatele mezi aplikacemi na internetu. Tam kde je potřeba autentizace uživatele do webových aplikaci, je více využíván protokol SAML. [56]

2.6.4 Řízení přístupu k síti (NAC)

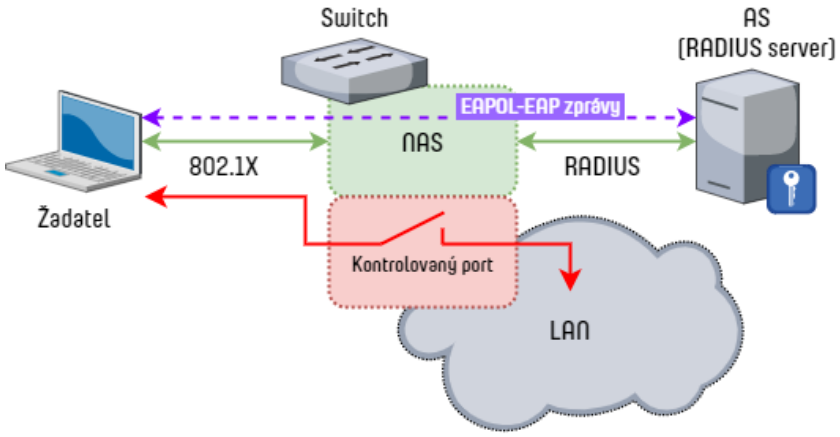
NAC je obecný termín pro řadu technologií používaných k autentizaci a autorizaci uživatelů a zařízení při jejich připojení do sítě, ale také metody a nástroje pro jejich omezení.

Protokoly popsané v předchozích kapitolách jsou převážně využívány pro řízení přístupu k prostředkům, které jsou umístěné v síti. Následující dva protokoly jsou navrženy pro centralizované řízení přístupu do sítě (RADIUS) nebo k síťovým prvkům (TACACS+). Oba poskytují služby autorizace, autentizace, a navíc také účtování (AAA):

- **Remote Access Dial In User Service (RADIUS)**: protokol umožňuje výměnu informací mezi síťovým přístupovým serverem (NAS), který připojuje zařízení uživatele do sítě, a autentizačním serverem (AS). NAS může být např. VPN server, bezdrátový přístupový bod nebo síťový switch s implementovaným protokolem 802.1X. AS je server RADIUS, který provádí autentizaci uživatele, autorizuje jeho přístup, předává NAS konfigurační síťové informace a provádí účtování. Komunikace mezi NAS a RADIUS není kompletně šifrovaná. Zabezpečené je pouze předání hesla. Ostatní údaje lze odposlechnout. RADIUS server může být pro účely autentizace napojen na adresářovou službu protokolem LDAP,
- **Terminal Access Controller Access-Control System Plus (TACACS+)**: jedná se o sadu protokolů, původně určených pro autentizaci a autorizaci uživatelů do UNIX a dalších terminálů a konzolí. V současnosti je využíván převážně pro řízení přístupu při správě síťových zařízení. Výhodou oproti RADIUS protokolu je nezávislé použití jednotlivých AAA funkcí a šifrování celého přenášeného paketu. Nelze jej však použít v rámci implementace 802.1X. [57]

Metodami pro omezení síťových přístupů na základě provedené autorizace je použití segmentace sítě, firewallu (viz předchozí kapitoly) a protokolu 802.1X:

- **IEEE 802.1X**: je protokol pracující na spojové vrstvě, dle ISO/OSI modelu a jeho účelem je vynutit autorizaci ještě před nastavením síťové konfigurace připojovaného zařízení k drátové či bezdrátové síti. Základní komponentou 802.1X je Extensible Authentication Protocol over LAN (EAPOL), který pracuje na síťové vrstvě a zprostředkovává výměnu packetů mezi žadatelem o ověření a jeho poskytovatelem. Dokud není žadatel ověřen, je mu povolena komunikace pouze řídícím kanálem 802.1X na AS a datový kanál je blokován. Po ověření žadatele, je datový kanál povolen (Obr. 8). [58]



Obrázek 8. 802.1X řízení přístupu, upraveno z: [58]

2.6.5 Identity a Access Management (IAM)

IAM je nástroj pro centralizovanou správu identit a přístupů. Proces správy zahrnuje identifikaci osoby, autentizaci a autorizaci pro přístup k aplikacím, systémům nebo sítím. Toho je docíleno přiřazením uživatelských rolí k identitě osoby (systém řízení přístupů RBAC). IAM se skládá ze dvou částí, které jsou spolu úzce spjaty:

- **Identity Management (IdM)**: organizační proces, který zajišťuje, aby uživatelé získaly odpovídající přístup k prostředkům v síti. IdM spravuje celý životní cyklus identity, od nástupu zaměstnance do organizace, po celou dobu jeho působení, až po jeho odchod. IdM spravuje nejen zaměstnance, ale i ostatní osoby s potřebou přístupu do systémů organizace (externí dodavatelé, partneři…),
- **Access Management (AM)**: zajišťuje bezpečnou autentizaci uživatelů a jejich autorizaci v systémech. Další funkce AM je poskytování SSO nebo bezpečného vícefaktorového ověření uživatelů. [59]

2.7 Kryptografie

Kryptografie je technika pro zabezpečení ukládaných nebo přenášených informací tak, aby se o nich dověděli a mohli je použít pouze určení příjemci. V síťové bezpečnosti je kryptografie zásadní technologie. Poskytuje funkce šifrování, digitální podepisování a hashování pro zajištění důvěrnosti, integrity a autentičnosti přenášených informací (viz *1.1.2 CIA triáda*) a autentizaci identit. Základní kryptografické metody jsou:

- **symetrické šifrování**: pro šifrování zprávy je použit stejný šifrovací klíč, jako pro dešifrování. Výhodou symetrického šifrování je jeho rychlost, nevýhodou nutnost

předat bezpečným způsobem šifrovací klíč od odesílatele k příjemci. Široce využívanými algoritmy pro symetrické šifrování jsou Data Encryption Standard (DES) a Advanced Encryption Standard (AES). V síťové bezpečnosti se symetrické šifrování používá např. u IPsec VPN,

- **asymetrické šifrování**: principem asymetrického šifrování je použití páru klíčů, které jsou rozdílné. Jedním klíčem se provádí šifrování a druhým dešifrování, přičemž jeden z klíčů je soukromý (zná ho jen příjemce nebo odesílatel, v závislosti na použití) a druhý je veřejný. Výhodou asymetrického šifrování je, že jeden z klíčů je veřejný a není jej třeba zabezpečeně přenášet mezi komunikujícími stranami. Nevýhodou je větší výpočetní náročnost a tím menší rychlost zpracování. Asymetrické šifrování se v síťové bezpečnosti využívá např. pro digitální podpis nebo distribuci symetrických klíčů. Často používané algoritmy jsou Rivest-Shamir-Adelman (RSA), Digital Signature Standard (DSS), Elliptic Curve Digital Signature Algorithm (ECDSA),
- **hash funkce**: je jednosměrná matematická funkce, používaná pro zajištění integrity dat. Vstupem funkce je libovolně dlouhý blok dat a výstupem je hash hodnota fixní délky. Změna jakéhokoliv bitu ve vstupních datech, způsobí změnu hodnoty hash. Z hash hodnoty nelze zpětně získat původní vstupní data. Využití hash funkce je, kromě ověřovaní autenticity zpráv, např. bezpečné ukládání hesel nebo práce s IPS signaturami při kontrole síťového provozu. [60]

V dnešní době nejpoužívanějším využitím asymetrické a symetrické kryptografie v síťové komunikaci, je protokol TLS. TLS je využíván např. ve webových prohlížečích při komunikaci s internetovými servery, pro e-mailovou komunikaci nebo pro VPN. Pro autentizaci protistran a výměnu symetrického klíče je použita asymetrická kryptografie a pro šifrovaní přenášených dat symetrická.

2.8 Zabezpečení koncového bodu

Koncový bod připojený do podnikové sítě, jakým je např. přenosný počítač uživatele, je častým zdrojem narušení její bezpečnosti. Dle výzkumu společnosti Ponemon Institute [61] byli v roce 2022 zaměstnanci nebo kontraktoři primárním zdrojem vnitřních hrozeb (56 % všech reportovaných incidentů). Zabezpečení koncových bodů je tedy důležitou vrstvou bezpečnostních opatření, kterému je potřeba věnovat náležitou pozornost. I když jsou síťový firewall (FW), antivir (AV) a další funkcionality (webový filtr, aplikační kontrola…)

implementovány na perimetru sítě, je jejich přítomnost důležitá i na koncovém bodu, a to minimálně ze dvou důvodů. Prvním důvodem je doporučená strategie „dual vendor“, kdy je na více vrstvách bezpečnostních opatření implementována stejná funkcionalita, ale jiného výrobce. To vede k vyšší odolnosti proti selhání nebo překonání bezpečnostní funkcionality na jedné z vrstev. Druhým důvodem je fakt, že uživatelé svá zařízení přenášejí a připojují do různých sítí, jejichž zabezpečení je na nižší úrovni, než je v interní podnikové síti. Součástí ochrany koncového bodu je „hardening“ zařízení, kdy uživatel (nebo případný útočník) nemá oprávnění zasahovat do firmware zařízení (např. do UEFI), měnit systémová nastavení OS nebo instalovat nepovolené aplikace. Samozřejmostí je šifrování datového úložiště. [62]

Ochrana koncového bodu bývá v podnikovém prostředí centrálně spravovaná, monitorována a může být zdrojem informací pro účinnější detekci bezpečnostních hrozeb a rychlejší reakci v rámci celé bezpečnostní infrastruktury – někdy nazýváno Cybersecurity Mesh Architecture (CSMA) nebo Security Fabric. [63]

2.9 Bezdrátové sítě

Bezpečnost drátových sítí LAN je podpořena faktem, že pro připojení je vyžadován fyzický přístup k síťovému prvku. U bezdrátové sítě tato bariera odpadá, proto je potřeba věnovat zabezpečení připojení větší úsilí. Původní technický standard pro bezdrátovou komunikaci v lokálních sítích IEEE 802.11, definoval poměrně slabý mechanismus pro zabezpečené připojení, Wired Equivalent Privacy (WEP). Po jeho prolomení definovala Wi-Fi Alliance zabezpečení Wi-Fi Protected Access (WPA), což byl výňatek z tehdy připravovaného dodatku standardu 802.11i. WPA2 již v plné šíři implementuje 802.11i, je také nazýván Robustní bezpečnostní síť (RSN), a WPA3 je jeho vylepšenou náhradou. Specifikace RSN definuje následující služby:

- **autentizace**: ověření uživatele AS a generování dočasných klíčů pro komunikaci bezdrátového klienta (STA) s přístupovým bodem (AP),
- **řízení přístupu**: vynucení autentizačních metod (použití různých autentizačních protokolů v závislosti na typu připojení), zajištění výměny klíčů a řízení směrování zpráv,
- **zajištění důvěrnosti a integrity**: použití kryptografie na úrovní spojové vrstvy modelu ISO/OSI. [64]

Bezpečnost podle standardu IEEE 802.11i se týká pouze komunikace mezi AP a STA. Komunikace od STA dále do sítě musí být zabezpečena na vyšších síťových vrstvách. Iniciální autentizace využívá buď předsdíleného klíče (PSK) nebo protokolu EAPOL v případě použití 802.1X v podnikovém módu WPA. V obou případech je vygenerován hlavní klíč, z kterého jsou následně generovány další klíče potřebné pro komunikaci mezi STA a AP. V případě osobního módu WPA zajišťoval autentizaci mechanismus Temporal Key Integrity Protocol (TKIP) a šifrování algoritmus Rivest Cipher 4 (RC4). WPA2 nahradil již nedostačující TKIP a RC4 mechanismem Cipher Block Chaining Message Authentication Code Protocol (CCMP) a šifrováním AES. WPA3 navíc nahradil zranitelný čtyřcestný „handshake" PSK více bezpečným Simultaneous Authentication of Equals (SAE). WEP a WPA není doporučeno, vzhledem k slabému zabezpečení, dále používat. Použití WPA3 je optimální možnost, avšak pokud je to potřeba, lze použít i WPA2 (některá zařízení v síti nepodporují WPA2). WPA3 je aktuálně nejbezpečnějším bezdrátovým protokolem i přes skutečnost, že již bylo zveřejněno několik bezpečnostních chyb, které lze zneužít k útoku na jeho bezpečnost. [64] [65]

2.10 Vysoká dostupnost

Princip zajištění vysoké dostupnosti byl popsán v kapitole *1.5.1 ISO/IEC 27002*, v odstavci *redundance zařízení pro zpracování informací*. V oblasti síťové bezpečnosti se jedná o redundanci aktivních síťových prvků a zařízení poskytujících síťové služby (DNS, DHCP, AS, NAS, NTP…) zapojováním do stohů nebo klastrů, redundanci jejich napájecích zdrojů, zálohu a redundanci přívodu elektrické energie, zdvojení konektivity k ISP a propojení mezi lokalitami či datacentry (ideálně několik různých poskytovatelů, použití SD-WAN), zdvojení páteřních propojovacích tras a další opatření. Do oblasti zajištění vysoké dostupnosti spadají také opatření popsané v kapitole *2.3.4 Datacentra*. Všechna tato opatření vedou primárně k zabezpečení jednoho z pilířů informační bezpečnosti – dostupnosti informací.

2.11 Monitoring aktivit

V předchozích kapitolách byly popsány opatření jednotlivých vrstev principu obrany do hloubky v oblasti síťové bezpečnosti a související technologie. Po implementaci všech bezpečnostních opatření, dle navrhnuté bezpečnostní strategie, je nezbytné kontinuálně kontrolovat jejich funkčnost a efektivitu. Správným monitoringem aktivit v síti a na všech

připojených zařízeních a systémech lze předcházet bezpečnostním incidentům, případně provádět neprodlená nápravná opatření při jejich vzniku. Na základě monitoringu lze také odhalovat bezpečnostní slabiny a nové hrozby a navrhovat vhodný způsob pro minimalizaci jejich vlivu na síťovou bezpečnost. Ukládání informací z monitorovacích nástrojů poskytuje možnost zpětného auditu, forenzní analýzy provozu, případně zajištění důkazů. Hlavní oblasti bezpečnostního monitoringu sítě jsou:

- **zajištění, sběr, vyhodnocování a ukládání logů v nástroji SIEM**: účelem nástroje Security Information and Event Management (SIEM) je shromažďovat záznamy událostí (logy) z ICT systémů, jejich ukládání, normalizace, vzájemná korelace a aktivní odezva při sepnutí nastavených pravidel. Vzájemné porovnání logů z více systémů umožňuje nalézt souvislosti indikující pokus o narušení bezpečnosti, který by jinak zůstal skrytý,
- **inspekce síťového toku**: síťové toky jsou detailním záznamem o proběhlé komunikaci mezi dvěma síťovými body. Systémy detekce anomálií a analýzy chování sítě (NBAD) umí na základě toků a strojového učení detekovat neobvyklé jevy a odchylky od běžné síťové komunikace. NBAD umožní odhalit bezpečnostní hrozby, které nelze detekovat na základě vyhodnocení logů ani pomocí známých signatur,
- **vyhodnocování chování uživatelů v síti a ICT systémech v nástroji UBA**: User Behavior Analytics (UBA) je nástroj pro vyhodnocování chování uživatelů v systémech ICT. UBA zpracovává vstupní data (např. logy ze systémů) strojovým učením a vytváří profily chování jednotlivých uživatelů napříč systémy v síti. Při zjištění odchylky od naučeného chování zvýší rizikové hodnocení uživatele. Poskytuje tak specialistům IT bezpečnosti další pohled na aktuální stav kybernetické bezpečnosti v organizaci, [1]
- **vyhodnocování bezpečnostních incidentů a včasná reakce pomocí platformy SOAR**: Security orchestration, automation and response (SOAR) je soubor SW nástrojů, které shromažďují data o bezpečnostních hrozbách, vyhodnocují bezpečnostní incidenty a umožňují na ně automatizovaně reagovat. Funkce SOAR se do jisté míry prolíná se systémem SIEM, avšak pro vyhodnocení hrozeb používá strojové učení, umělou inteligenci a umožňuje tak reagovat na zjištěné incidenty automatizovaně, s minimální lidskou účastí. Výhodou SOAR je hlavně rychlejší detekce incidentů a kratší reakční čas, lepší analýza zdrojových dat (lepší pochopení

kontextu bezpečnostních hrozeb) a jednodušší správa (zvýšení produktivity IT bezpečnostních týmů). [66]

Do oblasti bezpečnostního síťového monitoringu patří i systémy popsané v kapitole *2.4.2 IDS / IPS* a nástroje pro sledování stavu infrastruktury v reálném čase, využívající Simple Network Management Protocol (SNMP). Poslední jmenovaný nástroj je využíván převážně pro provozní monitoring a včasnou reakci při selhání některého z ICT systému. Je tedy součástí systému pro zajištění dostupnosti informací.

Obrana do hloubky vrstvením bezpečnostních opatření je účinnou strategií v boji proti útokům na síťovou bezpečnost. Každá z vrstev je důležitá a nezastupitelná. Aby byla obrana účinná, musejí opatření ve všech vrstvách působit společně. Při překonání jedné vrstvy útočníkem dojde k oslabení celkové bezpečnosti, ale nemělo by dojít k jejímu prolomení. Včasná detekce a reakce na incident by měla vést k uvedení stavu bezpečnosti na původní úroveň dříve, než dojde k překonání další vrstvy obrany.

3 HROZBY NARUŠENÍ SÍŤOVÉ BEZPEČNOSTI

Společně s technickým pokrokem a vylepšováním ochrany kybernetické bezpečnosti, narůstá i počet hrozeb a způsobů jejich provedení. Cílem kapitoly je popsat vybrané hrozby působící na síťovou bezpečnost, členěné dle vrstev referenčního modelu ISO/OSI, a popsat způsob jejich mitigace. Vzhledem k velkému množství existujících hrozeb a taktik útočníků, je vždy vybrána jedna typická pro každou vrstvu.

3.1 MITRE ATT&CK®

Pro popis taktik vybraných hrozeb je použita znalostní databáze MITRE ATT&CK®. *„MITRE ATT&CK® je celosvětově dostupná znalostní databáze taktik a technik protivníka založená na pozorování reálného světa. Znalostní báze ATT&CK se používá jako základ pro vývoj specifických modelů hrozeb a metodik v soukromém sektoru, ve státní správě a v komunitě produktů a služeb kybernetické bezpečnosti.“* [3] [67]

3.2 L1 – fyzická vrstva

Fyzická vrstva zajišťuje přenos dat po fyzickém médiu. Hrozbou může být např. úmyslné poškození fyzického média, což způsobí narušení dostupnosti informací. Tomu lze zabránit prostředky fyzické bezpečnosti, viz kapitola *2.2 Fyzická bezpečnost*. V případě překonání fyzické bezpečnosti existuje i hrozba neoprávněného přístupu do sítě:

- **technika ID: T1200, přidání hardware:** jednou z možností, jak získat iniciální přístup, je do sítě připojit vhodně nakonfigurovaný síťový hardware, aby útočník získal do sítě přístup, umožnil odposlech nebo pozměnění síťové komunikace. Takto upravený HW může k síti připojit i osoba, která má z nějakého důvodu povolený přístup do chráněného perimetru organizace (např. úklidová služba),
- **detekce**: detekovat neznámá zařízení v síti lze monitorováním síťových toků, např. nástrojem NBAD, jak bylo popsáno v kapitole *2.11 Monitoring aktivit*,

[3] MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

- **mitigace**: zavedení NAC s použitím protokolu 802.1X, viz kapitola *2.6.4 Řízení přístupu k síti (NAC)*. [68]

3.3 L2 – spojová vrstva

Na spojové vrstvě probíhá komunikace mezi dvěma body ve stejné síti, např. mezi dvěma počítači. Každé síťové rozhraní počítače má unikátní MAC adresu. Aby dva koncové body mohly spolu komunikovat, potřebují znát MAC adresu a IP adresu protistrany. Správnou MAC adresu získají díky protokolu pro překlad adres (ARP). Pokud vysílající bod potřebuje komunikovat na určitou IP adresu v síti, ale nezná MAC adresu příjemce, odešle všesměrový ARP požadavek do sítě. Všechna zařízení v síti požadavek přijmou, a to které má přidělenou požadovanou IP adresu, odešle zpět ARP zprávu odesílateli se svoji MAC adresou. Zařízení, které ARP požadavek odeslalo si získanou MAC adresu protistrany uloží do své mezipaměti. Protože je ARP bezstavový, hrozí jeho zneužití např. pro odposlech síťové komunikace:

- **technika ID: T1557.002, útočník uprostřed – otrávení mezipaměti ARP:** v síti může být umístěno zařízení útočníka, které naslouchá komunikaci v síti a zachytává všesměrové ARP požadavky. Pokud na vyslaný ARP požadavek odpoví odesílateli rychleji než skutečný vlastník IP adresy, získá odesílatel falešnou MAC adresu, kterou si uloží do své mezipaměti. Veškerou následnou komunikaci už bude oběť odesílat na podvrhnutou MAC adresu a útočník může odposlechnout nezabezpečené informace v komunikaci,
- **detekce:** opět lze detekovat neznámá zařízení v síti na základě analýzy síťového toku nebo vyhodnocovat ARP mezipaměť na koncových bodech a zjišťovat anomálie, jako je např. mapování více IP adres na jednu MAC adresu,
- **mitigace:** zapnutí funkcí DHCP Snooping a Dynamic ARP Inspection na síťových přepínačích. Přepínače si na základě DHCP požadavků vytvoří tabulku správných přiřazení IP a MAC adres a zablokují falešný provoz. [69]

3.4 L3 – síťová vrstva

Síťová vrstva umožňuje směrování komunikace mezi jakýmikoliv sítěmi propojenými směrovači, tedy i v internetu. Jednou z mnoha hrozeb, která často působí z prostředí internetu, je odepření služby (DoS), které má za následek narušení dostupnosti informací:

- **technika ID: T1498.001, odmítnutí služby v síti – přímé zaplavení sítě:** útočník se může pokusit zahltit oběť v síti zasláním velkého množství packetů z jednoho

zařízení (útok typu DoS) nebo jen několik packetů, ale z velkého množství různých zařízení, které před tím ovládl (botnet) – distribuovaný útok DoS (DDoS). Pro útok je obvykle použit bezstavový protokol Internet Control Message Protocol (ICMP), pracující na síťové vrstvě. Při DDoS útoku je generované obrovské množství síťového provozu, směrované z botnetu na jediný cíl, který nezvládá na požadavky odpovídat a tím se stane nedostupným i pro legitimní provoz,

- **detekce:** útok typu DoS/DDoS lze detekovat v jeho počátku sledováním síťového toku, opět např. nástrojem NBAD,
- **mitigace:** při detekci útoku lze celý příchozí síťový provoz odklonit na zařízení, které je schopné jeho závadnou část odfiltrovat a legitimní část vracet zpátky příjemci. Vzhledem k tomu, že velikost útoku často přesahuje kapacitu internetového připojení organizace, je potřeba filtraci provozu provádět na vyšší úrovni, u ISP nebo prostřednictvím dodavatelů specializujících se na tuto činnost. [70]

3.5 L4 – transportní vrstva

Komunikace na čtvrté síťové vrstvě mezi koncovými systémy probíhá prostřednictvím protokolů TCP a UDP, které vytváří mezi komunikujícími stranami spojení. Jednotlivá spojení se od sebe rozlišují číslem portu zdroje a cíle, které můžou nabývat hodnot 0-65535. Prvních 1024 portů je přidruženo specifickým serverovým službám a protokolům, např. port 443 je přiřazen Hypertext Transfer Protocol Secure (HTTPS) komunikaci, která je na internetu nejběžněji použita pro zobrazení webového obsahu. [71]

Síťové firewally mají své politiky založeny na kontrole IP adres a portů zdroje a cíle komunikace. Pokud organizace při kontrole síťového provozu spoléhá pouze na firewall, existuje hrozba obcházení nastavených politik:

- **technika ID: T1571, nestandardní port:** útočník může svoji komunikaci skrývat, nebo obcházet politiky na firewallu změnou čísla portu služby. Např. pro HTTPS komunikaci nepoužije port 443, ale 8088,
- **detekce:** prováděním analýzy packetu, nebo síťového toku, lze detekovat neobvyklé chování, které neodpovídá očekávání u služby dané číslem portu,
- **mitigace:** použití systému IPS, který umí dle známých signatur detekovat škodlivý provoz. Dalším opatřením může být nastavení firewall politik tak, aby zamítaly komunikaci na portech, které organizace nepoužívá pro legitimní provoz. [72]

3.6 L5 – relační vrstva

Aplikace prostřednictvím relací udržují spojení mezi komunikujícími stranami. Existují však i samostatné, neaplikační protokoly, které také fungují na relační vrstvě. Mezi takové protokoly patří např. Remote Procedure Call (RPC), Server Message Block (SMB) nebo SOCKS. Všechny jmenované jsou zneužitelné útočníkem:

- **technika ID: T1095, protokol jiné než aplikační vrstvy**: napadený počítač v interní síti může skrytě komunikovat s řídícími C&C servery útočníka např. prostřednictvím protokolu SOCKS. Jedná se o protokol, který zprostředkovává spojení mezi klientem a serverem v internetu přes proxy server. Napadený počítač naváže relaci na řídící server v internetu, který mu následně předává zpět pokyny k vykonání podvratných činností. Protože bývá SOCKS běžně v síti používán, komunikace útočníka může zůstat skryta,
- **detekce**: závadný provoz lze odhalit sledováním neobvyklých síťových toků, ale také na napadené na stanici softwarem pro ochranu koncového bodu. Detekce může probíhat korelací spuštěných procesů na stanici a používaných síťových protokolů. Při použití neobvyklého protokolu dojde k blokování provozu a předání události centrální správě ochrany koncového bodu,
- **mitigace**: vhodnou konfigurací firewallu a proxy serveru tak, aby byla odchozí komunikace do internetu omezena pouze na potřebné porty. Vhodné je také použití IPS. [73]

3.7 L6 – prezentační vrstva

Jednou z funkcí prezentační vrstvy je šifrování. Jak bylo popsáno v kapitole *2.7 Kryptografie*, šifrování zajistí důvěrnost přenášených dat v síti, tzn. obsah komunikace je chráněn před odposlechem. To je dobré v obraně proti odposlouchávacím taktikám útočníka, ale má to i své nevýhody:

- **technika ID T1573.002, šifrovaný kanál – asymetrická kryptografie**: co je u šifrování výhodné pro legitimní komunikaci, to je také dobře využitelné útočníkem pro skrytí jeho činnosti. Zatímco předchozí taktika spoléhala na ukrytí závadné komunikace v běžném síťovém provozu, použití asymetrické kryptografie úplně znemožní běžným kontrolním mechanismům detekovat závadný obsah. Popsanou techniku používá dnes většina malware nebo C&C komunikace,

- **detekce**: detekci lze opět provádět sledováním neobvyklých síťových toků, nekorespondujících s běžnou komunikací, ale účinnější je použití SSL inspekce,
- **mitigace**: číst obsah zašifrované komunikace a odhalit tak podezřelou aktivitu lze v určitých případech použitím SSL inspekce, jak je popsáno v kapitole *2.4.1 Firewall*, ve spojení s IPS nebo anti-malware systémem, který je součástí NGFW. [74]

3.8 L7 – aplikační vrstva

Nejvyšší vrstva ISO/OSI modelu poskytuje mnoho možností uživatelům aplikací, ale i útočníkům. Na sedmé vrstvě pracuje i mnoho zneužitelných síťových protokolů. Aplikační vrstva na jedné straně tvoří rozhraní s nižšími komunikačními vrstvami a na druhé straně rozhraní, pro interakci s uživatelem:

- **technika ID T1566, phishing**: jedná se o velice rozmanitou techniku sociálního inženýrství, která je omezena pouze vynalézavostí útočníka. Základem je oběti elektronicky doručit podvodnou zprávu, vydávající se za zprávu od důvěryhodného odesílatele (banka, zásilková služba, e-shop, nadřízený…). Obsah zprávy většinou vybízí k okamžité reakci, např. kliknutí na odkaz nebo otevření přílohy. Příloha může po otevření spustit škodlivý kód nebo přesměrovat uživatele na podvodnou stránku, stejně jako v případě odkazu ve zprávě,
- **detekce**: filtrování e-mailů na základě vyhodnocení Sender Policy Framework (SPF) a DomainKeys Identified Mail (DKIM), analýza obsahu a hlaviček emailů, vyhodnocení odkazů a příloh ve zprávě,
- **mitigace**: blokování spustitelných příloh, anti-malware kontrola síťového provozu na perimetru i na koncovém bodu, správná konfigurace mailového serveru pro zamítnutí zpráv na základě SPF + DKIM, prevence školením uživatelů. [75]

Pro vybudování dostatečně odolné sítě nestačí pouze pořídit nejrůznější bezpečnostní technologie, ale je nutné znát techniky útočníka a způsoby obrany proti nim. Jedině tak lze bezpečnostní systémy správně nakonfigurovat a plně využít jejich potenciál.

II. PRAKTICKÁ ČÁST

4 NÁVRH SYSTÉMU ŘÍZENÍ PŘÍSTUPU

V první části práce byly položeny teoretické základy síťové bezpečnosti a řízení přístupu. Cílem praktické části práce je, na základě získaných teoretických vědomostí, navrhnout automatizovaný systém řízení přístupu k síťovým prostředkům, který bude spjatý s identitou uživatele. Použitý autorizační mechanismus pro přidělování oprávnění v rámci IAM bude RBAC. Vlastnosti identity budou následně využity pro kontrolu síťového provozu, jejich předáním do firewall politik. Auditní události systému budou vyhodnocovány systémem SIEM.

4.1 Zadání funkčních požadavků a parametrů

Před započetím technického návrhu systému je nezbytné stanovit rámcové zadání, tzn. funkční požadavky na systém a žádané parametry. Zadání vychází z potřeb organizace, kdy je třeba posoudit její:

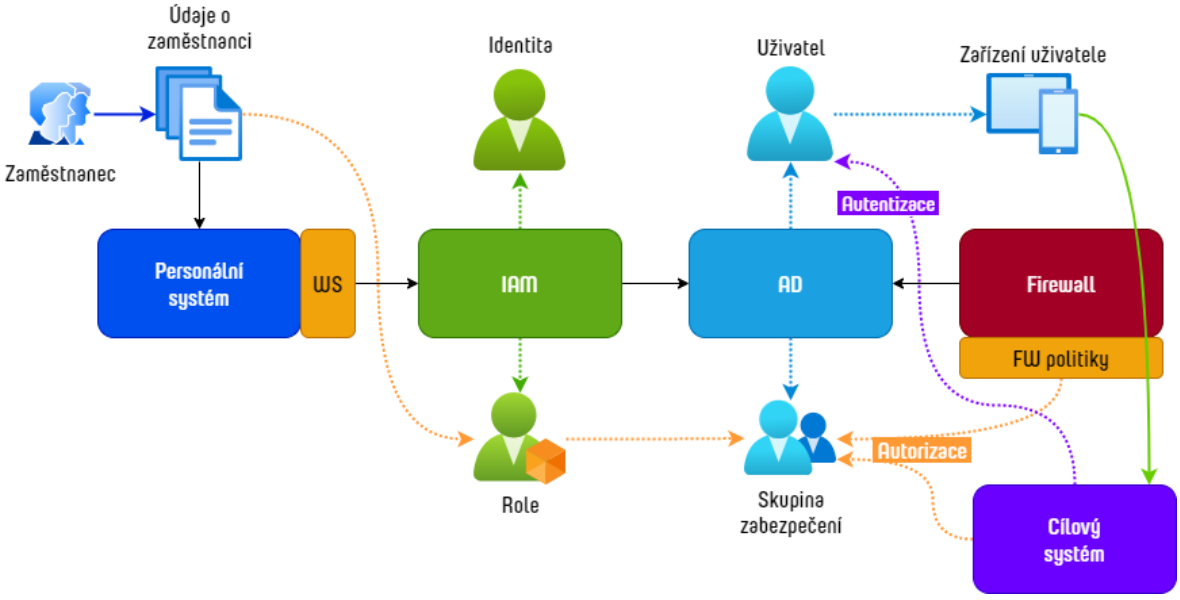
- **zaměření**: různá průmyslová odvětví mají svá specifika,
- **velikost**: důležité pro plánování kapacit navrhovaného systému,
- **legislativní prostředí**: na organizaci mohou být kladeny regulatorní nebo legislativní požadavky,
- **procesy**: pokud navržený systém bude vyžadovat změnu zavedených procesů, musí takové změny efektivitu procesů zlepšit, ne naopak,
- **stávající technické prostředí**: navržený systém by měl reflektovat používané technologie ICT organizace,
- **personální prostředky**: pořízení nového systému má vliv na využití lidských zdrojů v organizaci a schopnost rozšířit znalostní bázi,
- **finanční prostředky**: vynaložené náklady musejí být vzhledem k očekávaným přínosům přiměřené.

Pro účely této práce bude uvažovaná fiktivní organizace s následujícími parametry:

- název organizace: DP Test
- organizace poskytující finanční služby,
- působící lokálně v ČR, má jedno hlavní sídlo a dvě pobočky v různých lokalitách,
- počet zaměstnanců do 1000,
- dostatečné finanční i personální prostředky,
- stávající technické prostředí je popsáno v kapitole *4.2 Předpoklady pro nasazení*.

4.1.1 Business zadání

Údaje o zaměstnanci jsou při jeho přijetí do organizace zadány do personálního systému, zaměstnanci je přiřazena pracovní pozice a místo v organizační struktuře. Údaje zaměstnance jsou automatizovaně přeneseny do IAM, kde je vytvořena jeho digitální identita pro účely centralizovaného řízení přístupů v ICT systémech organizace. IAM automaticky přiřazuje role nově vzniklé identitě uživatele, na základě údajů získaných z personálního systému. Hlavním kritériem pro přidělení role je jeho pracovní pozice. IAM dle přidělených rolí automatizovaně vytváří uživatelský účet v AD a přiřazuje uživatele do skupin zabezpečení. AD je poskytovatelem autentizace a autorizace uživatelů pro ICT systémy. Komunikace uživatele v síti je omezena pouze na systémy, pro které získal uživatel autorizaci v IAM (byla mu pro cílový systém přidělena alespoň jedna role) a to bez ohledu na použité zařízení, připojené do firemní sítě. Přístup do systémů musí být umožněn uvnitř podnikové sítě a prostřednictvím VPN. Celý životní cyklus identity uživatele je automatizovaný, tzn. veškeré změny v pracovním vztahu zaměstnance se automaticky projeví změnou přístupových oprávnění, případně jejich odebráním při ukončení pracovního poměru. Audit přístupů k ICT systémům musí být nezávislý na vlastních auditních záznamech jednotlivých systémů. Tzn. musí být zaznamenán i neúspěšný pokus o síťovou komunikaci, který by nebyl zaznamenán cílovým systémem. Navržené řešení musí být odolné vůči selhání a musí respektovat definované parametry organizace. Zadání je graficky znázorněno na Obr. 9.



Obrázek 9. Blokové schéma business zadání (vlastní)

4.2 Předpoklady pro nasazení

Návrh řešení předpokládá využití stávající ICT infrastruktury organizace, doplněné o systémy pro řízení přístupu. Součástí návrhu řešení je konfigurace systémů tak, aby byly naplněny cíle práce. Vybrané technologie odpovídají charakteru a velikosti zvolené fiktivní organizace. Předmětem práce není popis výběru, pořízení, instalace a uvedení do provozu všech dotčených systémů. Předpoklady pro nasazení řešení jsou:

- funkční personální systém, obsahující data zaměstnanců a organizační strukturu. Datové sestavy pro import zaměstnanců do IAM, jsou přístupné na webové službě (WS) personálního systému,
- funkční doménový řadič organizace s adresářovou službou a certifikační autoritou,
- nakonfigurované servery poskytující síťové služby DNS, DHCP, NTP, RADIUS,
- nakonfigurované aktivní síťové drátové i bezdrátové prvky, podporující centrální správu,
- existující segmentace sítě vč. nakonfigurovaných VLAN na všech síťových zařízeních (detaily viz dále),
- NG firewall s podporou objektů identit v politikách pro řízení síťového provozu,
- síťově propojené lokality a segmenty sítě zakončené na NGFW v sídle organizace,
- koncová zařízení mají OS Microsoft (MS) Windows a macOS, mají nainstalovaný a centrálně spravovaný agent správy koncového bodu a jsou připojena do domény,
- použita serverová virtualizace, servery s OS MS Windows a Linux (distribuce založené na Red Hat Enterprise Linux),
- „on-site“ vývojové prostředí ve vlastním datacentru v sídle organizace, hostované produkční prostředí v datacentru poskytovatele,
- zavedený SIEM pro sběr a vyhodnocení logů,
- odolnost všech systémů proti výpadku,
- zajištěny licence, potřebné pro funkčnost všech uvedených systémů,
- vytvořené technické účty pro přístup k požadovaným službám v síti (*Příloha P VII: Seznam použitých technických účtů*),
- ostatní provozní systémy a služby, které organizace vyžaduje (není zahrnuto v této práci).

Řešení bude postaveno na technologiích a zařízeních vybraných výrobců, avšak principiálně bude přenositelné do jakéhokoliv prostředí, které splňuje popsané předpoklady pro nasazení.

4.2.1 Segmentace sítě

V zadání je vyžadováno blokování sítové komunikace mezi zařízením uživatele a cílovým systémem, pokud nemá uživatel přidělenou žádnou z rolí opravňující přístup. Požadavku lze dosáhnout implementací síťové segmentace, případně mikrosegmentace v případě Zero trust konceptu. Protože omezení síťového provozu v rámci stejného segmentu (směr východ-západ) není vyžadován, bude dostačovat vhodné rozdělení sítě do segmentů, umožňující řídit provoz ve směru sever-jih. Segmenty jsou uzavřeny do logických sítí (VLAN), mezi kterými je směrován a firewallem řízen síťový provoz, viz kapitola *2.3.2 Logické sítě (VLAN)*. Popis síťových segmentů je v tabulce (Tab. 4). Segmentace je zjednodušená, ve fiktivní organizaci jsou vynechány některé sítě, které by v organizaci podobné velikosti a zaměření byly přítomny. Např. servisní sítě pro 802.1X, síť pro zařízení nepodporující 802.1X, síť pro BYOD zaměstnanců, pro tiskárny, audiovizuální a konferenční techniku, VoIP telefonii, systémy fyzické bezpečnosti, kamerový systém a další. Více by byly rozděleny také sítě uživatelů, ať už z důvodu vytvoření menších „broadcast“ domén nebo z důvodů bezpečnostních. Služby a servery by z důvodu odolnosti proti selhání byly rozprostřeny a duplikovány ve více prostředích. Pro účely práce je zjednodušená segmentace dostačující.

Tabulka 4. Segmentace sítě

VLAN ID	Prostředí	Lokalita	Účel	Podsíť
10	Provozní	Sídlo organizace	Management síťových prvků a serverů v LAN	10.0.10.0/24
20			Provozní servery (PROVOZ)	10.0.20.0/24
30			Aplikační servery (APP)	10.0.30.0/24
40			Databázové servery (DB)	10.0.40.0/24
50			Bezpečnostní servery (ITB)	10.0.50.0/24
60			Uživatelé – sídlo	10.0.60.0/23
65			Uživatelé – VPN	10.0.65.0/22
300			Spojovací síť provozní FW	172.30.0.0/29
70			Management síťových prvků a serverů v DMZ	10.0.70.0/24
80			DMZ	10.0.80.0/24
90			Síť pro hosty	10.0.90.0/24

VLAN ID	Prostředí	Lokalita	Účel	Podsíť
100		Pobočka 1	Management síťových prvků v pobočce 1	10.0.100.0/24
110			Uživatelé – pobočka 1	10.0.110.0/24
120		Pobočka 2	Management síťových prvků v pobočce 2	10.0.120.0/24
130			Uživatelé – pobočka 2	10.0.130.0/24
140	Vývojové	Sídlo organizace	Aplikační servery (APP)	10.0.140.0/24
150			Databázové servery (DB)	10.0.150.0/24
160			Testovací servery (TEST)	10.0.160.0/24
170			DMZ	10.0.170.0/24
180	Produkční	Hostované datacentrum	Management síťových prvků a serverů v LAN	10.0.180.0/24
190			Aplikační servery (APP)	10.0.190.0/24
200			Databázové servery (DB)	10.0.200.0/24
210			Management síťových prvků a serverů v DMZ	10.0.210.0/24
220			DMZ	10.0.220.0/24
301			Spojovací síť produkční FW	172.30.0.8/29

4.3 Síťová topologie

Schéma sítě v příloze *P I: Přehledový síťový diagram* znázorňuje logické rozmístění serverů a systémů v jednotlivých síťových segmentech. Vyobrazené přepínače s označením *VLAN ID: [číslo]* jsou virtuální, rozprostřené mezi několik fyzických přepínačů, jejichž management je umístěný v různých VLAN. Pro účely ověření funkčnosti je celé řešení postavené ve virtualizovaném testovacím prostředí. V následujících oddílech jsou popsány požadavky na síťovou komunikaci jednotlivých služeb řešení.

4.3.1 Základní síťové služby

Základní síťové služby poskytují přidělování IP adres zařízením, překlad doménových názvů na IP adresy a synchronizaci času. Požadavky na dostupnost základních služeb viz tabulka (Tab. 5).

Tabulka 5. Požadavky na základní síťové služby, data čerpána z: [71]

Služba	Poskytuje	Port služby	Dostupné pro
Přidělování IP adres a síťové konfigurace	DHCP server *dhcp.dp-test.cz*	UDP/67	Všechna zařízení v rámci VLAN a pro DHCP relay z ostatních VLAN
Překlad inerních doménových názvů	Interní DNS server *dns.dp-test.cz*	UDP/53 TCP/53	Všechna zařízení v interní síti i v ostatních lokalitách připojených VPN, transfer zón
Překlad ostatních doménových názvů	Externí DNS server *dns.my-isp.cz*	UDP/53 TCP/53	Přeposílání DNS požadavků, transfer zón
Synchronizace času	NTP server / Doménový řadič *ntp.dp-test.cz dc.dp-test.cz*	UDP/123	Všechna zařízení v interní síti i v ostatních lokalitách připojených VPN

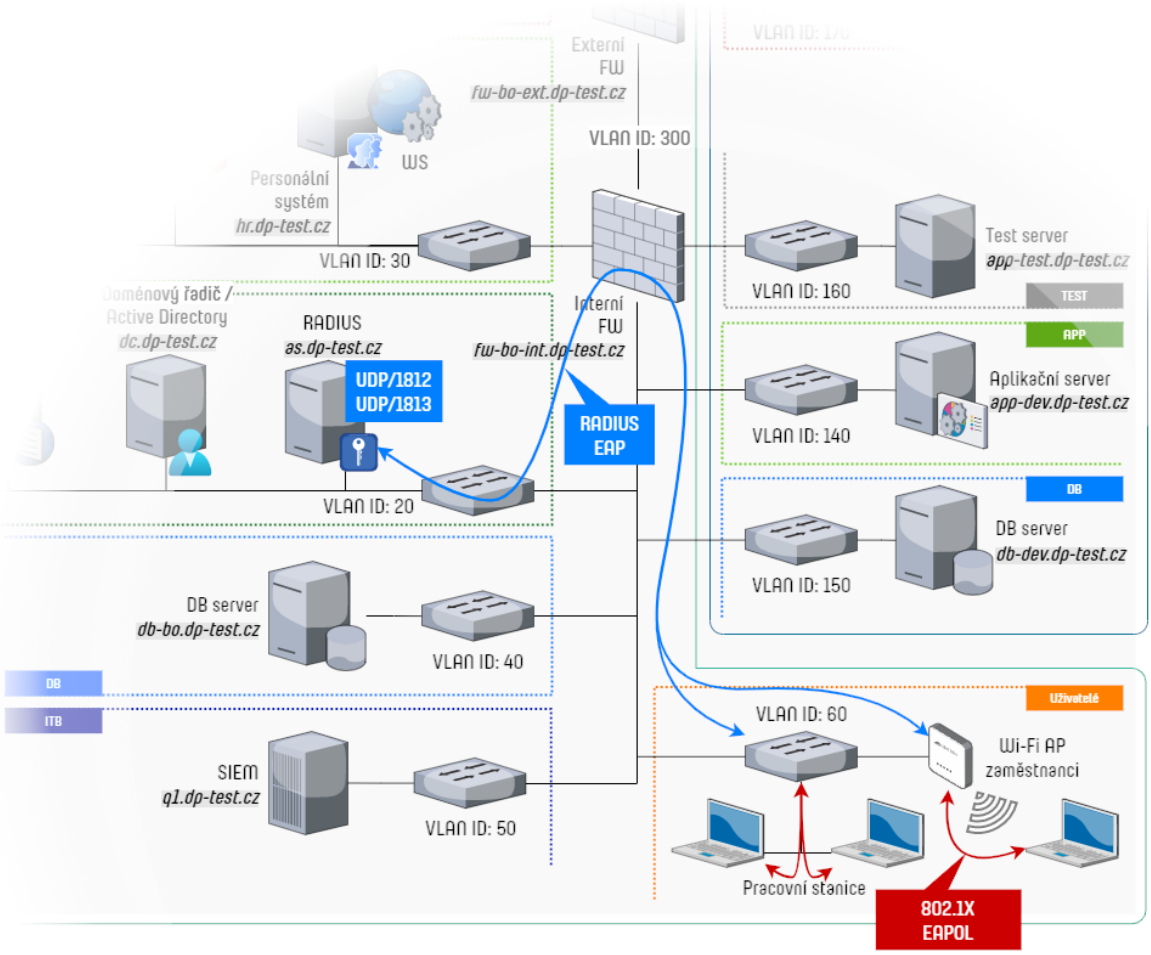
4.3.2 Autentizace, autorizace a doménové politiky

Autentizace a autorizace probíhá na více úrovních. První úrovní je NAC pro připojení koncových zařízení uživatelů do interní sítě a jejich umístění do správné VLAN. Realizováno je protokoly 802.1X a RADIUS, jak bylo popsáno v kapitole *2.6.4 Řízení přístupu k síti (NAC)* a jak je znázorněno na obrázku (Obr. 10). Druhou úrovní je ověřování uživatelů a technických účtů ve všech systémech, vůči AD. AD je součástí řadiče domény, který poskytuje řadu dalších funkcí pro správu domény a připojených objektů (Tab. 6).

Tabulka 6. Síťové požadavky pro autentizaci a autorizaci, data čerpána z: [71]

Služba	Poskytuje	Port služby	Dostupné pro
NAC	NAS (přepínač, AP podporující 802.1X)		Koncová zařízení uživatelů připojována drátově / bezdrátově k síti
	RADIUS server *as.dp-test.cz*	UDP/1812 UDP/1813	NAS
Autentizace a autorizace LDAP/S	AD na doménovém řadiči *dc.dp-test.cz*	TCP/389 TCP/636	Všechna zařízení a systémy v interní síti i v ostatních lokalitách připojených VPN
Autentizace, autorizace	Doménový řadič	TCP/88 TCP/135	Všechna zařízení v interní síti i v ostatních lokalitách

Služba	Poskytuje	Port služby	Dostupné pro
Kerberos, doménové politiky (RPC, SMB)	*dc.dp-test.cz*	TCP/445 TCP/ 49152-65535	připojených VPN, připojená do MS Windows domény



Obrázek 10. NAC – 802.1X a RADIUS (vlastní)

4.3.3 Fortinet Single Sign-On (FSSO) a SSL VPN

Systém jednotného přihlášení je tvořen produkty Fortinet – FortiClient, FortiGate, FortiAuthenticator a adresářovou službou AD. SSO funkcionalita je rovněž použita pro předávání identity uživatele firewallu a je funkční při připojení koncového zařízení v interní sítí přímo i prostřednictvím VPN. Ověření identity během procesu VPN připojení je doplněno druhým faktorem, formou potvrzení „push“ notifikace ve spárované mobilní aplikaci FortiToken Mobile. Souhrn komunikace pro zajištěni SSO je popsán v tabulce (Tab. 7) a znázorněn v příloze *P II: Fortinet Single Sign-On a SSL VPN diagram*. Detailně je celý SSO proces a předávání identity popsán v následujících kapitolách.

Tabulka 7. Fortinet Single Sign-On síťové požadavky, data čerpána z: [76]

Služba	**Poskytuje**	**Port služby**	**Dostupné pro**
SSO dotazování / autentizace	FortiAuthenticator *fac.dp-test.cz*	TCP/8000	FortiGate v interní síti a VPN
		TCP/8001	FortiClient v interní síti a VPN
NAC (RADIUS) pro VPN		UDP/1812 UDP/1813	FortiGate v interní síti
Přijetí potvrzení push notifikace		TCP/443	FortiToken Mobile ve všech sítích
SSL VPN	FortiGate *fw-bo-int.dp-test.cz*		FortiClient, webový prohlížeč, ve všech sítích
Autentizace	AD *dc.dp-test.cz*	TCP/389 TCP/636	FortiAuthenticator FortiGate

4.3.4 Propojení lokalit

Sídlo organizace je s pobočkami a hostovaným datacentrem propojeno „site-to-site“ IPsec VPN tunely, vybudovanými mezi interními firewally, viz tabulka (Tab. 8).

Tabulka 8. Síťové požadavky na propojení lokalit, data čerpána z: [71]

Služba	**Poskytuje**	**Port služby**	**Dostupné pro**
IPsec VPN (ESP, IKE, NAT-T)	Interní FW v každé lokalitě *fw-bo-int.dp-test.cz* *fw-pd-int.dp-test.cz* *fw-br1/2.dp-test.cz*	IP/50 UDP/500 UDP/4500	FW v lokalitách navzájem, dostupné přes internet

4.3.5 Centrální správa koncových bodů

Každé zařízení uživatele má nainstalován SW FortiClient, který je centrálně spravovaný serverem FortiClient Endpoint Management Server (EMS). Síťová komunikace je popsána v tabulce (Tab. 9).

Tabulka 9. Síťové požadavky pro správu koncových bodů, data čerpána z: [76]

Služba	**Poskytuje**	**Port služby**	**Dostupné pro**
Centrální správa koncového bodu	FortiClient EMS *ems.dp-test.cz*	TCP/8013 TCP/10443 TCP 445	Všechny koncové body s FortiClient SW ve všech sítích
Připojení FortiOS		TCP/8015	FortiGate

4.3.6 Audit systémů a zasílání výstrah

Auditní logy ze všech systémů a zařízení jsou přeposílány protokolem syslog do SIEM, kde jsou ukládány a vyhodnocovány. Auditní logy z produktů Fortinet mohou být nejprve zaslány na server FortiAnalyzer, kde jsou zpracovány a následně přeposlány do SIEM. Na základě vyhodnocení logů jsou zasílány výstrahy elektronickou komunikací (Tab. 10).

Tabulka 10. Síťové požadavky na zasílání auditních logů, data čerpána z: [71] [76]

Služba	Poskytuje	Port služby	Dostupné pro
Sběr, ukládání a vyhodnocování logů	SIEM *q1.dp-test.cz*	TCP/514 UDP/514	Všechny systémy a zařízení v interní síti i v propojených lokalitách VPN
	FortyAnalyzer *faz.dp-test.cz*		FortiClient FortyAuthenticator FortiGate FortiClient EMS
Odesílání e-mailových výstrah	SMTP server *smtp.dp-test.cz*	TCP/25	SIEM, případně další servery

4.3.7 Přístup uživatelů a správců k systémům

Všechny systémy a aplikace, které jsou součástí navrhovaného systému, poskytují webové grafické uživatelské rozhraní (Web GUI). V některých případech je dostupná i SSH konzole, viz Tab. 11.

Tabulka 11. Síťové požadavky na uživatelský přístup k systémům

Služba	Poskytuje	Port služby	Dostupné pro
Web GUI (HTTPS)	IAM *iam.dp-test.cz* Personální systém *hr.dp-test.cz* FortiGate (SSL VPN web portál) *fw-bo-int.dp-test.cz* FortiAuthenticator *fac.dp-test.cz* Podnikové aplikace	TCP/443	Všechny uživatele v interní síti, ve všech lokalitách, přes VPN a případně z internetu přes reverzní proxy
	Všechna síťová zařízení, systémy a jednotlivé aplikace řešení		Správce v interní síti a přes SSL VPN
SSH konzole	IAM *iam.dp-test.cz*	TCP/22	Správce v interní síti a přes SSL VPN

Služba	Poskytuje	Port služby	Dostupné pro
	Linuxové servery Síťová zařízení		

4.3.8 Ostatní komunikace

V modelové síti jsou pro doplnění umístěny další servery – souborové, databázové, aplikační a proxy. Služby na serverech mohou komunikovat na různých portech a pro účely této práce není potřeba uvádět kompletní výčet požadavků na jejich síťovou komunikaci. Většina komunikace v síti probíhá šifrovaně a předpokládá se funkční systém distribuce interních i veřejných certifikátů. Další detaily komunikace v síti budou upřesněny v následujících kapitolách.

4.3.9 Přehled IP adresace

V příloze *P III: Soupis hostitelů a IP adres* je uveden výčet IP adres zařízení a serverů, umístění v síti, překlad doménových jmen a jejich popis.

4.4 Personální systém

Personální systém stoji v navrhovaném řešení na počátku celého procesu řízení přístupu k ICT na základě identity uživatele. Pro přehlednost jsou v tabulce (Tab. 12) použité pojmy vztahující se k osobě pracující pro organizaci.

Tabulka 12. Osoba – související pojmy

Pojem	Popis	V systémech
Osoba	Fyzická osoba obecně, bez bližšího určení	Není relevantní
Pracovník	Jakákoliv osoba, vykonávající práci pro organizaci, bez ohledu na typ pracovního vztahu. Může se jednat o zaměstnance, brigádníka, kontraktora nebo externistu	Není relevantní
Zaměstnanec	Fyzická osoba, mající hlavni pracovní poměr v organizaci	Personální systém, IAM
Brigádník	Fyzická osoba, mající s organizací uzavřenou dohodu o provedení práce nebo o pracovní činnosti	Personální systém, IAM
Pracovní pozice	Vymezuje druh činností pracovníka, kterou vykonává pro organizaci	Personální systém, IAM

Pojem	Popis	V systémech
Pracovní místo	Určuje pozici pracovníka v organizační struktuře	Personální systém, IAM
Organizační jednotka	Sdružuje více pracovních míst nebo jiných organizačních jednotek, většinou podle oddělení, úseku, divize atp.	Personální systém, IAM
Organizační struktura	Hierarchické uspořádání organizačních jednotek	Personální systém, IAM
Kontraktor	Zaměstnanec jiné organizace, která poskytuje outsourcing pracovní síly na základě obchodní smlouvy	IAM
Externista	Zaměstnanec jiné organizace, která poskytuje outsourcing služeb na základě obchodní smlouvy	IAM
Identita	Digitální identita pracovníka, spravována systémem IAM	IAM
Uživatel	Uživatel ICT systému. Uživatelem může být jakýkoliv pracovník, který má v libovolném systému vytvořený uživatelský účet	V kterémkoliv ICT systému
Účet	Účet vytvořený v ICT systému, umožňující přístup. Účet může být uživatelský nebo technický	V kterémkoliv ICT systému

Zaměstnanec je personálním oddělením přijat na specifikovanou pracovní pozici. Pracovník personálního oddělení (personalista) zadává do personálního systému osobní a pracovní údaje o zaměstnanci, a přiřazuje mu pracovní místo, ke kterému se váže pracovní pozice. Správně vyplněné údaje jsou důležité pro správnou funkčnost celého řešení. Můžeme zároveň tvrdit, že personální systém je zdrojem pravdy pro ostatní navázané systémy a jakákoliv změna údajů provedena v personálním systému se projeví i v ostatních systémech.

4.4.1 Vymezení přenášených údajů

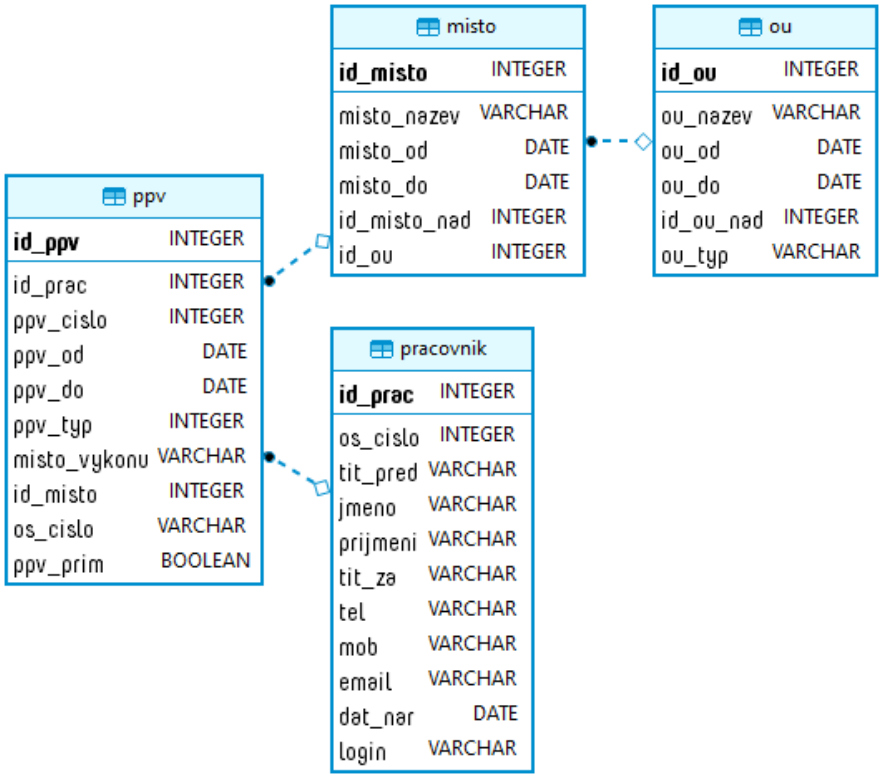
Do IAM není účelné přenášet veškeré údaje obsažené v personálním systému, ale pouze takové, které jsou využitelné pro identifikaci pracovníka a pro řízení jeho oprávnění v systémech:

- **nacionále pracovníka**: jméno, příjmení, tituly, datum narození,
- **kontaktní údaje**: pracovní telefon, pracovní e-mailová adresa, místo výkonu práce,
- **identifikační údaje**: přiřazené přihlašovací jméno, osobní číslo,

- **údaje o pracovní pozici**: název, přiřazené pracovní místo,
- **údaje o pracovním místě**: název, nadřazené pracovní místo, přiřazená organizační jednotka

4.4.2 Datové sestavy

Údaje určené pro přenos je nutné strukturovat tak, aby bylo v IAM možné ze získaných dat vytvořit unikátní identitu každého pracovníka a zrekonstruovat celou organizační strukturu. K tomuto účelu byly vytvořeny čtyři provázané datové sestavy (Obr. 11), popsané



Obrázek 11. ER diagram datových sestav personálního systému (vlastní)

Ve sloupci *„Klíč“* je v tabulce vždy uvedeno, zda se jedná o primární klíč (PK) nebo klíč cizí (FK), s odkazem na zdroj: sestava[atribut].

Tabulka 13. Datová sestava „pracovnik“

Název atributu	Popis	Klíč
id_prac	Unikátní identifikátor pracovníka	PK
os_cislo	Přidělené osobní číslo	
tit_pred	Titul před jménem	

Název atributu	Popis	Klíč
jmeno	Jméno	
prijmeni	Příjmení	
tit_za	Titul za jménem	
tel	Telefon	
mob	Mobilní telefon	
email	E-mail	
dat_nar	Datum narození	
login	Unikátní přihlašovací jméno	

Tabulka 14. Datová sestava „ppv“

Název atributu	Popis	Klíč
id_ppv	Unikátní identifikátor pracovního vztahu	PK
id_prac	Unikátní identifikátor pracovníka	FK: pracovnik[id_prac]
os_cislo	Přidělené osobní číslo	
ppv_cislo	Pořadové číslo pracovního vztahu	
ppv_od	Počátek platnosti pracovního vztahu	
ppv_do	Konec platnosti pracovního vztahu	
ppv_typ	Typ pracovního úvazku	
ppv_prim	Označení primárního pracovního úvazku	
misto_vykonu	Místo výkonu práce	
id_misto	Unikátní identifikátor pracovního místa	FK: misto[id_misto]

Tabulka 15. Datová sestava „misto“

Název atributu	Popis	Klíč
id_misto	Unikátní identifikátor pracovního místa	PK
misto_nazev	Název pracovního místa	
misto_od	Počátek platnosti pracovního místa	

Název atributu	Popis	Klíč
misto_do	Konec platnosti pracovního místa	
id_misto_nad	Unikátní identifikátor pracovního místa nadřízeného	
id_ou		FK: ou[id_ou]

Tabulka 16. Datová sestava „ou“

Název atributu	Popis	Klíč
id_ou	Unikátní identifikátor organizační jednotky	PK
ou_kod	Kód organizační jednotky	
ou_nazev	Název organizační jednotky	
ou_od	Počátek platnosti organizační jednotky	
ou_do	Konec platnosti organizační jednotky	
id_ou_nad	Unikátní identifikátor nadřazené organizační jednotky	
ou_typ	Typ organizační jednotky	

4.4.3 Webová služba

Datové sestavy jsou vytvářeny databázovým pohledem a vystaveny webovou službou dostupnou na adrese: https://hr.dp-test.cz/ws/.

4.5 Správa identit – CzechIdM

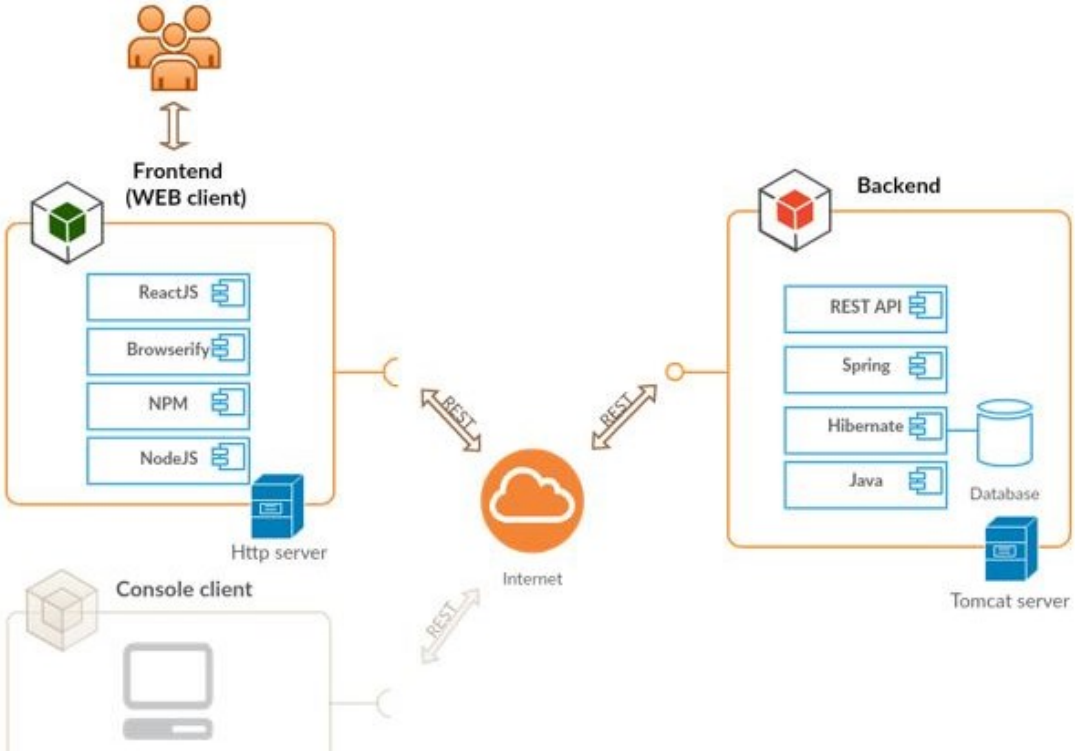
Pro IAM roli v navrhnutém řešení byl vybrán SW nástroj CzechIdM – Identity Manager od české společnosti BCV solutions. CzechIdM je vydáván pod svobodnou licencí (MIT license) a jedná se o otevřený systém, nabízející kompletní správu identit, plnou automatizaci jejich životního cyklu a detailní audit všech událostí. [77]

Základní funkce IAM, které poskytuje CzechIdM jsou:

- správa životního cyklu uživatelských identit,
- řízení přístupu na základě rolí,
- vytváření automatických rolí,
- „provisioning“ (zajištění) / „deprovisioning“ uživatelských účtů,
- synchronizace uživatelů mezi systémy,
- autentizace a autorizace uživatelů,

- systém jednotného přihlášení,
- federovaná správa identit,
- rozhraní RESTful API,
- detailní auditování. [77]

CzechIdM poskytuje webové rozhraní pro správu a také pro vlastní obsluhu uživatelů. Webové rozhraní komunikuje s „backendem“ aplikace přes RESTful API, které je možné využít také pro integraci s dalšími systémy (Obr. 12).



Obrázek 12. Architektura CzechIdM [77]

4.5.1 Životní cyklus identity v IAM

Založením zaměstnance v personálním systému dojde k automatickému vytvoření digitální identity uživatele v IAM. Identita externisty nebo kontraktora je vytvořena přímo v IAM správcem nebo může být vytvořena prostřednictvím API z jiného systému. Identita uživatele zůstává neaktivní až do data počátku platnosti pracovního vztahu zaměstnance nebo jiného pracovníka, dle platné smlouvy. K identitě jsou přiřazeny role definované v automatických rolích. Ve chvíli aktivace identity, jsou na základě přiřazených rolí vytvořené uživatelské účty v propojených systémech a nastavena odpovídající oprávnění. Pokud uživatel potřebuje další role, může si o ně ve webovém rozhraní IAM požádat sám, nebo o role požádá jeho nadřízený. V IAM je pro schválení žádosti o přidělení role nastaven pracovní postup

(popsáno dále). Zaměstnanec během svého působení v organizaci může měnit pracovní pozice. Každá taková změna provedená v personálním systému je synchronizována do IAM a automatické role změní role přiřazené k identitě. Správce IAM může kdykoliv provést audit přidělených rolí a iniciovat žádost o jejich přidání nebo odebrání. Na konci platnosti pracovního vztahu zaměstnance nebo při ukončení spolupráce s se smluvním pracovníkem, dojde k automatické deaktivaci identity uživatele a odebrání rolí. V propojených systémech poté dojde k deaktivaci uživatelských účtů, odebrání oprávnění a případně i k odstranění účtů. Životní cyklus identity je znázorněn na Obr. 13.

Obrázek 13. Životní cyklus identity (vlastní)

4.5.2 Pracovní postupy pro schvalování žádostí

Každá žádost o přidělení role podléhá schválení podle nastaveného pracovního postupu (workflow). Ve workflow (a v celém systému IAM) vystupuje několik základních aktérů:

- **uživatel**: kterýkoliv pracovník, mající v IAM vytvořený profil. Má do IAM přístup, může si zobrazit přidělené role, podávat vlastní žádosti o přidělení nových rolí, změnu nebo odebrání stávajících rolí, měnit své heslo, zobrazit svůj profil, vedoucího, pracovní pozice a jejich detaily, zobrazit své žádosti a jejich stav a další uživatelské funkce,
- **vedoucí**: uživatel, který je dle organizační struktury nadřízený jiným uživatelům. Má stejné možnosti jako běžný uživatel, navíc může provádět stejné činnosti i u všech uživatelů, kteří jsou jeho podřízení (kromě změny jejich hesla) a může schvalovat žádosti o přidělení nebo změnu rolí podřízených uživatelů, pokud je tak role nastavena,
- **garant**: má oprávnění stejná, jako běžný uživatel, ale má navíc možnost schvalovat žádostí o role do aplikací, za které je zodpovědný. Může se jednat o vlastníka aktiva, nebo je mu tato zodpovědnost delegována.

Další účastníci procesů v IAM mohou být definování rolí, např. helpdesk, security a další. CzechIdM disponuje detailním nastavením oprávnění pro většinu existujících funkcí, díky tomu lze vytvořit IAM role se specifickými oprávněními. Zvláštní IAM rolí je Administrátor s oprávněním spravovat celý IAM bez omezení.

Workflow pro schvalování žádostí lze ovlivnit globálně v konfiguraci systému a nastavením parametru „kritičnost“ u každé role. Pracovní postupy dle nastavení kritičnosti jsou popsány v tabulce (Tab. 17).

Tabulka 17. Workflow dle kritičnosti role

Kritičnost	Schvaluje
0	Žádost nevyžaduje schválení, je přiřazena ihned po podání žádosti
1	Žádost schvaluje nadřízený uživatele
2	Žádost schvaluje garant aplikace
3	Žádost schvaluje uživatel s přiřazenou IAM rolí: Security

Workflow je možné definovat vlastní a přidělení role podmínit např. schválením na více úrovních.

4.5.3 Napojené systémy

Po schválení žádosti o přidělení, nebo změnu role, dochází k vlastní realizaci v napojených systémech. Propojení IAM a cílových systémů se provádí prostřednictvím konektorů. Seznam podporovaných konektorů je dostupný on-line, v dokumentaci výrobce: https://wiki.czechidm.com/devel/documentation/adm/systems/connectors [78].

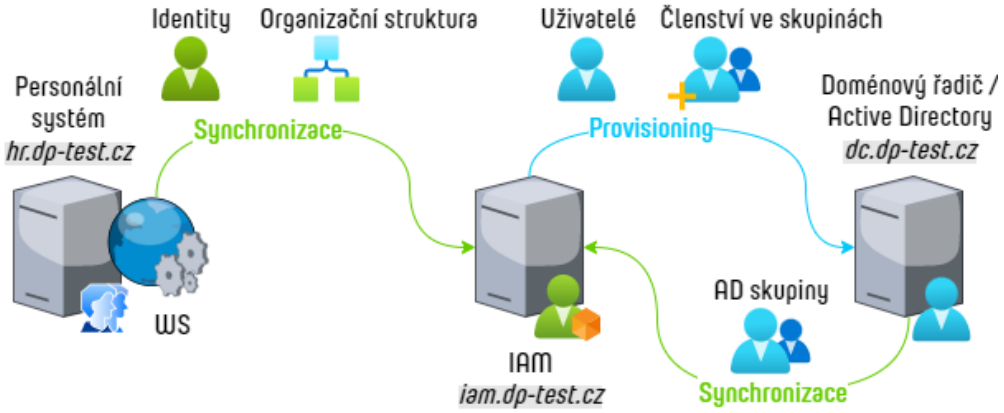
Po napojení systému do IAM lze provádět provisioning uživatelů a jejich oprávnění:

- vytvoření / odebrání uživatelského účtu v cílovém systému,
- aktivace / deaktivace účtu,
- přiřazení / odebrání uživatele ve skupinách zabezpečení,
- přiřazení / odebrání licence…

Opačným směrem lze z napojeného systému do IAM např.:

- synchronizovat uživatele a organizační strukturu (personální systém),
- synchronizovat skupiny zabezpečení (vytvořit role v IAM),
- získávat informace o uživatelích…

Pro účely této práce bude IAM napojen dvěma konektory – do personálního systému a do Active Directory (Obr. 14).



Obrázek 14. IAM – napojení systémů (vlastní)

Většina systémů a aplikací umožňuje některý ze způsobů napojení, ať už jsou provozovány on-site nebo v cloudovém prostředí. Datová výměna mezi aplikacemi v cloudu je nejčastěji

uskutečněna prostřednictvím API, přesto ale existují výjimky, kdy je aplikace uzavřena, nebo API není veřejně poskytováno. Pro takové případy CzechIdM nabízí možnost, přiřazovat role tzv. virtuálním systémům. Po schválení požadované role nedojde k automatickému provisioningu do cílové aplikace. Místo toho je zaslána e-mailová notifikace správci aplikace (realizátor) s pokyny k vytvoření uživatele a nastavení požadovaných oprávnění. Realizátor po provedení ruční konfigurace v cílové aplikaci potvrdí v IAM realizaci.

4.5.4 Databázový výměník s personálním systémem

Databázový výměník, který běží na stejném serveru jako IAM, transformuje data získaná z WS do vhodné podoby. Parametry připojení k WS personálního systému jsou:

- **Url**: adresa WS (https://hr.dp-test.cz/ws/),
- **User**: technický účet pro připojení k webové službě (iam-hr),
- **Password**: heslo technického účtu,
- **Dataset**: název sestavy (pracovnik, ppv, místo, ou).

Každý den jsou pravidelně, spouštěným skriptem, načítány změny v personálním systému a upravovány hodnoty v databázovém výměníku (provádí rozdílovou synchronizaci). Výměník obsahuje položky, z nichž IAM načítá údaje do atributů identit, kontraktů a organizací a slouží tedy jako zdroj dat. Načtené položky jsou ukládány do databáze (DB) „vymenik“ (Obr. 15) do tabulek a pohledů dle popisu v tabulce (Tab. 18). V pohledech jsou data vhodně upravena pro načítání do IAM, zpracování a uložení v hlavní DB.

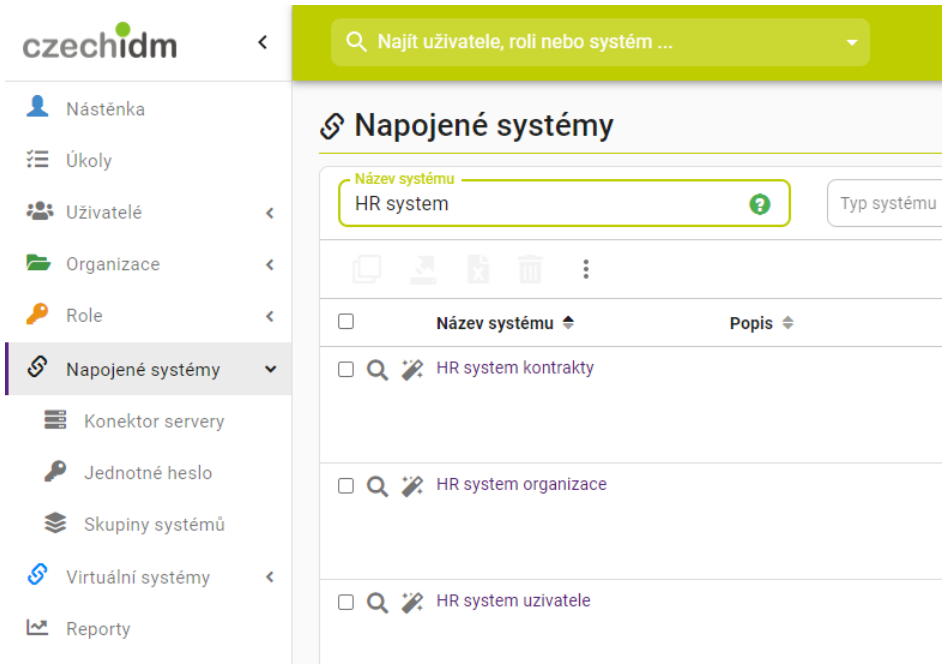
```
vymenik=# \dt+
                          List of relations
 Schema |         Name          | Type  |    Owner    |  Size   | Description
--------+-----------------------+-------+-------------+---------+-------------
 public | organizacni_jednotky  | table | vymenik | 41 kB   |
 public | ppv                   | table | vymenik | 208 kB  |
 public | pracovni_mista        | table | vymenik | 111 kB  |
 public | zamestnanci           | table | vymenik | 198 kB  |
(4 rows)

vymenik=# \dv+
                          List of relations
 Schema |      Name       | Type |    Owner    |  Size   | Description
--------+-----------------+------+-------------+---------+-------------
 public | ppv_not_deleted | view | vymenik | 0 bytes |
 public | v_org_structure | view | vymenik | 0 bytes |
(2 rows)
```

Obrázek 15. Databázový výměník (vlastní)

Tabulka 18. Tabulky a pohledy databázového výměníku

Popis	Sestava person. systému	Tabulka výměníku	Pohled výměníku
Identita uživatele	pracovnik	zamestnanci	
Kontrakty uživatele	ppv	ppv	ppv_not_deleted
Pracovní místo uživatele	misto	ppv pracovni_mista	ppv_not_deleted v_org_structure
Organizační jednotky	ou	organizacni_jednotky	v_org_structure

Výměník je do IAM napojen pomocí tří konektorů typu Database Table Connector (Obr. 16).



Obrázek 16. Napojení databázového výměníku do IAM (vlastní)

Základními konfiguračními parametry pro připojení k výměníku jsou:

- **Host**: název databázového serveru (localhost),
- **Port**: port, na kterém databázová služba naslouchá (5432),
- **User**: název technického účtu s oprávněním čtení z databáze (iam-db),
- **User Password**: heslo technického účtu,
- **Database**: název databáze výměníku (vymenik),
- **Table**: název tabulky (např. zamestnanci, ppv…),
- **Key Column**: unikátní identifikátor řádku tabulky (id),

- **Change Log Column (sync)**: atribut určující poslední změnu záznamu, pro potřeby rozdílové synchronizace (last_update_time).

Mapování a případná úprava atributů pro každý konektor je popsána v příloze *P V: Mapování atributů DB výměníku*.

4.5.5 Webové grafické rozhraní a API

Uživatelům a správcům systému IAM je dostupné webové grafické rozhraní, které umožňuje intuitivní práci a správu funkcionalit, popsaných v předchozích kapitolách. Základní popis Web GUI je uveden v příloze *Příloha P IV: Popis webového grafického rozraní IAM*.

IAM může být cenný zdroj informací o uživatelích, jejich vlastnostech a přidělených rolích pro další podnikové aplikace. Např. lze efektivně vyčítat organizační strukturu nebo identity uživatelů obohacené o další údaje. Veškeré informace IAM vystavuje na svém aplikačním rozraní (API), dostupném na adrese: https://iam.dp-test.cz/idm/api.

4.6 Adresářová služba

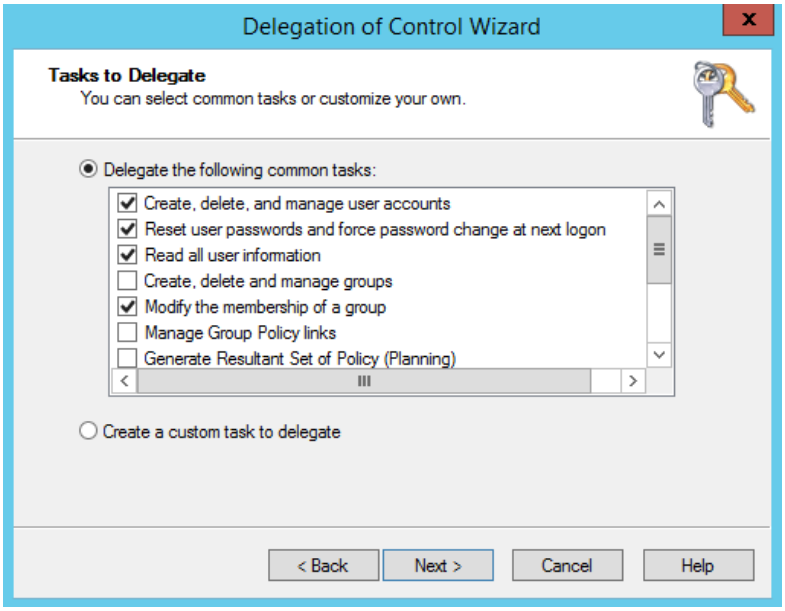
Součástí doménového řadiče (dc.dp-test.cz) je adresářová služba Active Directory, vůči které jsou autentizováni a autorizováni uživatelé do ICT systémů organizace. Uživatelské účty zakládá a spravuje IAM, stejně jako členství ve skupinách zabezpečení. Konfigurace AD je následující:

- název domény: dp-test.cz,
- technický účet pro IAM s právem zápisu do AD: CN=iam-ad,OU=DPT-Accounts,DC=dp-test,DC=cz,
- organizační jednotky (OU) pro objekty účtů, skupin a počítačů s delegovaným oprávněním pro technický účet iam-ad (Tab. 19),
- potřebná oprávnění, delegovaná pro technický účet iam-ad (Obr. 17).

Tabulka 19. Seznam OU v AD domény dp-test.cz

Účel	Základní organizační jednotka	Oprávnění pro účet iam-ad
Uživatelské účty	OU=DPT-Users,DC=dp-test,DC=cz	Ano
Technické účty	OU=DPT-Accounts,DC=dp-test,DC=cz	Ne
Skupiny zabezpečení Distribuční skupiny	OU=DPT-Groups,DC=dp-test,DC=cz	Ano

Účel	Základní organizační jednotka	Oprávnění pro účet iam-ad
Koncová zařízení uživatelů	OU=DPT-Computers,DC=dp-test,DC=cz	Ne
Servery	OU=DPT-Servers,DC=dp-test,DC=cz	Ne



Obrázek 17. Delegace oprávnění pro technický účet (vlastní)

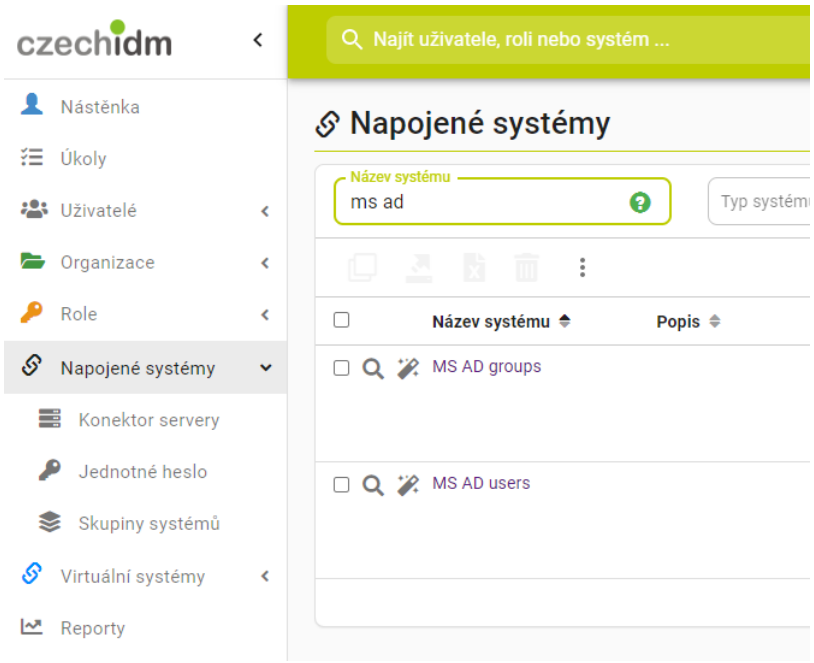
4.6.1 Konektor AD

IAM může spravovat libovolný atribut uživatelského účtu v AD prostřednictvím „WinRM + AD Connector“ konektorů (Obr. 18). Členství uživatele v AD skupinách je spravován atributem „member“.

V konektoru je definována konfigurace pro připojení k AD. Základními konfiguračními parametry jsou:

- **Server host name**: název serveru doménového řadiče (dc.dp-test.cz),
- **Server port**: port, na kterém AD služba naslouchá (636),
- **Faiover**: názvy serverů záložních doménových řadičů,
- **Principal**: název technického účtu pro připojení k AD (iam-ad),
- **Principal password**: heslo technického účtu,
- **Root suffixes**: OU, ve kterém chceme spravovat uživatelské účty (OU=DPT-Users,DC=dp-test,DC=cz),

- **User search scope**: hodnota určuje, zda chceme spravovat objekty pouze v daném OU (container) nebo i v podřízených OU (subtree),
- **Entry object classes**: třídy objektů, které chceme spravovat,
- **Base contexts for user entry searches**: stejné, jako Root suffixes (OU=DPT-Users,DC=dp-test,DC=cz),
- **Base contexts for group entry searches**: OU, ve kterém chceme spravovat skupiny (OU=DPT-Groups,DC=dp-test,DC=cz).



Obrázek 18. Napojení AD konektory do IAM (vlastní)

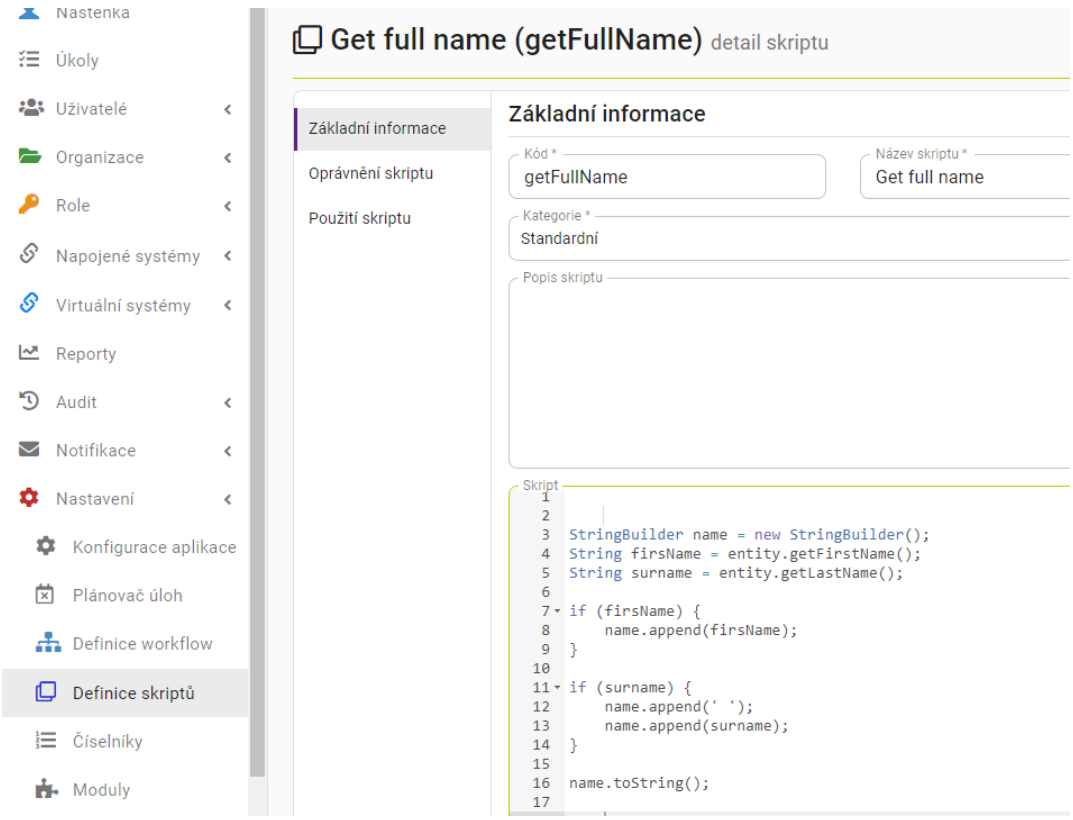
Mapování atributů je znázorněno v příloze *P VI: Mapování atributů AD*. Konektor „MS AD users“ je použit k propisování (provisioningu) údajů z IAM do AD a konektor „MS AD groups“ k synchronizaci skupin z AD do IAM.

Přímo mapované atributy pro provisioning z IAM do AD jsou pouze:

- firstName, AD atribut: givenName,
- email, AD atribut: mail a mailNickname,
- username, AD atribut: sAMAccountName,
- lastName, AD atribut: sn.

Všechny ostatní atributy jsou dopočítávány dle logiky popsané ve skriptech, které zaručí správné dosazení hodnoty, případně její smazání při deaktivaci identity. Příkladem může být AD atribut „displayName“, který se standardně skládá z jména a příjmení uživatele. V nastavení mapování je v poli „Transformace do systému“ volán skript „getFullName“,

umístěný v definici skriptů. Ve skriptu jsou podmínky kontrolující existenci hodnot „firstName“ a „lastName“ a funkce pro jejich spojení do jednoho řetězce (Obr. 19).



Obrázek 19: Skript getFullName (vlastní)

4.7 Vznik identity uživatele

Na vzorovém zaměstnanci bude ukázán, krok po kroku, proces založení jeho digitální identity v IAM synchronizací z personálního systému.

4.7.1 Založení zaměstnance do personálního systému

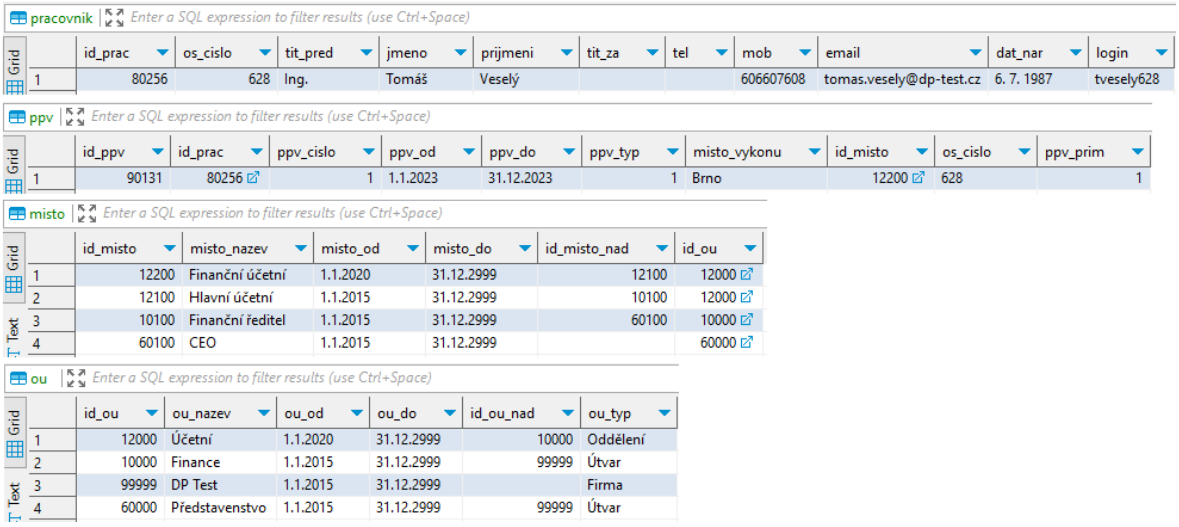
Předpokládejme fiktivního zaměstnance, dle tabulky (Tab. 20). Zaměstnanec Tomáš Veselý nastoupil na pozici „Finanční účetní“ na účetním oddělení. Všichni zaměstnanci na tomto oddělení mají mít oprávnění:

- pro čtení i zápis na sdílený disk \\fs.dp-test.cz\uctarna,
- do modulu „Účetnictví“ na aplikačním serveru ve vývojovém prostředí app-dev.dp-test.cz,
- přijímat e-maily zaslané na distribuční skupinu uctarna@dp-test.cz,
- využívat firemní Wi-Fi,
- připojit se vzdáleně prostřednictvím VPN.

Tabulka 20. Údaje o zaměstnanci v personálním systému

Položka	**Hodnota**
Jméno	Tomáš
Příjmení	Veselý
Osobní číslo	628
Login	tvesely628
Datum narození	6. 7. 1987
Mobil	606607608
E-mail	tomas.vesely@dp-test.cz
Název pracovní pozice	Finanční účetní
Zařazení v org. struktuře	DP TEST – Finance – Účetní – Finanční účetní
Nastoupil	1. 1. 2023
Konec platnosti prac. poměru	31. 12. 2023
Místo výkonu práce	Brno
Typ pracovního úvazku	Hlavní pracovní poměř

Personální systém pro IAM vystaví na webové službě sestavy s daty zaměstnance a jeho pracovního úvazku (Obr. 20).



pracovnik

	id_prac	os_cislo	tit_pred	jmeno	prijmeni	tit_za	tel	mob	email	dat_nar	login
1	80256	628	Ing.	Tomáš	Veselý			606607608	tomas.vesely@dp-test.cz	6. 7. 1987	tvesely628

ppv

	id_ppv	id_prac	ppv_cislo	ppv_od	ppv_do	ppv_typ	misto_vykonu	id_misto	os_cislo	ppv_prim
1	90131	80256	1	1.1.2023	31.12.2023	1	Brno	12200	628	1

misto

	id_misto	misto_nazev	misto_od	misto_do	id_misto_nad	id_ou
1	12200	Finanční účetní	1.1.2020	31.12.2999	12100	12000
2	12100	Hlavní účetní	1.1.2015	31.12.2999	10100	12000
3	10100	Finanční ředitel	1.1.2015	31.12.2999	60100	10000
4	60100	CEO	1.1.2015	31.12.2999		60000

ou

	id_ou	ou_nazev	ou_od	ou_do	id_ou_nad	ou_typ
1	12000	Účetní	1.1.2020	31.12.2999	10000	Oddělení
2	10000	Finance	1.1.2015	31.12.2999	99999	Útvar
3	99999	DP Test	1.1.2015	31.12.2999		Firma
4	60000	Představenstvo	1.1.2015	31.12.2999	99999	Útvar

Obrázek 20. Datové sestavy personálního systému (vlastní)

Pro kontrolu přenesených dat se připojíme SSH konzolí k IAM a databázi „vymenik“ a provedeme několik databázových dotazů:

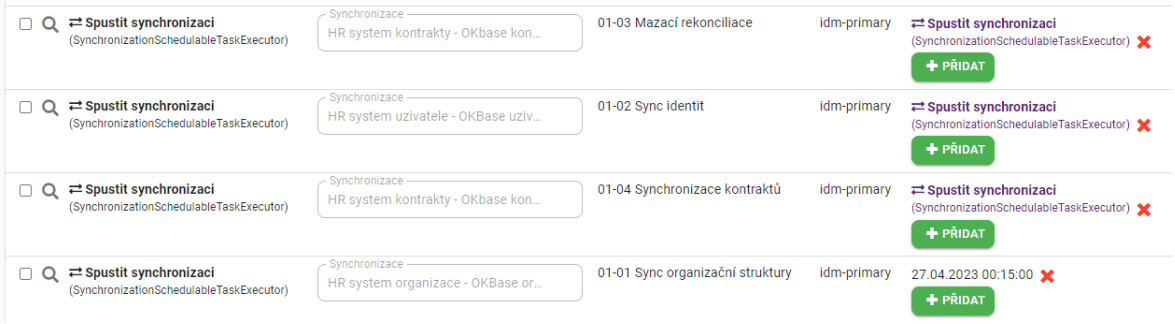
- SELECT * FROM zamestnanci WHERE id='80256';
- SELECT * FROM ppv_not_deleted WHERE id_zam='80256';
- SELECT * FROM pracovni_mista WHERE id='12200';
- SELECT * FROM v_org_structure WHERE id='12000';

Porovnáme výsledek (Obr. 21) s daty v sestavách.

```
   vymenik=# SELECT * FROM zamestnanci WHERE id='80256';
   id   | jmeno | prijmeni | titul_pred | titul_za | telefon |   mobil   |          mail           |
--------+-------+----------+------------+----------+---------+-----------+-------------------------+
 80256 | Tomáš | Veselý   | Ing.       |          |         | 606607608 | tomas.vesely@dp-test.cz |


 osobni_cislo |  ldap_ucet   |     datum_naroz     | deleted |      last_update_time
--------------+--------------+---------------------+---------+----------------------------
 628          | tomas.vesely | 1987-07-06 00:00:00 |         | 2023-04-26 17:21:38.313618
(1 row)

vymenik# SELECT * FROM ppv_not_deleted WHERE id_zam='80256';
  id    | id_zam | osobni_cislo |     platnost_od     |     platnost_do     | cislo_uvazku | primarni |
--------+--------+--------------+---------------------+---------------------+--------------+----------+
 90131 | 80256  | 628          | 2023-01-01 00:00:00 | 2023-12-31 00:00:00 | 1            | t        |

 id_prac_mista | id_evid_stavu | deleted |      last_update_time      |  nazev_pozice   | misto_vykonu_prace
---------------+---------------+---------+----------------------------+-----------------+--------------------
 12200         | 1             | f       | 2023-04-26 17:21:39.224952 | Finanční účetní | Brno
(1 row)

vymenik=# SELECT * FROM pracovni_mista WHERE id='12200';
  id   |     nazev      |     platnost_od     |     platnost_do     | id_utvaru | id_nadraz_prac_mista |
-------+----------------+---------------------+---------------------+-----------+----------------------+
 12200 | Finanční účení | 2020-01-01 00:00:00 | 2999-12-31 00:00:00 | 12000     | 12100                |

 deleted |      last_update_time
---------+----------------------------
 f       | 2023-04-26 17:21:40.202659
(1 row)

vymenik=# SELECT * FROM v_org_structure WHERE id='12000';
   id   | nazev  |     platnost_od     |     platnost_do     | id_nadraz |      last_update_time      |
--------+--------+---------------------+---------------------+-----------+----------------------------+
 12000 | Účetní | 2020-01-01 00:00:00 | 2999-12-31 00:00:00 | 10000     | 2023-04-26 17:21:40.759009 |

 deleted |     typ_objektu
---------+----------------------
 f       | organizacni_jednotka
(1 row)
```

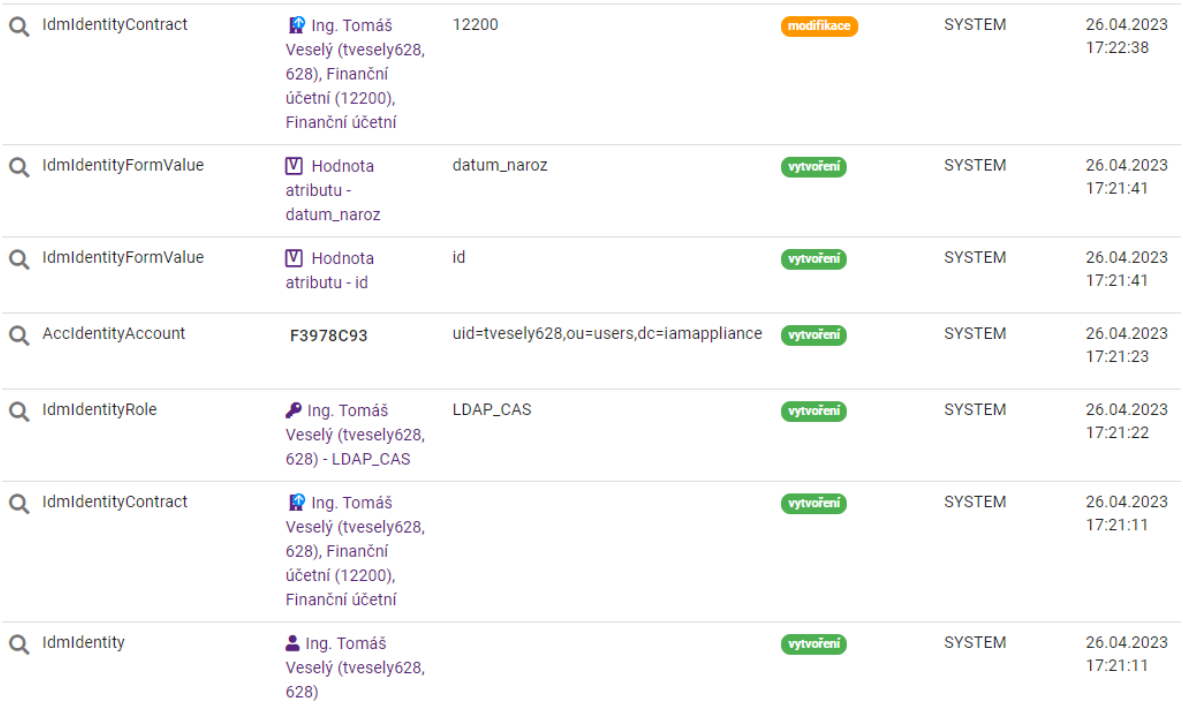
Obrázek 21. Databázové dotazy do výměníku (vlastní)

Po synchronizaci datového výměníku jsou spuštěny plánované synchronizační úlohy. Nastavení synchronizace se provádí přímo v DB konektorech, kde je také uložena časová značka poslední synchronizace a detailní logy všech proběhlých synchronizací. To je užitečné při investigaci synchronizačních problémů. Konfiguraci plánování spuštění synchronizačních úloh lze najít v nastavení IAM, v menu „Plánování úloh“, společně s auditními záznamy spuštěných úloh (Obr. 22).



Obrázek 22. Plány spuštění synchronizací s databázovým výměníkem (vlastní)

Audit poskytuje i identita uživatele (Obr. 23). Každá operace vytvoření nebo úpravy identity uživatele, je tedy detailně auditovaná během všech zúčastněných procesů v IAM.



Obrázek 23. Ukázka z auditu vytvoření identity (vlastní)

4.8 Přiřazení rolí uživateli

Uživatel by měl dle business zadání automaticky získat všechny potřebné role, které mu zaručí přístup a oprávnění ve vybraných aplikacích. Vhodným způsobem je vytvoření „balíčku“ rolí, který je uživateli přiřazen dle jeho pracovního zařazení. Lze si vybrat, zda má být jeho pracovní zařazení vyhodnoceno dle umístění jeho pracovního místa v organizační struktuře, nebo dle názvu pracovní pozice.

4.8.1 Typy rolí

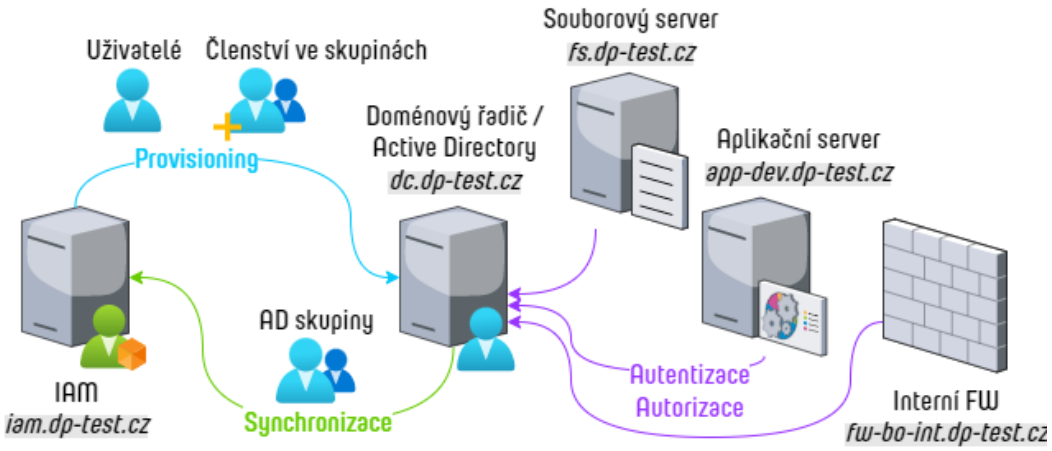
V IAM existuje několik typů rolí, které můžeme rozlišit podle způsobu jejich použití:

- **IAM role**: role, která nastavuje uživateli oprávnění v rámci samotného IAM (nemá vliv na oprávnění v jiných systémech). Např. uživatel, administrátor, helpdesk… Každý uživatel, kterému je v IAM vytvořena identita, automatický získává roli s uživatelským oprávněním,
- **role napojených systémů**: skupiny oprávnění nebo zabezpečení, které jsou vytvořeny v napojených systémech a do IAM se synchronizují (např. role AD skupin). Po přiřazení role uživateli v IAM se účet uživatele automaticky stává členem skupiny na napojeném systému,
- **role virtuálních systémů**: role vytvořené v IAM, přiřazené virtuálním systémům (viz kapitola *4.5.3 Napojené systémy)*. Po přiřazení role uživateli, musí realizátor provést ruční konfiguraci na cílovém systému,
- **business role**: „balíček“ několika rolí, uskupených podle zadaných kritérií. Kritériem může být pracovní pozice uživatele, která určuje potřebu přístupu do vybraných systémů a s definovanými oprávněními. Další kritéria mohou být např. účast na konkrétním projektu nebo potřeba vykonávat nějaký proces. Business role může obsahovat kterýkoliv předchozí typ role,
- **automatická role**: výše popsané role mohou být uživatelům přiřazovány automaticky. Automatické role jsou v IAM definovány pomocí podmínek, které mohou porovnávat informace získané z identity uživatele.

4.8.2 Konfigurace rolí

Uživateli budou v IAM přiřazovány role pro cílové systémy, vytvořené ze synchronizovaných AD skupin. Cílové systémy tak nejsou přímo napojené na IAM, ale využívají služeb AD pro autentizaci a autorizaci uživatelů, zatímco IAM přiřazuje uživatelům členství v AD skupinách (Obr. 24).

Skupinu v AD musí oprávněný správce vytvoř ručně, dle zadání (globální / univerzální skupina zabezpečení, distribuční skupina…). Synchronizací AD skupin do IAM dojde k automatickému vytvoření rolí. Synchronizace skupin se podobně, jako synchronizace personálního systému nastavuje v konfiguraci konektoru a její spuštění v plánovači úloh.



Obrázek 24. Napojení cílových systémů (vlastní)

Po vytvoření role v IAM následuje její konfigurace. Konfigurační možnosti jsou:

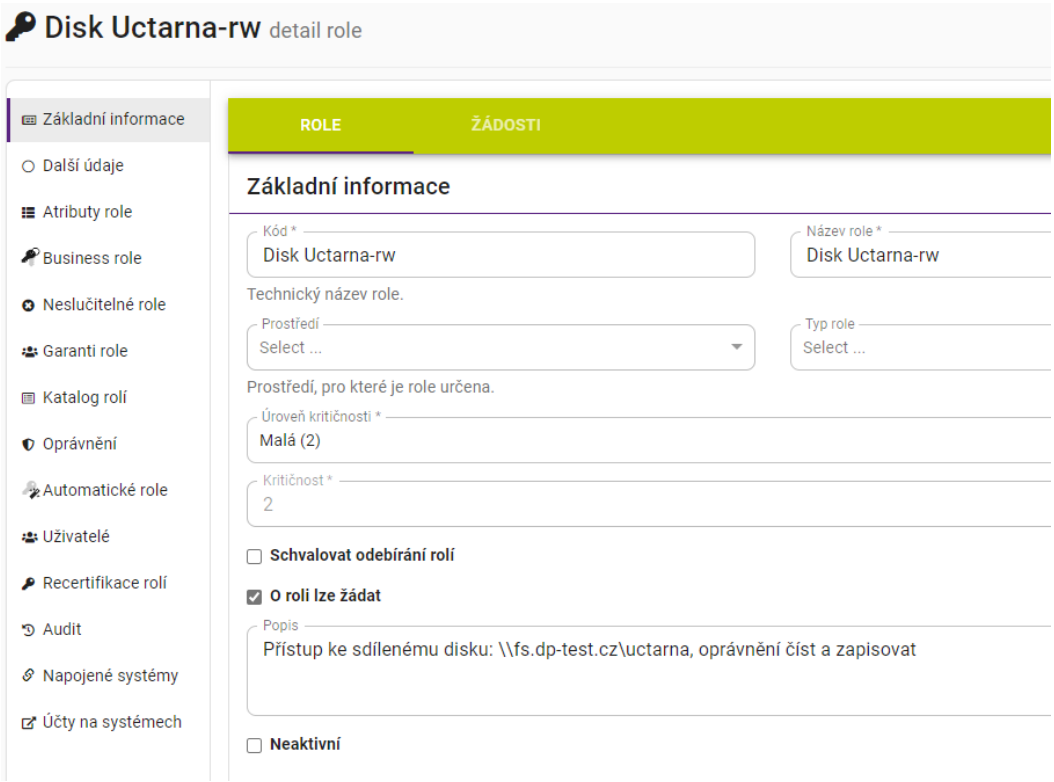
- nastavení úrovně kritičnosti (Tab. 17),
- vynucení schvalování odebíraných rolí,
- povolení o roli žádat,
- nastavení stavu role (aktivní / neaktivní),
- určení garanta role (kdo bude schvalovat žádosti o přidělení role, pokud je nastavena úroveň kritičnosti 2),
- vytvoření business role,
- vytvoření automatické role,
- nastavení prostředí, typu role, dodatečných atributů, neslučitelných rolí a další (v této práci nebude využito).

Základní nastavení rolí bylo provedeno dle Tab. 21. Ukázka konfigurace role na obrázku (Obr. 25).

Tabulka 21. Základní nastavení rolí

Název role	Krit.	Schval. odebrání	Povol. žádat	Aktiv.	Garant
Disk Uctarna-rw	2	Ne	Ano	Ano	Role: IAM – Hlavní účetní
APP-Ucetnictvi-dev	2	Ne	Ano	Ano	Role: IAM – Hlavní účetní
uctarna@dp-test.cz	2	Ne	Ano	Ano	Role: IAM – Hlavní účetní
DP-test-Wi-Fi	3	Ne	Ne	Ano	Role: IAM – IT Security
DP-test-VPN	3	Ne	Ne	Ano	Role: IAM – IT Security

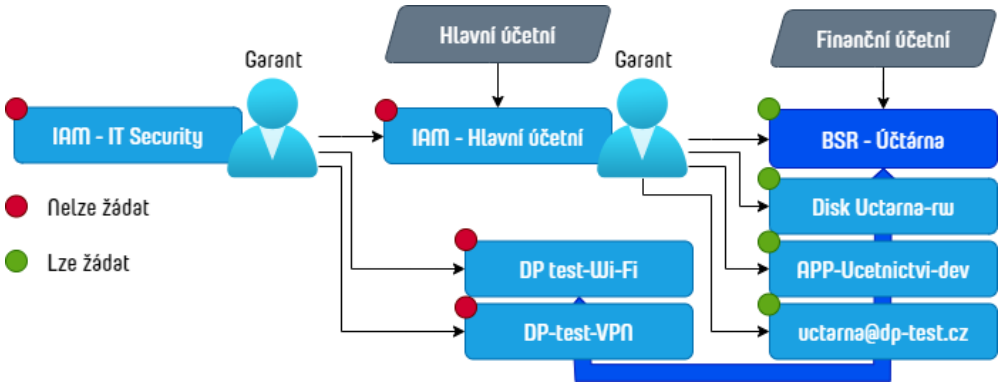
Garant prvních tří rolí je dán IAM rolí „Hlavní účetní“. O přístup na Wi-Fi a VPN nelze samostatně žádat.



Obrázek 25. Konfigurace role (vlastní)

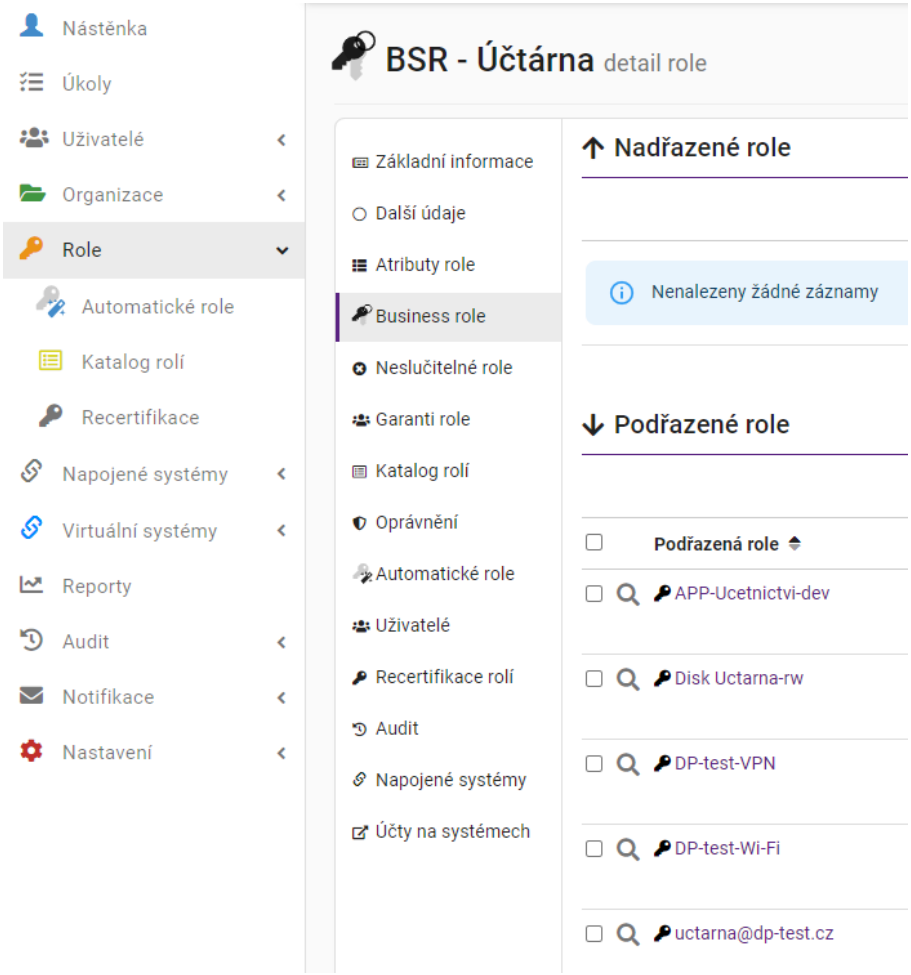
4.8.3 Vytvoření business role

Business role se bude jmenovat „BSR – Účtárna“ a bude obsahovat všechny role uvedené v tabulce (Tab. 21). Přidělována má být automaticky všem zaměstnancům s pracovní pozicí, spadající do oddělení účtárny a půjde o ni zažádat i manuálně. Garantem pro schvalování bude zaměstnanec s automaticky přidělenou rolí „IAM – Hlavní účetní“, dle pracovní pozice, bez možnosti manuální žádosti (Obr. 26).



Obrázek 26. Diagram business role „BSR – Účtárna“ (vlastní)

Konfigurace business role se provádí přidáním podřízených rolí ve formuláři „Business role“ v nastavení role (Obr. 27).



Obrázek 27. Konfigurace business role (vlastní)

4.8.4 Vytvoření automatické role

Hlavním požadavkem business zadání je celý proces automatizovat. Business roli nechceme primárně přidělovat na základě schválení manuální žádosti, ale automaticky. Pro tento účel využijeme funkce automatických rolí. Konfiguraci automatické role lze provést přímo v nastavení role. Existují dvě možnosti, jak automatickou roli vytvořit:

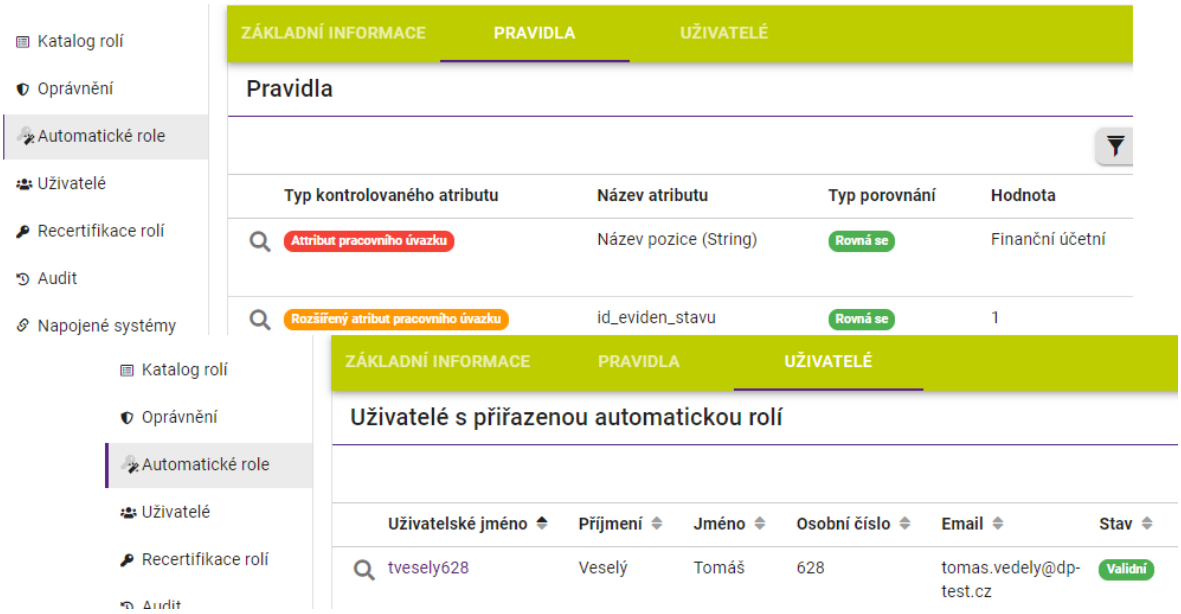
- **dle organizační struktury**: role se přiřadí organizační jednotce a nastaví se způsob šíření (bez šíření, nahoru, dolů),
- **na základě atributů**: lze vytvořit pravidla, kombinující atributy identity anebo pracovního úvazku, podmínky a hodnoty.

Využijeme druhou možnost a vytvoříme automatickou roli na základě atributů (Tab. 22).

Tabulka 22. Podmínky automatické role

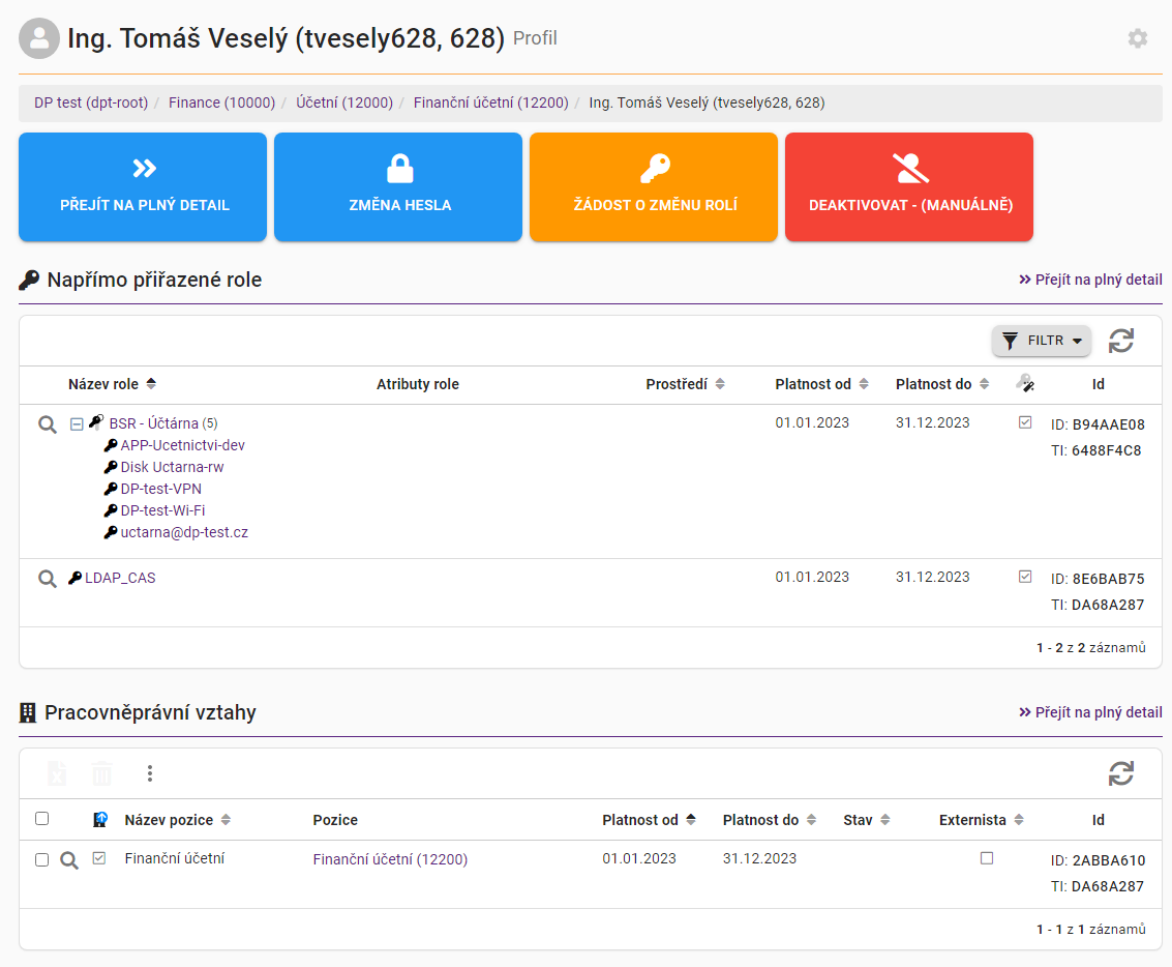
Typ atributu	Název atributu	Podmínka	Hodnota
Atribut pracovního úvazku	Název pozice	Rovná se	Finanční účetní
Rozšířený atribut pracovního úvazku	id_eviden_stavu	Rovná se	1

Podmínka „id_eviden_stavu = 1“ omezuje platnost pravidla pouze na zaměstnance s aktivním pracovním úvazkem na hlavním pracovním poměru (každý personální systém může mít jiný číselník pro typ pracovního úvazku). Vytvoření automatické role je podmíněno schválením garantem (pro roli „BSR – Účtárna“ je garant dán rolí „IAM – Hlavní účetní“). Konfigurace a výsledek schválené automatické role je znázorněn na obrázku (Obr. 28).



Obrázek 28. Konfigurace automatické role (vlastní)

Jediným manuálním vstupem celého popsaného procesu bylo zadání nacionálů zaměstnance do personálního systému a přiřazení pracovní pozice umístěné v organizační struktuře organizace. Veškeré následné kroky procesu byly provedeny zcela automatizovaně a dílčím výsledkem je vytvoření digitální identity uživatele s přiřazenými rolemi, které odpovídají jeho pracovnímu zařazení (Obr. 29). Přiřazení rolí v IAM je promítnuto do Active Directory formou členství ve stejnojmenných skupinách, vůči kterým je uživatel autorizován v napojených ICT systémech.



Obrázek 29. Identita uživatele s přiřazenými rolemi (vlastní)

4.9 Přehledové schéma použitých technologií Fortinet

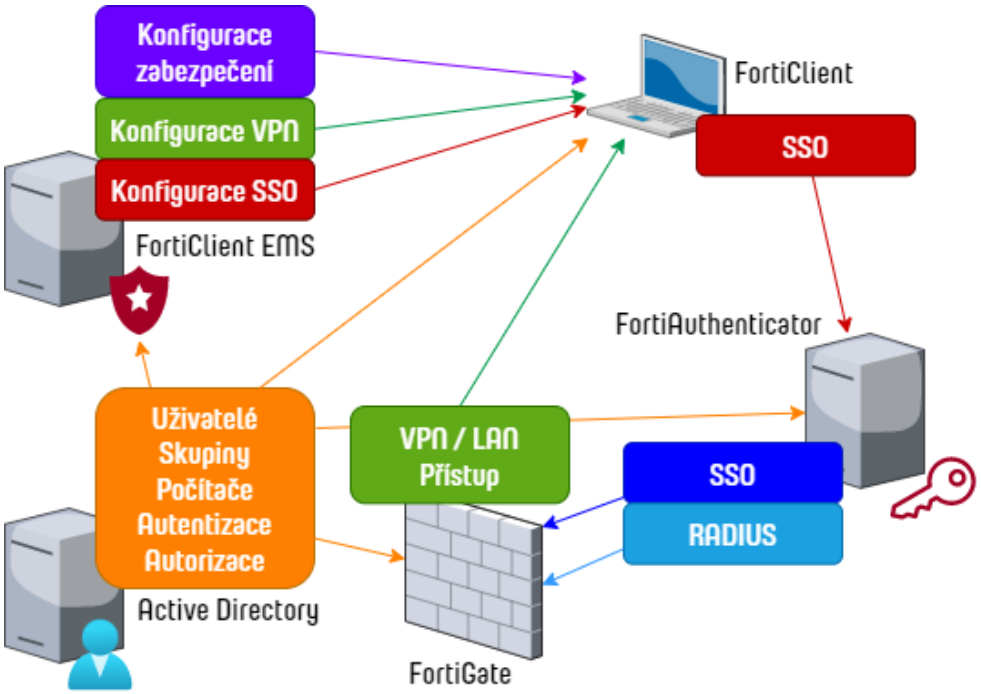
V předchozích kapitolách praktické části práce bylo docíleno stavu, kdy zaměstnanec získá v IAM svoji digitální identitu, role a členství v AD skupinách. Následující kapitoly popisují využití identity a členství ve skupinách k řízení přístupu k síťovým prostředkům.

Navazující část řešení využívá technologie výrobce síťových zařízení Fortinet. Pro dosažení cíle práce budou použity systémy a aplikace:

- **FortiClient**: agent správy koncového bodu,
- **FortiClient EMS**: centrální správa koncového bodu,
- **FortiAuthenticator**: autentizační služba,
- **FortiGate**: Firewall.

Stručný popis předávání identity mezi systémy je následující. FortiClient je SW instalovaný na zařízení uživatele a je vstupním předpokladem pro zajištění a předání identity uživatele

přihlášeného na zařízení, a jednotného přihlášení. FortiClient EMS centrálně spravuje všechny instalace FortiClient a předává jim konfiguraci, která mimo jiné obsahuje i nastavení spojení se systémem FortiAuthenticator, na který FortiClient předává svoji identitu v rámci SSO. FortiAuthenticator je autentizační server, který identitu poskytuje ostatním systémům. Zajišťuje také AAA, jako RADIUS sever pro připojení VPN klientů. Firewall FortiGate řídí přístup mezi segmenty sítě a terminuje VPN připojení uživatelů. K oběma účelům využívá služeb systému FortiAuthenticator, ze kterého získává identity použité ve FW pravidlech a ověřuje uživatele připojující se na VPN. Všechny jmenované systémy využívají pro různé účely adresářovou službu Active Directory (Obr. 30).



Obrázek 30. Přehledové schéma Fortinet (vlastní)

4.10 Agent správy koncového bodu – FortiClient

Zaměstnanci ke své práci používají firemní zařízení – koncové body, které jsou připojeny k doménovém řadiči, jsou členy domény „dp-test.cz“, vůči které se ověřují po spuštění operačního systému. Objekty uživatelských zařízení jsou uloženy v Active Directory a spravovány skupinovými politikami (GPO). Členem domény může být zařízení s OS Windows, macOS i LINUX. V dalších kapitolách práce bude, pro ověření nastaveného procesu řízení přístupu, použito zařízení s OS MS Windows 11 Pro, verze 22H2.

4.10.1 FortiClient

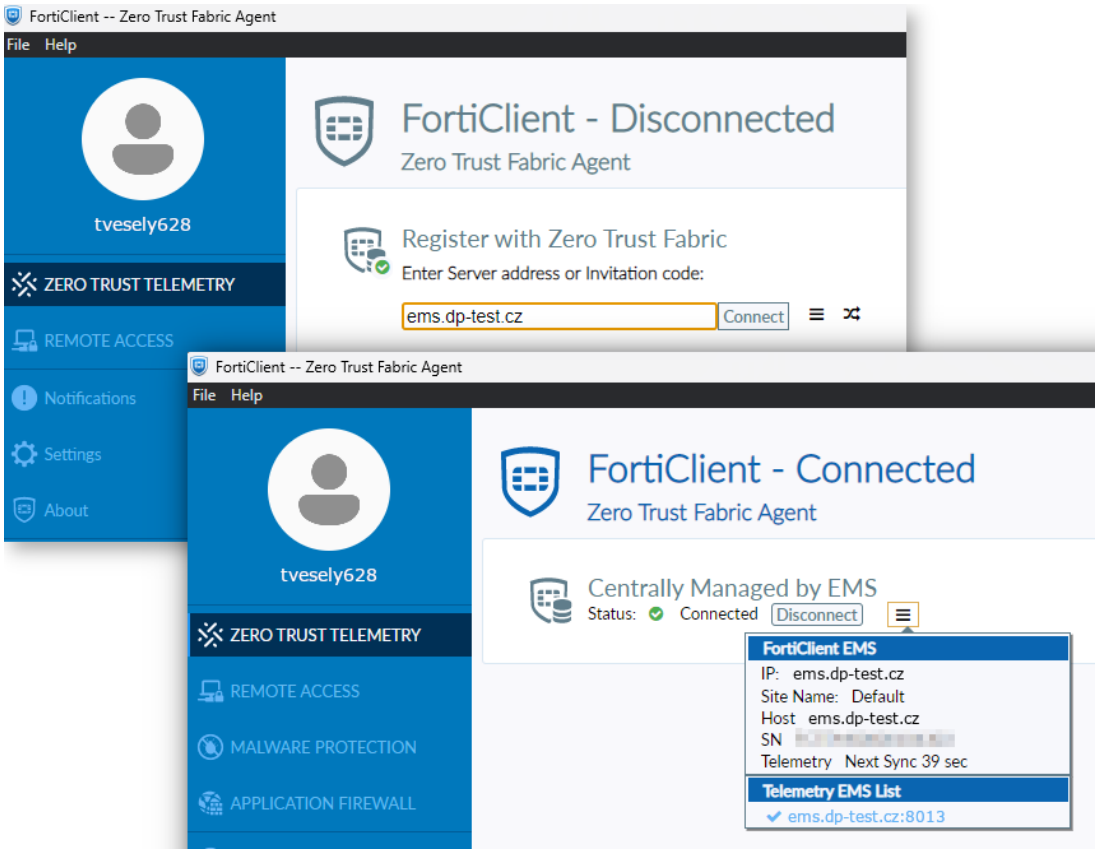
Komplexní ochranu zařízení uživatele zajišťuje instalovaný SW FortiClient (FC). Všechny jeho funkce lze vyčíst na stánkách výrobce [79], pro účely práce budou využity zejména následující funkcionality:

- Fortinet Single Sign-On (FSSO),
- SSL VPN s MFA ověřením.

Všechny funkce FC jsou centrálně spravovány. Nastavení firewallu, aplikační kontroly nebo webového filtru na zařízení tak mohou vhodně doplňovat technologie, poskytující obdobné služby na síťovém NGFW.

Na testovacím zařízení je instalován FortiClient verze 7.0.8., připojený k centrální správě FortiClient EMS na serveru „ems.dp-test.cz“ (Obr. 31). Abychom mohli služby FC využít, je potřeba zajistit odpovídající licence. V našem případě jsou potřeba licence:

- FortiClient Security Fabric Agent: plná verze klienta,
- FortiClient SSO Mobility Agent: funkce jednotného přihlášení,
- FortiTokenMobile: MFA mobilní aplikace s podporou „push“ notifikace.



Obrázek 31. Připojení FortiClient k EMS (vlastní)

4.10.2 SSO

FC s licencí FortiClient SSO Mobility Agent poskytuje službu FSSO, která zajistí identifikaci uživatele koncového bodu. FSSO převezme identitu přihlášeného uživatele z OS Windows a šifrovaným spojením ji předá FortiAuthenticatoru (FAC), bez nutnosti uživatele znovu vyzvat k ověření. FAC je následně v roli IdP pro FortiGate (*Příloha P II: Fortinet Single Sign-On a SSL VPN diagram*, kapitola *4.3.3 Fortinet Single Sign-On (FSSO) a SSL VPN* a kapitola *4.12 Autentizační služba – FortiAuthenticator*).

4.11 Centrální správa koncového bodu – FortiClient EMS

EMS poskytuje automatizované prostředky pro správu koncových bodů s instalovaným FC:

- vzdálené nasazení FC do počítačů s OS Windows,
- aktualizace profilů FC na koncových bodech ve všech sítích, jako je správa antiviru, webového filtru, VPN a aktualizace signatur,
- správa registrací koncových bodů s automatickým přiřazením profilů dle organizační jednotky v AD,
- správa koncových bodů, například informace o stavu zařízení, stavu FC, informace o signaturách, bezpečnostních událostech atd. [80]

Verze EMS použitá v řešení je 7.0.8.

4.11.1 Připojení koncového bodu do EMS

Logika správy v koncových bodů v EMS je založena na třech komponentech:

- **skupiny koncových bodů**: do skupiny je zařízení přiřazeno na základě:
  - členství v organizační jednotce v AD (skupiny jsou vytvořeny dle OU),
  - podmínek definovaných v pravidle (IP, OS, číslo instalátoru FC),
  - ručního přiřazení,
- **politiky koncových bodů**: skupinám přiřazují konfigurační profily,
- **profily koncových bodů**: konfigurační profily modulů FortiClienta (VPN, malware ochrana, firewall, webový filtr…).

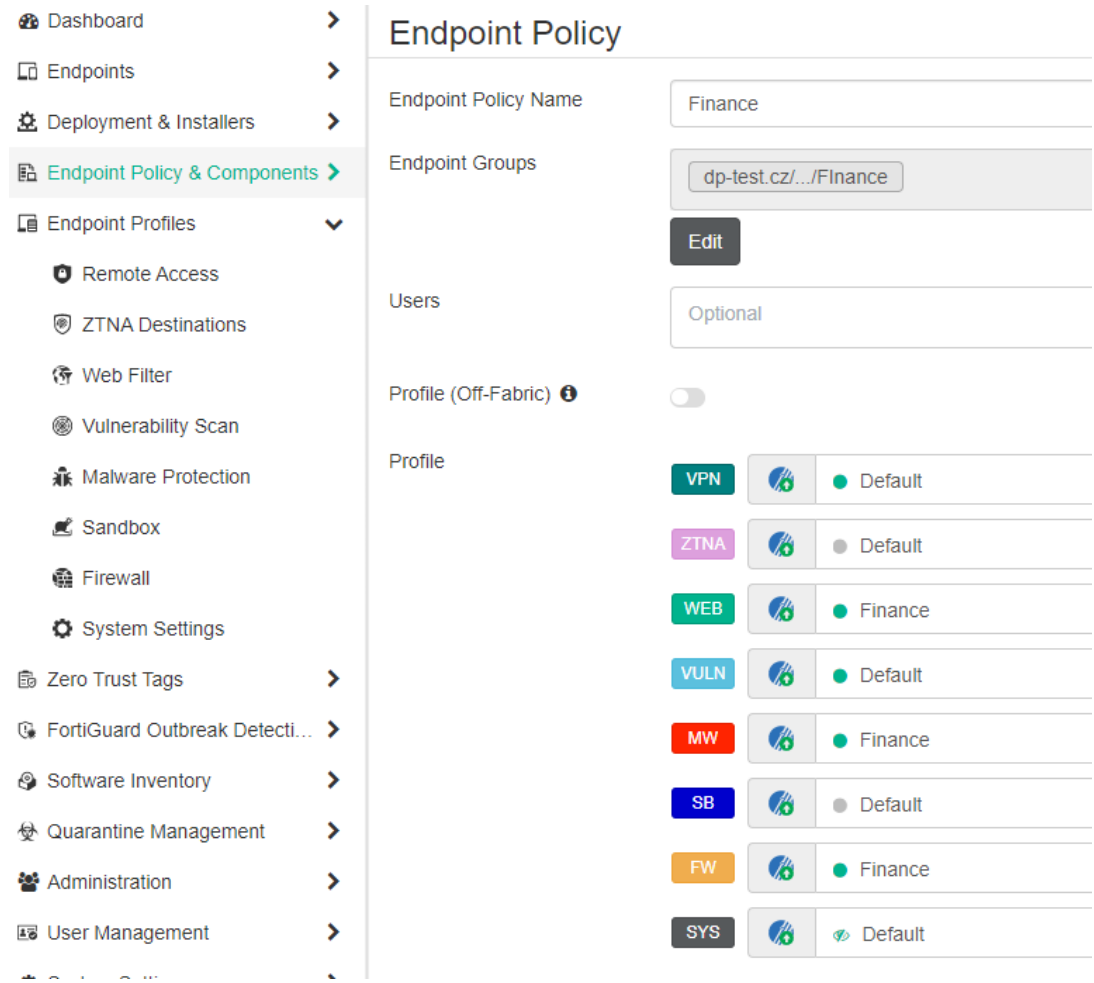
Instalátor FC je k dispozici ke stažení z URL adresy EMS (https://ems.dp-test.cz/Installers) a obsahuje konfiguraci pro připojení k EMS a přiřazení profilu. Instalaci FC na zařízení a připojení k EMS je možné provést automatizovaně a bezobslužně.

Pro získání seznamu zařízení v doméně potřebujeme znát následující základní konfigurační parametry (položka Endpoints, Manage Domains):

- **Hostname**: které adresářové služby se má EMS dotazovat (dp-test.cz),
- **Port**: port připojení k AD (636),
- **Distinguished name**: organizační jednotka, kterou chceme vyčítat (OU=DPT-Computers,DC=dp-test,DC=cz),
- **Username:** název technického účtu pro připojení k AD (ems-ad)**,**
- **Password**: heslo k technickému účtu.

V „OU=DPT-Computers,DC=dp-test,DC=cz“ existují podřízené OU, dle jednotlivých úseků v organizační struktuře, ve kterých jsou umístěny zařízení uživatelů. Distinguished name zařízení uživatele Tomáš Veselý je: „CN=NTB-628,OU=Finance,OU=DPT-Computers,DC=dp-test,DC=cz“. Skupina koncových bodů se tedy jmenuje „Finance“.

Skupině „Finance“ přiřadíme politiku koncových bodů (Obr. 32)

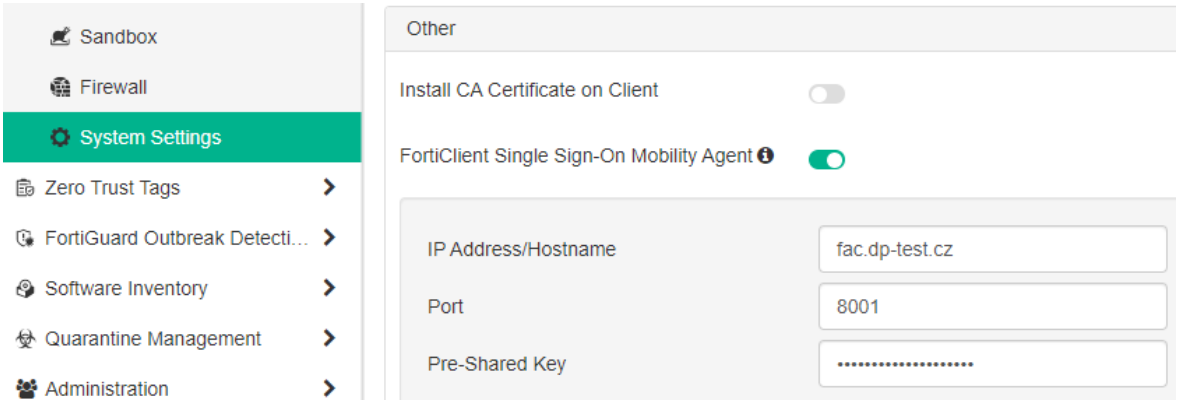


Obrázek 32. Přiřazení politiky koncových bodů (vlastní)

Jednotlivé profily nakonfigurujeme dle požadavků organizace. Pro další postup je stěžejní nastavení FortiClient SSO Mobility Agenta.

4.11.2 Konfigurace FSSO

Aby bylo možné využít FSSO, musí být FC instalovaný na koncovém bodu centrálně spravován EMS. Při konfiguraci FC profilu v EMS (Endpoint Profiles, Systém Settings, vybraný profil) je zadán předsdílený klíč pro symetrické šifrování komunikace mezi FC a FAC (Obr. 33). Stejný klíč je zadán v konfiguraci služby FortiClient SSO Mobility Agent ve FAC.



Obrázek 33. Konfigurace FSSO pro FC na koncových bodech (vlastní)

4.11.3 Konfigurace VPN

K otestování funkčnosti řízení přístupu použijeme také vzdálené připojení SSL VPN. Nastavení připojení provedeme v EMS profilu VPN (položka Endpoint Profiles, Remote Access). Profil následně přiřadíme v politice koncových bodů. Základní položky konfigurace jsou:

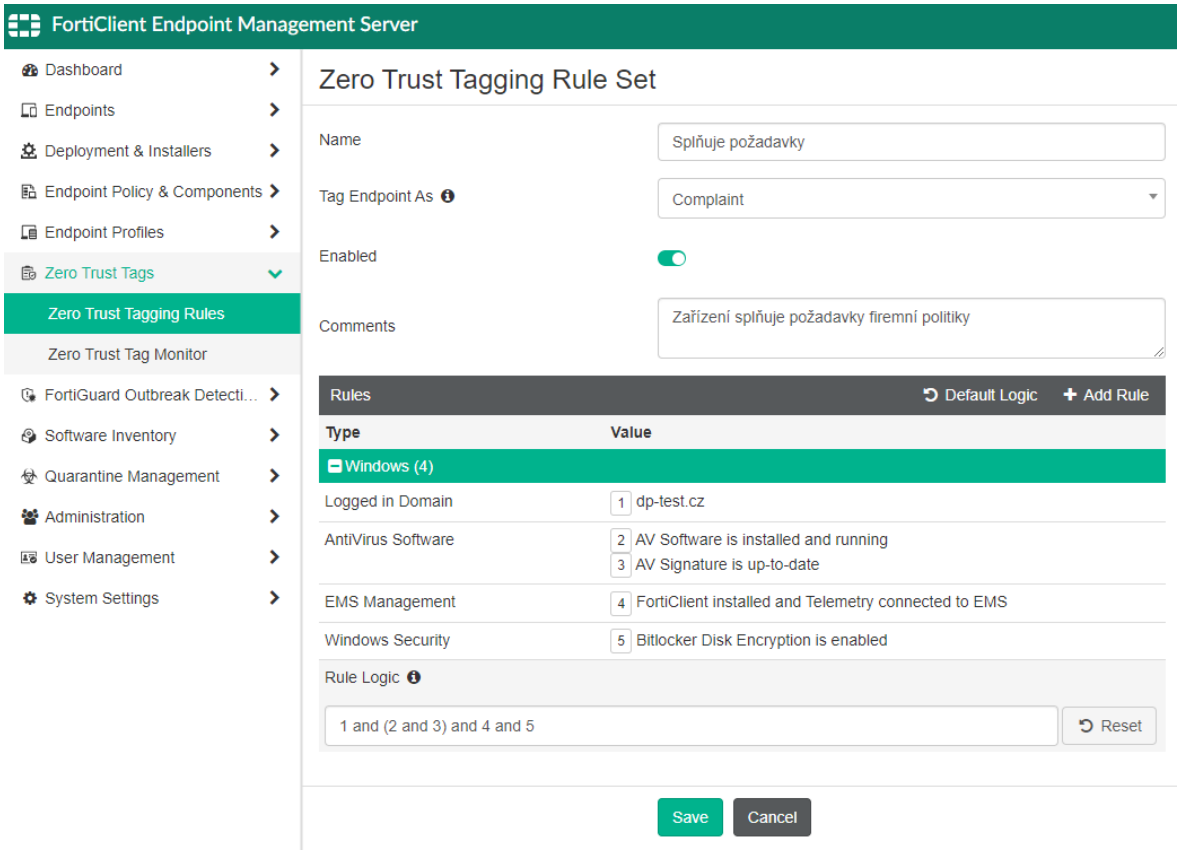
- zapnutí SSL VPN,
- vytvoření konfigurace VPN tunelu:
  - **Name**: název VPN tunelu, který uvidí uživatelé v FC v nabídce „Remote Access“,
  - **Type**: zvolíme SSL VPN,
  - **Remote Gateway**: DNS název, směrující na IP adresu na rozhraní FW FortiGate, která je vyhrazena pro VPV připojení,
  - ostatní nestavení zvolíme dle požadavků organizace.

4.11.4 Klasifikační značky

EMS je rovněž serverem pro předávání informací o zařízeních. FortiGate připojením k EMS získává dodatečné informace o zařízeních, jako jsou klasifikační značky. Pravidlem lze definovat, na základě kterých podmínek získá spravované zařízení značku. FortiGate může ve FW politice značku vyhodnocovat a povolit síťové spojení pouze za předpokladu, že je zařízení zahajující komunikaci označené požadovanou značkou.

Pro zvýšení zabezpečení, při řízení síťového přístupu, může být použita klasifikační značka, např. „Complaint“ s následujícím nastavením (Zero Trust Tags, Zero Trust Tagging Rules):

- zařízení připojené do domény „dp-test.cz“,
- FC je na zařízení nainstalovaný a spravovaný EMS,
- antivirová ochrana je aktivní a obsahuje aktuální signatury,
- pevný disk zařízení je šifrovaný (Obr. 34).



Obrázek 34. Definování značek v EMS (vlastní)

4.12 Autentizační služba – FortiAuthenticator

FortiAuthenticator je server pro správu přístupů a jednotné přihlášení. Poskytuje služby:

- identifikace uživatele v síti,
- vynucování zásad založených na identitách v síti (v sítích postavených na technologiích Fortinet),
- jednoduché a bezpečné MFA ověřování ve spojení s technologií FortiToken,
- správu certifikátů pro podnikové bezdrátové sítě a VPN,
- správu hostů v drátových i bezdrátových sítích,
- SSO pro interní i cloudové sítě. [81]

Instalovaná verze FAC je 6.4.4. V navrhovaném řešení plní FAC následující úkoly:

- **zprostředkovává FSSO**:
  - od FC, instalovaném na zařízení uživatele, přebírá informaci o přidělených IP adresách na jeho síťových rozhraních, spárovaných s identitou přihlášeného uživatele,
  - FAC odpovídá na dotazy FortiGate, týkající se identity komunikujících IP adres, při zpracování FW pravidel,
- **autentizuje uživatele**: vícefaktorově ověřuje uživatele, připojující se prostřednictvím VPN.

FAC vyžaduje licence na počet aktivních uživatelů, které spravuje (např. počet uživatelů synchronizovaných z AD). Další licence závisí na funkcionalitách, které plánujeme využít, viz *4.10.1 FotiClient*.

4.12.1 Služby FAC

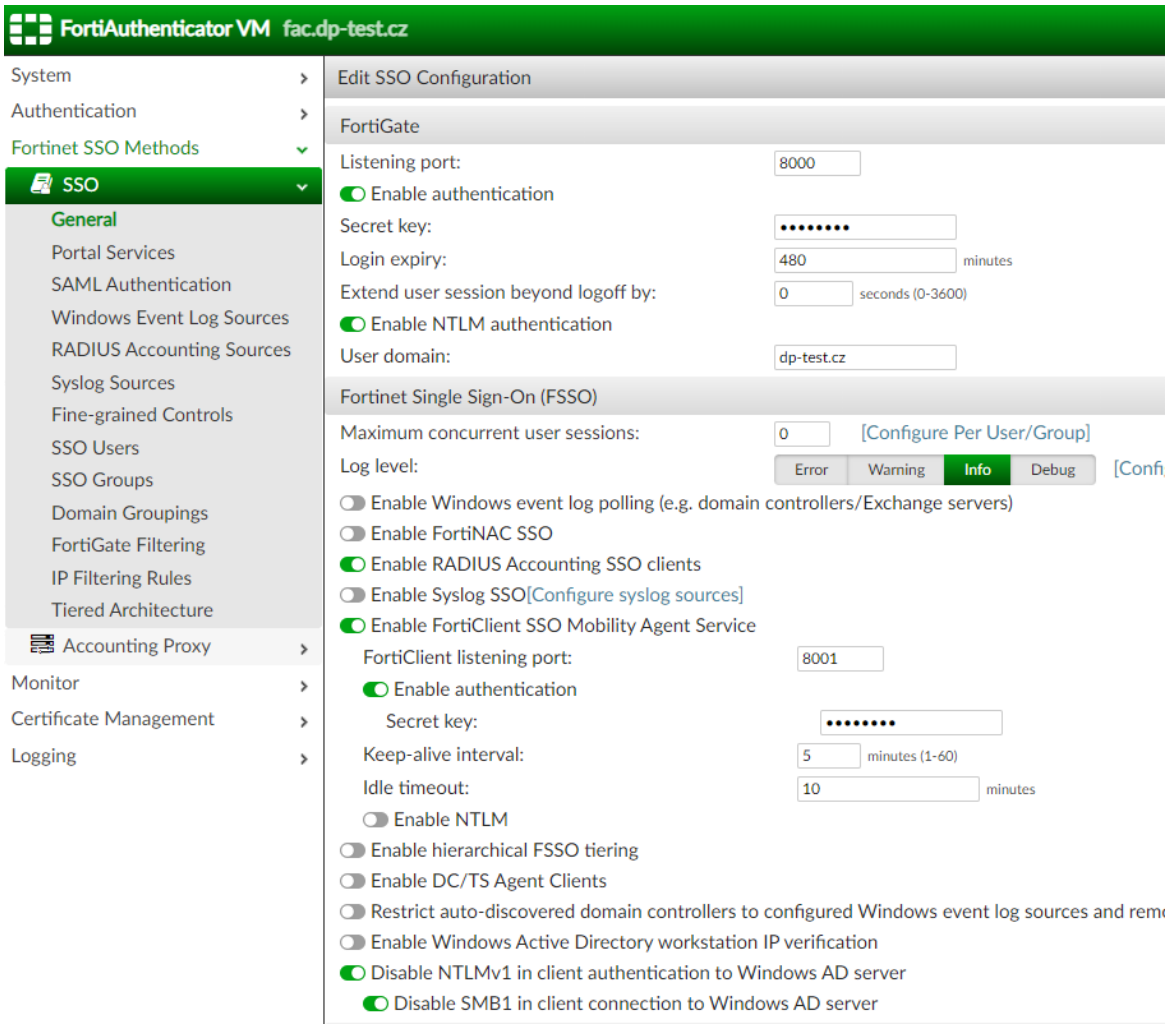
FAC je autentizační server, který kromě FSSO poskytuje služby RADIUS, LDAP, OAuth i SAML. Zároveň může být i klientem jmenovaných služeb. Pro dosažení cíle této práce potřebujeme FAC nakonfigurovat jako:

- FSSO server,
- RADIUS server pro autentizaci a autorizaci uživatelů přistupujících do sítě prostřednictvím VPN,
- LDAP klient pro autentizaci uživatelů vůči AD domény „dp-test.cz“.

4.12.2 FSSO server

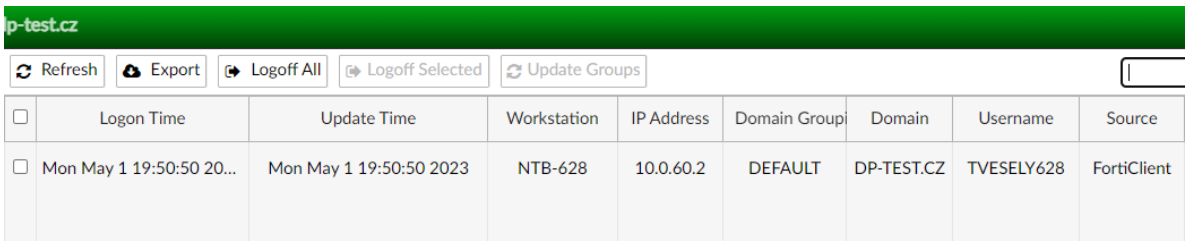
Pro předávání jednotného přihlášení nastavíme parametry pro FW FortiGate na jedné straně a pro FC na straně druhé (Fortinet SSO Methods, SSO, General). V obou případech povolíme autentizaci, nastavíme předsdílený klíč, případně upravíme porty, na kterých má

FAC naslouchat a upravíme časové limity. Službu FortiClient SSO Mobility Agent Service je potřeba povolit (Obr. 35).



Obrázek 35. Konfigurace FSSO (vlastní)

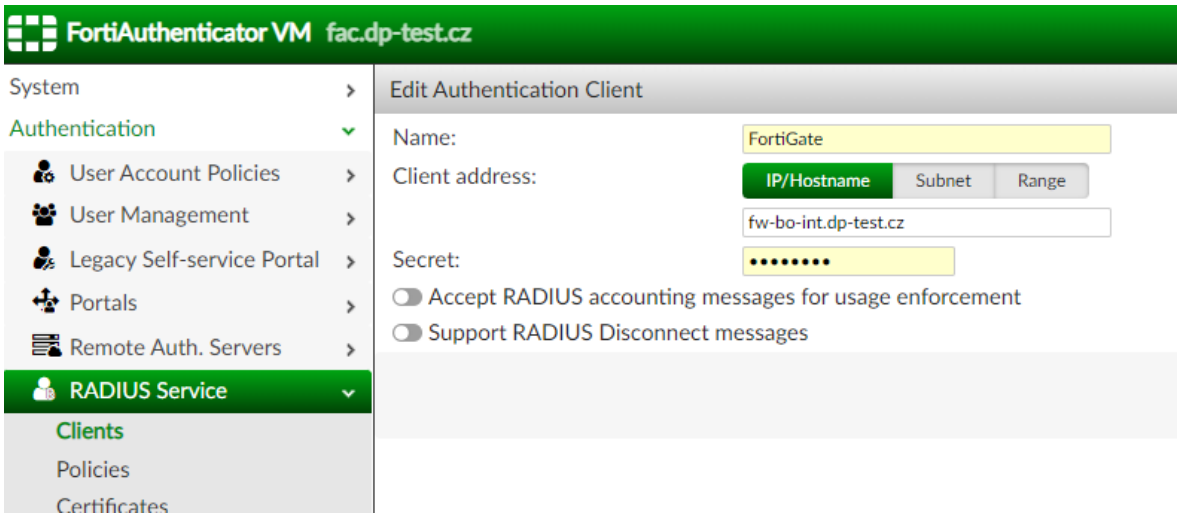
Pro FortiClient SSO Mobility Agent Service musí být předsdílený klíč totožný s klíčem, který jsme zadali v EMS, viz *4.11.2 Konfigurace FSSO*. Funkčnost příjmu FSSO od FC můžeme ověřit v monitoringu (položka Monitor, SSO, Obr. 36).



Obrázek 36. Monitoring SSO (vlastní)

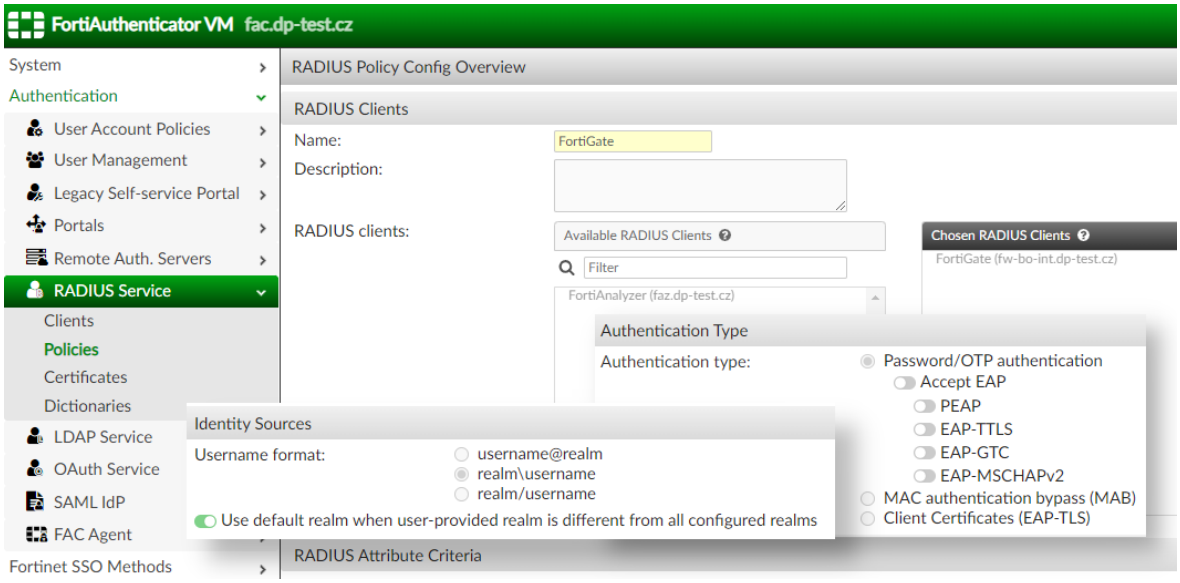
4.12.3 RADIUS server

Na začátku navázání VPN připojení jsou uživatelé vyzváni k ověření své identity. FW FortiGate terminuje VPN připojení (je v roli NAS) a požadavek na autentizaci a autorizaci předává na FAC (v roli AS) protokolem RADIUS. Aby FortiGate mohl dotazovat FAC, musí být nastaven jako autentizovaný RADIUS klient. Konfiguraci provedeme dle obrázku (Obr. 37) (Authentication, RADIUS Service, Clients), zadáme název hostitele klienta (fw-bo-int.dp-test.cz) a vyplníme sdílené tajemství.



Obrázek 37. Konfigurace RADIUS klienta (vlastní)

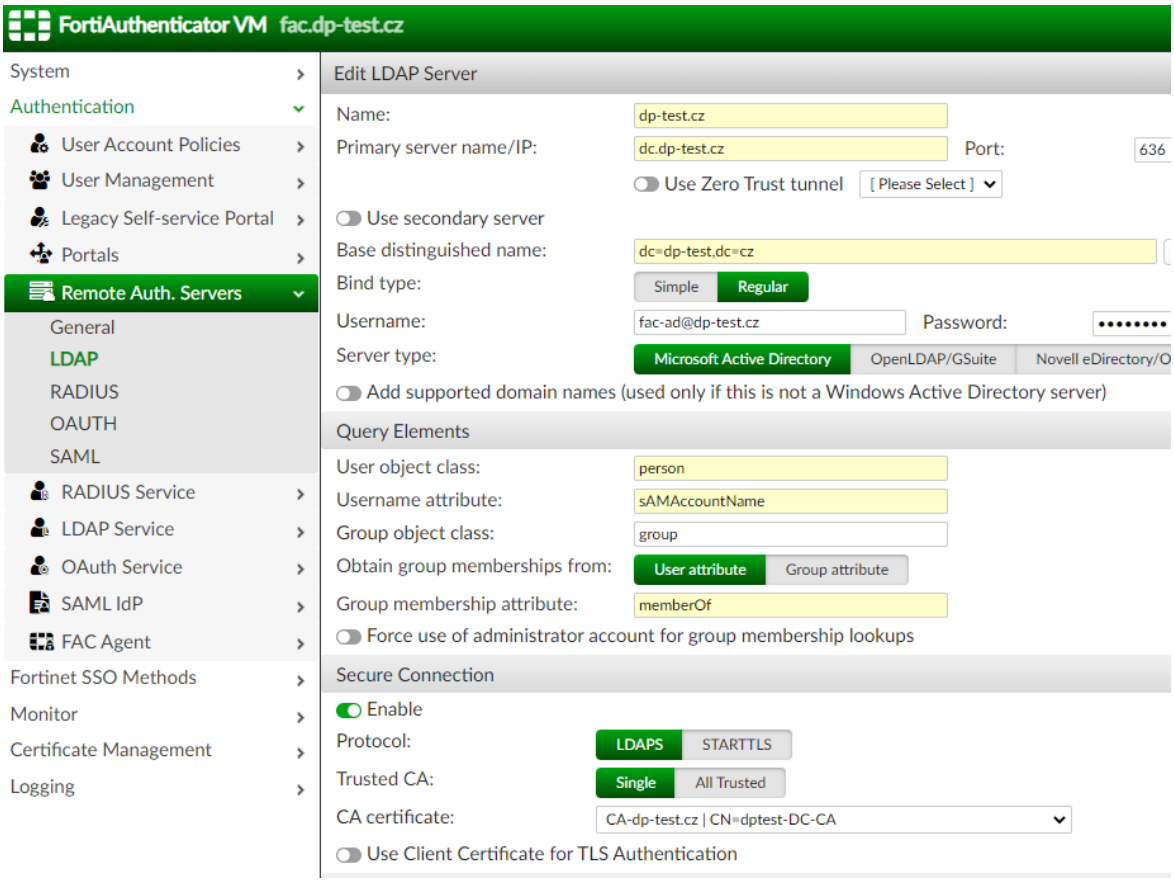
V dalším kroku přidáme RADIUS politiku, která určuje povolený způsob ověření a formát uživatelského jména. Zvolíme RADIUS klienta vytvořeného v předchozím kroku, zvolíme typ autentizace „Password“ a formát uživatelského jména „realm\username“ (Obr. 38).



Obrázek 38. Konfigurace RADIUS politiky (vlastní)

4.12.4 LDAP klient

RADIUS server může využívat vzdálené autentizační servery pro ověření uživatelů. V navrhnutém řešení bude autentizaci poskytovat AD na serveru „dc.dp-test.cz“. Kromě autentizace bude AD poskytovat skupiny zabezpečení a informaci o členství. Konfigurace je vyobrazena na obrázku (Obr. 39).



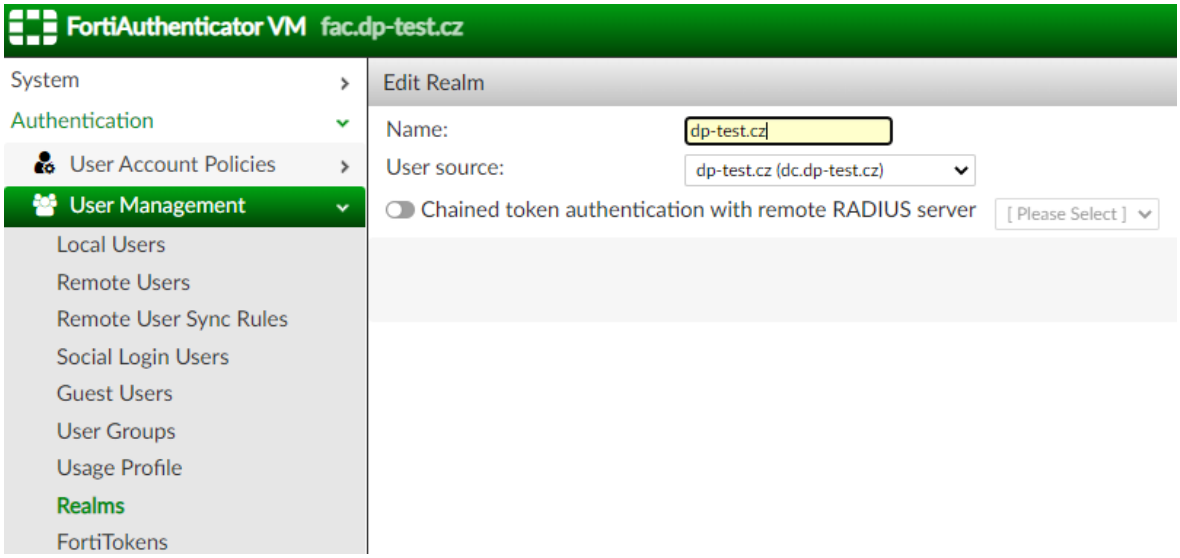
Obrázek 39. Konfigurace LDAP klienta (vlastní)

Hlavními konfiguračními parametry jsou (Authentication, Remote Auth. Servers, LDAP):

- **Name**: název LDAP připojení, který budeme používat v dalším nastavení,
- **Primary server name**: doménový řadič (dc.dp-test.cz). V reálné organizaci vyplníme i sekundární řadiče domén,
- **Base distinguished name**: organizační jednotka, ve které chceme prohledávat objekty (DC=dp-test,DC=cz),
- **Username**: název technického účtu pro připojení k AD (fac-ad),
- **Password**: heslo k technickému účtu.
- **Server type**: typ adresářové služby (Microsoft Active Directory),
- **User object class**: třída objektu, která definuje uživatele (person),

- **Username attribute:** atribut objektu, ve kterém je uloženo uživatelské jméno (sAMAccountName),
- **Group object class**: třída objektu, která definuje skupinu zabezpečení (group),
- **Obtain group memberships from**: zvolíme, zda chceme členství ve skupinách načítat z objektu uživatele nebo skupiny (User attribute),
- **Group membership attribute**: v závislosti na předchozí volbě uvedeme název atributu členství ve skupině (memberOf),
- povolíme bezpečné připojení LDAPS a zvolíme certifikát certifikační autority (CA-dp-test.cz).

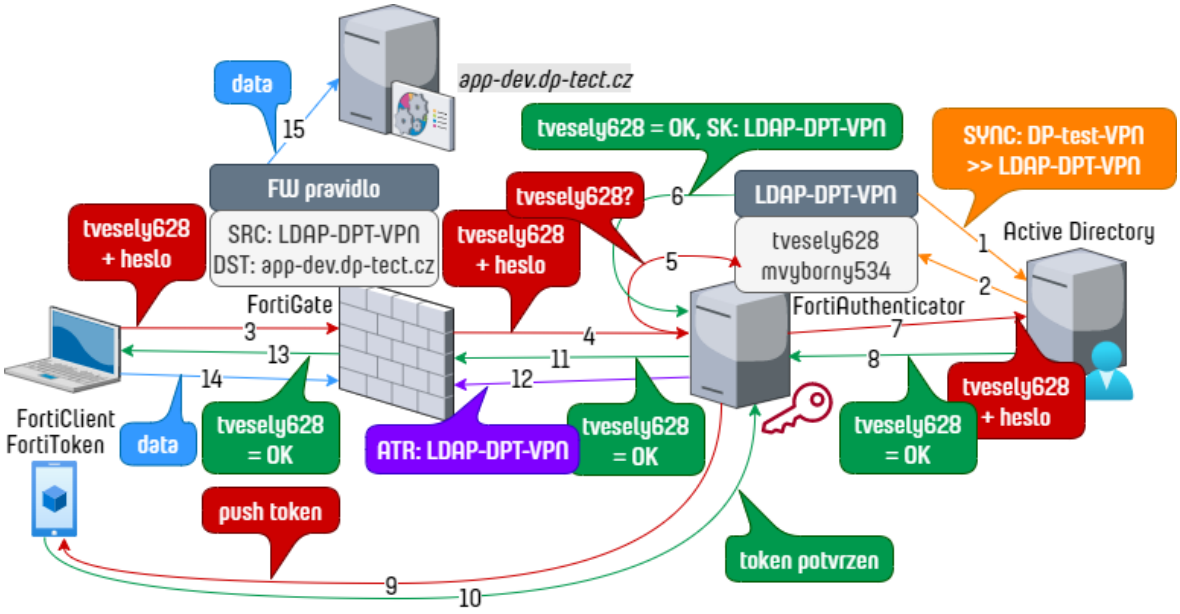
Pro použití vzdálené LDAP autentizace s RADIUS serverem je třeba vytvořit oblast (realm), viz obr. 40 (Authentication, User Management, Realms).



Obrázek 40. Vytvoření oblasti (vlastní)

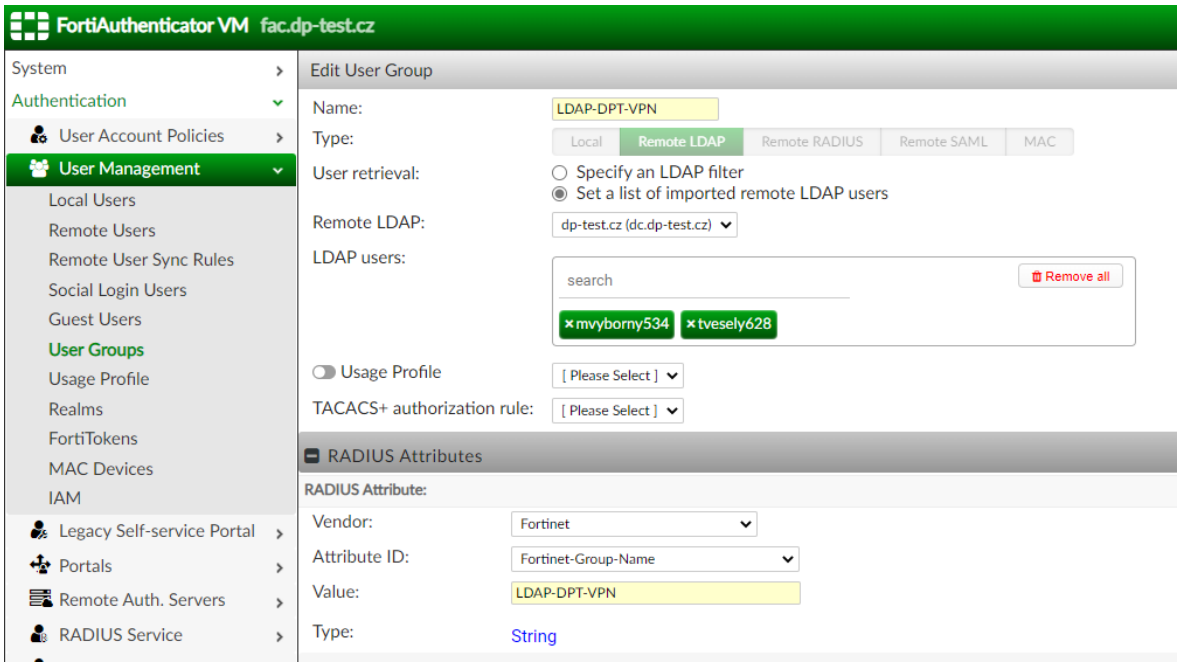
4.12.5 Vytvoření a synchronizace skupiny pro autorizaci VPN připojení

V AD máme již vytvořenou skupinu zabezpečení „DP-test-VPN“, jejichž členové jsou automatizovaně přidělování z IAM. Protože RADIUS autentizační server pro FortiGate je FAC, potřebujeme AD skupinu synchronizovat do uživatelské skupiny ve FAC. Na FortiGate RADIUS-Access-Request bude, při úspěšné autentizaci uživatele a porovnání členství ve FAC skupinách, vracet FAC RADIUS-Access-Accept doplněný atributem Fortinet-Group-Name s hodnotou dle názvu shodující se FAC skupiny. Fortinet-Group-Name atribut použije FortiGate v definici vlastních uživatelských skupin, využitelných např. ve FW pravidlech (Obr. 41).



Obrázek 41. Proces autentizace uživatele na VPN (vlastní)

Prvním konfiguračním krokem je vytvoření FAC uživatelské skupiny (Authentication, User Management, User Groups), pro synchronizaci uživatelů z AD skupiny „DP-test-VPN“ (Obr. 42).



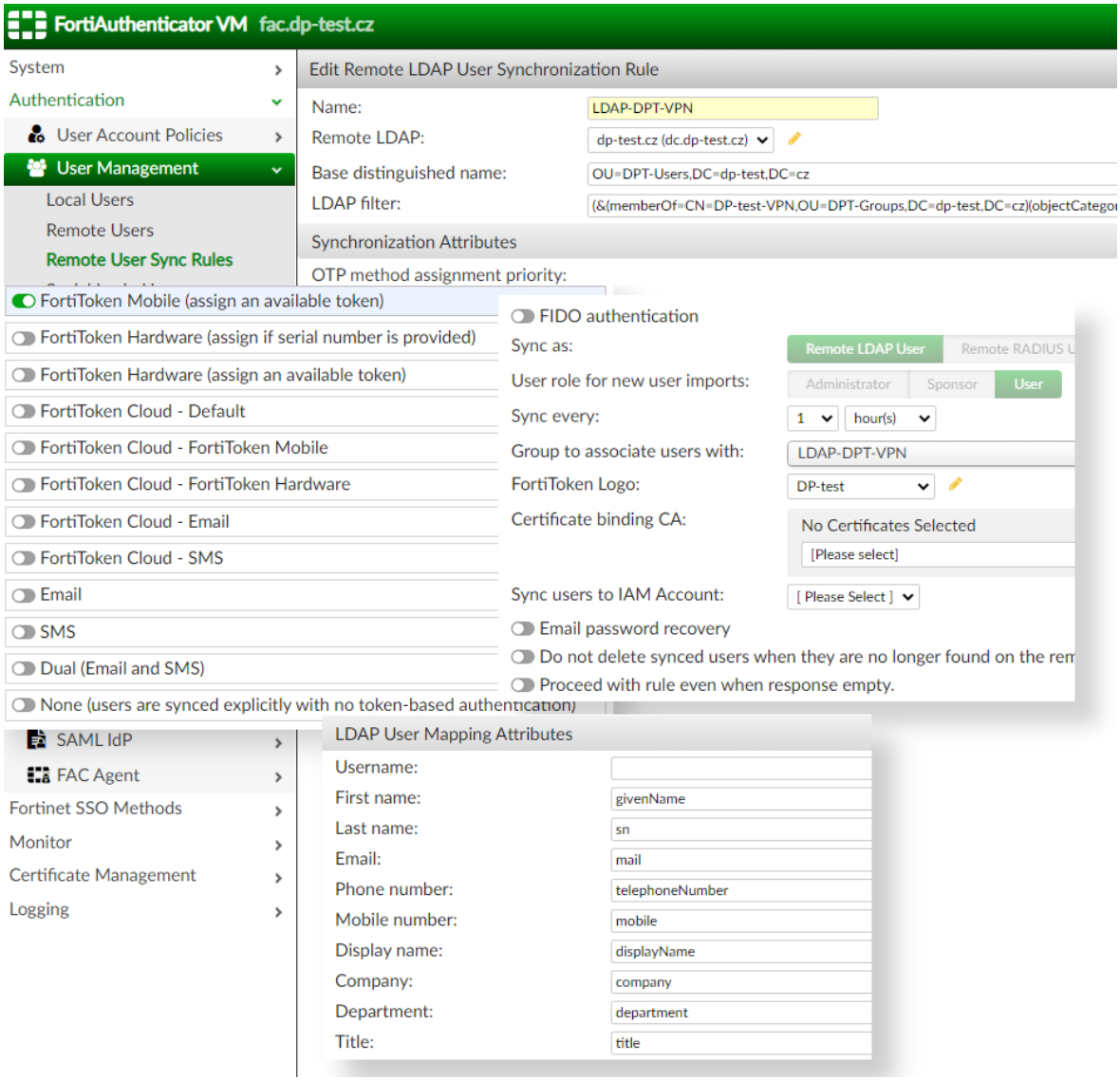
Obrázek 42. Konfigurace FAC skupiny uživatelů (vlastní)

Konfigurační parametry jsou:

- **Name**: název skupiny, na který se budeme odkazovat v další konfiguraci (LDAP-DPT-VPN),

- **User retrieval**: zvolíme „Set a list of…“. Nebudeme plnit ručně, ale synchronizací, viz dále,
- **Remote LDAP**: zvolíme dříve vytvořený vzdálený LDAP server (dc.dp-test.cz),
- **RADIUS Attribut – Vendor / Attribute ID**: FAC obsahuje databázi výrobců a používaných atributů. Vybereme „Fortinet“ a „Fortinet-Group-Name“,
- **Value**: hodnota, kterou budeme posílat na FortiGate (LDAP-DPT-VPN).

Na obrázku (Obr. 42) jsou vidět v poli LDAP users dva členové skupiny. Ve skutečnosti zajistíme automatické plnění FAC skupiny až v dalším konfiguračním kroku (Obr. 43).



Obrázek 43. Konfigurace synchronizace uživatelů do FAC skupiny (vlastní)

Skupinu budeme plnit podle členství v AD skupině „DP-test-VPN“. V konfiguraci (Authentication, User Management, Remote User Sync Rules) jsou stěžejní následující parametry:

- **Name**: pojmenování synchronizačního pravidla (LDAP-DPT-VPN),
- **Remote LDAP**: zvolíme dříve vytvořený vzdálený LDAP server (dc.dp-test.cz),
- **Base distinguished name**: organizační jednotka, ve které chceme prohledávat objekty uživatelů (OU=DPT-Users,DC=dp-test,DC=cz),
- **LDAP filter**: důležitý parametr, na kterém závisí správné určení uživatelů v AD skupině. Použijeme syntaxi pro LDAP filtrování „(&(memberOf=CN=DP-test-VPN,OU=DPT-Groups,DC=dp-test,DC=cz)(objectCategory=Person) (!(UserAccountControl:1.2.840.113556.1.4.803:=2)))“. Filtr vymezuje hledání na objekty třídy „person“ (uživatele), kteří mají přiřazenou skupinu „DP-test-VPN“ a zároveň jsou aktivní [82].
- **OTP method assignment priority**: jako druhý faktor ověření uživatele použijeme potvrzení push notifikace, zaslané do aplikace FortiToken Mobile v mobilním telefonu,
- **Sync as / User role**: „Remote LDAP Users“ / „Users“,
- **Sync every**: nastavíme časový interval pro synchronizaci,
- **Group to associate users with**: zvolíme cílovou FAC skupinu pro synchronizaci, vytvořenou v předchozím kroku,
- **LDAP User Mapping Attributes**: propojíme atributy FAC skupiny s atributy AD skupiny.

4.13 Firewall – FortiGate

Na síťovém firewallu, je provoz řízen vyhodnocováním parametrů síťového spojení, jako je IP adresa, port služby a rozhraní. Ve FW politikách lze v případě UTM nebo NGFW použít i další objekty funkcí na vyšších vrstvách ISO/OSI. Ve všech případech se jedná o identifikaci komunikujících hostitelů, které nejsou z pohledu FW spojeni s konkrétním uživatelem. Aby se mohl FW rozhodovat při řízení síťového provozu také podle identity uživatele, musí znát ve chvíli navázání spojení, kdo vlastní zdrojovou IP adresu, nebo musí uživatele vyzvat při zahájení relace k autentizaci. Při návrhu řešení jsem zvolil metodu, která bude vyžadovat minimální interakci s uživatelem. FAC, konfigurovaný dle postupu v předchozích kapitolách, umožní v reálném čase autentizovat IP adresy v komunikaci, procházející přes FW FortiGate. FAC firewallu dodá nejen identitu IP adresy, ale také členství identifikovaného uživatele ve všech AD skupinách.

FortiGate je Next-Generation Firewall, nabízející mnoho pokročilých služeb síťové ochrany, jako je „Zero Trust“ síťový přístup, SW definované sítě, dešifrování a kontrola síťového provozu, poskytuje automatickou ochranu proti hrozbám za použití umělé inteligence a strojového učení. Pro akceleraci výkonu používá FortiGate vlastní HW architekturu a procesory. Dle Gartner® Magic Quadrant™ reportu je FortiGate lídrem trhu v kategorii síťových firewallů (Obr. 44). [83]

Obrázek 44. Magic Quadrant for Network Firewalls [83]

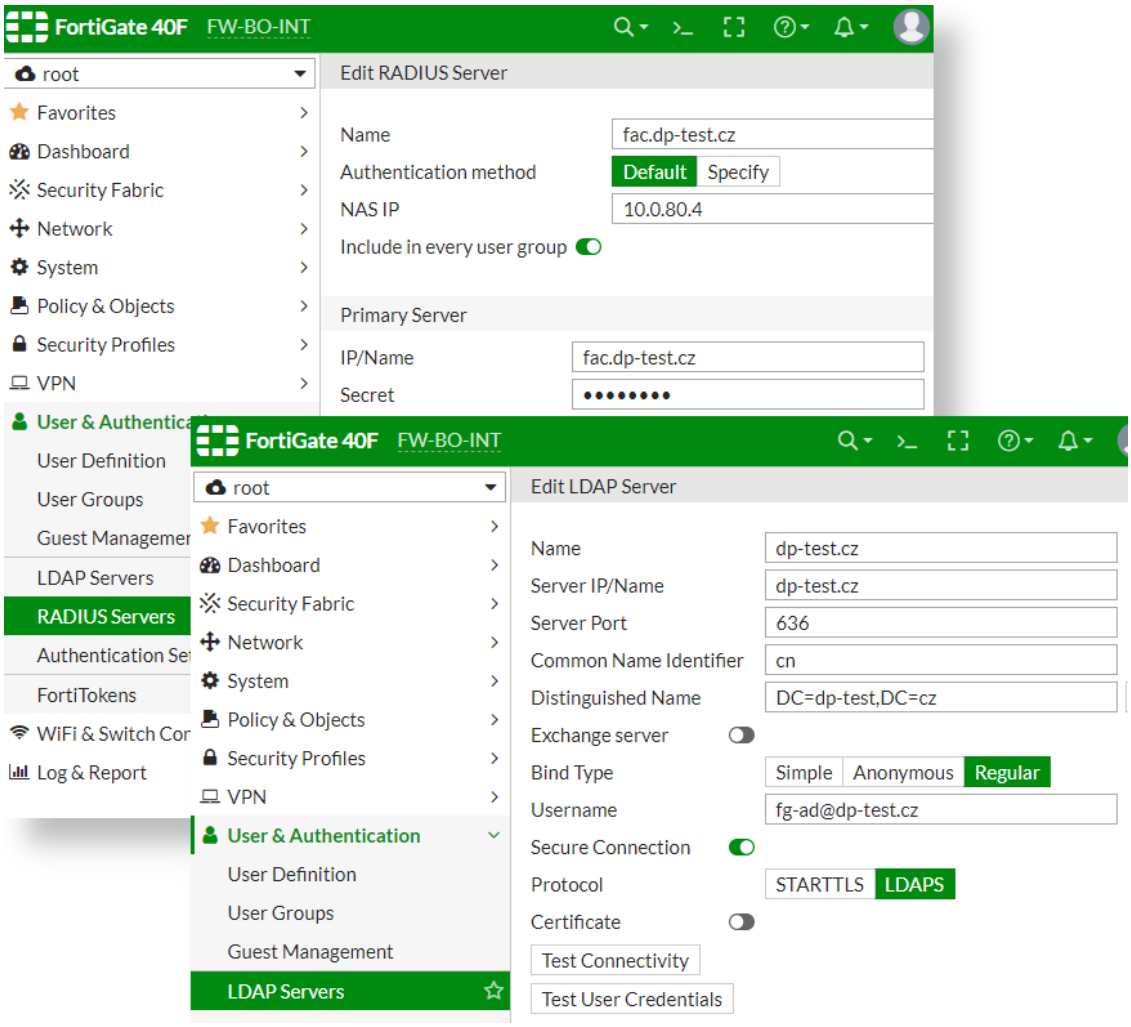
V řešení je použit FortiGate 40F s OS FortiOS ve verzi 6.4.12. Na FortiGate je potřeba, v rámci navrhovaného řešení, konfigurovat následující služby:

- připojení k LDAP a RADIUS serveru,
- externí konektor pro FSSO,
- SSL VPN,
- FW pravidla.

4.13.1 Konfigurace připojení FortiGate k LDAP a RADIUS serveru

Připojením k AD získá FortiGate možnost vyčítat uživatele a skupiny zabezpečení z domény „dp-test.cz“ a provádět porovnání s údaji získanými prostřednictvím FSSO z FAC serveru. Pro konfiguraci (User & Authentications, LDAP servers) zadáme základní údaje (Obr. 45):

- **Name**: název na který se budeme odkazovat v další konfiguraci (dp-test.cz),
- **Server Name**: název doménového řadiče nebo domény (dp-test.cz),
- **Server Port**: port, na kterém služba AD naslouchá (636 pro LDAPS),
- **Common Name Identifier**: identifikátor atributu jména objektu (cn),
- **Distinguished Name**: dn základního OU pro vyhledávání (DC=dp-test,DC=local),
- **Bind Type**: Regular,
- **Username**: název technického účtu pro připojení k AD (fg-ad),
- zvolíme **Secure Connection**, **Protocol** (LDAPS) a tlačítkem Test User Credentials vložíme přihlašovací údaje a ověříme funkčnost.



Obrázek 45. Konfigurace LDAP a RADIUS serveru ve FortiGate (vlastní)

Pro připojení k RADIUS serveru (FAC), který bude ověřovat VPN připojení, použijeme při konfiguraci (User & Authentications, RADIUS servers) údaje (Obr. 45):

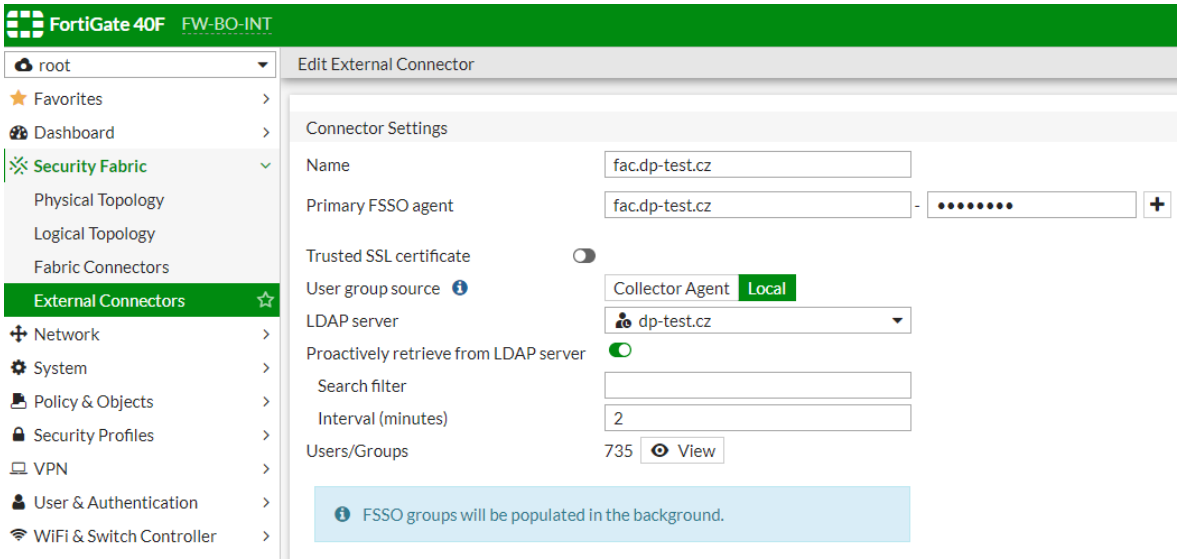
- **Name**: název na který se budeme odkazovat v další konfiguraci (fac.dp-test.cz),
- **NAS IP**: IP adresa FAC (10.0.80.4),

- **Primary Server Name**: doménové jméno FAC (fac-dp-test.cz),
- **Secret**: sdílené tajemství, stejné jako jsme zadali na FAC při konfiguraci RADIUS serveru (kapitola *4.12.3 RADIUS server*).

4.13.2 Konfigurace externího konektor pro FSSO

Připojení k příjmu FSSO z FAC se provádí externím konektorem (Security Fabric, External Connector), typu „FSSO Agent on Windows AD“ (Obr. 46), který vytvoříme s následujícími parametry:

- **Name**: název konektoru (fac.dp-test.cz),
- **Primary FSSO agent**: doménový název FAC (fac.dp-test.cz) a předsdílený klíč, který jsme zadali ve FAC v SSO konfiguraci pro FortiGate (kapitola *4.12.2 FSSO server*),
- **User group source**: LDAP server, z kterého budou čerpány objekty uživatelů (dp-test.cz vytvořený v předchozí kapitole),
- nastavíme proaktivní načítaní z LDAP serveru a interval v minutách.



Obrázek 46. Konfigurace externího konektoru FSSO (vlastní)

4.13.3 Konfigurace SSL VPN

Konfigurace SSL VPN tunelu spočívá ve:

- vytvoření IP adresního rozsahu (Policy & Objects, Addresses), přidělovaného připojeným zařízením (10.0.65.0/22),

- konfigurace SSL VPN portálu (VPN, SSL-VPN Portals), kde se nastavují parametry tunelu (full, split, web…) a přiřazuje IP adresní rozsah. Pro účely práce je vytvořen portál s názvem „DPT-SSL-VPN-Default“ a nastavením „full tunnel“,
- konfigurace oblastí (VPN, SSL-VPN Realms), které umožňují uživateli výběr více různých portálů, s různými nastaveními, pro VPN připojení,
- konfigurace VPN připojení (VPN, SSL-VPN Settings, Connection Settings), s volbou rozhraní pro VPN, certifikátu a dalších síťových nastavení a služeb,
- mapování autentizace a oblasti na portál. Mapování přiřadí uživateli správný VPN portál dle jeho autentizace.

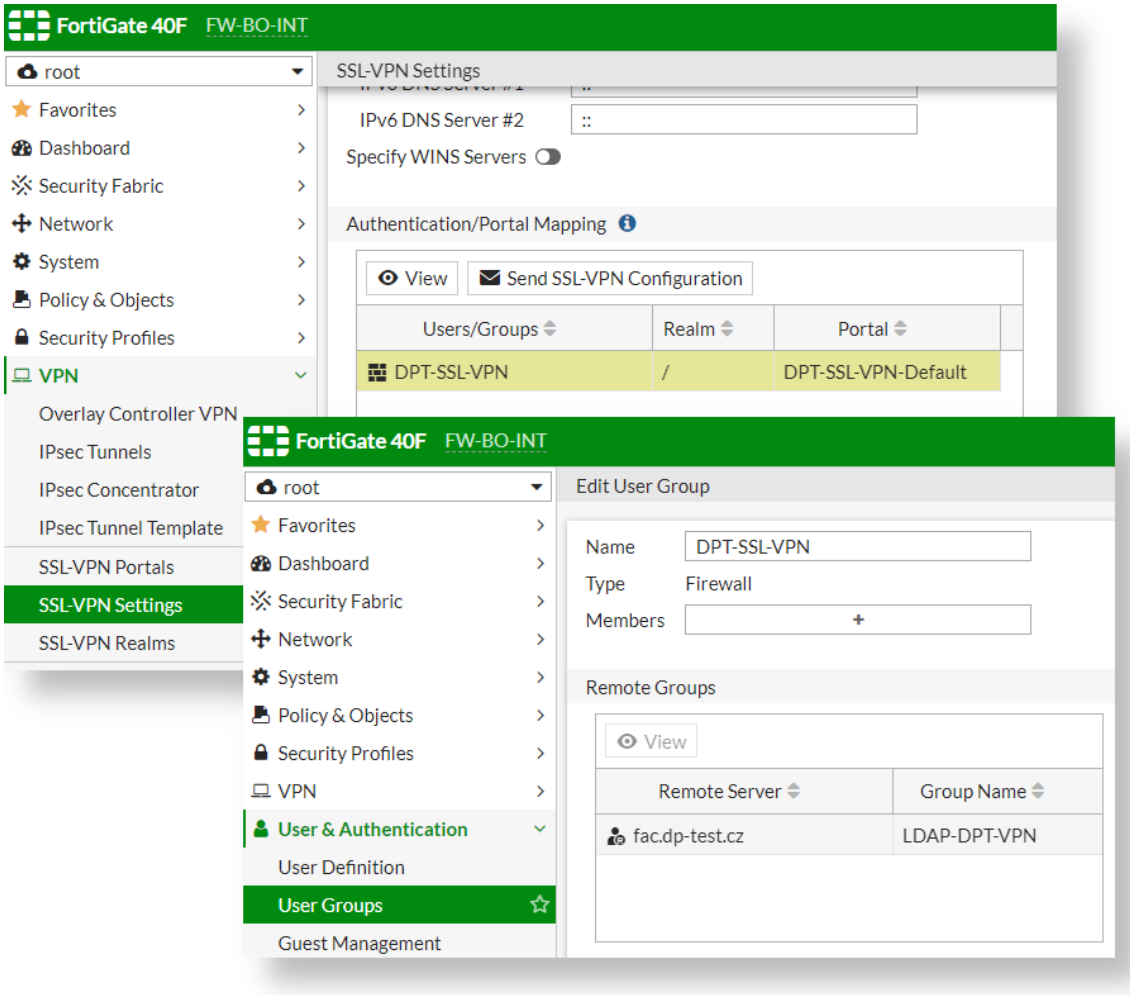
První čtyři konfigurační kroky budou provedeny, dle běžných postupů a preferencí organizace. V práci bude popsán krok poslední – mapování autentizace a oblasti na portál. Nejprve je potřeba vytvořit uživatelskou skupinu, která bude navázaná na RADIUS atribut Fortinet-Group-Name, poskytnutý FAC a následně skupinu použít v mapování portálu. Tzn. po procesu ověření prostřednictvím FAC, dojde k přiřazení skupiny uživateli ve FortiGate na základě hodnoty atributu Fortinet-Group-Name a následnému přiřazení správného nastavení VPN tunelu, definovaného v SSL-VPN portálu.

Nastavení uživatelské skupiny (User & Authentication, User Groups) provedeme s parametry (Obr. 47):

- **Name**: název skupiny, kterou později použijeme při mapování (DPT-SSL-VPN),
- **Type**: typ skupiny (Firewall),
- **Remote Groups**:
    - **Remote Server**: RADIUS server (FAC), nakonfigurovaný v kapitole *4.13.1 Konfigurace připojení FortiGate k LDAP a RADIUS serveru* (fac.dp-test.cz),
    - **Group Name**: RADIUS atribut Fortinet-Group-Name (LDAP-DPT-VPN).

Vytvořenou skupinu namapujeme na výchozí oblast a vytvořený portál (Obr. 47) v nastavení SSL-VPN (VPN, SSL-VPN Settings, Authentication/Portal Mapping):

- **Users/Groups**: skupiny vytvořena v předchozím kroku (DPT-SSL-VPN),
- **Realm**: Default,
- **Portal**: portál s požadovaným nastavením tunelu pro skupinu (DPT-SSL-VPN-Default).



Obrázek 47. Mapování skupiny na RADIUS atribut (vlastní)

4.13.4 Konfigurace FW pravidel

V tomto bodě návrhu řešení máme splněny veškeré předpoklady pro použití identity uživatele při řízení síťového přístupu na firewallu. Identitu získanou FSSO můžeme nyní aplikovat ve FW pravidlech (FSSO identitu máme i na VPN, nemusíme tedy v pravidle použít VPN identitu danou FortiGate skupinou DPT-SSL-VPN). IAM uživateli Tomáš Veselý přidělil automaticky role pro přístup k několika systémům prostřednictvím navázaných AD skupin. Jejich využití bude následující:

- **Disk Uctarna-rw**: použije se ve FW pravidle pro síťový přístup na server „fs.dp-test.cz“, službou SMB a v nastavení oprávnění ve složce „\Uctarna“,
- **APP-Ucetnictvi-dev**: použije se ve FW pravidle pro síťový přístup na server „app-dev.dp-test.cz“, službou HTTPS a přidělení oprávnění do modulu „Účetnictví“ v obchodní aplikaci,

- **uctarna@dp-test.cz**: využitelné pro potřeby poštovního serveru, např. MS Exchange k distribuci e-mailů,
- **DP-test-Wi-Fi**: využitelné pro ověření klienta RADIUS serverem „as.dp-test.cz“ při 802.1X požadavku na připojení k Wi-Fi přístupovému bodu,
- **DP-test-VPN**: již bylo využito ve FAC (kapitola *4.12.5 Vytvoření a synchronizace skupiny pro autorizaci VPN připojení*).

V následujících příkladech bude provedena konfigurace FW pravidel pro první dva uvedené případy použití (Tab. 26 a 27). Na pravidlech je možné zapnout bezpečnostní profily antiviru, webového a DNS filtru, aplikační kontroly, IPS a další, vč. zapnutí SSL inspekce. Využití jmenovaných služeb vyžaduje provedení specifických konfigurací, které nejsou předmětem této práce a nebude jich využito.

Před konfigurací FW pravidel byly vytvořeny VLAN rozhraní (Network, Interfaces), adresní objekty (Policy & Objects, Addresses) a objekty služeb (Policy & Objects, Services), dle tabulek (Tab. 23–25). Předpokladem jsou rovněž funkční IPsec VPN do ostatních lokalit.

Tabulka 23. Vytvořené VLAN rozhraní

Name	**Interface**	**VLAN ID**	**Role**	**Addr. mode**	**IP/Netmask**	**DHCP Server: Relay IP**
SRV-BO-APP	LAN	30	LAN	Manual	10.0.30.1/24	10.0.20.4
SRV-DEV-APP	LAN	140	LAN	Manual	10.0.140.1/24	10.0.20.4
USR-BO	LAN	60	LAN	Manual	10.0.60.1/23	10.0.20.4

Tabulka 24. Vytvořené adresní objekty

Typ	**Cate-gory**	**(Group) Name**	**Type**	**IP/Netmask Members FQDN**	**Interface**
IP Range/Subnet	Address	USR-BO-NET	Subnet	10.0.60.0/23	USR-BO
IP Range/Subnet	Address	USR-BR-1-NET	Subnet	10.0.110.0/24	IPS-VPN-BR-1
IP Range/Subnet	Address	USR-BR-2-NET	Subnet	10.0.130.0/24	IPS-VPN-BR-2
IP Range/Subnet	Address	USR-VPN-NET	Subnet	10.0.65.0/22	SSL-VPN tunnel interface
Address Group	IPv4	USR-NET	Group	USR-BO-NET USR-BR-1-NET	

Typ	Cate-gory	(Group) Name	Type	IP/Netmask Members FQDN	Interface
				USR-BR-2-NET USR-VPN-NET	
FQDN	Address	fs.dp-test.cz	FQDN	fs.dp-test.cz	SRV-BO-APP
FQDN	Address	app-dev.dp-test.cz	FQDN	app-dev.dp-test.cz	SRV-DEV-APP

Tabulka 25. Vytvořené objekty služeb

Name	Category	Protocol Type	Address	Destination Port
SMB	File Access	TCP/UDP/SCTP	IP Range 0.0.0.0	TCP/445
HTTPS	Web Access	TCP/UDP/SCTP	IP Range 0.0.0.0	TCP/443

Tabulka 26. FW pravidlo pro přístup na souborový server

Položka	Hodnota	Popis
Name	Pristup na sdileny souborovy server	
Incoming Interface	Any	Příchozí provoz bude přicházet z LAN i VPN (tato dvě rozhraní nelze v podmínce kombinovat)
Outgoing Interface	SRV-BO-APP	VLAN rozhraní aplikačních serverů pro back office
Source	USR-NET	Zdrojové IP rozsahy uživatelských VLAN
	FSSO skupina pro ověření identity: CN=Disk Uctarna-rw,OU=DPT-Groups,DC=dp-test,DC=cz	
Destination	fs.dp-test.cz	Název hostitele souborového serveru
Schedule	always	Přístup nebude omezen časem připojení
Service	SMB	Přístup bude povolen pouze na cílový port služby SMB
Action	Accept	Povolení komunikace
Log Allowed Traffic	All Sessions	Zapnutí logování veškeré komunikace
Enable this policy	true	Povolení pravidla

Tabulka 27. FW pravidlo pro přístup na aplikační vývojový server

Položka	**Hodnota**	**Popis**
Name	Pristup na aplikacni server DEV	
Incoming Interface	Any	Příchozí provoz bude přicházet z LAN i VPN (tato dvě rozhraní nelze v podmínce kombinovat)
Outgoing Interface	SRV-DEV-APP	VLAN rozhraní aplikačních serverů pro vývojové prostředí
Source	USR-NET	Zdrojové IP rozsahy uživatelských VLAN
	FSSO skupina pro ověření identity: CN=APP-Ucetnictvi-dev,OU=DPT-Groups,DC=dp-test,DC=cz	
Destination	app-dev.dp-test.cz	Název hostitele souborového serveru
Schedule	always	Přístup nebude omezen časem připojení
Service	HTTPS	Přístup bude povolen pouze na cílový port služby HTTPS
Action	Accept	Povolení komunikace
Log Allowed Traffic	All Sessions	Zapnutí logování veškeré komunikace
Enable this policy	true	Povolení pravidla

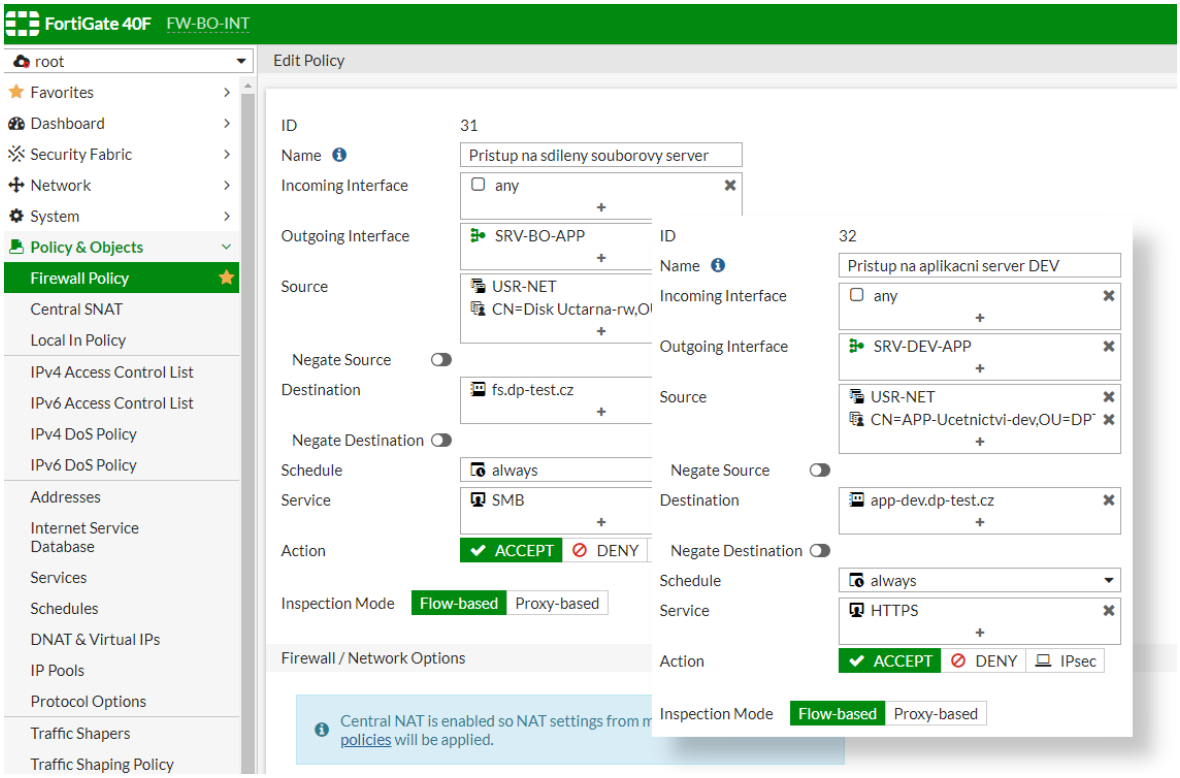
Výsledná pravidla jsou vyobrazena na obrázku (Obr. 48). FW pravidlo bude ve shodě, pokud budou splněny všechny definované podmínky. V podmínce „Source“ jsou mezi adresními objekty (AO) a objekty identity (IO) logické operace, viz (Rov. 1).

$$true = (AO_1 \, V \, AO_2 \ldots V \, AO_n) \wedge (IO_1 \, V \, IO_2 \ldots V \, IO_n) \quad (1)$$

Přičemž AO musí být vždy použito a může být samostatně, IO nemusí být použito (pokud nepotřebujeme v pravidle použít identitu) a nemůže být samostatně bez uvedení AO.

V podmínce „Destination“ mohou být použity objekty typu FQDN. FortiGate vždy překládá název hostitele na aktuální IP adresu prostřednictvím DNS dotazu.

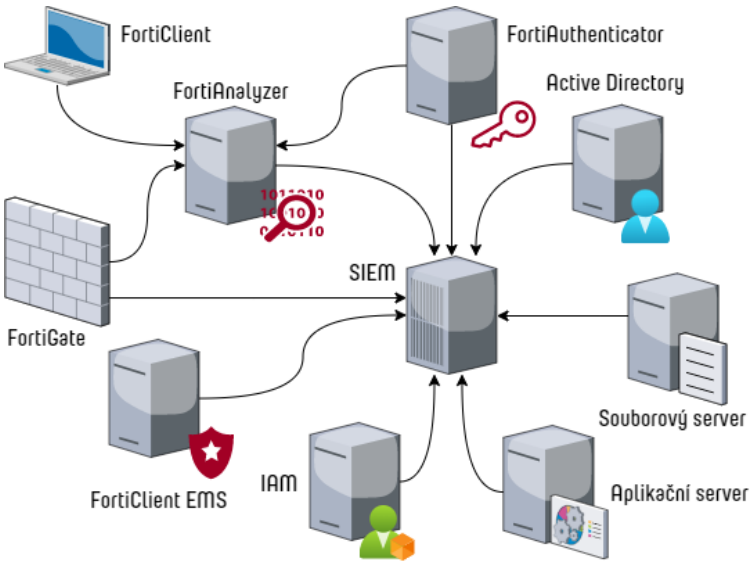
Aby uživateli fungovaly výše vytvořená FW pravidla i z VPN, musí existovat alespoň jedno další FW pravidlo, ve kterém je použit interface „SSL-VPN tunnel interface“. Může se jednat např. o pravidlo povolující síťové služby, jako je DNS nebo přístup na AD.



Obrázek 48. Výsledná FW pravidla (vlastní)

4.14 Bezpečnostní monitoring systému

Bezpečnostní monitoring navrženého řešení je založený na sběru logů ze všech participujících systémů a jejich následné vyhodnocování systémem FortiAnalyzer (FAZ) a SIEM. Schéma na obrázku (Obr. 49) znázorňuje přenos událostí logů mezi systémy. V některých případech je vhodné nebo potřebné logy zasílat do FAZ.



Obrázek 49. Přenos logů do SIEM (vlastní)

4.14.1 Konfigurace zasílání logů

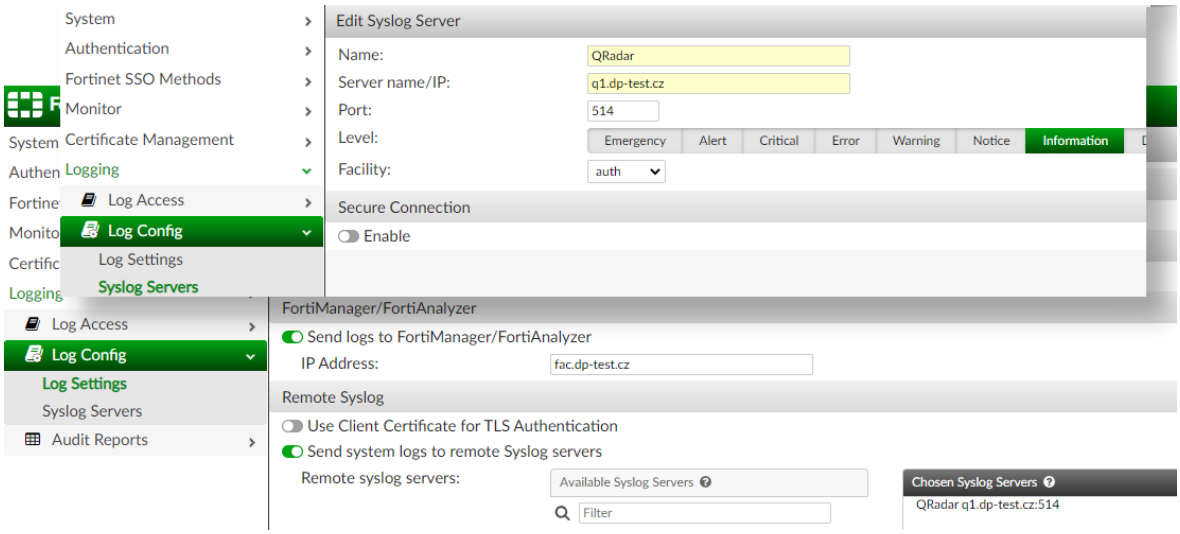
Do SIEM jsou předávány a následně vyhodnocovány logy ze všech systémů, včetně síťových prvků, databází, OS serverů, aplikací atd. V rámci navrhovaného řešení bude popsána konfigurace přenosu logů do nástroje FotiAnalyzer a SIEM QRadar.

FortiClient zasílá logy do FAZ, který je umístěný v DMZ, čímž je umožněn příjem logů z kterékoliv sítě. Následně jsou logy přeposílány do SIEM. Konfigurace logování FC se provádí v EMS v profilu systémového nastavení (Endpoint Profiles, System Settings, Log). Po zapnutí volby „Upload Logs to FortiAnalyzer“ vybereme typy logů, které požadujeme zasílat, interval zasílání, retenci a název hostitele (faz.dp-test.cz). Protože budou logy zasílány i z veřejných sítí, vynutíme šifrování zapnutím volby „SSL Enabled“

Logy z **EMS** budeme zasílat přímo do SIEM (není umožněno zasílání logu do dvou různých destinací současně). V nastavení logování (System Settigs, Log Settings) zvolíme úroveň logování (Info), retenci logů, v položce „Send system log messaages externally“ vybereme volbu „SysLog a vyplníme parametry pro přenos logů:

- **SysLog server address**: v našem případě doménový název SIEM (q1.dp-test.cz),
- **SysLog server port**: uvedeme standardní syslog port (514),
- **Data protocol**: TCP (lze použít i UDP, ale pouze pro události kratší 4KB).

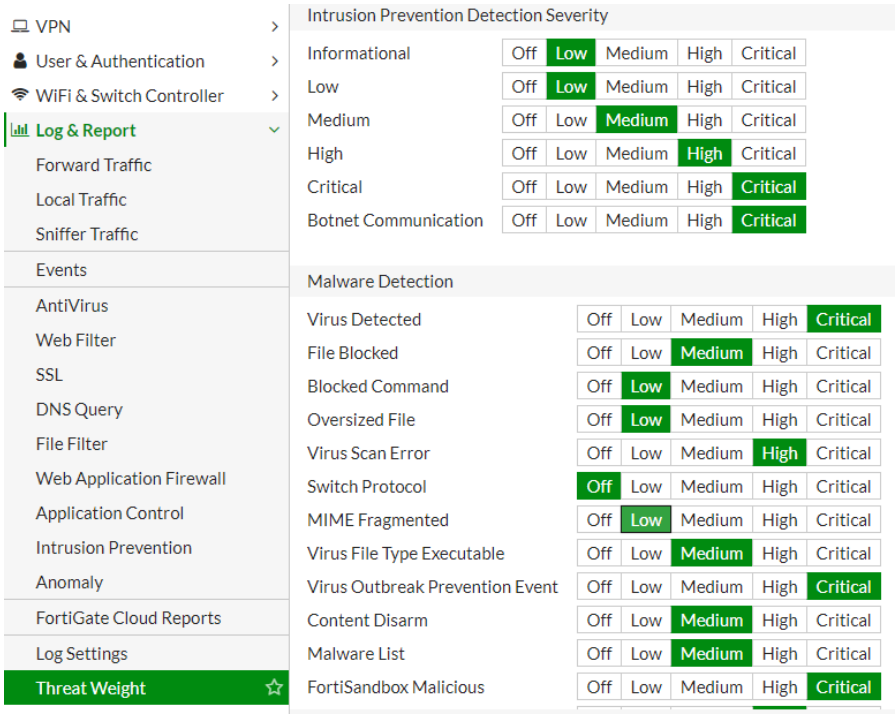
V systému **FortiAuthenticator** je logování věnována celá sekce (Logging). Logy budeme zasílat současně do FortiAnalyzeru i SIEM (Obr. 50). Nejprve vytvoříme syslog server (Logging, Log Config, Syslog Servers) vyplněním údajů pro zasílání na SIEM, stejně jako v případě EMS. Zvolíme úroveň logování (Info).



Obrázek 50. Konfigurace přeposílání logů ve FAC (vlastní)

Nastavíme zasílání logů (Logging, Log Config, Log Settings) na FAZ zapnutím volby „Send Logs to FortiAnalyzer“ a vepsáním doménového názvu (faz.dp-test.cz). V sekci „Remote Syslog zapneme volbu „Send systém logs to remote Syslog servers“ a vybereme název serveru vytvořeného v předchozím kroku.

Logování ve **FortiGate** je, vzhledem k důležitosti logů FW pravidel a dalších bezpečnostních a provozních služeb, věnována velká pozornost. FortiGate má vytvořené grafické rozhraní pro detailní prohlížení logů ze všech jim poskytovaných služeb. U každé lze podrobně nastavit váhy pro výpočet kritičnosti události (ukázka na Obr. 51), přeposílání na FAZ a další syslog server. U každého jednotlivého FW pravidla je možné zvolit, zda vyžadujeme logování všech relací, procházejících pravidlem nebo jen bezpečnostních událostí.

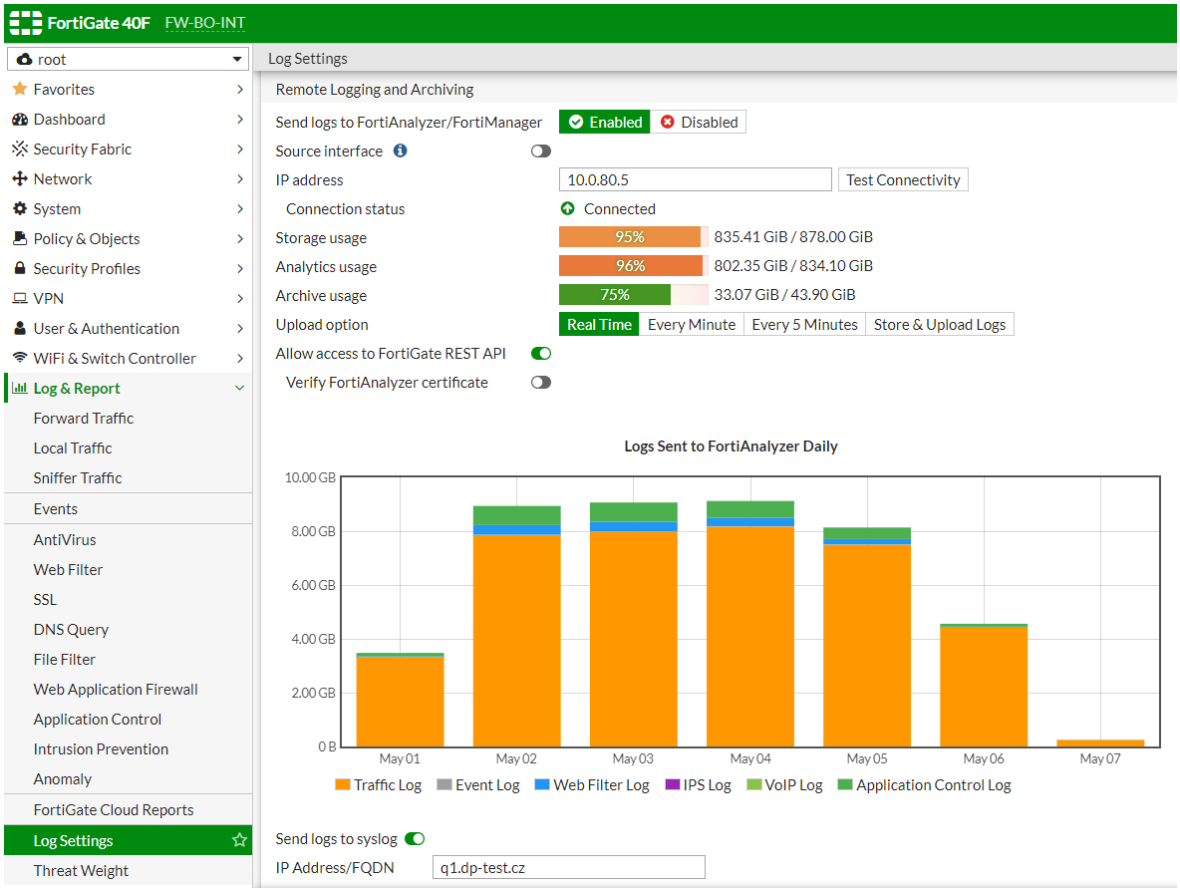


Obrázek 51. Ukázka nastavení vah detekovaných událostí (vlastní)

Logy FortiGate budeme současně přeposílat na FAZ i do SIEM. Provedeme konfiguraci (Log & Report, Log Settings) v sekci „Remote Logging and Archiving“:

- **Send logs to FortiAnalyzer**: zapneme volbu pro přeposílání logu do FAZ,
- **IP address**: vepíšeme IP adresu FAZ (10.0.80.5),
- **Upload option**: zvolíme zasílání logů v reálném čase (Real Time),
- **Send logs to syslog**: povolíme volbu a do pole „IP Address/FQDN“ vepíšeme doménový název SIEM (q1.dp-test.cz).

V grafu lze odečíst množství logů přeposlaných do FAZ z jednotlivých služeb (Obr. 52).



Obrázek 52. Konfigurace přeposílání logů ve FortiGate (vlastní)

IAM logy jsou zasílány do SIEM nástrojem **rsyslog** z prostředí OS Linux. V konfiguraci (Obr. 53) je nastaveno přeposílání logu webové proxy. Vzhledem k faktu, že front-end IAM získává data prostřednictvím volání API back-endu, obsahuje log kompletní informaci o každé aktivitě uživatele. Zasílat lze i další logy systému, včetně logu back-endu.

```
[root@localhost rsyslog.d]# cat 09_web-proxy_fwd.conf
:programname, isequal, "web-proxy" {
        action (type="omfwd" protocol="udp" target="q1.dp-test.cz" port="514")
}
```

Obrázek 53. Konfigurace přeposílání logu z IAM, upraveno z: [84]

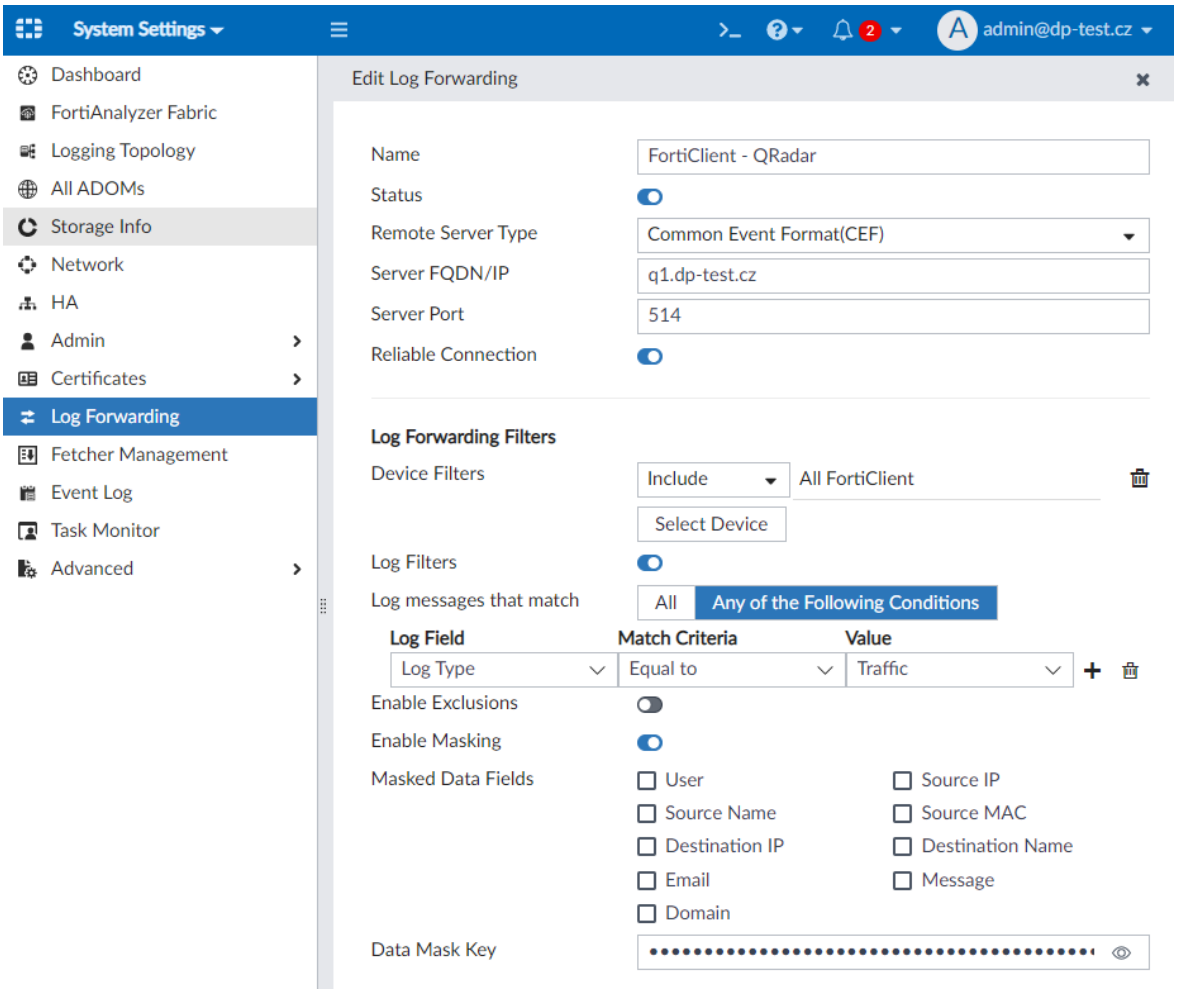
ActiveDirectory na doménové řadiči a **souborový server** jsou provozovány na OS Windows Server. Ve Windows jsou logy, které potřebujeme získávat, ukládány do Security Event Logu, který je v pravidelných intervalech vyčítán nástrojem WinCollect a předáván do SIEM QRadar. Nastavení vyžaduje konfiguraci politik na Windows serverech, konfiguraci WinCollect serveru i QRadar SIEM a bylo provedeno dle postupů uvedených v práci „*Bezpečnostní monitoring uživatelů v informačních systémech*“ [1].

4.14.2 FortiAnalyzer

FortiAnalyzer automaticky shromažďuje, ukládá a analyzuje logy ze všech bezpečnostních zařízení Fortinet. Umožňuje identifikovat síťové anomálie v reálném čase, sledovat dodržování předpisů, vytvářet reporty, vyhledávat události pomocí různých kritérií. Na jednom místě zobrazuje přehled, který umožní odhalit potenciální bezpečnostní hrozby a optimalizovat síť. [85]

Pro účely této práce bude FAZ (ve verzi 7.2.2) sloužit především pro přeposílání logů z FortiClienta do SIEM. Ostatní Fortinet systémy byly nastaveny pro zasílání logů na SIEM přímo. Každé zařízení, které zasílá logy do FAZ, musíme autorizovat (Device Manager, Unautorized Devices). Vybereme zařízení, klikneme na „Authorize“ a pojmenujeme.

Konfigurace přeposílání logů (Systém Settings, Log Forwarding) umožňuje detailně nastavit filtrování událostí, dle mnoha kritérií. Další možností je maskovat vybrané informace v logu (Obr. 54).



Obrázek 54. Konfigurace přeposílání logů z FAZ do SIEM (vlastní)

Provedeme konfiguraci s následujícími parametry:

- **Name**: název konfigurace (FortiClient – QRadar),
- **Remote Server type**: logy budou formátovány dle zvoleného typu. Z možného výběru je pro SIEM nejlepší volbou typ „Common Event Format“,
- **Server FQDN**: doménový název destinace přeposílání logů (q1.dp-test.cz),
- **Server Port**: uvedeme standardní syslog port (514),
- **Reliable Connection**: zapnutím volby bude použito TCP spojení, místo UDP,
- **Log Forwarding Filters**:
    - **Device Filters**: budeme přeposílat pouze logy FortiClient. Zvolíme „Include“ a tlačítkem „Select Device“ zobrazíme nabídku, ve které zvolíme „FortiClient“ (ve správci zařízení jsme pojmenovali DPT-FC),
- volbu „Log Filters“ ani „Enable Masking“ nepoužijeme. Na obrázku (Obr. 54) je jen pro ukázku.

Nastavíme rovněž zasílání systémových logů FAZ do SIEM (Systém Settings, Advanced, Syslog Server). Přidáme server a nastavíme parametry stejně, jako v předchozích krocích (název, FQDN „q1.dp-test.cz“, port 514). Reliable Connection nemusíme zapínat, systémové logy nejsou tolik obsáhlé.

4.14.3 SIEM – QRadar

Vyhodnocování logů bude prováděno v nástroji IBM QRadar SIEM, verze 7.5.0. S tímto nástrojem mám bohaté praktické zkušenosti, které budou využity při tvorbě korelačních pravidel a analýze výsledků v následujících kapitolách.

QRadar přijímá logy zasílané protokolem syslog automaticky komponentou „QRadar Event Collector“, bez nutnosti nastavení příjmu. Úkolem kolektoru je logy normalizovat a předat ke zpracování komponentě „QRadar Event Processor“, kde dochází k vyhodnocování událostí na základě definovaných pravidel. Aby kolektor mohl provádět normalizaci, je pro každý přijímaný log nutné vytvořit „zdroj logů“ (Log Source), ve kterém se mimo jiné definuje struktura logů. Ta je popsána v Device Support Module (DSM). IBM dodává množství již předpřipravených DSM, ale lze vytvořit i vlastní. [1]

Při monitoringu systému řízení přístupu můžeme využít k analýze logy z několika systémů (FortiClient, FortGate, FortiAuthenticator, doménový řadič / ActiveDirectory, souborový server, IAM server), pro které vytvoříme v QRadaru zdroj logů. Konfigurace se prování

v modulu „IBM QRadar Log Source Management“ (Admin, Apps, QRadar Log Source Management). IBM poskytuje k použití v QRadaru hotové DSM, pro všechny systémy Fortinet. U všech konfigurací zdrojů logů (Tab. 28 a 29) budou shodně nastaveny parametry:

- **Coalescing Events**: sdružení stejných událostí do jedné (No),
- **Store Event Payloads**: uchování celého obsahu události (Yes).

Položka „Log Source Type“ určuje použitý DSM.

Tabulka 28. Konfigurace Log Source Fortinet systémů

Položka	**FortiClient**	**FortiAuthenticator**	**FortiGate**	**IAM server**
Log Source Type	Fortinet FortiClient Logs	Fortinet FortiAuthenticator	Fortinet FortiGate Security Gateway	Linux OS
Protocol Type	Syslog			
Log Source Identifier	DPT-FC	10.0.80.4	10.0.10.1	iam.dp-test.cz

Tabulka 29. Konfigurace Log Source ostatních systémů

Položka	**Doménový řadič**	**Souborový server**
Log Source Type	Microsoft Windows Security Event Log	
Protocol Type	WinCollect	
Log Source Identifier	dc.dp-test.cz	fs.dp-test.cz
Domain	dp-test.cz	dp-test.cz
User Name (Password)	wc-ad	wc-fs
Pooling Interval (ms)	3000	
Event Log Pool Protocol	MSEVEN6	
Standard Log Types	Security, Systém, Application, Directory Service	Security, Systém, Application,
Event Types	Všechny volby	
WinCollect Agent	WinCollect - dc.dp-test.cz	WinCollect - fs.dp-test.cz

4.14.4 Ukázka logů a ověření funkčnosti

Na prvním obrázku (Obr. 55) je auditní událost z AD, která značí vytvoření objektu uživatele systémem IAM (událost je zkrácená).

```
<13>May 04 14:30:15 dc.dp-test.cz AgentDevice=WindowsLog  AgentLogFile=Security
PluginVersion=7.3.1.22  Source=Microsoft-Windows-Security-Auditing
Computer=dc.dp-test.cz  OriginatingComputer=10.0.20.2  User=  Domain=
EventID=4720  EventIDCode=4720  EventType=8  EventCategory=13824
RecordNumber=443599153  TimeGenerated=1683203414  TimeWritten=1683203414
Level=Log Always  Keywords=Audit Success
Task=SE_ADT_ACCOUNTMANAGEMENT_USERACCOUNT  Opcode=Info  Message=A user account was
created.  Subject:  Security ID:  DPTEST\iam-ad  Account Name:  iam-ad  Account
Domain:  DPTEST  Logon ID:  0x748A92EE  New Account:  Security ID:
DPTEST\tvesely628  Account Name:  tvesely628  Account Domain:  DPTEST
Attributes:  SAM Account Name: tvesely628  Display Name:  Tomáš Veselý  User
Principal Name: tvesely628@dp-test.cz...
```

Obrázek 55. Ukázka logu AD (vlastní)

Ze zvýrazněných polí lze vyčíst:

- **Computer**: ze kterého Windows serveru událost pochází,
- **EventID=4720, Message**: ID pro vytvoření nového uživatele a textový popis,
- **Subject: Security ID**: učet, který objekt vytvořil,
- **New Account: Security ID**: objekt, který byl vytvořen,
- **Display Name**: jeden z vytvořených atributů objektu.

Na obrázku (Obr. 56) je vyobrazena událost ze SW FortiClient instalovaného na zařízení uživatele. Z logu lze vyčíst mnoho užitečných informací, ale zásadní je zvýrazněná část, informující o změně IP adresy v rámci FSSO.

```
May 07 13:55:51 DPT-FC CEF:0|Fortinet|FortiClient-EMS|6.4,build9999|0|fsso
securityevent ipchange|4|start=May 07 2023 13:55:51
deviceExternalId=FCTEMS0000125883 ad.vd=default ad.itime=1683463574
ad.fctsn=FCT8003525322351 ad.logver=1 ad.logid=96980 cat=securityevent
ad.subtype=fsso ad.eventtype=status deviceSeverity=info
ad.uid=12232BC01A5C4344BC7A0DC80ED7C45A dhost=NTB-628 ad.pcdomain=dp-test.cz
ad.deviceip=192.168.1.9 ad.devicemac=8c-8f-c5-f8-01-b6 ad.site=default
ad.fctver=7.0.8.0427 ad.fgtserial=N/A ad.emsserial=FCTEMS0000125883
ad.usingpolicy=Finance ad.os=Microsoft Windows 11 Professional Edition 64-bit
(build 22621) duser=tvesely628 msg=Single Sign-On event act=ipchange
destinationDnsDomain=DP-TEST.CZ Workstation Name:NTB-628 IP:10.0.65.2
FAC:10.0.80.4 succeeded to send session info TICC:3055784 TID:9592 tz="+0000"
```

Obrázek 56. Ukázka logu SW FortiClient (vlastní)

Další ukázka události (Obr. 57) pochází z FW FortiGate a oznamuje úspěšné připojení do sítě použitím VPN. Ze zvýrazněných částí získáme informace např. o vzdálené IP adrese připojujícího se klienta, uživatelské jméno a skupinu ve FortiGate, která je aplikovatelná ve FW pravidlech.

```
<190>date=2023-05-07 time=14:46:09 devname="FW-BO-INT" devid="FG6F1D5579223953"
eventtime=1683463569656415088 tz="+0200" logid="0101039424" type="event"
subtype="vpn" level="information" vd="root" logdesc="SSL VPN tunnel up"
action="tunnel-up" tunneltype="ssl-web" tunnelid=320467124 remip=94.113.156.110
user="tvesely628" group="DPT-SSL-VPN" dst_host="N/A" reason="login successfully"
msg="SSL tunnel established"
```

Obrázek 57. Ukázka logu FW FortiGate (vlastní)

Poslední ukázka je opět z logu FortiGate (Obr. 58). Událost značí úspěšný průchod vytvořeným FW pravidlem ID 31, povolující přístup k souborovému serveru (událost byla zkrácena). Při testu bylo přistoupeno ke sdílenému úložišti v síťové cestě: \\fs.dp-test.cz\uctarna.

```
<189>date=2023-05-08 time=00:35:46 devname="FW-BO-INT" devid="FG6F1D5579223953"
eventtime=1683498947034762860 tz="+0200" logid="0000000020" type="traffic"
subtype="forward" level="notice" vd="root" srcip=10.0.65.2 srcport=26471
srcintf="ssl.root" srcintfrole="undefined" dstip=10.0.30.4 dstport=445
dstintf="Pol" dstintfrole="lan" srccountry="Reserved" dstcountry="Reserved"
sessionid=1900499665 proto=6 action="accept" policyid=31 policytype="policy"
poluuid="9a6edf1a-ele3-5e1b-7ecc-ae724bfd0323" policyname="Pristup na sdileny
souborovy server" user="TVESELY628" group="CN=Disk
Uctarna-rw,OU=DPT-Groups,DC=dp-test,DC=cz" authserver="Fortiautenticator"
service="SMB" trandisp="noop" duration=7281 sentbyte=14555 rcvdbyte=15816
sentpkt=145 rcvdpkt=129 appcat="unscanned" sentdelta=52 rcvddelta=41
```

Obrázek 58. Ukázka logu FW pravidla z FortiGate (vlastní)

Význam zvýrazněných informací je následující:

- **type="traffic", subtype="forward", action="accept"**: jedná se o událost směrování provozu, který byl potvrzen (pravidlo provoz akceptovalo),
- **srcip**: zdrojová IP adresa (IP adresa z rozsahu VPN),
- **dstip, dstport**: cílová IP adresa (souborový server) a cílový port (služba SMB),
- **policyid, policyname**: identifikátor a popis FW pravidla (přístup na souborový server na základě identity),
- **user, group, authserver**: identifikovaný uživatel, skupina a server, který provedl autentizaci.

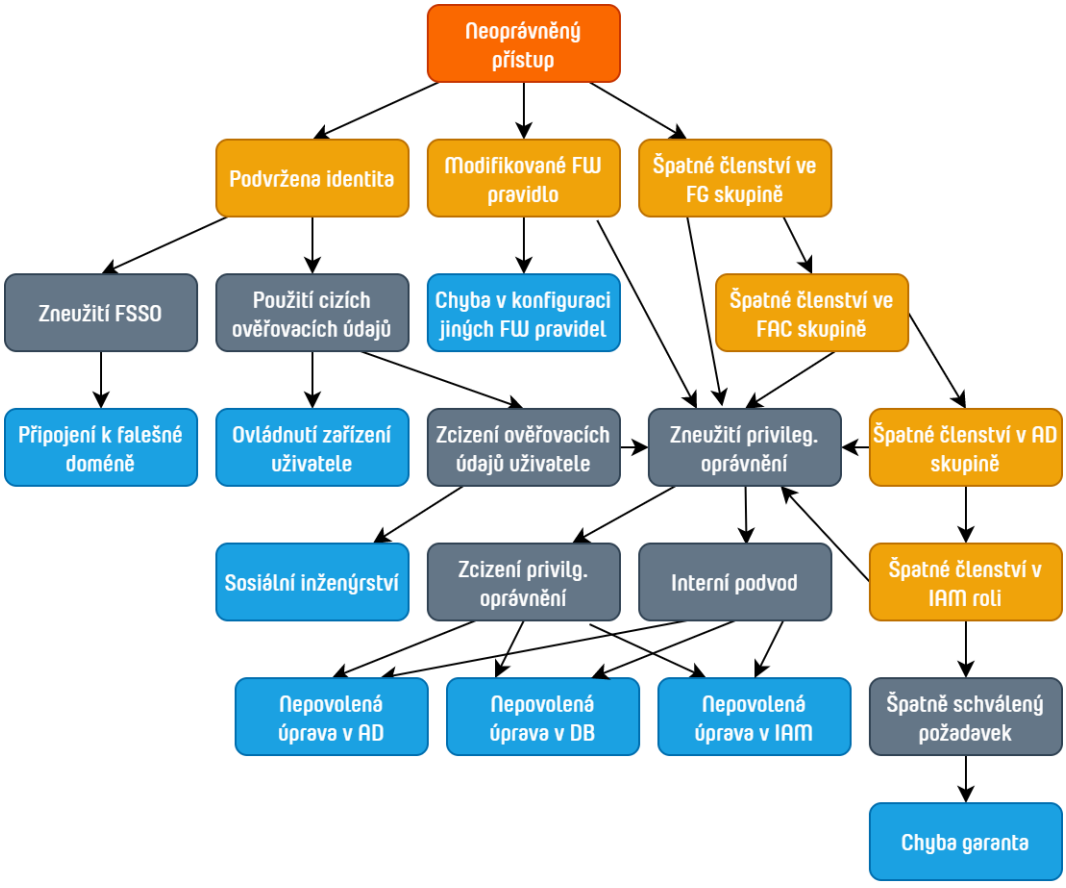
V kapitole byl představen návrh řešení řízení přístupů na základě identit a popsán kompletní postup při jeho realizaci. Byla provedena konfigurace všech systémů a nástrojů podílejících se na celém procesu, od vzniku identity až po její uplatnění při řízení síťových přístupů. Funkčnost řešení byla ověřována v průběhu konfigurace systémů, které na sebe funkčně navazují a v závěru potvrzena vyhodnocením logů.

5 MONITORING NEŽÁDOUCÍCH AKTIVIT A VYHODNOCENÍ

Cílem kapitoly je pokusit se najít slabá místa navrženého systému sérií testů odolnosti, vůči jednotlivým jejím částem, připravit pravidla v systému SIEM pro detekci takových pokusů, a případně navrhnout opatření ke snížení rizika překonání systému. Závěrem bude provedeno vyhodnocení odolnosti i celého navrženého řešení.

5.1 Nalezení slabin metodou FTA

Pro nalezení slabých mís byla použita metoda „Fault Tree Analysis“ (FTA), tedy analýza stromu poruchových stavů. Na obrázku (Obr. 59) je zjednodušený diagram FTA, kde každá spojnice má význam logického operátoru OR (nebo). Modře jsou vyznačeny příčiny, které je potřeba ošetřit.



Obrázek 59. FTA diagram (vlastní)

Opatření pro snížení rizik plynoucích z nalezených možných příčin překonání navrženého systému jsou následující:

- **zneužití FSSO**: FSSO založené na získávání identity prostřednictvím agenta „FortiClient SSO Mobility Agent“ by mohlo být zneužité k podvržení identity.

FortiClient by mohl být připojen k falešné, neautorizované doméně a ověřen falešným účtem. Tomu lze zabránit zapnutím NTLM autentizace v nastavení FAC FSSO (Fortinet SSO Methods, SSO, General, FSSO, Enable NTLM),

- **zcizení ověřovacích údajů uživatele**: zcizit ověřovací údaje uživatele lze mnoha způsoby. Nejběžnější metodou je vylákání údajů z uživatele prostřednictvím phishingu. Ke snížení tohoto rizika vedou opatření organizační (např. školení uživatelů) i technická, např. blokování nebezpečných e-mailových příloh, použití webového filtru, správné nastavení doménových záznamů (SPF, DKIM, DMARC), pomáhajících filtrovat příchozí e-maily atd. Identita uživatele může být zcizena jiným uživatelem, který má oprávnění ke správě AD (člen helpdesku, administrátor…), který má oprávnění vyresetovat heslo a následně identitu využít k přihlášení. Existují technické prostředky, jak pravděpodobnost takového jednání alespoň snížit (nasazení správy privilegovaného přístupu – PAM). Pro včasnou detekci bude konfigurováno pravidlo v SIEM „*DP: Heslo uživatele bylo změněno jinou osobou*“. Heslo lze v některých případech získat útokem silou (brute force attack). Tento typ útoku lze omezit správně implementovaným druhým faktorem ověření, zavedením ochrany proti opakovanému chybnému zadávání hesla (časový limit mezi pokusy) nebo blokováním účtu po několika špatných pokusech. Monitorovat jej budeme v SIEM, pomocí pravidla „*DP: Útok silou na ověření hesla*“,
- **zcizení ověřovacích údajů privilegovaného uživatele**: nelze takovou možnost úplně vyloučit i přes implementaci doporučených bezpečnostních opatření. K takovým opatřením náleží používaní speciálního administrátorského účtu (není používán k běžné práci uživatele) a vynucení dalších faktorů ověření (např. HW token). K detekci změn na účtu privilegovaného uživatele bude použito pravidlo v SIEM: „*DP: Na privilegovaném účtu byla provedena změna*“,
- **zneužití privilegovaného oprávnění**: ať už jde o aktivitu útočníka nebo o interní podvod, je užitečné monitorovat změny na klíčových systémech v rámci řízení přístupů. Privilegovaný uživatel má možnost měnit nastavení systémů. Musí být zavedeno oddělení rolí tak, aby jeden uživatel neměl oprávnění měnit konfiguraci na více klíčových systémech a aby neměl oprávnění ovlivnit auditní záznamy o takových činnostech. Pro detekci nepovolené úpravy členství v AD skupině bude v SIEM nastaveno pravidlo: „*DP: Změna členství v AD skupině mimo IAM*“.

K detekci pokusu o přímé přistoupení k DB IAM bude vytvořeno pravidlo: „*DP: Nepovolený přístup k DB IAM*“,

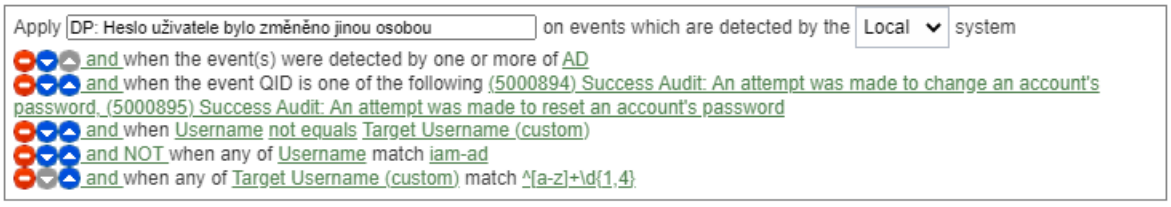
- **špatně schválený požadavek v IAM**: může se stát, že nedbalostí nebo úmyslem dojde ke schválení žádosti o roli v IAM, ke které by uživatel neměl mít oprávnění. K minimalizaci takových případů lze zavést dvě opatření. Prvním je, u zvláště citlivých rolí, nastavit schvalovací workflow tak, aby došlo k postupnému schválení více osobami (např. garant role a následně security manager). Druhým opatřením je zakázat možnost o roli žádat a přidělovat ji pouze automatickou rolí. Pro kontrolu dodržování prvního opatření bude zavedeno pravidlo v SIEM: „*DP: Neschválené přidání člena do skupiny Domain Admins*“.

5.2 SIEM – korelační pravidla

Pravidla budou konfigurována v IBM QRadar SIEM. Každé pravidlo bude doprovázet popis použitých podmínek a ověření funkčnosti provedením testu. V pravidlech bude nastavena odezva na sepnutí, která vytvoří událost v QRadaru a zašle pracovníkovi IT bezpečnosti upozornění e-mailem. Konfigurace pravidel je dostupná v nabídce „Offenses, Rules“.

5.2.1 DP: Heslo uživatele bylo změněno jinou osobou

Po nasazení systému IAM již není odůvodnitelné provádět jakékoliv změny na objektech uživatele přímo v AD. Vytváření, změny i zakázání uživatelského účtu v AD provádí IAM pod technickým účtem. To platí i pro reset hesla pracovníkem helpdesku, v případě že ho uživatel zapomene. Pravidlem (Obr. 60) budeme detekovat změnu uživatelského hesla, kterou neprovede uživatel sám nebo nebude provedena technickým účtem „iam-ad“.



Obrázek 60. Pravidlo pro detekci změny hesla uživatele (vlastní)

Podmínky pravidla:

- zdroj logů je zařazen do skupiny logů AD. Do této skupiny byl při konfiguraci umístěn zdroj logů „Doménový řadič“,

- identifikátor události je 8000894 (úspěšná změna hesla) nebo 5000895 (úspěšný reset hesla),
- uživatelský účet iniciátora změny hesla není shodný s cílovým účtem (vyloučí se běžné změny hesla uživatelem),
- uživatelský účet iniciátora změny hesla není „iam-ad“ (vyloučí se změny hesla provedené IAM),
- název cílového účtu odpovídá regulárnímu výrazu „^[a-z]+\d{1,4}“ (pokud je jasně daný formát uživatelského jména, vyloučíme tímto nastavením změny hesel u technických účtů).

Pro otestování pravidla byl proveden reset hesla uživatele „tvesely628“ uživatelem s privilegovaným oprávněním „bad-admin“. Byla vygenerovaná událost (Obr. 61) a e-mailové upozornění s detaily události.

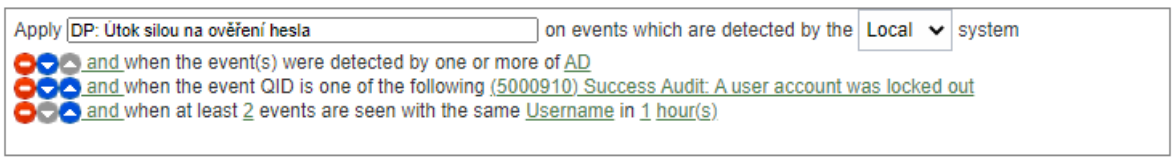
Event Information

Event Name	DP: Heslo uživatele bylo změněno jinou osobou						
Low Level Category	Object Modification Success						
Event Description	Heslo si nezměnil uživatel sám nebo nebylo změněno prostřednictvím IAM						
Magnitude	(9)	Relevance	10	Severity	8	Credibility	10
Username	bad.admin						
Start Time	9. 5. 2023 14:11:18	Storage Time	9. 5. 2023 14:11:18	Log Source Time	9. 5. 2023 14:11:18		
CRE Description (custom)	Heslo si nezměnil uživatel sám nebo nebylo změněno prostřednictvím IAM						
CRE Name (custom)	DP: Heslo uživatele bylo změněno jinou osobou						

Obrázek 61. Odezva na pravidlo pro detekci změny hesla uživatele (vlastní)

5.2.2 DP: Útok silou na ověření hesla

V doméně je aplikována politika uzamčení účtu na 15 minut v případě opakovaného chybného zadaní hesla. Pravidlo vyhodnocuje uzamčení účtu uživatele v AD. Pokud dojde k uzamčení účtu v nastavených limitech, pravidlo (Obr. 62) sepne.



Obrázek 62. Pravidlo pro detekci útoku silou na ověření hesla (vlastní)

Nevýhodou pravidla je určité množství falešně pozitivních hlášení, kdy si uživatel změní heslo a má na zařízení staré heslo pro ověřování uložené např. v připojení k síťové jednotce.

Podmínky pravidla:

- zdroj logů je zařazen do skupiny logů AD,
- identifikátor události je 5000910 (uzamčení účtu),
- účet je uzamčen minimálně 2x během hodiny.

Test proběhl opakovaným zadáním špatného hesla pro účet tvesely628, ve webové aplikaci s ověřením vůči AD. Sepnutí pravidla vyvolalo událost (Obr. 63) a e-mailové upozornění.

Event Information

Event Name	DP: Útok silou na ověření hesla						
Low Level Category	User Account Locked						
Event Description	Opakované uzamčení uživatelského účtu v AD, minimálně 2x za hodinu						
Magnitude	(8)	Relevance	10	Severity	5	Credibility	10
Username	tvesely628						
Start Time	9. 5. 2023 23:55:42	Storage Time	9. 5. 2023 23:55:42	Log Source Time	9. 5. 2023 23:55:42		
CRE Description (custom)	Opakované uzamčení uživatelského účtu v AD, minimálně 2x za hodinu						
CRE Name (custom)	DP: Útok silou na ověření hesla						

Obrázek 63. Odezva na pravidlo pro detekci útoku silou (vlastní)

5.2.3 DP: Na privilegovaném účtu byla provedena změna

Účty s oprávněním k administraci systémů nebo jejich částí musí být dobře zabezpečeny a monitorovány. Změny na účtech musí být bezodkladně vyhodnocovány a ověřovány s jejich vlastníky. Před vytvořením pravidla připravíme potřebné seznamy, které jsou v QRadaru uloženy v „reference data“ strukturách. Pro pravidlo použijeme „reference set“ tabulky (RS), které obsahují pouze jeden atribut s unikátními hodnotami (Tab. 30). Každá admin role odpovídá skupině v AD a je zastoupena jedním RS.

Tabulka 30. Seznamy privilegovaných účtů

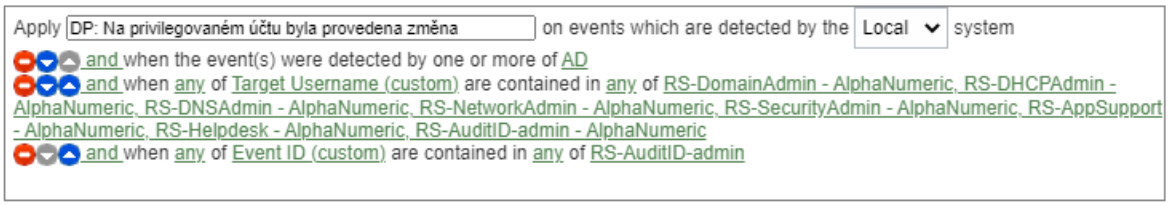
Admin role	Název reference setu	Přiřazené privilegované účty
Domain admin	RS-DomainAdmin	lipa, javor
DHCP admin	RS-DHCPAdmin	kastan, smrk
DNS admin	RS-DNSAdmin	lipa, javor

Admin role	Název reference setu	Přiřazené privilegované účty
Network admin	RS-NetworkAdmin	kastan, smrk
Security admin	RS-SecurityAdmin	modrin, vrba
App support	RS-AppSupport	topol, jinan
Helpdesk	RS-Helpdesk	sekvoje, orech, jedle, osika

Na účtech bude prováděn audit změn, podle RS „RS-AuditID-admin“ (Tab. 31). V pravidle (Obr. 64) dojde k porovnání ID události a uživatelského jména v obsahu auditní události s hodnotami v uvedených RS.

Tabulka 31. RS-AuditID-admin, ID událostí, čerpáno z: [86]

ID	Popis
4625	Účet se nepodařilo přihlásit
4723	Byl proveden pokus o změnu hesla účtu
4724	Byl proveden pokus o resetování hesla účtu
4725	Uživatelský účet byl zakázán
4726	Uživatelský účet byl odstraněn
4738	Byl změněn uživatelský účet
4740	Uživatelský účet byl zablokován
4767	Uživatelský účet byl odblokován
4781	Název účtu byl změněn



Obrázek 64. Pravidlo pro detekci změn na privilegovaném účtu (vlastní)

Podmínky pravidla:

- zdroj logů je zařazen do skupiny logů AD,
- název cílového účtu je obsažen v kterémkoliv z uvedených RS,

- ID události je uvedeno v RS „RS-AuditID-admin“.

Účet „javor“ byl zakázán, což způsobilo změnu atributu „User Account Control“ (UAC) a vyvolalo událost (Obr. 65) a odeslání notifikace (Obr. 66). V e-mailové notifikaci lze z přiložené události vyčíst informaci o změně (UAC 0x11 = účet je uzamčený).

Event Information

Event Name	DP: Na privilegovaném účtu byla provedena změna						
Low Level Category	User Account Changed						
Event Description	Byla provedena změna na administrátorském účtu						
Magnitude	(9)	**Relevance**	10	**Severity**	8	**Credibility**	10
Username	javor						
Start Time	10. 5. 2023 22:04:41	**Storage Time**	10. 5. 2023 22:04:41	**Log Source Time**	10. 5. 2023 22:04:41		
CRE Description (custom)	Byla provedena změna na administrátorském účtu						
CRE Name (custom)	DP: Na privilegovaném účtu byla provedena změna						

Obrázek 65. Odezva na pravidlo pro detekci změn na privileg. účtu (vlastní)

-----Original Message-----
From: qradar@dp-test.cz <qradar@dp-test.cz>
Sent: Wednesday, May 10, 2023 10:05 PM
To: itsecurity <itsecurity@dp-test.cz>
Subject: DP: Na privilegovaném účtu byla provedena změna Fired

The following is an automated response sent to you by the QRadar event custom rules engine:

May 10, 2023 10:04:41 PM CEST

Rule Name: DP: Na privilegovaném účtu byla provedena změna
Rule Description: Byla provedena změna na administrátorském účtu

Event Name: Success Audit: A user account was changed
Category: User Account Changed

Source Account Name: lipa
Target Security Group: N/A
Target Account Security ID: DPTEST\javor

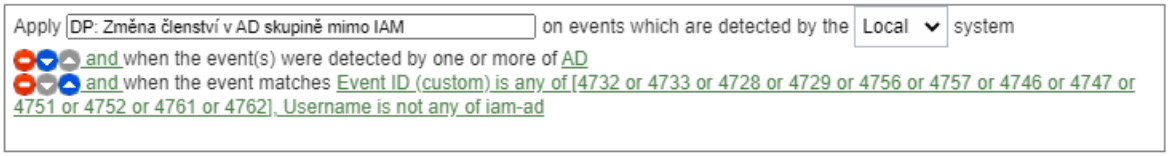
Log Source Name: DC: dc.dp-test.cz

<!--
Payload: <13> May 10 22:04:54 dc.dp-test.cz AgentDevice=WindowsLog AgentLogFile=Security PluginVersion=7.3.1.22 Source=Microsoft-Windows-Security-Auditing Computer= dc.dp-test.cz OriginatingComputer=10.0.20.2 User= Domain= EventID=4738 EventIDCode=4738 EventType=8 EventCategory=13824 RecordNumber=1045078 TimeGenerated=1683749081 TimeWritten=1683749081 Level=Log Always Keywords=Audit Success Task=SE_ADT_ACCOUNTMANAGEMENT_USERACCOUNT Opcode=Info Message=A user account was changed. Subject: Security ID: DPTEST\lipa Account Name: lipa Account Domain: DPTEST Logon ID: 0x1B41EE52 Target Account: Security ID: DPTEST\javor Account Name: javor Account Domain: DPTEST Changed Attributes: SAM Account Name: - Display Name: - User Principal Name: - Home Directory: - Home Drive: - Script Path: - Profile Path: - User Workstations: - Password Last Set: - Account Expires: - Primary Group ID: - AllowedToDelegateTo: - Old UAC Value: 0x10 New UAC Value: 0x11 User Account Control: Account Disabled User Parameters: - SID History: - Logon Hours: - Additional Information: Privileges: -

Obrázek 66. E-mailová notifikace o změně na privilegovaném účtu (vlastní)

5.2.4 DP: Změna členství v AD skupině mimo IAM

Změna členství všech skupin v AD má být prováděna výhradně dle rolí přidělených v IAM. Pokud bude pravidlem (Obr. 67) detekována změna členství ve skupině jiným účtem, než „iam-ad“, jedná se o narušení stanoveného procesu. Pro ukázku bylo pravidlo vytvořeno s podmínkou používající vyhledávací filtr, místo podmínek odkazujících na RS.



Obrázek 67. Pravidlo pro detekci nepovolených změn v AD skupině (vlastní)

Podmínky pravidla:

- zdroj logů je zařazen do skupiny logů AD,
- ID události odpovídá některé z uvedených hodnot (Tab. 32) a zároveň uživatelské jméno původce změny není „iam-ad“.

Při testu přidal pracovník helpdesku s účtem „osika“ sám sebe do AD skupiny „Disk Uctarna-rw“. Sepnuté pravidlo vytvořilo událost (Obr. 68) a odeslalo e-mailovou notifikaci.

Event Information

Event Name	DP: Změna členství v AD skupině mimo IAM						
Low Level Category	Group Member Update Attempt						
Event Description	Účet byl přidán/odebrán z/do skupiny v AD ručně. Tzn. požadavek nešel přes schvalovací work-flow v IAM						
Magnitude	(8)	Relevance	10	Severity	5	Credibility	10
Username	osika						
Start Time	10. 5. 2023 9:12:43	Storage Time	10. 5. 2023 9:12:43	Log Source Time	10. 5. 2023 9:12:43		
CRE Description (custom)	Účet byl přidán/odebrán z/do skupiny v AD ručně. Tzn. požadavek nešel přes schvalovací work-flow v IAM						

Obrázek 68. Odezva na pravidlo pro detekci nepovol. změn v AD sk. (vlastní)

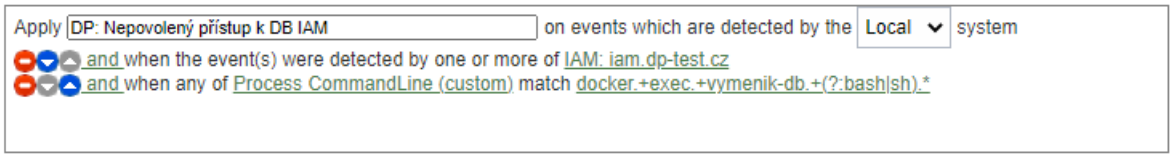
Tabulka 32. ID událostí změn členství v AD skupině, čerpáno z: [86]

Skupina	Typ skupiny	Přidání	Odebrání
Zabezpečení	Lokální	4732	4733
	Globální	4728	4729
	Universální	4756	4757
Distribuční	Lokální	4746	4747

Skupina	Typ skupiny	Přidání	Odebrání
	Globální	4751	4752
	Universální	4761	4762

5.2.5 DP: Nepovolený přístup k DB IAM

IAM ukládá veškerá data v PostgreSQL DB, ke které má přístup pouze aplikace samotná a aplikační podpora z lokální Docker konzole na serveru „iam.dp-test.cz“. Za běžného provozu by ke kontejneru s DB neměl nikdo přistupovat. Pravidlo bude vyhodnocovat, zda někdo přistoupí do kontejneru s DB (Obr. 69). Pravidlo využije auditních událostí OS Linux, na kterém je IAM provozován.



Obrázek 69. Pravidlo pro detekci přístupu do kontejneru s IAM DB (vlastní)

Podmínky pravidla:

- zdroj logů je OS Linux na serveru, kde je provozován IAM,
- příkaz zadaný v konzoli odpovídá regulárnímu výrazu, který popisuje posloupnost příkazů pro spuštění interaktivního terminálu Dockeru s DB IAM.

Přes SSH klienta bylo provedeno připojení k serveru „iam.dp-test.cz“ a připojení do DB „vymenik-db“ (Obr. 70).

```
Last login: Tue May  2 12:45:11 2023 from 10.0.65.4
[topol@dp-test.cz@iam ~]$ sudo docker exec -it vymenik-db bash
[sudo] password for topol@dp-test.cz:
root@vymenik-db:/# su postgres
postgres@vymenik-db:/$ psql
psql (12.5 (Debian 12.5-1.pgdg100+1))
Type "help" for help.

postgres=# \c vymenik
You are now connected to database "vymenik" as user "postgres".
vymenik=#
```

Obrázek 70. Připojení do DB IAM v Docker kontejneru (vlastní)

Konfigurované pravidlo vyhodnotilo správně událost a vyvolalo definovanou akci (Obr. 71).

Event Information

Event Name	DP: Nepovolený přístup k DB IAM						
Low Level Category	Access Permitted						
Event Description	Bylo uskutečněno připojení do kontejneru databáze IAM						
Magnitude	(9)	Relevance	10	Severity	8	Credibility	10
Username	topol@dp-test.cz						
Start Time	12. 5. 2023 0:24:41	Storage Time	12. 5. 2023 0:24:41	Log Source Time	12. 5. 2023 0:24:41		
CRE Description (custom)	Bylo uskutečněno připojení do kontejneru databáze IAM						
CRE Name (custom)	DP: Nepovolený přístup k DB IAM						

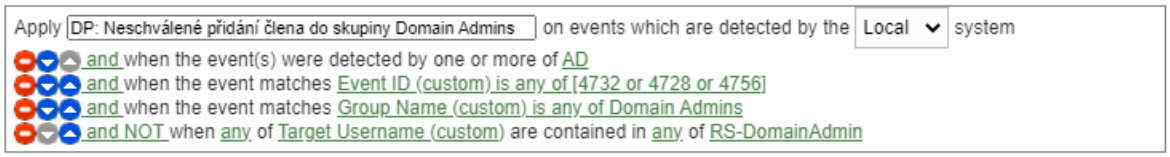
Obrázek 71. Odezva na pravidlo pro detekci přístupu do DB kontejneru (vlastní)

5.2.6 DP: Neschválené přidání člena do skupiny Domain Admins

Členství ve vestavěných AD skupinách zabezpečení, jako jsou např. „Domain / Enterprise Admins“ a ve zvláště důležitých skupinách, musí být důsledně řízeno a kontrolováno. Musí být vypracován proces pro jejich přidělování i odebírání a každá změna ve skupinách prověřena. V pravidle (Obr. 73) je nastaveno ověření procesu přidělení role Domain Admins v IAM kontrolou, zda je přidělovaný název účtu uveden v RS schválených účtů pro danou skupinu. Do RS se účet přidává automatizovaně jiným pravidlem, na základě výsledné události schválení, z logu z IAM (Obr. 72). V IAM prochází příslušná role schvalovacím workflow s kontrolou „čtyř očí“ (garant role + security manager).

```
May 12 18:56:57 iam.dp-test.cz czechidm[1437]: 2023-05-12 18:56:57.784  INFO
205540842 --- [event-task-executor-9] AUDIT.ROLE_ASSIGNMENT.CREATE.log :
result:[SUCCESS] targetName:[javor]
targetUUID:[27d1e266-c18a-4287-95ff-3d453d329894] subjectName:[Domain admin]
subjectUUID:[b84bc638-b51a-5836-834b-8e52b646f381] performedByName:[khornil54]
performedByUUID:[7165af74-f613-9912-b232-533682f188cb]
transactionUUID:[69eab616-f7e9-4bb3-861f-846a3s2dde11] detail:[]
```

Obrázek 72. Událost logu IAM – schválení přidání role (vlastní)



Obrázek 73. Pravidlo pro detekci porušení procesu schválení v IAM (vlastní)

Podmínky pravidla:

- zdroj logů je zařazen do skupiny logů AD,
- ID události odpovídá některé z uvedených hodnot (Tab. 32),
- prověřovaná AD skupina je „Domain Admins“,
- název cílového účtu není uveden v RS „RS-DomainAdmin“, který obsahuje předem schválené a ověřené účty.

Pro otestování byl přidán ručně účet „tvesely628“ do skupiny „Domain Admins“ v AD. Sepnuté pravidlo vygenerovalo událost na obrázku (Obr. 74).

Event Information

Event Name	DP: Neschválené přidání člena do skupiny Domain Admins						
Low Level Category	Group Member Added						
Event Description	Účet byl nepovoleně přidán do skupiny Domain Admins - nebylo provedeno schválení v IAM						
Magnitude	(8)	Relevance	10	Severity	5	Credibility	10
Username	sekvoje						
Start Time	12. 5. 2023 11:40:40	Storage Time	12. 5. 2023 11:40:40	Log Source Time	12. 5. 2023 11:40:40		
CRE Description (custom)	Účet byl nepovoleně přidán do skupiny Domain Admins - nebylo provedeno schválení v IAM						
CRE Name (custom)	DP: Neschválené přidání člena do skupiny Domain Admins						

Obrázek 74. Odezva na pravidlo pro detekci porušení procesu schválení (vlastní)

5.3 Vyhodnocení navrženého systému a jeho odolnosti

Navržený systém odpovídá požadavkům na funkčnost, stanoveným v úvodu kapitoly. Celý proces řízení přístupu je automatizovaný a založený na identitě uživatele, která je předávána mezi technologickými celky systému. Přenos identity byl ověřen od zařízení uživatele, až po FW pravidlo, odpovědné za udělení síťového přístupu na koncový systém. Funkční testy probíhaly na zařízení s OS Windows, ale dle SW specifikace výrobce [79] jsou použité technologie plně podporované i na macOS a částečně i na Linux. Navržené řízení přístupu je pouze vertikální (server – jih), systém by šel vylepšit zavedením „Zero Trust“ konceptu, bez nutnosti náhrady navržených komponentů. Identifikovaná slabá místa lze ošetřit navrženými opatřeními tak, aby nesnižovala odolnost systému a byla zachována důvěryhodnost procesu přidělování oprávnění. Významným opatřením jsou kontrolní mechanismy založené na auditu událostí z logů systémů. Pravidla vytvořena v nástroji SIEM zajistí efektivní bezpečnostní monitoring systému a rychlou rekci v případě pokusu o jeho překonání.

ZÁVĚR

V úvodu práce byly představeny základní pilíře informační bezpečnosti, kterými jsou důvěrnost, integrita a dostupnost. Za každým z těchto pilířů se schovává nepřeberné množství bezpečnostních opatření, které vytváří bariéru před neustále rostoucím množstvím hrozeb. Neomezeným zdrojem pro vznik a působení hrozeb na informační bezpečnost je kyberprostor, který je propojen celosvětovou sítí internet. Hlavním tématem teoretické části práce je síťová bezpečnost, která se společně s řízením přístupů prolíná všemi oblastmi kybernetické, potažmo informační bezpečnosti. V práci byly představeny základní principy, jako je vrstvení bezpečnostních opatření, ale i podrobný výčet opatření dle souboru norem ISO 27000, který je cennou inspirací při budování nejen síťové bezpečnosti. Rostoucího nebezpečí v kyberprostoru si jsou vědomy i řídící orgány států a společenství, které nechtějí legislativně zaostávat. V práci byly představeny současné i připravované zákony a nařízení s tématikou kyberbezpečnosti a ochrany osobních údajů.

Princip vrstvení bezpečnostních opatření byl v práci aplikován na síťovou bezpečnost a rozpracován do detailu od bezpečnostní strategie, přes segmentaci sítě až po řízení přístupů a monitoring. Tento přehled může čtenáři sloužit pro celkovou orientaci v dané problematice a pochopit všechny vzájemné vazby mezi opatřeními k zajištění síťové bezpečnosti. V závěru teoretické části práce jsou popsány vybrané hrozby působící na síťovou bezpečnost v jednotlivých vrstvách sítě dle referenčního modelu ISO/OSI. Pro každou hrozbu jsou uvedeny používané techniky útočníka a návrh, jak hrozbu detekovat a ošetřit. Výběr, dle vlastních praktických zkušeností, reprezentuje časté typy útoků, kterým je potřeba věnovat pozornost a být na jejich vliv připraven.

V praktické části práce je podrobně popsán návrh a realizace systému řízení přístupu k síťovým prostředkům, který využívá digitální identitu uživatele a vlastnosti jeho pracovního vztahu. Jedná se návod typu „krok za krokem“ s popisem a vysvětlením každého postupu. Všechny kroky na sebe navazují a správnost postupu je průběžně ověřována dílčími výsledky. Návrh lze pomyslně rozdělit na tři větší celky. Účelem prvního je automatizovaně získat data o zaměstnanci z personálního systému, vytvořit identitu uživatele a za pomoci získaných informací udělit správná oprávnění na základě rolí (IAM). Druhý celek je souborem technologií (Fortinet), které dokáží identitu přenášet od uživatele směrem k technickým zařízením a využít ji k autentizaci, autorizaci a udělovaní oprávnění v síti. Posledním celkem jsou systémy, sbírající z celého procesu (ze zúčastněných systémů)

auditní záznamy, které jsou na základě vytvořených pravidel vyhodnocovány (SIEM) a poskytují tak bezpečnostní kontrolu pro potvrzení správnosti udělených přístupů. Konfigurace pravidel doprovází popis jejich vytvoření a praktický test ověřující jejich funkčnost.

Praktická část práce byla vytvořena s ohledem na přenositelnost řešení do praxe, ať už přímo, za využití stejných či podobných technologií, nebo nepřímo, jako znalostní báze pro pochopení dílčích kroků a pro přípravu vlastního návrhu řešení.

SEZNAM POUŽITÉ LITERATURY

[1] LIŠKA, Petr. *Bezpečnostní monitoring uživatelů v informačních systémech*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2021, 120 s. (165 108 znaků). Dostupné také z: http://hdl.handle.net/10563/46192. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav bezpečnostního inženýrství. Vedoucí práce Jašek, Roman.

[2] Kybernetická bezpečnost. In: KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity* [online]. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2019, s. 39-45 [cit. 2023-02-01]. CZ.NIC. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

[3] POŽÁR, Josef. *Základy teorie informační bezpečnosti*. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

[4] *Zákon ze dne 23. července 2014: o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. In: . ČESKO, 2014, 181/2014. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=27231

[5] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6. Dostupné také z: https://cybersecurity.cz/data/slovnik_v310.pdf

[6] WALKOWSKI, Debbie. What Is the CIA Triad?. In: *F5 Labs* [online]. Seattle: F5 Networks, 2023 [cit. 2023-02-05]. Dostupné z: https://www.f5.com/labs/learning-center/what-is-the-cia-triad

[7] MARKS, Paul. Cybersecurity and the Parkerian Hexad. In: *Industry News* [online]. Beaconsfield: StaffHost, 2021 [cit. 2023-02-10]. Dostupné z: https://www.staffhosteurope.com/blog/2019/03/cybersecurity-and-the-parkerian-hexad

[8] The Parkerian Hexad: The CIA Triad Model Expanded. In: *Lewis University Department of Computer & Mathematical Sciences* [online]. Romeoville: Lewis

University, 2023 [cit. 2023-02-10]. Dostupné z: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

[9] Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření. In: *Ministerstvo vnitra České republiky* [online]. Praha: Ministerstvo vnitra České republiky, 2023 [cit. 2023-02-10]. Dostupné z: http://www.mvcr.cz/soubor/koncepce-pdf

[10] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. In: *Úřední věstník Evropské unie*. L 194/1. Dostupné také z: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[11] Legislativní vývoj kybernetické bezpečnosti v ČR. In: KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity* [online]. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2019, s. 87-94 [cit. 2023-02-01]. CZ.NIC. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

[12] Legislativa. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2023 [cit. 2023-02-10]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

[13] *Zákon ze dne 4. dubna 2000: o ochraně osobních údajů a o změně některých zákonů*. In: . Praha: ČESKO, Ročník 2000, částka 32, 101/2000. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3420

[14] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. In: *Úřední věstník Evropské unie*. L 281/31. Dostupné také z: https://eur-lex.europa.eu/eli/dir/1995/46/oj

[15] *Ústavní zákon České národní rady ze dne 16. prosince 1992: Ústava České republiky*. In: . Praha: ČESKO, ročník 1993, částka 1, 1/1993. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5989

[16] *Zákon ze dne 12. března 2019: o zpracování osobních údajů*. In: . Praha: ČESKO, ročník 2019, částka 47, 110/2019. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=38632

[17] *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. In: . L 119/1. Dostupné také z: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[18] Co je GDPR - Ochrana osobních údajů. In: *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Praha: Ministerstvo vnitra ČR, 2023 [cit. 2023-02-12]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx

[19] EPrivacy. In: *Deloitte Česká republika* [online]. Praha: Deloitte, 2023 [cit. 2023-02-12]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/risk/articles/eprivacy.html

[20] Nová směrnice EU o bezpečnosti sítí a informací. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2023 [cit. 2023-02-12]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=145

[21] *Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011*. In: . L 333/1. Dostupné také z: http://data.europa.eu/eli/reg/2022/2554/oj

[22] DORA: Nařízení EU o digitální provozní odolnosti finančních institucí. In: *Deloitte Česká republika* [online]. Praha: Deloitte, 2023 [cit. 2023-02-12]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/risk/solutions/eu-dora-digital-operational-resilience-act-for-financial-services.html

[23] Fundamental Security Design Principles. In: STALLINGS, William. *Cryptography and network security: principles and practice*. Seventh edition. Boston: Pearson, 2017, s. 34-37. Global edition. ISBN 978-1-292-15858-7.

[24] PATEL, Sonal. Securing Industrial Control Systems: A Holistic Defense-In-Depth Approach. In: *POWER Magazine: News & Technology for the Global Energy Industry* [online]. Rockville: Access Intelligence, 2023 [cit. 2023-02-12]. Dostupné z: https://www.powermag.com/securing-industrial-control-systems-a-holistic-defense-in-depth-approach/

[25] Referenční model OSI. In: PUŽMANOVÁ, Rita. *TCP/IP v kostce*. 2., upr. a rozš. vyd. České Budějovice: Kopp, 2009, s. 42-49. ISBN 978-80-7232-388-3.

[26] Popis vrstev referenčního modelu OSI. In: PUŽMANOVÁ, Rita. *TCP/IP v kostce*. 2., upr. a rozš. vyd. České Budějovice: Kopp, 2009, s. 49-58. ISBN 978-80-7232-388-3.

[27] FROEHLICH, Andrew a Linda ROSENCRANCE, Kara GATTINE, ed. OSI model (Open Systems Interconnection). In: *TechTarget* [online]. Newton: TechTarget, 2023 [cit. 2023-02-18]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/OSI

[28] FROEHLICH, Andrew. What is transport layer?. In: *TechTarget* [online]. Newton: TechTarget, 2023 [cit. 2023-02-18]. Dostupné z: https://www.techtarget.com/searchnetworking/definition/Transport-layer

[29] *ISO27k infosec management standards* [online]. Napier: IsecT, 2023 [cit. 2023-02-18]. Dostupné z: https://www.iso27001security.com/

[30] ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*. Third edition. Geneva: International Organization for Standardization, 2022.

[31] ISO/IEC 27002:2022. *Information security, cybersecurity and privacy protection — Information security controls*. Third edition. Geneva: International Organization for Standardization, 2022.

[32] ISO/IEC 27033 IT network security. In: *ISO27k infosec management standards* [online]. Napier: IsecT, 2023 [cit. 2023-02-18]. Dostupné z: https://www.iso27001security.com/html/27033.html

[33] ISO/IEC 27033-1:2015. *Information technology - Security techniques - Network security: Part 1: Overview and concepts*. Second edition. Geneva: International Organization for Standardization, 2015.

[34] ISO/IEC 27033-2:2012. *Information technology - Security techniques - Network security: Part 2: Guidelines for the design and implementation of network security*. First edition. Geneva: International Organization for Standardization, 2012.

[35] ISO/IEC 27033-3:2010. *Information technology - Security techniques - Network security: Part 3: Reference networking scenarios - Threats, design techniques and control issues*. First edition. Geneva: International Organization for Standardization, 2010.

[36] ISO/IEC 27033-4:2014. *Information technology - Security techniques - Network security: Part 4: Securing communications between networks using security gateways*. First edition. Geneva: International Organization for Standardization, 2014.

[37] ISO/IEC 27033-5:2013. *Information technology - Security techniques - Network security: Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*. First edition. Geneva: International Organization for Standardization, 2013.

[38] ISO/IEC 27033-6:2016. *Information technology - Security techniques - Network security: Part 6: Securing wireless IP network access*. First edition. Geneva: International Organization for Standardization, 2016.

[39] ISO/IEC DIS 27033-7, Information technology – Network security — Part 7: Guidelines for network virtualization security. In: *ISO - International Organization for Standardization* [online]. Geveva: International Organization for Standardization, 2023 [cit. 2023-02-25]. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:27033:-7:dis:ed-1:v1:en

[40] What is a Cyber Strategy?. In: DIOGENES, Yuri a Erdal OZKAYA. *Cybersecurity – Attack and Defense Strategies*. Third Edition. Birmingham: Packt Publishing, 2022, s. 53-55. ISBN 978-1-80324-877-6.

[41] Computer Security Strategy. In: STALLINGS, William a Lawrie BROWN. *Computer Security: Principles and Practice*. Fourth Edition. Upper Saddle River: Pearson Education, 2018, s. 60-62. ISBN 978-0-13-479410-5.

[42] Fyzická bezpečnost. In: KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity* [online]. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2019, s. 411-424 [cit. 2023-02-01]. CZ.NIC. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

[43] Rozdělení sítě jako základní prvek zajištění bezpečnosti. In: KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity* [online]. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2019, s. 426-429 [cit. 2023-02-01]. CZ.NIC. ISBN 978-80-88168-34-8. Dostupné z: https://knihy.nic.cz/files/edice/cybersecurity.pdf

[44] Firewall Location and Configurations. In: STALLINGS, William a Lawrie BROWN. *Computer Security: Principles and Practice*. Fourth Edition. Upper Saddle River: Pearson Education, 2018, s. 424-420. ISBN 978-0-13-479410-5.

[45] Network Security. In: DIOGENES, Yuri a Erdal OZKAYA. *Cybersecurity – Attack and Defense Strategies*. Third Edition. Birmingham: Packt Publishing, 2022, s. 343-367. ISBN 978-1-80324-877-6.

[46] What Is Microsegmentation? - Palo Alto Networks. In: *Palo Alto Networks* [online]. Santa Clara: Palo Alto Networks, 2023 [cit. 2023-03-08]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-microsegmentation

[47] What Is the Zero Trust Security Model?. In: *Fortinet* [online]. Sunnyvale: Fortinet, 2023 [cit. 2023-03-08]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/what-is-the-zero-trust-network-security-model

[48] Firewalls. In: RAWAL, Bharat, Gunasekaran MANOGARAN a Alexender PETER. *Cybersecurity and Identity Access Management*. Singapore: Springer Nature, 2022, s. 117-127. ISBN 978-981-19-2657-0.

[49] Ochrana na rozhraní sítí. In: KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity* [online]. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2019, s. 455-462 [cit. 2023-02-01]. CZ.NIC. ISBN 978-80-88168-34-8.

[50] LOSHIN, Peter. IPsec vs. SSL VPN: Comparing speed, security risks and technology. In: *TechTarget* [online]. Newton: TechTarget, 2023 [cit. 2023-02-18]. Dostupné z: https://www.techtarget.com/searchsecurity/tip/IPSec-VPN-vs-SSL-VPN-Comparing-respective-VPN-security-risks

[51] Access Control. In: STALLINGS, William a Lawrie BROWN. *Computer Security: Principles and Practice*. Fourth Edition. Upper Saddle River: Pearson Education, 2018, s. 161-217. ISBN 978-0-13-479410-5.

[52] Authorization. In: RAWAL, Bharat, Gunasekaran MANOGARAN a Alexender PETER. *Cybersecurity and Identity Access Management*. Singapore: Springer Nature, 2022, s. 150. ISBN 978-981-19-2657-0.

[53] Manage the Identification and Authentication of People, Devices, and Services. In: RAWAL, Bharat, Gunasekaran MANOGARAN a Alexender PETER. *Cybersecurity and Identity Access Management*. Singapore: Springer Nature, 2022, s. 149-156. ISBN 978-981-19-2657-0.

[54] Implement and Manage Authorization Mechanisms. In: RAWAL, Bharat, Gunasekaran MANOGARAN a Alexender PETER. *Cybersecurity and Identity Access Management*. Singapore: Springer Nature, 2022, s. 167-171. ISBN 978-981-19-2657-0.

[55] BROWN, Schuyler. LDAP vs. Active Directory: Everything You Need to Know. In: *StrongDM* [online]. Burlingame: StrongDM, 2023 [cit. 2023-03-16]. Dostupné z: https://www.strongdm.com/blog/ldap-vs-active-directory

[56] BROWN, Schuyler. SAML vs. OAuth: Everything You Need to Know. In: *StrongDM* [online]. Burlingame: StrongDM, 2023 [cit. 2023-03-16]. Dostupné z: https://www.strongdm.com/blog/saml-vs-oauth

[57] WOLAND, Aaron. RADIUS versus TACACS+. In: *Network World.com* [online]. Needham: IDG Communications, 2023 [cit. 2023-03-21]. Dostupné z: https://www.networkworld.com/article/2838882/radius-versus-tacacs.html

[58] IEEE 802.1X Port-based Network Access Control. In: STALLINGS, William. *Cryptography and network security: principles and practice*. Seventh edition. Boston: Pearson, 2017, s. 527-529. Global edition. ISBN 978-1-292-15858-7.

[59] ROSENCRANCE, Linda a Craig MATHIAS. Identity management (ID management). In: *TechTarget* [online]. Newton: TechTarget, 2023 [cit. 2023-02-18]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/identity-management-ID-management

[60] Cryptographic Tools. In: STALLINGS, William a Lawrie BROWN. *Computer Security: Principles and Practice*. Fourth Edition. Upper Saddle River: Pearson Education, 2018, s. 68-99. ISBN 978-0-13-479410-5.

[61] 2022 Ponemon Cost of Insider Threats Global Report. In: *Proofpoint US* [online]. Sunnyvale: Proofpoint, 2023 [cit. 2023-03-26]. Dostupné z: https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats

[62] Ochrana koncových počítačových systémů. In: KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity* [online]. 1. vyd. Praha: CZ.NIC, z.s.p.o., 2019, s. 480-481 [cit. 2023-02-01]. CZ.NIC. ISBN 978-80-88168-34-8.

[63] What Is Cybersecurity Mesh? Applications and Advantages. In: *Fortinet* [online]. Sunnyvale: Fortinet, 2023 [cit. 2023-03-26]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity-mesh

[64] IEEE 802.11i Wireless LAN Security. In: STALLINGS, William. *Cryptography and network security: principles and practice*. Seventh edition. Boston: Pearson, 2017, s. 595-609. Global edition. ISBN 978-1-292-15858-7.

[65] IREI, Alissa a Jessica SCARPATI. Wireless Security: WEP, WPA, WPA2 and WPA3 Differences. In: *TechTarget* [online]. Newton: TechTarget, 2023 [cit. 2023-02-18]. Dostupné z: https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

[66] What is SOAR (Security Orchestration, Automation and Response)?. In: *TechTarget* [online]. Newton: TechTarget, 2023 [cit. 2023-02-18]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/SOAR

[67] *MITRE ATT&CK*® [online]. Bedford: MITRE, © 2015-2022 [cit. 2023-03-27]. Dostupné z: https://attack.mitre.org/

[68] Hardware Additions, Technique T1200 - Enterprise. In: *MITRE ATT&CK*® [online]. Bedford: MITRE, © 2015-2022 [cit. 2023-03-27]. Dostupné z: https://attack.mitre.org/techniques/T1200/

[69] Adversary-in-the-Middle: ARP Cache Poisoning, Sub-technique T1557.002 - Enterprise. In: *MITRE ATT&CK*® [online]. Bedford: MITRE, © 2015-2022 [cit. 2023-03-27]. Dostupné z: https://attack.mitre.org/techniques/T1557/002/

[70] Network Denial of Service: Direct Network Flood, Sub-technique T1498.001 - Enterprise. In: *MITRE ATT&CK*® [online]. Bedford: MITRE, © 2015-2022 [cit. 2023-03-27]. Dostupné z: https://attack.mitre.org/techniques/T1498/001/

[71] Service Name and Transport Protocol Port Number Registry. In: *Internet Assigned Numbers Authority* [online]. Los Angeles: Internet Assigned Numbers Authority, 2023 [cit. 2023-03-28]. Dostupné z: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

[72] Non-Standard Port, Technique T1571 - Enterprise. In: *MITRE ATT&CK*® [online]. Bedford: MITRE, © 2015-2022 [cit. 2023-03-27]. Dostupné z: https://attack.mitre.org/techniques/T1571/

[73] Non-Application Layer Protocol, Technique T1095 - Enterprise. In: *MITRE ATT&CK*® [online]. Bedford: MITRE, © 2015-2022 [cit. 2023-03-27]. Dostupné z: https://attack.mitre.org/techniques/T1095/

[74] Encrypted Channel: Asymmetric Cryptography, Sub-technique T1573.002 - Enterprise. In: *MITRE ATT&CK*® [online]. Bedford: MITRE, © 2015-2022 [cit. 2023-03-27]. Dostupné z: https://attack.mitre.org/techniques/T1573/002/

[75] Phishing, Technique T1566 - Enterprise. In: *MITRE ATT&CK*® [online]. Bedford: MITRE, © 2015-2022 [cit. 2023-03-27]. Dostupné z: https://attack.mitre.org/techniques/T1566/

[76] Ports and Protocols: FortiGate / FortiOS 6.4.0. In: *Fortinet Documents Library* [online]. Sunnyvale: Fortinet, 2023 [cit. 2023-04-08]. Dostupné z: https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/

[77] *CzechIdM Identity Manager* [online]. Praha: BCV solutions, 2023 [cit. 2023-04-16]. Dostupné z: https://wiki.czechidm.com/

[78] Supported connectors. In: *CzechIdM Identity Manager* [online]. Praha: BCV solutions, 2023 [cit. 2023-04-16]. Dostupné z: https://wiki.czechidm.com/devel/documentation/adm/systems/connectors

[79] FortiClient Fabric Agent for Endpoint Security. In: *Fortinet* [online]. Sunnyvale: Fortinet, 2023 [cit. 2023-03-26]. Dostupné z: https://www.fortinet.com/products/endpoint-security/forticlient

[80] EMS Administration Guide: Introduction. In: *Fortinet Documents Library* [online]. Sunnyvale: Fortinet, 2023 [cit. 2023-04-08]. Dostupné z: https://docs.fortinet.com/document/forticlient/7.2.0/ems-administration-guide/24450/introduction

[81] Network & User Identity Authentication Services | FortiAuthenticator. In: *Fortinet* [online]. Sunnyvale: Fortinet, 2023 [cit. 2023-03-26]. Dostupné z: https://www.fortinet.com/products/identity-access-management/fortiauthenticator

[82] GEELEN, Peter a Richard MUELLER. Active Directory: LDAP Syntax Filters. In: *Microsoft Community Wiki* [online]. Redmond: Microsoft, 2015 [cit. 2023-05-02]. Dostupné z: https://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx

[83] 2022 Gartner® Magic Quadrant™ | Network Firewall | Fortinet. In: *Fortinet* [online]. Sunnyvale: Fortinet, 2023 [cit. 2023-03-26]. Dostupné z: https://www.fortinet.com/solutions/gartner-network-firewalls

[84] Remote log forwarding. In: *IAM appliance - Administrator Guide* [online]. Praha: BCV solutions, 2023 [cit. 2023-05-07]. Dostupné z: https://doc.czechidm.com/doc-admin-guide/1.2/monitoring/remote-log-forwarding.html#_configuring_log_forwarding

[85] Network Analytics for Large & Complex Networks | FortiAnalyzer. In: *Fortinet* [online]. Sunnyvale: Fortinet, 2023 [cit. 2023-03-26]. Dostupné z: https://www.fortinet.com/products/management/fortianalyzer

[86] SMITH, Randy Frankli. Free Quick Reference Chart for the Windows Security Log. In: *Randy Franklin Smith's Ultimate Windows Security* [online]. Beaverton: Monterey Technology, ©2006-2023 [cit. 2023-05-10]. Dostupné z: https://www.ultimatewindowssecurity.com/securitylog/quickref/Default.aspx

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ABAC	Attribute-Based Access Controls
ACL	Access Control Lists
AD	Active Directory
AES	Advanced Encryption Standard
AM	Access Management
AO	Adresní objekt
AP	Access Point
API	Application Programming Interface
ARP	Address Resolution Protocol
AS	Authentication Server
AV	Antivir
BYOD	Bring your Own Device
C&C	Command and Control
CCMP	Cipher Block Chaining Message Authentication Code Protocol
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity and Availability
CSMA	Cybersecurity Mesh Architecture
DAC	Discretionary Access Controls
DB	Databáze
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
DMZ	Demilitarized Zone

DNS	Domain Name System
DORA	Digital Operational Resilience Act
DoS	Denial-of-service
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DRC	Disaster Recovery Center
DSL	Digital Subscriber Line
DSS	Digital Signature Standard
EAPOL	Extensible Authentication Protocol over LAN
ECDSA	Elliptic Curve Digital Signature Algorithm
EMS	Endpoint Management Server
EPS	Elektronická požární signalizace
ER	Entity Relationship
ESP	Encapsulating Security Payload
FAC	FortiAuthenticator
FAZ	FortiAnalyzer
FC	FortiClient
FG	FortiGate
FGN	Fortinet-Group-Name
FK	Foreign Key
FSSO	Fortinet Single Sign-On
FW	Firewall
GDPR	General Data Protection Regulation
GPO	Group Policy Object
GSM	Global System for Mobile Communications
HIDS	Host Intrusion Detection System

HTTP	Hypertext Transfer Protocol
HW	Hardware
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICT	Information and Communications Technology
IdM	Identity Management
IdP	Identity Provider
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IO	Objekt identity
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
ISO	International Organization for Standardization
ISP	Internet service provider
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LLC	Logical Link Control
MaAC	Mandatory Access Control
MAC	Media Access Control

MFA	Multi-factor Authentication
MS	Microsoft
MZS	Mechanické zábranné systémy
NAC	Network Access Control
NAS	Network Access Server
NAT	Network Address Translation
NAT-T	NAT-Traversal
NBAD	Network Behavior Anomaly Detection
NBÚ	Národní bezpečnostní úřad
NDIS	Network Intrusion Detection System
NFS	Network File System
NGFW	Next-Generation Firewall
NIS	Network and Information Security
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OAuth	Open Authorization
OS	Operační systém
OSI	Open Systems Interconnection
OTT	Over-The-Top
OU	Organizational Unit
PAM	Privileged Access Management
PDC	Primary Data Centre
PK	Primary Key
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-shared Key
PZTS	Poplachové zabezpečovací a tísňové systémy
RADIUS	Remote Access Dial In User Service

RBAC	Role-Based Access Control
RC4	Rivest Cipher 4
RDP	Remote Desktop Protocol
REST	Representational state transfer
RPC	Remote Procedure Call
RSA	Rivest-Shamir-Adelman
RSN	Robust Security Network
RuBAC	Rule-Based Access Control
SAE	Simultaneous Authentication of Equals
SAML	Security Assertion Markup Language
SDN	Software-Defined Networking
SD-WAN	Software-defined Wide Area Network
SIEM	Security Information and Event Management
SKV	Systémy kontroly vstupu
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Service Provider
SPF	Sender Policy Framework
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	Single Sign-On
STA	Station
SW	Software
TACACS+	Terminal Access Controller Access-Control System Plus
TBAC	Task-based access control

TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
UDP	User Data Protocol
UEFI	Unified Extensible Firmware Interface
UTM	Unified Threat Management
VLAN	Virtual Local Area Networks
VPN	Virtual Private Network
VSS	Video Surveillance System
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WS	Web Services

SEZNAM OBRÁZKŮ

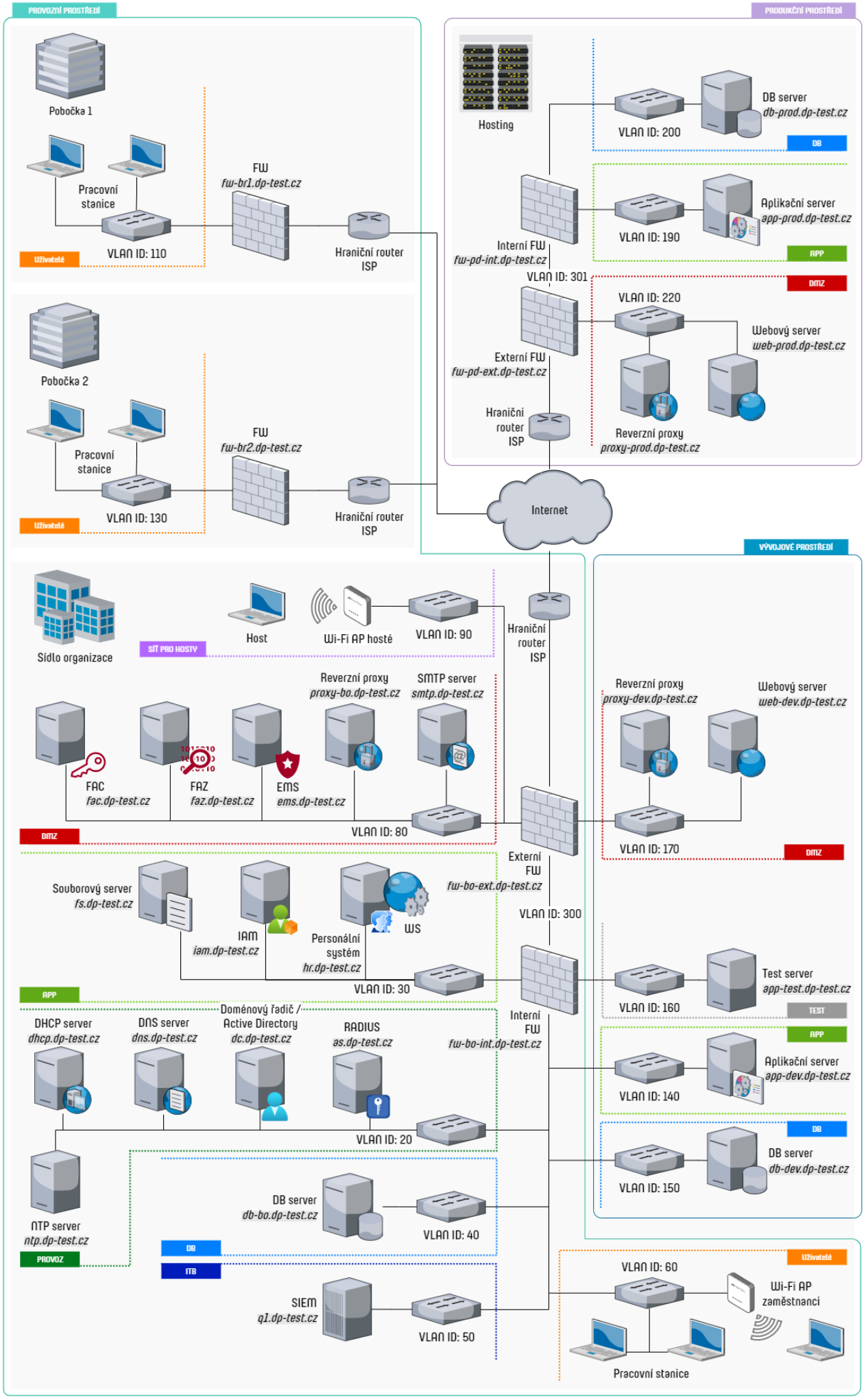
SEZNAM TABULEK

SEZNAM PŘÍLOH

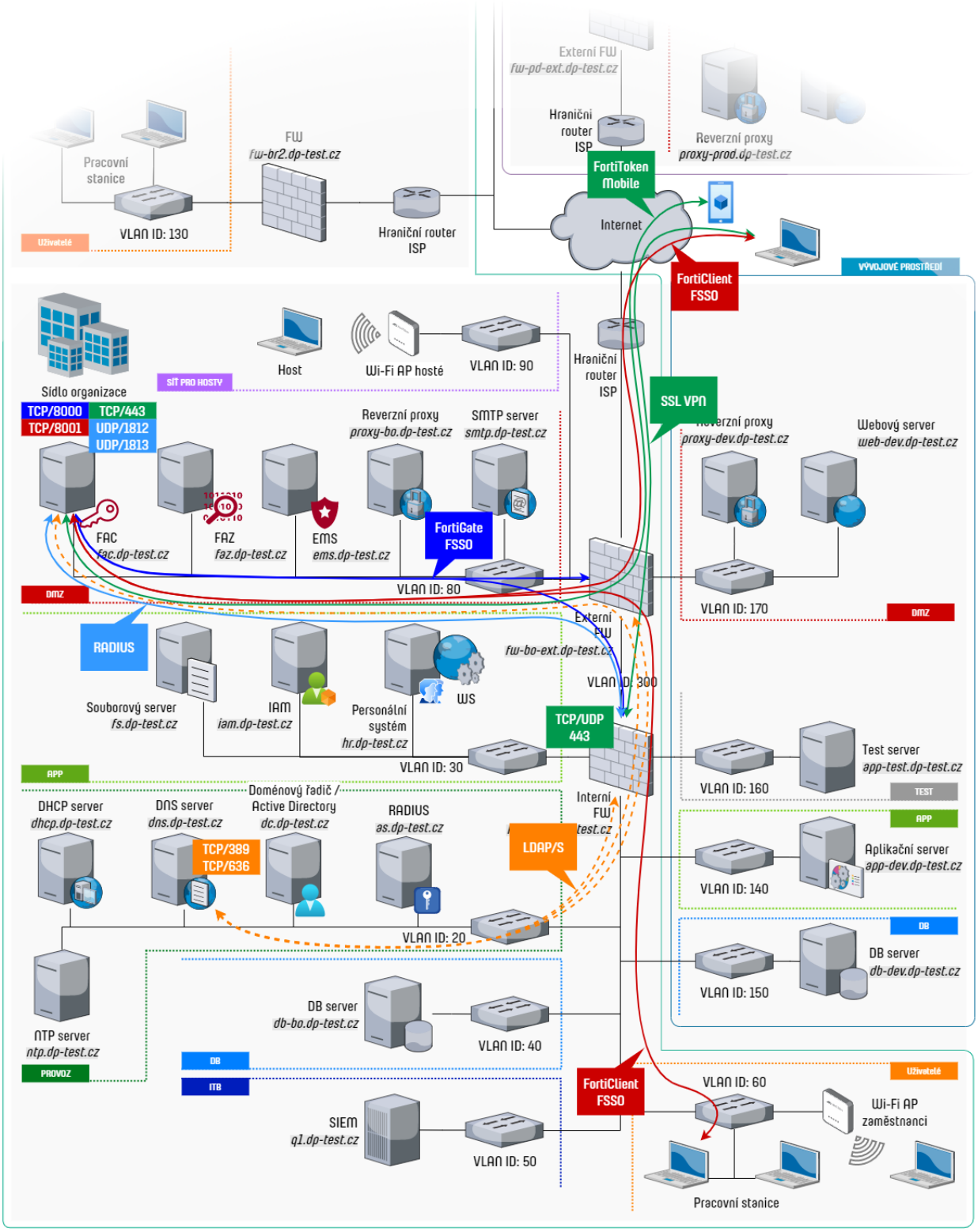
PŘÍLOHA P I: PŘEHLEDOVÝ SÍŤOVÝ DIAGRAM

Popis segmentů v přehledovém síťovém diagramu (na následující samostatné stránce):

VLAN ID	Prostředí	Lokalita	Účel
10	Provozní	Sídlo organizace	Manag. síťových prvků a serverů v LAN
20			Provozní servery (PROVOZ)
30			Aplikační servery (APP)
40			Databázové servery (DB)
50			Bezpečnostní servery (ITB)
60			Uživatelé – sídlo
65			Uživatelé – VPN
300			Spojovací síť provozní FW
70			Manag. síťových prvků a serverů v DMZ
80			DMZ
90			Síť pro hosty
100		Pobočka 1	Manag. síťových prvků v pobočce 1
110			Uživatelé – pobočka 1
120		Pobočka 2	Manag. síťových prvků v pobočce 2
130			Uživatelé – pobočka 2
140	Vývojové	Sídlo organizace	Aplikační servery (APP)
150			Databázové servery (DB)
160			Testovací servery (TEST)
170			DMZ
180	Produkční	Hostované datacentrum	Manag. síťových prvků a serverů v LAN
190			Aplikační servery (APP)
200			Databázové servery (DB)
210			Manag. síťových prvků a serverů v DMZ
220			DMZ
301			Spojovací síť produkční FW


PROVOZNÍ PROSTŘEDÍ
PRODUKČNÍ PROSTŘEDÍ
Pobočka 1
Pracovní stanice
VLAN ID: 110
Uživatelé
FW
fw-br1.dp-test.cz
Hraniční router ISP
Hosting
DB server
db-prod.dp-test.cz
VLAN ID: 200
DB
Aplikační server
app-prod.dp-test.cz
VLAN ID: 190
APP
Interní FW
fw-pd-int.dp-test.cz
VLAN ID: 301
DMZ
VLAN ID: 220
Webový server
web-prod.dp-test.cz
Externí FW
fw-pd-ext.dp-test.cz
Hraniční router ISP
Reverzní proxy
proxy-prod.dp-test.cz
Pobočka 2
Pracovní stanice
VLAN ID: 130
Uživatelé
FW
fw-br2.dp-test.cz
Hraniční router ISP
Internet
VÝVOJOVÉ PROSTŘEDÍ
Sídlo organizace
SÍŤ PRO HOSTY
Host
Wi-Fi AP hosté
VLAN ID: 90
Hraniční router ISP
Reverzní proxy
proxy-bo.dp-test.cz
SMTP server
smtp.dp-test.cz
FAC
fac.dp-test.cz
FAZ
faz.dp-test.cz
EMS
ems.dp-test.cz
DMZ
VLAN ID: 80
Reverzní proxy
proxy-dev.dp-test.cz
Webový server
web-dev.dp-test.cz
VLAN ID: 170
DMZ
Externí FW
fw-bo-ext.dp-test.cz
VLAN ID: 300
Souborový server
fs.dp-test.cz
IAM
iam.dp-test.cz
Personální systém
hr.dp-test.cz
WS
APP
VLAN ID: 30
Interní FW
fw-bo-int.dp-test.cz
Test server
app-test.dp-test.cz
VLAN ID: 160
TEST
APP
Aplikační server
app-dev.dp-test.cz
VLAN ID: 140
DB
DB server
db-dev.dp-test.cz
VLAN ID: 150
Doménový řadič / Active Directory
DHCP server
dhcp.dp-test.cz
DNS server
dns.dp-test.cz
dc.dp-test.cz
RADIUS
as.dp-test.cz
VLAN ID: 20
NTP server
ntp.dp-test.cz
PROVOZ
DB server
db-bo.dp-test.cz
VLAN ID: 40
DB
ITB
SIEM
q1.dp-test.cz
VLAN ID: 50
Uživatelé
VLAN ID: 60
Wi-Fi AP zaměstnanci
Pracovní stanice

PŘÍLOHA P II: FORTINET SINGLE SIGN-ON A SSL VPN DIAGRAM



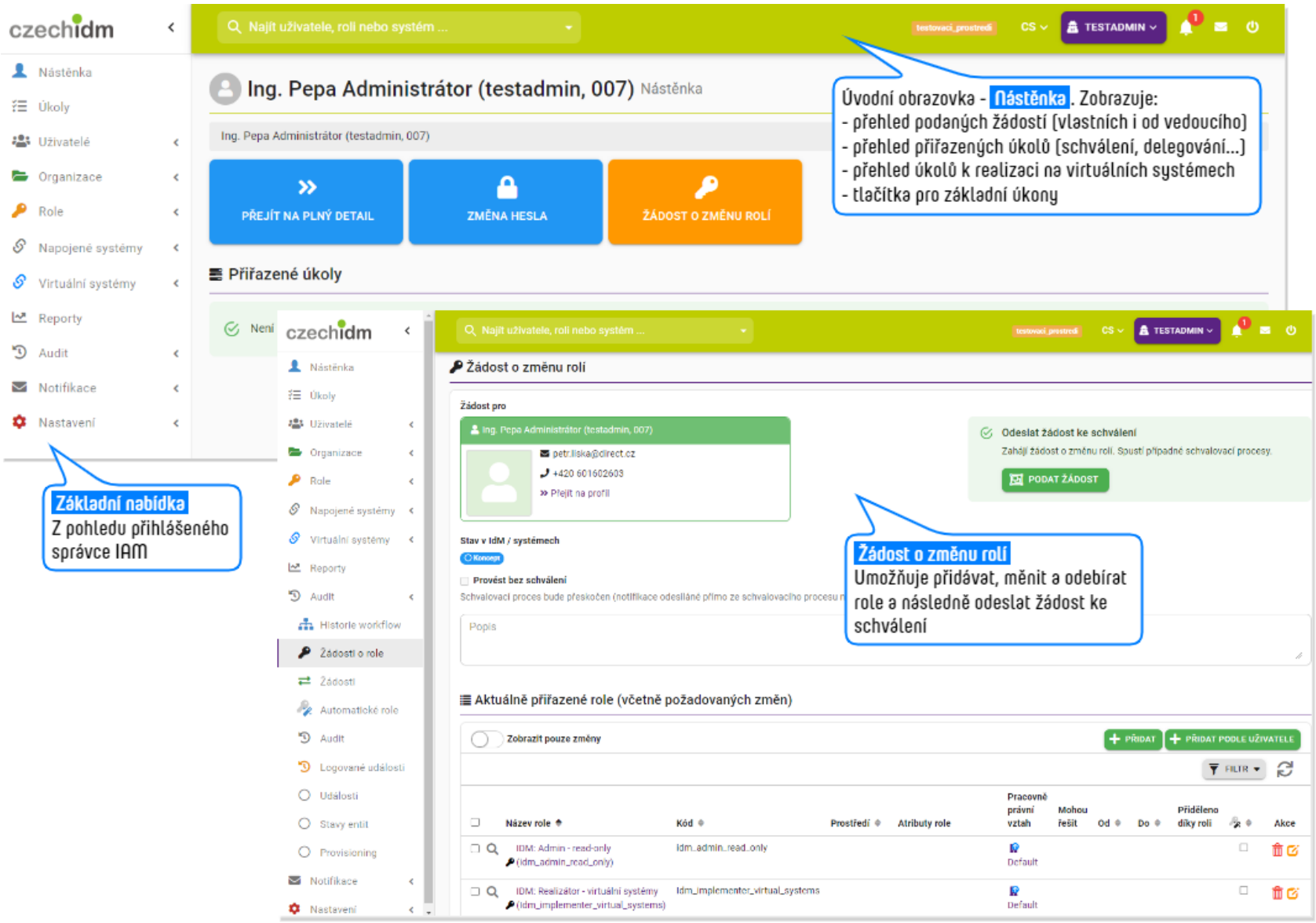
PŘÍLOHA P III: SOUPIS HOSTITELŮ A IP ADRES

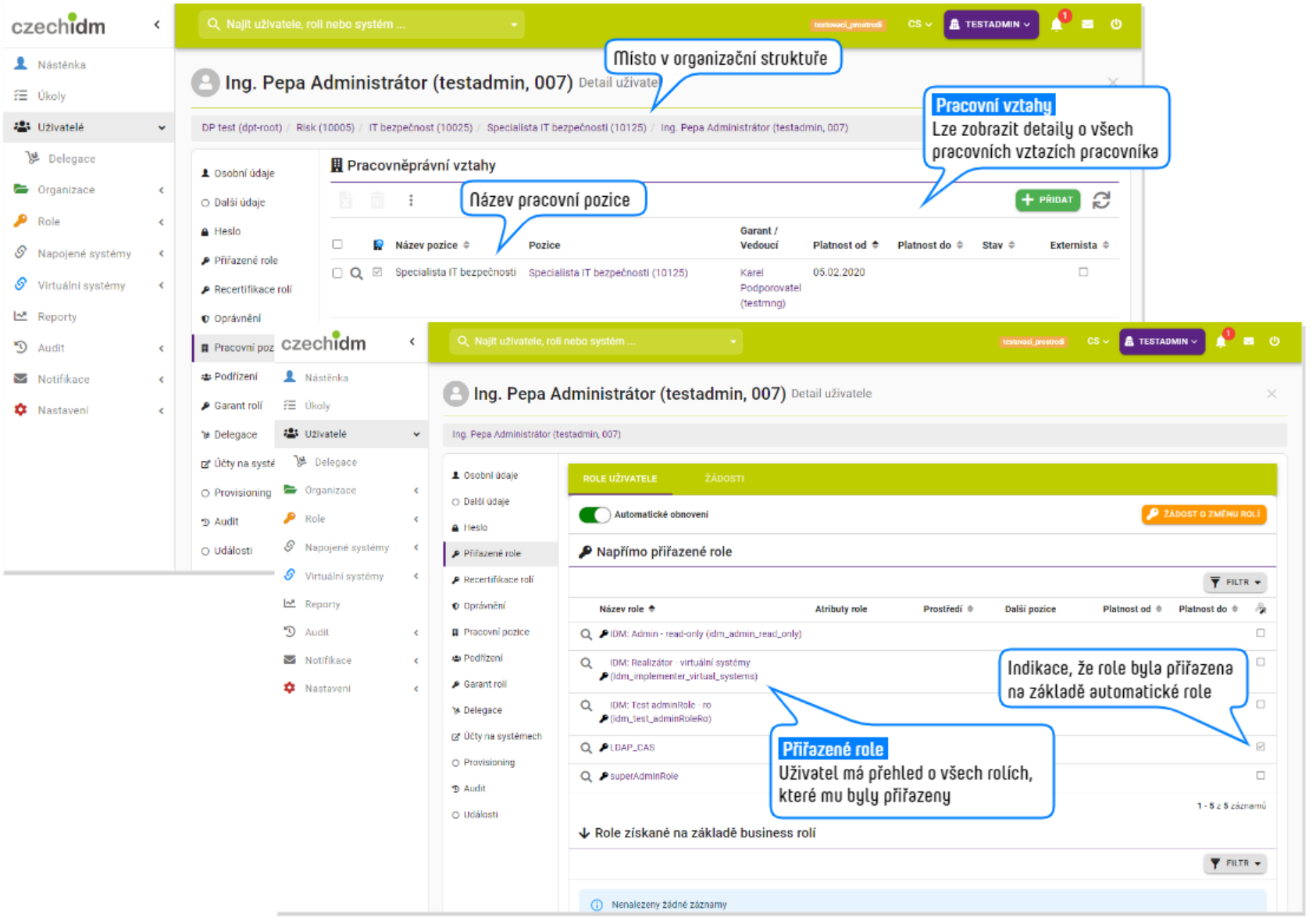
Jméno hostitele	IP adresa	VLAN ID	Popis
fw-bo-int.dp-test.cz	10.0.10.1	10	Výchozí brána pro VLAN ID: 10, management interního provozního FW
sw-bo-int.dp-test.cz	10.0.10.2		Management interního provozního přepínače, VLAN ID: 10-60, 140-160
….dp-test.cz	10.0.10.3...		Management karty serverů v int. provozní síti, přístupové body a management bezdrátové sítě, virtualizační servery…
	10.0.20.1	20	Výchozí brána pro VLAN ID: 20
dc.dp-test.cz	10.0.20.2		Doménový řadič s adresářovou službou
dns.dp-test.cz	10.0.20.3		DNS server
dhcp.dp-test.cz	10.0.20.4		DHCP server
as.dp-test.cz	10.0.20.5		RADIUS server
ntp.dp-test.cz	10.0.20.6		NTP server
	10.0.30.1	30	Výchozí brána pro VLAN ID: 30
hr.dp-test.cz	10.0.30.2		Personální systém
iam.dp-test.cz	10.0.30.3		IAM
fs.dp-test.cz	10.0.30.4		Souborový server
	10.0.40.1	40	Výchozí brána pro VLAN ID: 40
db-bo.dp-test.cz	10.0.40.2		Databázový server pro provozní prostředí
	10.0.50.1	50	Výchozí brána pro VLAN ID: 50
q1.dp-test.cz	10.0.50.2		SIEM
	10.0.60.1	60	Výchozí brána pro VLAN ID: 60
ntb…dp-test.cz	10.0.60.2...		Zářízení uživatelů v sídle organizace
	10.0.65.1	65	Výchozí brána pro VLAN ID: 65
ntb…dp-test.cz	10.0.65.2...		Zářízení uživatelů na VPN
fw-bo-ext.dp-test.cz	10.0.70.1	70	Výchozí brána pro VLAN ID: 70, management externího prvozního FW
sw-bo-ext.dp-test.cz	10.0.70.2		Management DMZ provozního přepínače, VLAN ID: 80, 90, 170

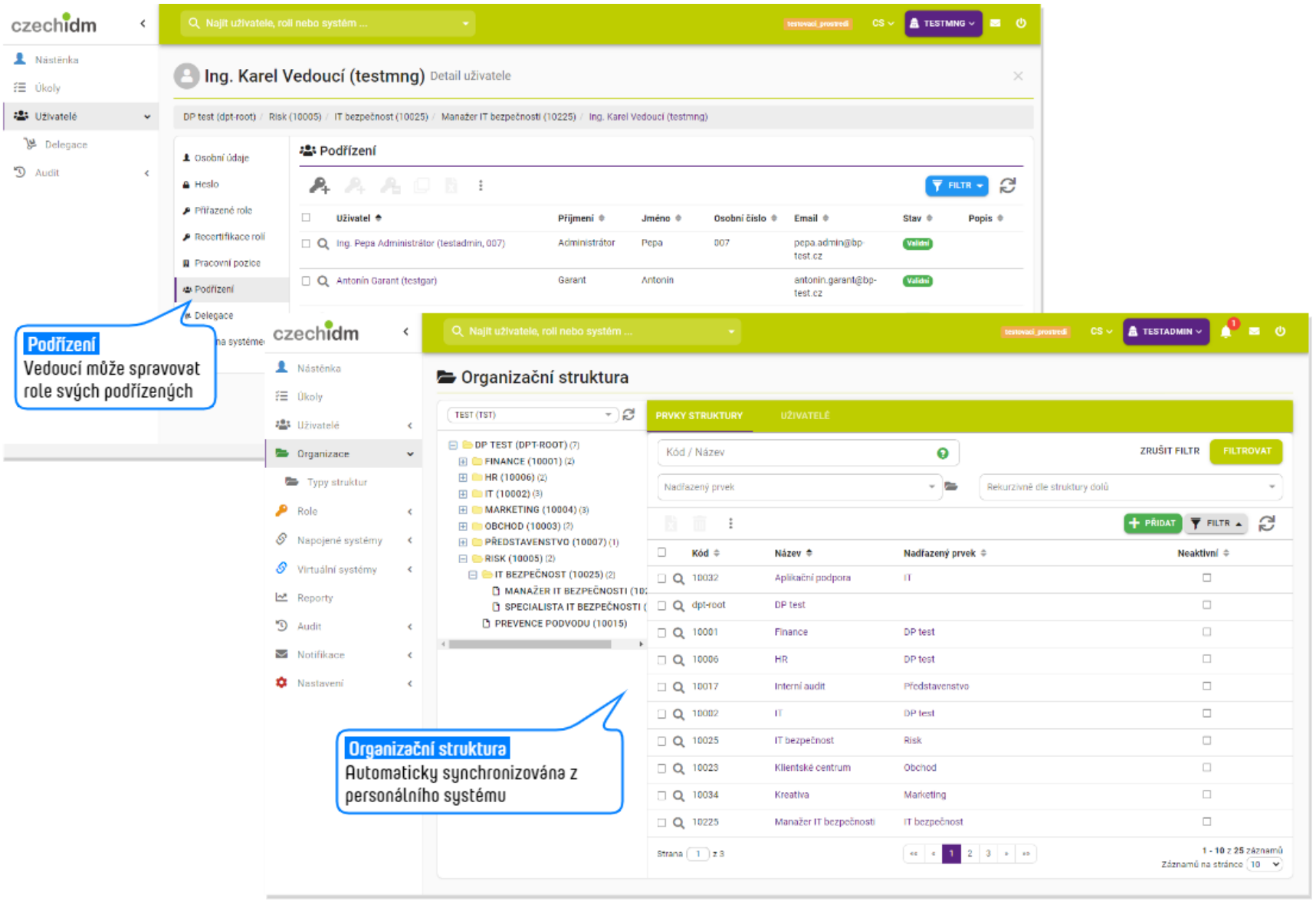
Jméno hostitele	IP adresa	VLAN ID	Popis
…dp-test.cz	10.0.70.3…		Management karty serverů v ext. provozní síti, přístupové body a management bezdrátové sítě, virtualizační servery…
	10.0.80.1	80	Výchozí brána pro VLAN ID: 80
smtp.dp-test.cz	10.0.80.2		SMTP server
proxy-bo.dp-test.cz	10.0.80.3		Reverzní proxy pro provozní servery
fac.dp-test.cz	10.0.80.4		FortiAuthenticator
faz.dp-test.cz	10.0.80.5		FortiAnalyzer
ems.dp-test.cz	10.0.80.6		FortiClient EMS
	10.0.90.1	90	Výchozí brána pro VLAN ID: 90
	10.0.90.2…		Zařízení hostů
fw-br1.dp-test.cz	10.0.100.1	100	Výchozí brána pro VLAN ID: 100, management FW pobočky 1
	10.0.100.2		Management přepínače pobočky 1, VLAN ID: 110
	10.0.110.1	110	Výchozí brána pro VLAN ID: 110
ntb…dp-test.cz	10.0.110.2…		Zářízení uživatelů na pobočce 1
fw-br2.dp-test.cz	10.0.120.1	120	Výchozí brána pro VLAN ID: 120, management FW pobočky 2
	10.0.120.2		Management přepínače pobočky 2, VLAN ID: 130
	10.0.130.1	130	Výchozí brána pro VLAN ID: 130
ntb…dp-test.cz	10.0.130.2…		Zářízení uživatelů na pobočce 2
	10.0.140.1	140	Výchozí brána pro VLAN ID: 140
app-dev.dp-test.cz	10.0.140.2		Aplikační vývojový server
	10.0.150.1	150	Výchozí brána pro VLAN ID: 150
db-dev.dp-test.cz	10.0.150.2		Databázový server pro vývojové prostředí
	10.0.160.1	160	Výchozí brána pro VLAN ID: 160
app-test.dp-test.cz	10.0.160.2		Testovací server pro vývojové prostředí
	10.0.170.1	170	Výchozí brána pro VLAN ID: 170

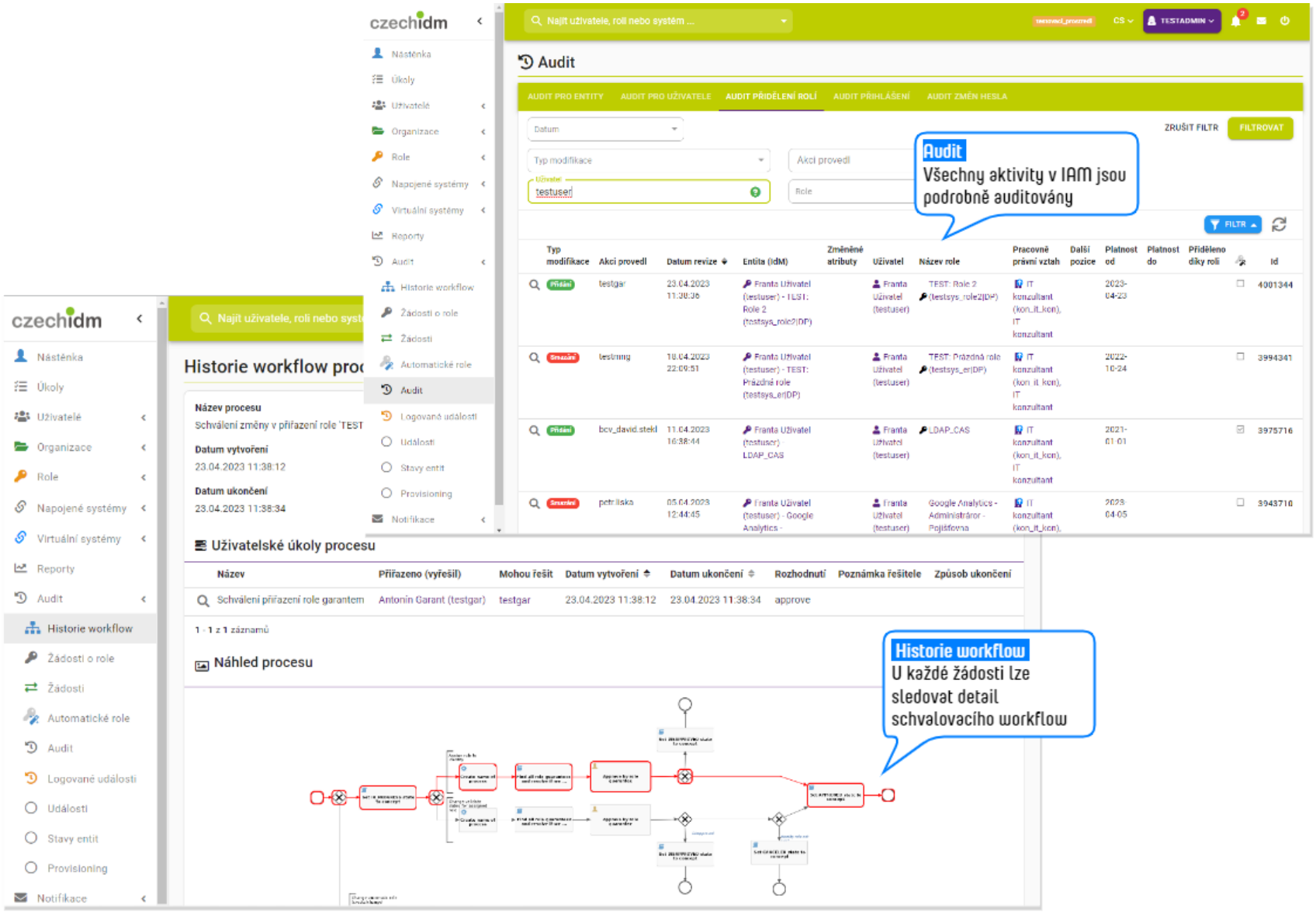
Jméno hostitele	IP adresa	VLAN ID	Popis
proxy-dev.dp-test.cz	10.0.170.2		Reverzní proxy pro vývojové servery
web-dev.dp-test.cz	10.0.170.3		Webový vývojový server
fw-pd-int.dp-test.cz	10.0.180.1	180	Výchozí brána pro VLAN ID: 180, management interního produkčního FW
sw-pd-int.dp-test.cz	10.0.180.2		Management interního produkčního přepínače, VLAN ID: 190, 200
…dp-test.cz	10.0.180.3…		Management karty serverů v int. produkční síti, virtualizační servery…
	10.0.190.1	190	Výchozí brána pro VLAN ID: 190
app-prod.dp-test.cz	10.0.190.2		Aplikační prodikční server
	10.0.200.1	200	Výchozí brána pro VLAN ID: 200
db-prod.dp-test.cz	10.0.200.2		Databázový server pro produkční prostředí
fw-pd-ext.dp-test.cz	10.0.210.1	210	Výchozí brána pro VLAN ID: 210, management externího produkčního FW
sw-pd-ext.dp-test.cz	10.0.210.2		Management DMZ produkčního přepínače, VLAN ID: 220
…dp-test.cz	10.0.210.3…		Management karty serverů v ext. produkční síti, virtualizační servery…
		220	Výchozí brána pro VLAN ID: 220
proxy-prod.dp-test.cz			Reverzní proxy pro produkční servery
web-prod.dp-test.cz			Webový produkční server
	172.30.0.1	300	Interní provozní FW, spojovací rozhraní
	172.30.0.2		Exteerní provozní FW, spojovací rozhraní
	172.30.0.9		Interní produkční FW, spojovací rozhraní
	172.30.0.10		Exteerní produkční FW, spojovací rozhraní

PŘÍLOHA P IV: POPIS WEBOVÉHO GRAFICKÉHO ROZRANÍ IAM

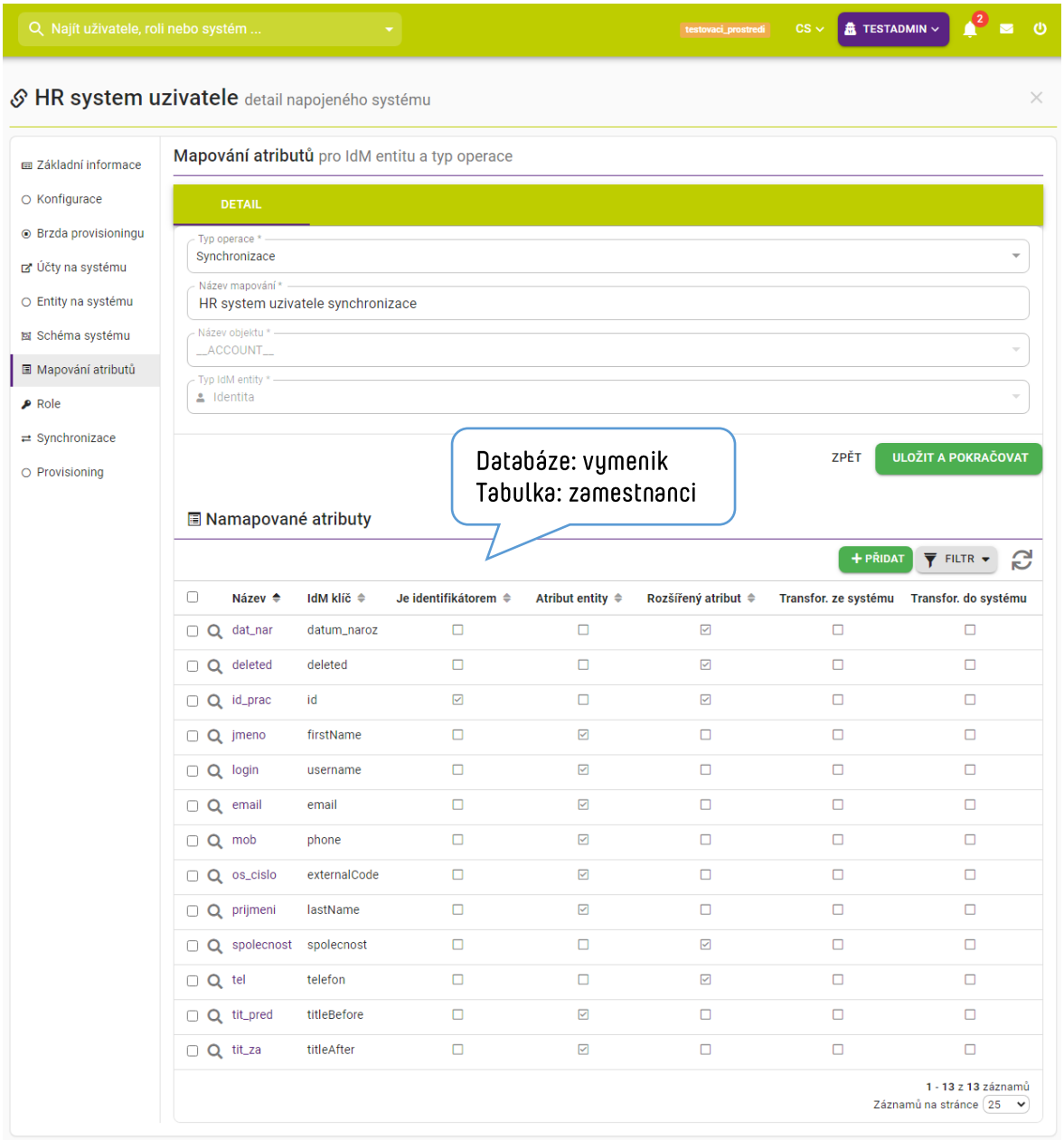



Místo v organizační struktuře
Pracovní vztahy
Lze zobrazit detaily o všech pracovních vztazích pracovníka
Název pracovní pozice
Přiřazené role
Uživatel má přehled o všech rolích, které mu byly přiřazeny
Indikace, že role byla přiřazena na základě automatické role

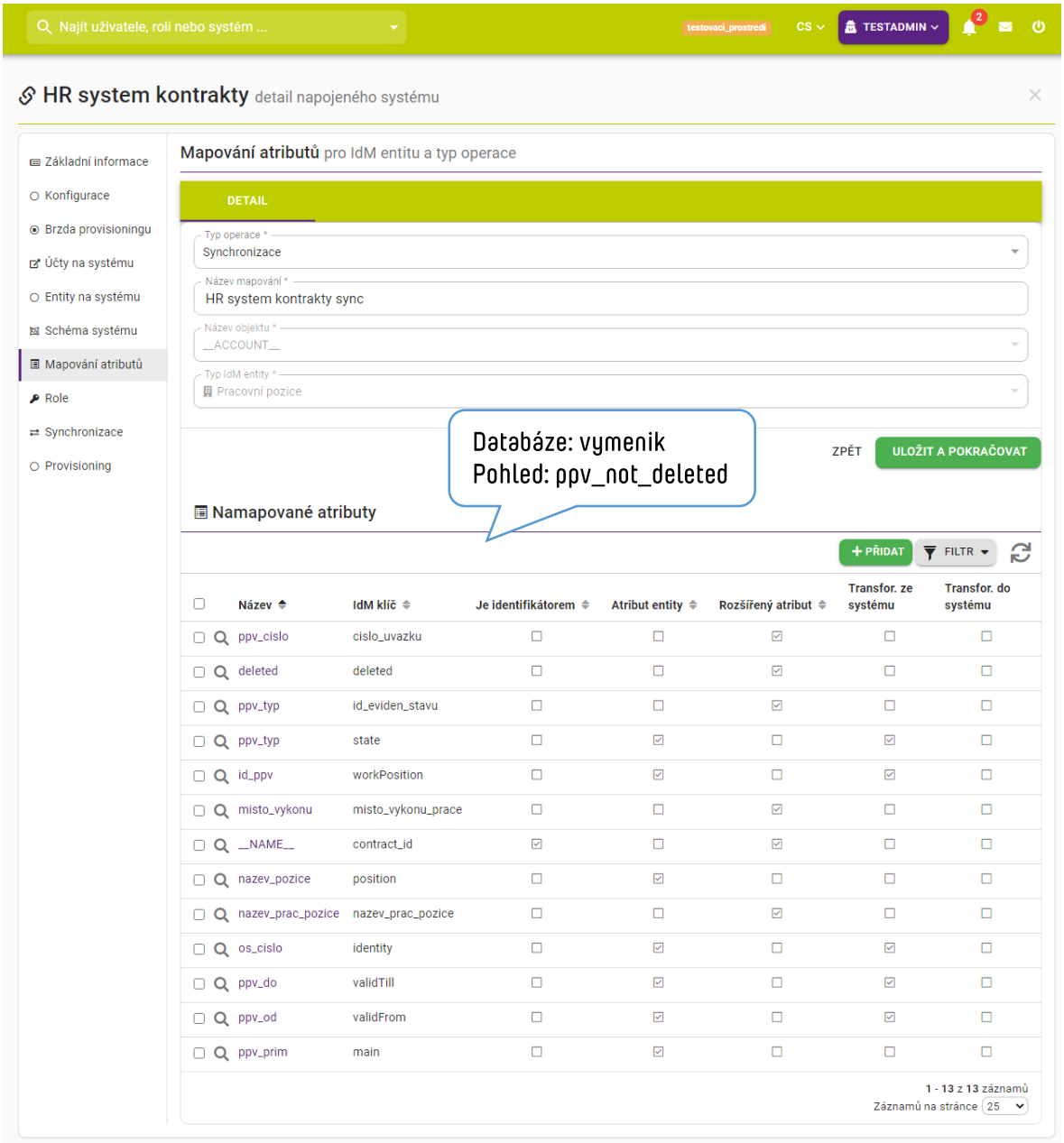

czechidm
Najít uživatele, roli nebo systém ...
testovací_prostředí
CS
TESTMNG
Nástěnka
Úkoly
Uživatelé
Delegace
Audit
Ing. Karel Vedoucí (testmng) Detail uživatele
DP test (dpt-root) / Risk (10005) / IT bezpečnost (10025) / Manažer IT bezpečnosti (10225) / Ing. Karel Vedoucí (testmng)
Osobní údaje
Heslo
Přiřazené role
Recertifikace rolí
Pracovní pozice
Podřízení
Delegace
Podřízení
FILTR
Uživatel
Příjmení
Jméno
Osobní číslo
Email
Stav
Popis
Ing. Pepa Administrátor (testadmin, 007)
Administrátor
Pepa
007
pepa.admin@bp-test.cz
Validní
Antonín Garant (testgar)
Garant
Antonín
antonin.garant@bp-test.cz
Validní
Podřízení
Vedoucí může spravovat role svých podřízených
czechidm
Najít uživatele, roli nebo systém ...
testovací_prostředí
CS
TESTADMIN
Nástěnka
Úkoly
Uživatelé
Organizace
Typy struktur
Role
Napojené systémy
Virtuální systémy
Reporty
Audit
Notifikace
Nastavení
Organizační struktura
TEST (TST)
PRVKY STRUKTURY
UŽIVATELÉ
DP TEST (DPT-ROOT) (7)
FINANCE (10001) (2)
HR (10006) (2)
IT (10002) (3)
MARKETING (10004) (3)
OBCHOD (10003) (7)
PŘEDSTAVENSTVO (10007) (1)
RISK (10005) (2)
IT BEZPEČNOST (10025) (2)
MANAŽER IT BEZPEČNOSTI (10
SPECIALISTA IT BEZPEČNOSTI (
PREVENCE PODVODU (10015)
Kód / Název
ZRUŠIT FILTR
FILTROVAT
Nadřazený prvek
Rekurzivně dle struktury dolů
PŘIDAT
FILTR
Kód
Název
Nadřazený prvek
Neaktivní
10032 Aplikační podpora IT
dpt-root DP test
10001 Finance DP test
10006 HR DP test
10017 Interní audit Představenstvo
10002 IT DP test
10025 IT bezpečnost Risk
10023 Klientské centrum Obchod
10034 Kreativa Marketing
10225 Manažer IT bezpečnosti IT bezpečnost
Strana 1 z 3
1 - 10 z 25 záznamů
Záznamů na stránce 10
Organizační struktura
Automaticky synchronizována z personálního systému


czechidm
Najít uživatele, roli nebo systém ...
TESTADMIN
Nástěnka
Úkoly
Uživatelé
Organizace
Role
Napojené systémy
Virtuální systémy
Reporty
Audit
Historie workflow
Žádosti o role
Žádosti
Automatické role
Logované události
Události
Stavy entit
Provisioning
Notifikace
Audit
AUDIT PRO ENTITY
AUDIT PRO UŽIVATELE
AUDIT PŘIDĚLENÍ ROLÍ
AUDIT PŘIHLÁŠENÍ
AUDIT ZMĚN HESLA
Datum
Typ modifikace
Akci provedl
Uživatel
testuser
Role
ZRUŠIT FILTR
FILTROVAT
FILTR
Audit
Všechny aktivity v IAM jsou podrobně auditovány
Typ modifikace
Akci provedl
Datum revize
Entita (IdM)
Změněné atributy
Uživatel
Název role
Pracovně právní vztah
Další pozice
Platnost od
Platnost do
Přiděleno díky roli
Id
Přidání
testgar
23.04.2023 11:38:36
Franta Uživatel (testuser) - TEST: Role 2 (testsys_role2|DP)
Franta Uživatel (testuser)
TEST: Role 2 (testsys_role2|DP)
IT konzultant (kon_it_kon), IT konzultant
2023-04-23
4001344
Smazání
testming
10.04.2023 22:09:51
Franta Uživatel (testuser) - TEST: Prázdná role (testsys_er|DP)
Franta Uživatel (testuser)
TEST: Prázdná role (testsys_er|DP)
IT konzultant (kon_it_kon), IT konzultant
2022-10-24
3994341
Přidání
bcv_david.stekl
11.04.2023 16:38:44
Franta Uživatel (testuser) - LDAP_CAS
Franta Uživatel (testuser)
LDAP_CAS
IT konzultant (kon_it_kon), IT konzultant
2021-01-01
3975716
Smazání
petr.liska
05.04.2023 12:44:45
Franta Uživatel (testuser) - Google Analytics -
Franta Uživatel (testuser)
Google Analytics - Administrátor - Pojišťovna
IT konzultant (kon_it_kon),
2023-04-05
3943716
Historie workflow pro
Název procesu
Schválení změny v přiřazení role 'TEST
Datum vytvoření
23.04.2023 11:38:12
Datum ukončení
23.04.2023 11:38:34
Uživatelské úkoly procesu
Název
Přiřazeno (vyřešil)
Mohou řešit
Datum vytvoření
Datum ukončení
Rozhodnutí
Poznámka řešitele
Způsob ukončení
Schválení přiřazení role garantem
Antonin Garant (testgar)
testgar
23.04.2023 11:38:12
23.04.2023 11:38:34
approve
1 - 1 z 1 záznamů
Náhled procesu
Historie workflow
U každé žádosti lze sledovat detail schvalovacího workflow

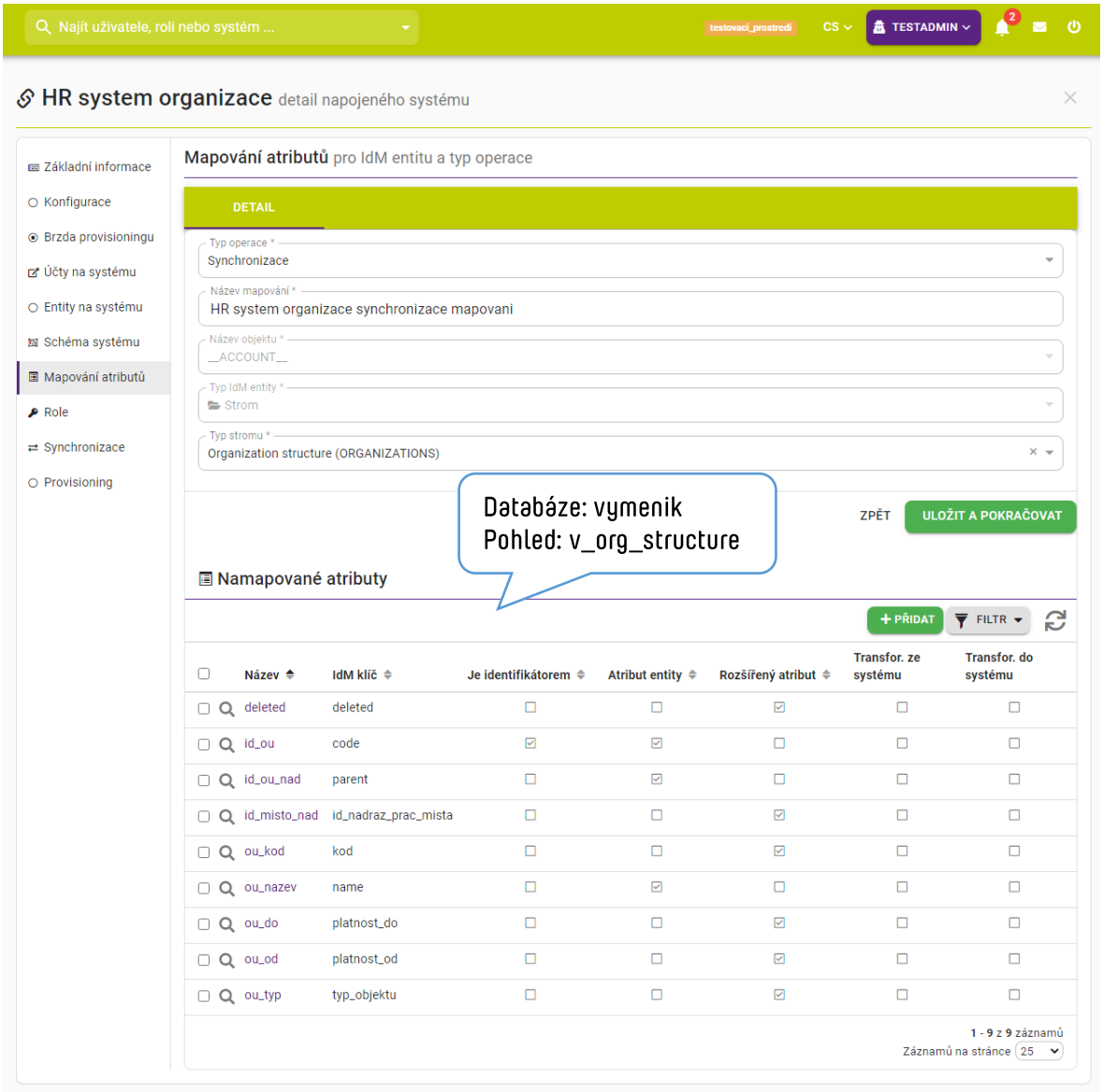
PŘÍLOHA P V: MAPOVÁNÍ ATRIBUTŮ DB VÝMĚNÍKU



- **deleted**: hodnota dosazená na základě ukončení pracovního vztahu.

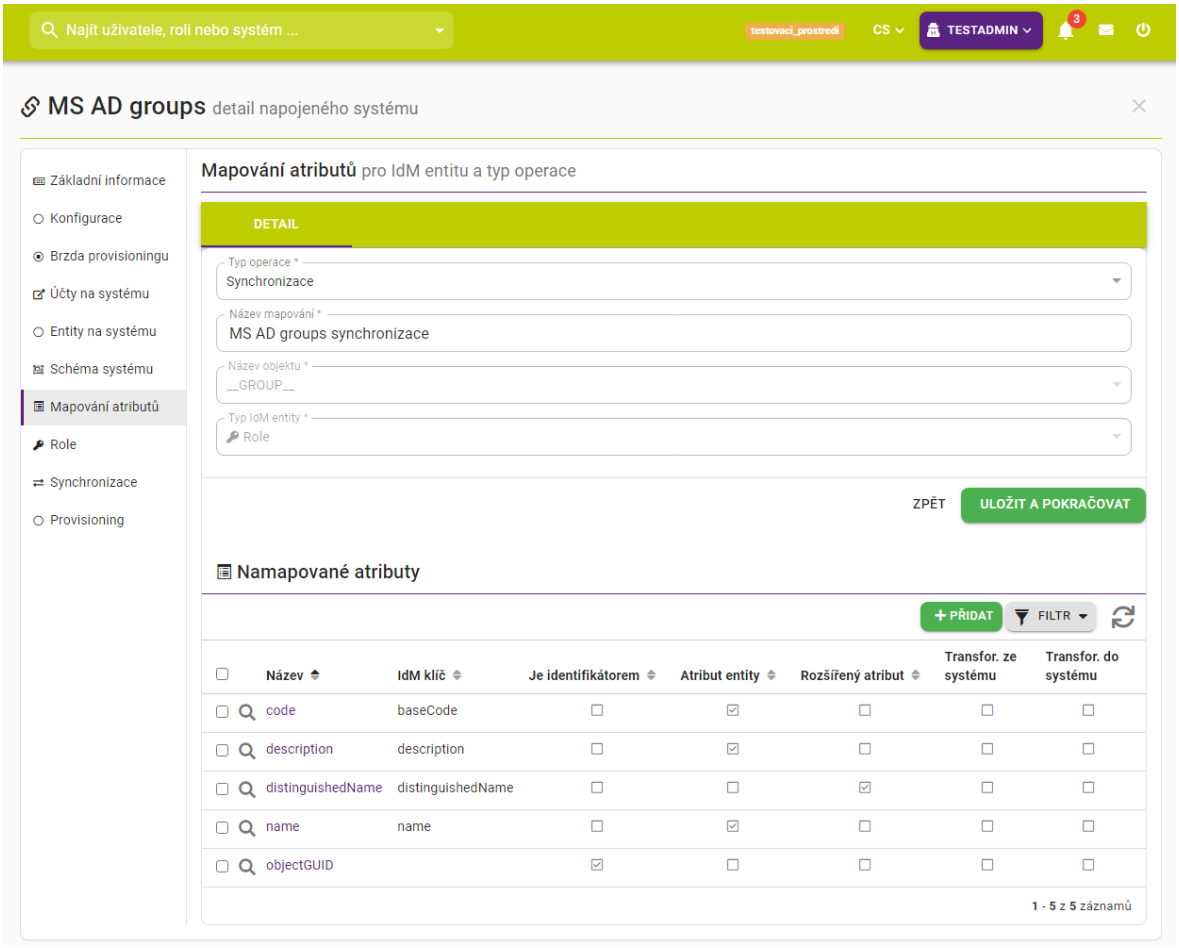


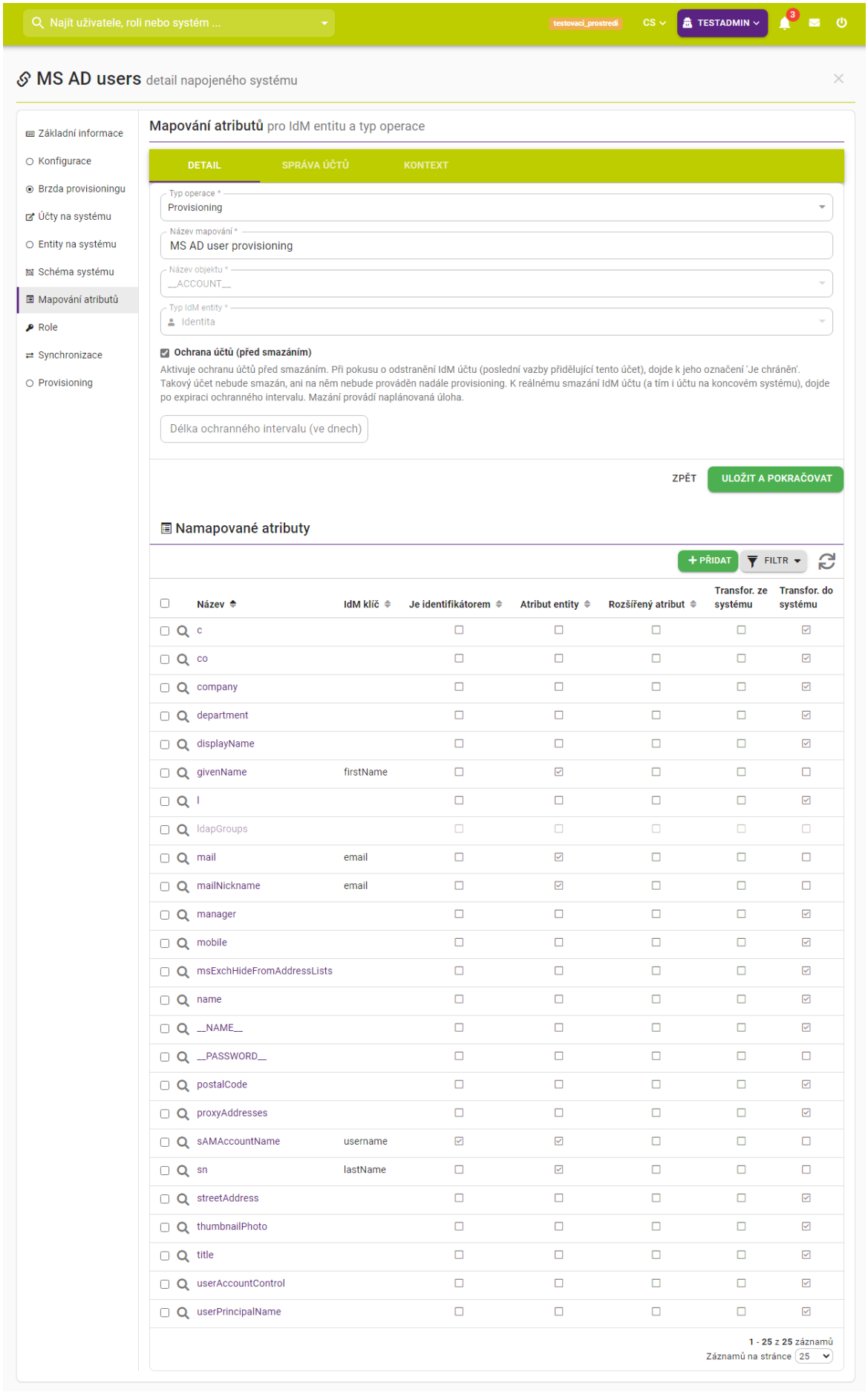
- **deleted**: hodnota dosazená na základě ukončení pracovního vztahu,
- **state**: hodnota transformovaná z ppv_typ na state – určuje, zda je typ úvazku aktivní (pro určité typy úvazků je identita zneaktivněna),
- **workPosition**: dosadí kód pracovní pozice,
- **identity**: z osobního čísla získá ID uživatele.



- **deleted**: hodnota dosazená na základě ukončení pracovního vztahu.

PŘÍLOHA P VI: MAPOVÁNÍ ATRIBUTŮ AD




Najít uživatele, roli nebo systém ...
testovaci_prostredi
CS
TESTADMIN
3
MS AD users detail napojeného systému
Základní informace
Konfigurace
Brzda provisioningu
Účty na systému
Entity na systému
Schéma systému
Mapování atributů
Role
Synchronizace
Provisioning
Mapování atributů pro IdM entitu a typ operace
DETAIL
SPRÁVA ÚČTŮ
KONTEXT
Typ operace *
Provisioning
Název mapování *
MS AD user provisioning
Název objektu *
__ACCOUNT__
Typ IdM entity *
Identita
Ochrana účtů (před smazáním)
Aktivuje ochranu účtů před smazáním. Při pokusu o odstranění IdM účtu (poslední vazby přidělující tento účet), dojde k jeho označení 'Je chráněn'. Takový účet nebude smazán, ani na něm nebude prováděn nadále provisioning. K reálnému smazání IdM účtu (a tím i účtu na koncovém systému), dojde po expiraci ochranného intervalu. Mazání provádí naplánovaná úloha.
Délka ochranného intervalu (ve dnech)
ZPĚT
ULOŽIT A POKRAČOVAT
Namapované atributy
+ PŘIDAT
FILTR
Název
IdM klíč
Je identifikátorem
Atribut entity
Rozšířený atribut
Transfor. ze systému
Transfor. do systému
c
co
company
department
displayName
givenName
firstName
l
ldapGroups
mail
email
mailNickname
email
manager
mobile
msExchHideFromAddressLists
name
__NAME__
__PASSWORD__
postalCode
proxyAddresses
sAMAccountName
username
sn
lastName
streetAddress
thumbnailPhoto
title
userAccountControl
userPrincipalName
1 - 25 z 25 záznamů
Záznamů na stránce
25

PŘÍLOHA P VII: SEZNAM POUŽITÝCH TECHNICKÝCH ÚČTŮ

Technické účty jsou uloženy v AD na doménovém řadiči „dc.dp-test.cz“ v „OU=DPT-Accounts,DC=dp-test,DC=cz“.

Název účtu	Pro systém	Cílový systém	Účel
iam-hr	IAM *iam.dp-test.cz*	Personální systém, WS *https://hr.dp-test.cz/ws/*	Synchronizace dat z person. systémů do DB výměníku
iam-ad	IAM *iam.dp-test.cz*	AD *dc.dp-test.cz*	Čtení a vytváření objektů v AD, autentizace
iam-db	IAM *iam.dp-test.cz*	IAM, DB „vymenik“ *localhost*	Synchronizace dat z DB výměníku do IAM
ems-ad	EMS *ems.dp-test.cz*	AD *dc.dp-test.cz*	Čtení objektů z AD, autentizace
fac-ad	FAC *fac.dp-test.cz*	AD *dc.dp-test.cz*	Čtení objektů z AD, synchronizace skupin, autentizace
fg-ad	FortiGate *fw-bo-int.dp-test.cz*	AD *dc.dp-test.cz*	Čtení objektů z AD, autentizace
wc-ad	QRadar *q1.dp-test.cz*	WinCollect na řadiči domény *dc.dp-test.cz*	Čtení logů z Microsoft Windows Security Event Log
wc-fs	QRadar *q1.dp-test.cz*	WinCollect na souborovém serveru *fs.dp-test.cz*	Čtení logů z Microsoft Windows Security Event Log