Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Webový portál pro přístup hostů do bezdrátové sítě pomocí Identity Service Engine

Martin Novák

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Martin Novák

Veřejná správa a regionální rozvoj

Název práce

Webový portál pro přístup hostů do bezdrátové sítě pomocí Identity Service Engine

Název anglicky

Web portal for guest access to wireless network using Identity Service Engine

---

Cíle práce

Hlavním cílem práce je vytvořit webový portál pro návštěvníky veřejné výzkumné instituce v prostředí Converged Access tak, aby bylo možné se pomocí mobilních zařízení připojit do otevřené bezdrátové sítě, provést registraci a získat konektivitu do sítě internet po dobu návštěvy.
Dílčím cílem práce je analýza současného stavu technologií v organizaci a možnosti nasazení webového portálu pro hosty. Dále pak navrhnout další technologický vývoj organizace po konci udržitelnosti projektu financovaného z Operačního programu Výzkum a vývoj pro inovace.

Metodika

Práce je založena na studiu odborné a vědecké literatury. Teoretická část se bude skládat z literární rešerše zabývající se danou problematikou.

Získané znalosti budou aplikovány v praktické části, kde bude analyzován proces tvorby portálu pro externí uživatele, následně bude provedeno srovnávání očekávaného a dosaženého výsledku. Na základě poznatků z případové studie a z analýzy odborných zdrojů bude syntetizován závěr práce.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

Cisco, Supervisor Engine 8-E, Identity Service Engine (ISE), Converged Access, Self-Registered Guest Portal

---

Doporučené zdroje informací

CCNA Wireless 200-355 Official Cert Guide. Indianapolis, Indiana, USA: Cisco Press, 2016. ISBN 978-1-58714-457-8.

ITIL Practitioner Guidance. London, United Kingdom: AXELOS, 2016. ISBN 9780113314874.

WALLACE, Kevin. CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Indianapolis, IN 46240 USA: Cisco Press, 2015. ISBN 978-1-58720-559-0.

WOLAND, Aaron a Jamey HEARY. Cisco ISE for BYOD and Secure Unified Access. Second Edition. Indianapolis, Indiana 46240 USA: Cisco Press, 2017. ISBN 978-1-58714-473-8.

WOLAND a Kevin REDMON. CCNP Security SISAS 300-208 Official Cert Guide. Indianapolis, Indiana, USA: Cisco Press, 2015, 928 s. ISBN 978-1-58714-426-4.

Předběžný termín obhajoby

2018/19 LS – PEF

Vedoucí práce

Ing. Alexandr Vasilenko, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 11. 9. 2018

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2018

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 21. 03. 2019

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Webový portál pro přístup hostů do bezdrátové sítě pomocí Identity Service Engine" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 29.3.2019 _____

Poděkování

Tímto bych rád poděkoval vedoucímu diplomové práce Ing. Alexandru Vasilenkovi, Ph.D. za cenné profesionální rady, individuální přístup, připomínky a metodické vedení práce.

Webový portál pro přístup hostů do bezdrátové sítě pomocí Identity Service Engine

Abstrakt

Práce se v teoretické části zabývá vytvořením webového portálu pro návštěvníky ve výzkumné organizaci. Popisuje principiální možnosti řešení přístupu hostů k bezdrátovému připojení a sítovou infrastrukturu Converged Access. Infrastruktura poskytuje konvergované řešení v oblasti drátového a bezdrátového připojení s možností správy obou prostředí z jednoho místa. V teoretické části se práce zabývá dvěma dílčími cíli: možností nasazení webového portálu pro hosty a analýzou současného stavu technologií v organizaci.

V rámci vlastní práce je popsán proces nasazení produktu Identity Service Engine od vytvoření instance virtuálního stroje, jeho instalace, provedení základního nastavení pro webového rozhraní a je nastíněna problematika certifikátu pro administrátorské rozhraní a pro webový portál. Konfigurace je znázorněna pomocí funkčních bloků, které jsou uspořádány do schématu reprezentující nastavení drátového i bezdrátového připojení na prvku síťové infrastruktury.

Posledním dílčím cílem bylo navrhnout další technologický vývoj v organizaci. Pro ověření vhodnosti navrhnuté technologie byl proveden Proof of Concept softwarově-definovaných sítí, jenž potvrdil vhodnost pro danou výzkumnou instituci.

Klíčová slova: Supervisor Engine 8-E, Identity Service Engine, Converged Access, Self-Registered Guest Portal, softwarově-definované sítě, Centrální Webová Autentizace, Lokální Webová Autentizace, Proof of Concept

Web portal for guest access to wireless network using Identity Service Engine

Abstract

The essay discusses the theory of creating a web-based guest access portal for the research organization visitors. It describes principal possibilities of wireless guest access users in the Converged Access solution. The network infrastructure offers converged solution for wired and wireless access and a single point of management. The two other objectives are discussed in the theoretical part: the possibility of deploying a web-based guest access solution and the analysis of the current technologies status in the organization.

The complete deployment of the Identity Service Engine is described in the main part of the essay starting with the VM installation, configuration of the web user interface and the security considerations regarding different certificates for guest access and management users. The configuration is visualized in the block chart which represents wireless and wired connection to the network infrastructure.

Last essay objective was to propose the technology evolvement in the organization. A Proof of Concept of software defined network was carried out to evaluate the suggested proposal. It showed that the drafted solution was appropriate for the given research organization.

Keywords: Supervisor Engine 8-E, Identity Service Engine (ISE), Converged Access, Self-Registered Guest Portal, software-defined networking, Central Web Authentication, Local Web Authentication, Proof of Concept

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

ISE	Identity Service Engie
WLC	Wireless Controller (Bezdrátový řadič)
CAPWAP	Control And Provisioning of Wireless Access Points
SSO	Statefull Switchover
AP	Wireless Access Point (bezdrátový přístupový bod)
FQDN	Fully Qualified Domain Name (Plně specifikované doménové jméno)
ITIL	Information Technology Infrastructure Library
MA	Mobility Agent
MC	Mobility Controller
UAP	Usage Acceptable Policy

1 Úvod

Předkládaná práce je zaměřena na popis nasazení webového portálu pro hosty. Práce je rozdělena na teoretickou a praktickou část. Teoretická část popisuje principy technologie Converged Access, možnosti webové autentizace klientů, projektově orientovanou přípravu a zásady podle kterých bude postupováno.

Hlavním Cílem této diplomové práce je vytvořit webový portál pro návštěvníky veřejné výzkumné instituce v prostředí Converged Access tak, aby bylo možné se pomocí mobilních zařízení připojit do otevřené bezdrátové sítě, provést registraci a získat konektivitu do sítě internet po dobu návštěvy. Hlavní cíl práce je rozdělena do tří částí. První část se bude zabývat instalací produktu Identity Service Engine, nastavením bezpečností opatření a napojením na infrastrukturu organizace. V druhé část bude popsána topologie sítě se zaměřením na tunelování bezdrátového provozu generovaného klienty směrem k bezdrátovému řadiči a nastavení bezdrátového řadiče a přepínače. K vypracování této části bude použito blokového schéma, kde jednotlivé bloky reprezentují nastavení přepínače. Třetí část popíše vytvoření hostovského portálu, možnosti jeho kustomizace, nastavení Identity Service Engine pro Centrální Webovou Autentizaci. Tato část bude rozdělena na nastavení pravidel pro autentizaci a autorizaci.

Práce obsahuje tři dílčí cíle. Analýzu současného stavu technologií v organizaci, který se zabývá škálovatelností a prvky inovativnosti dané technologie v době vzniku. Výběr vhodného výrobce technologie pro nasazení webového portálu pro hosty, je popsán v druhém dílčím cíli a zabývá se způsobem výběru a hodnocením možných produktů. Třetí dílčí cíl pak rozpracovává problematiku návrhu dalšího technologický vývoje organizace po konci udržitelnosti projektu financovaného z operačního programu Výzkum a vývoj pro inovace období 2007–2013.

Důvodem pro výběr tohoto tématu byla aktuálnost nasazené technologie v oblasti státní a veřejné správy a aktuální situace v oblasti zpracování osobních údajů v návaznosti na GDPR, i stále větší prosazování trendu poskytování nových služeb hostům institucí při zachování bezpečnosti a dodržení vnitropodnikových bezpečnostních politik.

Zároveň zde existuje možnost rozšířit obzory o problematice tématu přístupu hostů do bezdrátové sítě řešené pomocí Identity Service Engine potenciálním čtenářům této práce.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem práce je vytvořit webový portál pro návštěvníky veřejné výzkumné instituce v prostředí Converged Access tak, aby bylo možné se pomocí mobilních zařízení připojit do otevřené bezdrátové sítě, provést registraci a získat konektivitu do sítě internet po dobu návštěvy. Dílčím cílem práce je analýza současného stavu technologií v organizaci a možnosti nasazení webového portálu pro hosty. Dále pak navrhnout další technologický vývoj organizace po konci udržitelnosti projektu financovaného z Operačního programu Výzkum a vývoj pro inovace.

2.2 Metodika

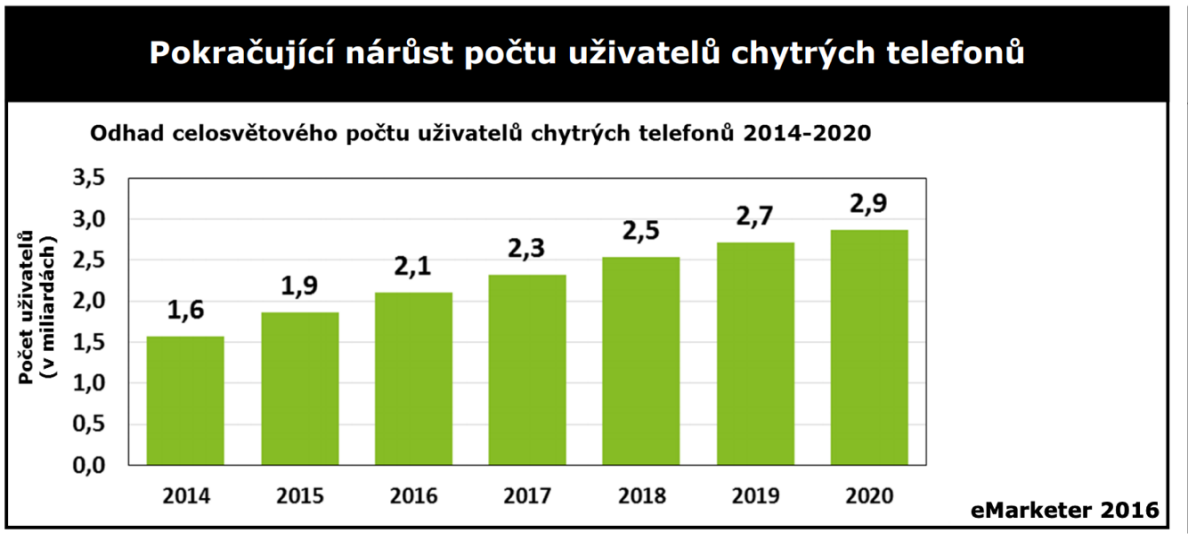
Práce je založena na studiu odborné a vědecké literatury. Teoretická část se bude skládat z literární rešerše zabývající se danou problematikou. Získané znalosti budou aplikovány v praktické části, kde bude analyzován proces tvorby portálu pro externí uživatele, následně bude provedeno srovnávání očekávaného a dosaženého výsledku. Na základě poznatků z případové studie a z analýzy odborných zdrojů bude syntetizován závěr práce.

3 Teoretická východiska

Aktuální trendy v oblasti poskytování služeb IT

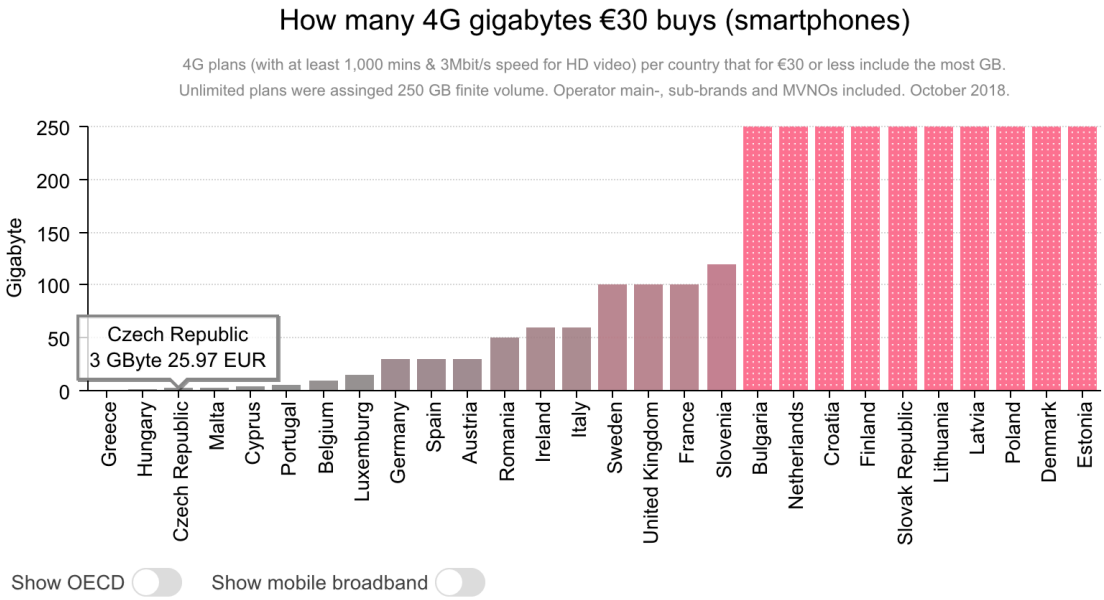
- Růst počtu chytrých telefonů
- Vysoká cena mobilních dat
- Výrobci odstraňují LAN konektor
- Rostoucí počet uživatelů sociálních sítí
- Cloud jako způsob konzumování služeb
- Poskytování stejných služeb ve stejné kvalitě nehledě na způsob připojení

Nárůst počtu mobilních zařízení, který ilustruje Obrázek 1. Reprezentuje aktuální trend přechodu uživatelů na mobilní zařízení a jejich využití v každodenním životě uživatelů.



Obrázek 1: Nárůst počtu uživatelů chytrých telefonů – převzato z Koncepce Smart Prague do roku 2030

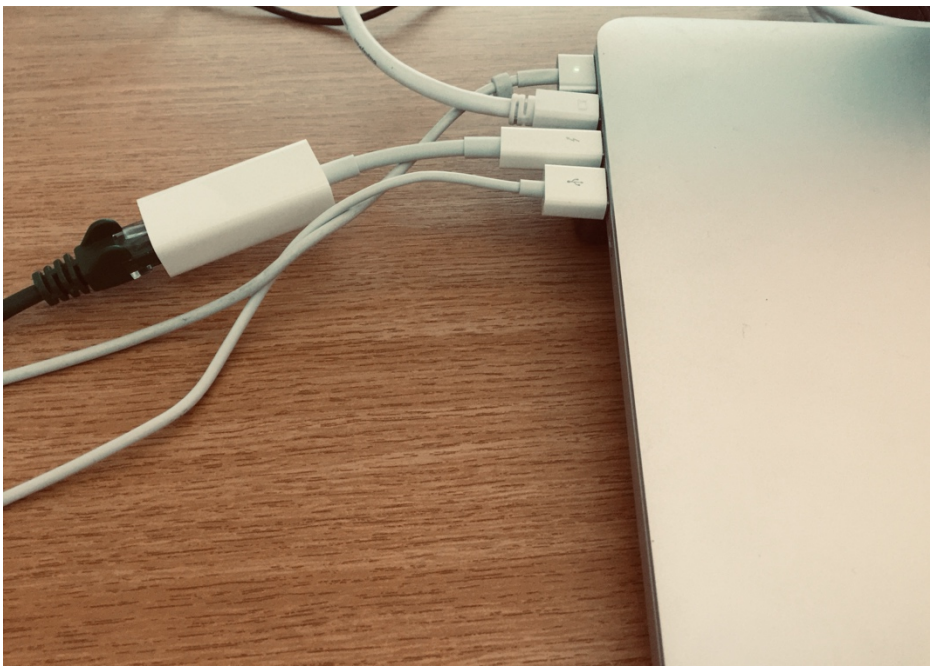
Uživatelé stále více spoléhají na možnosti bezdrátového připojení pro svá zařízení, a to díky vysokým cenám mobilních dat v přepočtu na MB v porovnání s ostatními evropskými státy.



Obrázek 2: Porovnání objemu mobilních dat za 30 € – převzato z Rewheel Research

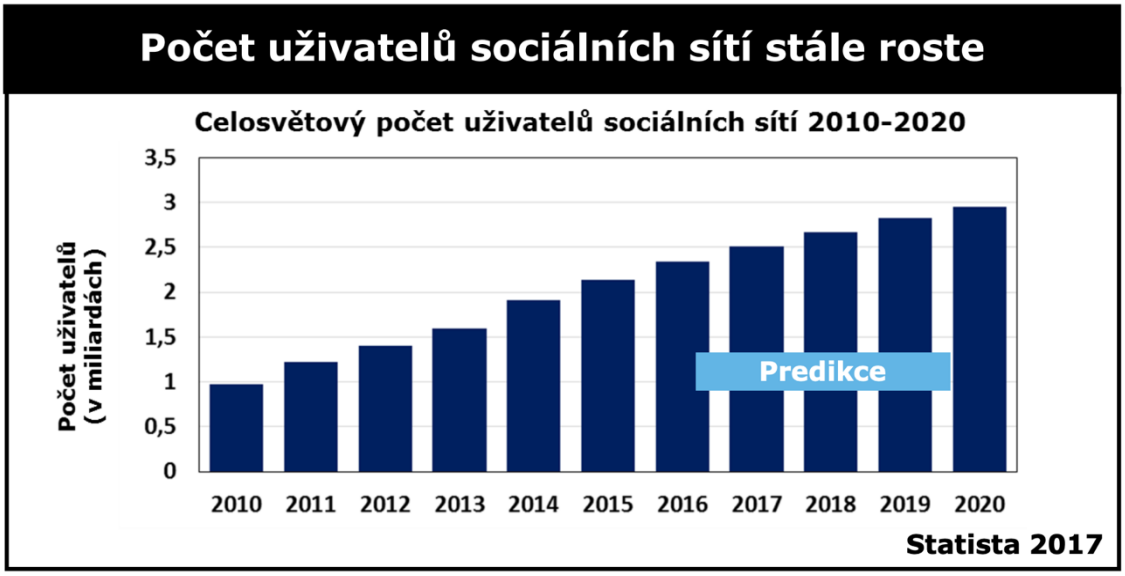
Nárůstem počtu uživatelů roste i datových provoz bezdrátových klientů, který ovlivňuje i trend cloudových služeb a přenosu obsahu z těchto cloudových uložišť. Uživatelé tak vytvářejí tlak na poskytování kvalitního a vysoce propustného Wi-Fi připojení. Bezdrátové připojení již tedy není chápáno jako doplňková služba. Aktuálním trendem je poskytování stejných služeb pro koncové uživatele nehledě na médium pomocí, kterého jsou připojeni.

Dalším z trendů v oblasti chytrých zařízení je výroba stále užších zařízení. Následkem výroby takto tenkých zařízení je nutnost odstraňování rozměrově náročných portů jako je např. Ethernetový port, který umožňoval připojení pomocí síťového kabelu s koncovkou RJ-45.



Obrázek 3: Externí ethernetový adapter (vlastní zpracování)

Dle mého názoru je poskytování Wi-Fi připojení hostům je v roce 2019 již naprostým standardem. Nárůst počtu uživatelů sociálních sítí ilustruje Obrázek 4



Obrázek 4: Nárůst počtu uživatelů sociálních sítí – převzato z Koncepce Smart Prague do roku 2030

Tato specifika vytváří tlak pro poskytování návštěvnických Wi-Fi sítí. A to již v souvislosti s nárůstem počtu uživatelů sociálních sítí, kteří díky vysoké ceně mobilního připojení využívají právě tyto otevřené sítě.

3.1 Principiální možnosti řešení hostovského přístupu

Mezi principiální možnosti realizace přístup hostů k bazálnímu internetovému připojení patří zejména: otevřená bezdrátová síť, bezdrátová síť chráněná předdefinovaným sdíleným heslem, Hotspot portál, Hostovský portál, pomocí kterého je realizován přístup v následující práci a BYOD řešení, které je mimo rozsah této práce a nebude v práci bude zmíněno jen obecně a okrajově.

- Otevřená bezdrátová síť

Výhodou řešení je jednoduchost jak z pohledu správce infrastruktury, tak koncových uživatelů. Dle mého názoru je v roce 2019 bezpečnostním rizikem poskytovat otevřenou bezdrátovou síť bez šifrování s nemožností přímé identifikace koncového uživatele a požadavku na přijmutí politiky organizace (UAP).

- Bezdrátová síť chráněná předdefinovaným sdíleným heslem

Řešení je založena na Wi-Fi Protected Access 2 kdy klienti využívají k připojení stejné heslo/klíč. Identifikace klienta je omezena na okamžik získání hesla, kdy při registraci je možné získat údaje koncového uživatele a jeho souhlas s UAP. Taková způsob registrace je administrativně nenáročný, informace o klientovi jsou aktuální pouze v době získání přístupu a nezabrání sdílení klíče mezi uživateli, kteří se nechtějí registrovat.
Tento způsob zabezpečení bezdrátové sítě byl dle projektu wifileaks v roce 2018 nejrozšířenějším způsobem v České republice.

- Hotspot portál

Webové rozhraní portálu pro přihlášení uživatelů do sítě je realizováno přeš přístup to otevřené bezdrátové sítě. Po přihlášení je datový provoz uživatele přesměrován na webový portál provozovatele, kde se pro přihlášení využívá zejména: přijmutí politiky UAP, zadání n místného kódu, který v případě rychlého občerstvení může být např. součástí daňového dokladu, přihlášení pomocí účtu sociální sítě anebo v případě ubytovacího zařízení lze využít přihlášení pomocí čísla pokoje a příjmení ubytovaného. Náročnost daného řešení na implementaci je pak středně snadné až obtížné.

- Hostovský portál

Stejně jako u Hotspot portálu je po přihlášení do otevřené bezdrátové sítě přesměrován datový provoz uživatele na webový portál. Toto řešení rozšiřuje možnosti identifikace koncových uživatelů, kdy uživatel při registraci musí např. zadat: Jméno, Příjmení, e-mail, e-mail osoby, jenž v organizaci navštěvuje a další požadované informace. Výhodou je pak vhodnost řešení jak pro hosty, tak pro externisty, kteří mohou být na základě dalších pravidel přesměrováni na BYOD portál a získat tak přístup k službám, které spravují.

- eduroam

Akademická síť eduroam lze chápat jako možnost hostovského přístupu pro specifickou a omezenou skupinu uživatelů. Tito uživatelé jsou například zaměstnanci nebo studenti vysokých škol, ústavů akademie věd a další. Uživatelé pak mohou využívat připojení i například na nádraží kdy jsou ověřeni na základě svých přihlašovacích údajů.

- BYOD

Využitím komponenty BYOD (Bring Your Own Device / Zaměstnanci si mohou přinést svá vlastní mobilní zařízení a využívají je k přístupu k sdíleným službách organizace), která je integrovatelná do webového portálu, lze povolit přístup zaměstnancům pracujících v areálu, kteří potřebují získat bazální konektivitu bez nutnosti registrace, a to na základě jejich uživatelského účtu generovaného na základě platného úvazku k vědecké organizaci.

Zmíněná funkcionalita usnadňuje přechod studentů do pracovního poměru, a to na v případě kdy zaměstnanec již není studentem, tím je jeho studentský účet v rámci akademické sítě eduroam ukončen a zároveň čeká na dokončení procesních operací nutných k získání údajů navázaných na svého akademického zaměstnavatel, jenž mu zajistí účet nutný pro přístup do sítě eduroam. Příkladem BYOD konfigurátoru je eduroam Configuration Assistant Tool (CAT).

Porovnání zmíněných principiálních možností poskytování hostovského přístupu je shrnuto v komparativní tabulce Tabulka 1

	Hostovský přístup	Otevřená bezdrátová síť	WPA 2 PSK	Hot spot portal	BYOD	eduroam
Jednoducho st obsluhy	Středně snadné	Velmi snadní	Snadné	Snadné	Střední	Snadné
Náročnost implementa ce ze strany provozovat ele	Středně Obtížné	Jednoduché	Velmi snadné	Středně snadné/ obtížné	Středně obtížná / obtížná	Středně Snadná/ obtížný
Možnost identifikace koncového uživatele	Jednoznač né rozlišení klienta	Bez možnosti identifikace	Bez možnosti identifikac e	Bez možnosti identifik ace	Jednoznač né rozlišení klienta	Jednozna čné rozlišení klienta
Možnost souhlasu klienta s AUP	Ano	Bez možnosti nasazení	Bez možnosti nasazení	Ano	Ano	Ne
Šifrování provozu v WiFi provozu	Izolace provozu mezi klienty	Nelze provádět	Stejné heslo pro všechny	Izolace provozu mezi klienty	Velmi vysoká bezpečnos t	Velmi vysoká bezpečno st
Vhodnost pro hosta	Vhodné	Velmi nevhodné	Nevhodné	Středně vhodné	Nevhodné	Vhodné
Vhodnost pro externistu	Vhodné	Velmi nevhodné	Velmi nevhodní	Velmi nevhodní	Velmi vhodné	Nevhodn é

Tabulka 1: Komparativní tabulka srovnání možností hostovského přístupu (vlastní zpracování)

3.2 Možnosti nasazení webového portálu pro hosty

Webové prohlížeč je součástí každodenního života uživatelů využívajících připojení k sítí internet. Díky rozšíření chytrých zařízení, které vlastní nebo s ním pracuje každý uživatel, nehledě na platformu na, které pracuje má vestavěný nebo doinstalovaný webový prohlížeč.

Uživatelé využívající webový portál přistupují k této službě zejména pomocí mobilních zařízení jako je např. notebook, tablet smartphone atd. Webový portál je vhodné řešení poskytování bazálního připojení hostů díky automatickému přesměrování jejich datového provozu při asociaci do otevřené bezdrátové sítě. Díky automatickému přesměrování datového provozu uživatele je využívání služby webového portálu uživatelsky přívětivé a nevyžaduje žádnou další interakci ze strany uživatele, aby získal možnost se přihlásit nebo zaregistrovat do bezdrátové sítě.

Při návrhu uživatelské rozhraní pro webový portál bylo využito grafického návrhu pomocí drátového modelu. Byla rozpracována vizuální podoba jednotlivých částí portálu tak, aby svojí grafickou podobou odpovídali jednotné grafické identitě používaní v organizaci. Pomocí registrace skrze webový portál je získána a ověřena identita uživatele. Uživatel před povolením přístupu do sítě musí potvrdit souhlas s pravidly používání sítě.

Pří procesu a registrace a následně při opakovaném přihlášení má uživatel možnost využít přesměrování na stránku uživatelské podpory. V případě požadavku na asistenci ze strany IT oddělení tak uživatel získává přímo informace, jak kontaktovat podporu a urychlit tím řešení svého problému.

Mezi požadované funkce portálu patří zejména: registrace prováděna samotným hostem, možnost vyžadování potvrzení souhlasu s pravidly používání, možnosti automatického zasílání údajům hostů, a to zejména pomocí e-mailu nebo SMS zprávou, možnost odkazovat na externí webovou stránku jejímž účelem bude obsahovat informace o pravidlech používání.

Obrázek 5: Návrh uživatelského rozhraní webového portálu pomocí drátového modelu (vlastní zpracování)

Na základě vnitřních předpisů a politiky rozvoje infrastruktury v organizaci byla sestavena pravidla pro výběr nejvhodnější produktu pro provozování portálu pro hosty.

Jako hlavní kritéria při výběru produktu byla vybrána podpora ze strany výrobce, podpora dalších funkcí a využitelnost v projektu obnovy infrastruktury. Dále pak rozsáhlé možnosti grafické úpravy samotného portálu tak, aby byl v souladu s jednotnou grafickou identitou organizace. Poslední z kritérií je stěžejní zejména pro dílčí cíl práce, a to pro návrh dalšího technologické vývoje v organizaci.

Produkt	Open Source řešení	Komerční produkt	Podpora ze strany výrobce	Podpora ze strany komunity	Podpora dalších funkcí	Využitelnost v projektu obnova infrastruktury	Pokročilé grafické úpravy portálu
ISE							
Zeroshell							
ChilliSpot							
Wifidog							
N2S							
Aruba ClearPass							

Tabulka 2: Rozhodovací matice produktu (vlastní zpracování)

Nevýhodou Open Source řešení se ukázala často nedostatečná dokumentace bez možnosti zakoupení podpory a využitelnost v projektu obnovy infrastruktury. Řešení od společnosti N2S nabízelo pouze cloudové řešení bez možnosti hostovat službu na serverech organizace. Problematickou část také představovala chybějící dokumentace k implementaci na platformě Converged Access a nemožnost využít produkt v projektu obnovy infrastruktury. Produkt Aruba Clear Pass, který i přes to že splnil celou řadu požadovaných kritérii nebyl schopen nabídnout přímou podporu v projektu obnovy infrastruktury, a proto byl vyloučen.

Výhodou pro volbu ISE pro poskytování služby webového portálu pro hosty pomocí Centrální Webové Autentizace (CWA), je jeho integrace výrobcem již v době představení technologie. Dále pak možnost využití produktu v projektu dalšího technologického vývoje v organizaci. Výrobce produktu dále poskytuje pokročilé možnosti tvorby a úpravy grafické stránky portálu a tím umožňuje jeho tvorbu do jednotného grafické identity organizace. Jeho úkolem je nahradit stávající drátové řešení u kterého již výrobce určil konec životního cyklu.
Na základě analýzy požadavků na funkce portálu, výběru produktu Identity Service Engie a zpracovaného drátového modelu grafické rozhraní budoucího webového portálu byl v kapitole 4.5 vytvořen webový portál pomocí nástroj ISE Portal Builder.

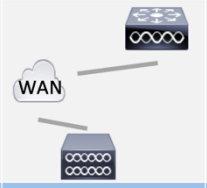
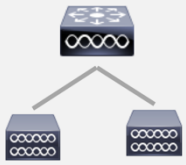
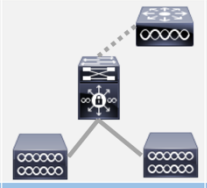
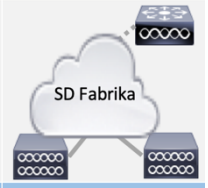
3.3 Identity Service Engine

Je ucelené řešení společnosti Cisco v oblasti řízení síťového přístupu. Produkt má v sobě integrované funkce jako např. RADIUS server, profilování, stav zařízení, jednotné místo pro správu a vymáhání politik, BYOD a řešení v oblasti hostovského přístup. Řešení se zejména vyznačuje rozsáhlou dokumentací výrobce, odbornými blogy popisující nastavení jednotlivých modulů, pravidelnými aktualizacemi ze strany výrobce a možností obrátit se v případě problémů na centrum technické podpory (TAC).

3.3.1 Bezdrátové připojení a jeho možnosti nasazení

Nasazení jednotlivých modelů, ve kterých je možné poskytovat bezdrátové připojení je závislé na konkrétních aplikací a přidané hodnotě, kterou má daná služba přinášet. Pro malé bezdrátové sítě, může být vhodný jak FlexConnect tak autonomní mód, kdy opět záleží na konkrétním řešení. Při budování nového kampusu pak bylo v době návrhu (2011-13) výhodnou volbou zvolení řešení pro kampusové sítě, které využívá jednotou infrastruktur pro drátové u bezdrátové připojení, má vysokou propustnost datového provozu, lze ho spravovat automatizovaně a centrálně z jednoho místa. To umožňuje rychle a efektivně vybudovat požadovanou infrastruktur s využitím menšího počtu zaměstnanců.

Aktuálním novinkou v této oblasti jsou sítě řízené záměrem, této oblasti je věnována kapitola Návrh technologického vývoje organizace.

	Autonomní mod	FlexConnect	Centralizovaný mod	Converged Access	SD Wireless a Access
					
	Malé bezdrátové sítě	Pobočky	Kampusy	Pobočky a Kampus	Pobočky a Kampus
Vhodné řešení	Pouze bezdrát	Pouze bezdrát	Pouze bezdrát	Drát i bezdrát	Drát i bezdrát
Benefity	Jednoduché řešení s výhodným poměrem cena/výkon.	Vysoce šáklovatelné řešní pro velké množství vzdálených poboček (lokalit). Bezdrátový řadič je uložen v centrálím datacentru.	Bezdrátový provoz je viditelný na centralizovaném bezdrátovém řadiči.	Společná platforma/infrastruktura pro drát i bezdrát. Jeden operační systém (IOS-XE). Opltimalizovaný výkon pro 802.11ac.	Společná platforma/infrastruktura pro drát i bezdrát.Infrastruktura řízená záměrem. Jednotné politky správy.
Klíčová hlediska	Omezený RRM, bez detekce cizích vysýlaných sítí	Pouze L2 roaming, nároky na kvalitu linky (latence)	Propustnost infrastruktruou	Na přístupové vrstvě prvky Catalyst 3650 a 3850 nebo Catyst 4K se SUP8-E	Využitelnost stávající infrastruktury organizace.

Obrázek 6: Možnosti nasazení bezdrátového připojené (vlastní zpracování)

3.4 Converged Access

Struktura Cisco Unified Access je postavena na následujících třech pilířích a to: jedné politice, správě a jedné sítí. Jedna politika je realizována skrze Identity Service Engine (ISE), který podporuje politiku managementu BYOD, profilování, stav zařízení a portály hostovského přístupu. Jeden správa je realizován skrze Cisco Prime Infrastructure, který nabízí kompletní správu drátové i bezdrátové sítě, uživatelský a přístrojově orientovaný pohled na síť a intuitivní postup při odstraňování problémů. Jedna síť je poskytována skrze Converged Access, který kombinuje bezdrátové sítě do jedné sjednocené infrastruktury.

Řešení pro konvergovaná přístup v rámci Unfied Acces je založeno na přepínačích Cisco Catalyst 3650, 3850, Catalyst 4500E Supervisor Engine 8E a hardwarovém bezdrátovém řadiči 5760.Jedna fyzická infrastrukturu pro drátovou i bezdrátovou konektivitu řešená pomocí platformy přepínačů Convrged acces s integrovanou funkcionalitou bezdrátového řadiče. [2, 3]

3.4.1 Fyzické entity Converge Access

- Mobility Kontrolér (MC)

Pracuje-li přepínač v módu Mobility kontrolér může přepínač provádět všechny typické úkoly Mobility Agenta a navíc: koordinace mobility, RRM a CleanAir koordinace v přiřazené mobility subdoméně. [2, 3]

Zajišťuje služby mobility managementu pro roamingové události. MC zasílá na jednotlivé MA, kteří patří do jedné subdomény konfigurační updaty jako název Switch Peer Group (SPG) a seznam jednotlivých členů SPG. [4]

- Mobility Agent (MA)

Mobility agent je základní mód, který je nastavený na přepínači vyexpedovaném z továrny. V tomto módu je přepínač schopný ukončovat CAPWAP tunely přístupových bodů a tím poskytovat konektivitu bezdrátovým klientů. Pracuje-li přepínač jako Mobility Agent udržuje lokální databázi bezdrátových klientů, vymáhá bezpečnostní politiku a politiku kvalitu služby (QoS) pro bezdrátové klienty a přístupové body. Licence typu IP Base je vyžadována pro mód Mobility Agent. [2, 3]

3.4.2 Logické entity Converge Access

- Mobility doména (MD)

Je celá doména, přes kterou je dostupný rychlý roaming pro všechny klienty.

MD lze definovat jako sbírku až několika mobility group (MG). Jako jednu mobility doménu lze chápat kampusovou sít. [2, 3]

- Mobility subdoména (MSD)

Je autonomní část mobility domény. Každá mobility subdoména obsahuje jeden mobility kontrolér (MC) a sbírku až několik Switch Peer Group (dále SPG). [2, 3]

- Mobility Group (MG)

Je sbírkou mobility subdomén, přes které je podporovaný rychlý roaming. Mobility grupa může být např. jedna až n budov uvnitř kampusu, přes kterou je podpora rychlého roamingu. [2,3]

- Switch Peer Group (SPG)

Je logická entita skládající se z Mobility Agentů, kteří chovají jako skupina pod Mobility kontrolérem v přiřazené mobility subdoméně. Nastavení SPG skupiny usnadňuje rychlý roaming mezi converged access přepínači v stejné SPG skupině a utváří full-mesh tolopogii CAPWAP tunelů mezi mobility agenty. [2, 3]

3.5 Webová autentizace klientů

Vývoj a změny v oblasti Webové Autentizace zobrazuje komparativní Tabulka 3. Jednotlivé typy autentizací popisují následující kapitoly. [1,5]

Lokální Webová Autentizace (LWA)	Centrální Webová Autentizace (CWA)
Autentizace hostů se provádí na konkrétním síťovém zařízení	Autentizace hostů se provádí centrálně na ISE
Každé síťové zařízení má svůj vlastní webový server a portál	Webový server a portál jsou provozovány centrálně na ISE
Nepodporuje funkci Změna Autority (CoA)	Podporuje funkci Změna Autority (CoA). To umožňuje služby využívající profilování a stavu zařízení.

Tabulka 3: Porovnání LWA a CWA (vlastní zpracování)

3.5.1 Lokální Webová Autentizace (LWA)

Jedná se o původní Webovou Autentizaci. Autentikátor přesměruje webový provoz na lokálně hostovaný webový portál kde uživatel zadá uživatelské jméno a heslo. [1, 5]

Tyto údaje jsou poslány skrze přepínač nebo bezdrátový řadič (WLC), ten pošle RADIUS žádost o přistup (Access-Request) na autentizační server obsahující uživatelské jméno a heslo získané z webového portálu. Lokální Webovou autentizací je tedy každý pokus o přihlášení přeposlaný přepínačem nebo bezdrátovým řadičem (WLC). [1, 5]

Webové stránky jsou uloženy na přepínači, ale jejich kustomizaci je velmi omezená. Dnešní společnosti využívají webové portálu upravené do jednotného vzhledu, který

odpovídá firemní politice a jednotné grafické identitě. Pro tyto společnosti není obecně tradiční LWA přijatelným řešení. [1, 5]

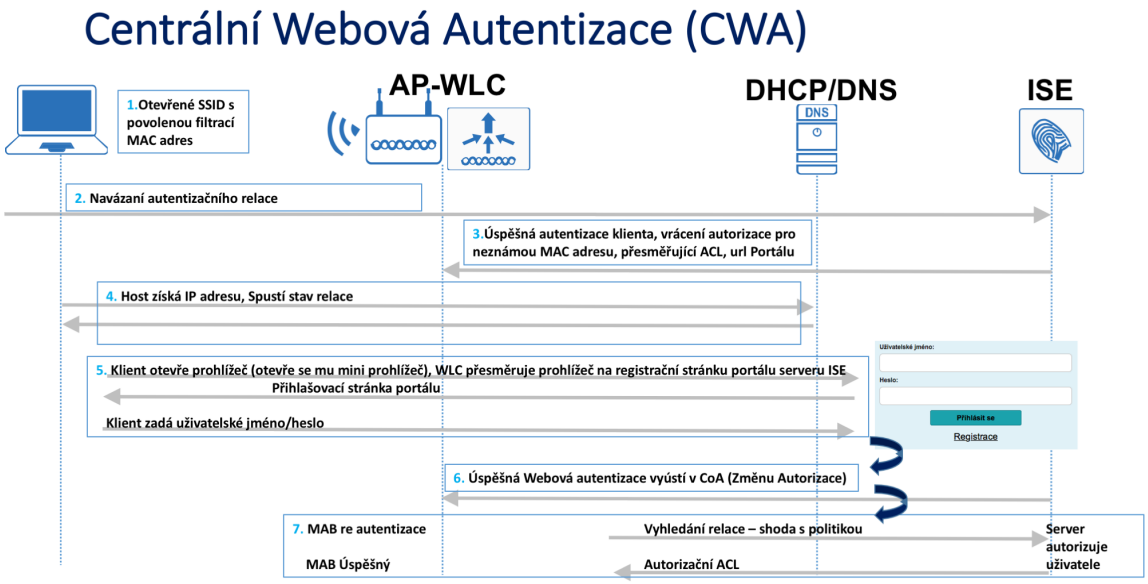
Při používání LWA na přepínačích neexistuje nativní podpora pro pokročilé služby jako je profilování hodnocení stavu zařízení, přijímaní politiky uživatelem, samo registraci zařízení i uživatele a změnu jeho hesla. [1, 5]

3.5.2 Centrální Webová Autentizace (CWA)

Centrální Webová Autentizace (CWA) je použita skrz celé řešení bezpečného přístupu. Přestože je Cisco ISE schopné podpory Lokálních Autentizačních Metod (LWA), jsou tyto metody typicky rezervovány pro síťová zařízení jiných výrobců. [1, 5]

Webová autentizace je pouze pro interaktivní uživatele, kteří mají webový prohlížeč, pomocí kterého uživatel zadá uživatelské jméno a heslo.

CWA podporuje všechny pokročilé služby jako je profilování hodnocení stavu zařízení, přijímaní politiky uživatelem, samo registraci zařízení i uživatele a změnu jeho hesla. [1, 5]



Obrázek 7: Princip Centrální Webové Autentizace (vlastní zpracování)

3.6 Information Technology Infrastructure Library (ITIL)

Zásady ITIL jsou založeny na zkušenostech tisíce organizací z celého světa. Každý, kdo přijme ITIL za své bude získávat prospěch z mnoha let složité získávaných znalostí. ITIL jako všechny každý jiný Framework/aplikační rámec, metodologie nebo filozofie je hodnotný jen tak jakého výsledku je pomocí něj dosaženo. Vždy je důležité mít na paměti jakého cíle má být dosaženo a proč toho má být dosaženo. Úspěch je závislí na aplikaci kritického úsudku za každé situace. Profesionál, který přijme IT Service and Management System (ITSM) a jeho klíčové vlastnosti má mnohem lepší šanci dosáhnout maximálního výsledku v oblasti managementu služeb. [6]

Při používání ITIL hovoříme o:

- Adopt/Přijmout – sloveso, jehož význam lze interpretovat jako „začít něco používat“. [6]

- Adapt/Přizpůsobit – sloveso, jehož význam lze interpretovat jako „změnit nebo upravit tak, aby se to hodilo k danému účelu nebo situaci“ [6]

3.6.1 Základní pojmy

V jádru ITIL a ITSM je koncept služby. Služby se zaměřují jak na poskytovatele služeb, tak na zákazníky. Služby se zaměřují na poskytovatele služeb a zákazníky.

- Poskytovatel služby – je organizace zajišťující služby jednomu nebo více jak interních, tak externích zákazníků. [6]

- Zákazník – je někdo kdo kupuje zbožní nebo služby. Osoba nebo skupina, která definuje a potvrzuje s cílovou úrovní služby je zákazníkem poskytovatele IT služeb. [6]

- Služba – je prostředkem dodání hodnoty zákazníkovy, která umožní dosažení výsledku, který zákazník požaduje bez vlastnictví specifických nákladů a rizik. [6]

Cílem služby je umožnit zákazníkovi získat nebo vlastní něco co chce bez toho, aby to musel vlastnit nebo se starat o části, které jsou nutné k získání toho po čem touží.
Je-li cílem zajistit, že služba přináší hodnotu, musíme si uvědomit, že hodnota pochází nejen z funkčnosti služby. [6]

- Hodnota – Benefity získané v poměru prostředků, které jsou do nich vloženy. Hodnota služby vychází z toho, čeho zákazníkovi umožňuje dosáhnout. Služba přináší hodnotu organizaci pouze tehdy, pokud je hodnota vnímána jako vyšší než cena za získání služby. Hodnotu lze chápat jako službu, proces, partnera a další co pomůže přinést hodnotu zákazníkovi. [6]

- Utility– jak je služba vhodná k danému účelu [6]

- Warranty – jak je služba vhodná pro dané užití [6]

I ta nejvíce žádaná funkcionalita je k ničemu není-li dodána na takové úrovni, která splní požadavky zákazníka.

- Outcome– je výsledek realizace a činnosti, následovaný procesem nebo poskytnutí IT služby. Daný termín se vztahuje jak k plánovanému, tak skutečnému výsledku. [6]

- Output – Jde o specializovaný produkt (hmotný nebo nehmotný), který je vyráběn, konstruován nebo vytvořen v důsledku plánované činnosti a předán jednomu nebo více uživatelům. [6]

3.6.2 9 principů ITIL Practitioner guidance

Výsledkem níže zmíněných principů bylo úspěšné dokončení projektu webového portál pro přístup hostů do bezdrátové sítě pomocí Identity Service Engine a v návaznosti na nově zavedené postupu došlo vzdělávání interních zaměstnanců organizace.

- Soustřeďte se na hodnotu – vše, co poskytovatel služeb potřebuje mapovat, přímo nebo nepřímo, na hodnotu pro zákazníka nebo organizaci. Toto je jeden z nejzákladnějších zásad ITIL a ITSM. Je to zákazník, kdo určuje, co pro něj má hodnot, nikoliv poskytovatel služby. Kontinuální zlepšování musí být zaměřeno na vylepšení, které povedou k větší přínosu pro zákazníka. [6]

- Navrhujte pro zkušenost – je důležité zachovat důraz nejen na obchodní/zákaznickou hodnotu, ale i na to, jakou zkušenost mají zákazníci a uživatelé při interakci se službami nebo poskytovateli služeb. Toto je často nazýváno "uživatelským zážitkem" a musí být aktivně řízen. [6]

- Začněte tam, kde jste – Odolejte pokušení začít od začátku a stavět něco nového, aniž byste zvážili, co je již k dispozici a lze použití. Na základě vize budoucnosti a na tom, jakou to přinese hodnotu zákazníkovi, je pravděpodobné, že v současný službách, procesech, programech, projektech, lidech apod. je mnoho z toho co lze použít k vytvoření budoucnosti. [6]

- Pracujte holisticky – Žádná služba nebo její součást nestojí samostatně. Výsledky poskytnuté organizaci nebo zákazníkovi budou nedostatečné, pokud poskytovatel služeb bude pracovat jen na části, a ne na celku. Výsledky jsou dodávány zákazníkovi prostřednictvím efektivního řízení komplexní integrace hardwaru, softwaru, dat, procesů, architektur, metrik, nástrojů, lidí a partnerů, které jsou všechny koordinovány tak, aby poskytovaly definovanou hodnotu. [6]

- Postupujte iterativně – Dokonce i obrovské iniciativy je třeba provést iterativně. Odolejte pokušení udělat vše najednou. Uspořádáním práce do menších, zvládnutelných sekcí, které mohou být provedeny a dokončeny včas, zaměřením na menší sekci je zlepšení lepší a snadnější na udržování. Zlepšení iterace může být sekvenční nebo simultánní, na základě na závislostí nebo jejich nedostatku. Klíčem je, aby každé individuální zlepšení bylo zvládnutelné a řízené, tak aby bylo zajištěno, že skutečné výsledky se časem vrátí v podobě dalších vylepšení. [6]

- Pozorujte přímo – Chcete-li vědět, co se skutečně děje, měřte/pozorujte to přímo. Nezapomeňte založit rozhodnutí na informacích, které jsou tak přesné, jak je to jen možné. Jít ke zdroji umožňuje snížit použití předpokladů, které pokud se ukázaly jako neopodstatněné, mohou být katastrofální, pro časové plány, rozpočty a kvalitu výsledku. [6]

- Buďte transparentní – Čím víc se lidé zajímají o to, co a proč se děje, tím víc lidé pomáhají, a méně se brání. Udělat věci tak transparentní, jak je to jen možné. [6]

- Spolupracujte – pokud jsou správní lidé zapojeni správným způsobem, tak z zlepšování benefitují a to protože jsou k dispozici. [6]

- Udržujte jednoduchost– Pokud proces, služba, akce, metrika apod. Neposkytuje žádnou hodnotu/produkt nebo žádný užitečný výsledek, pak jej odstraňte.
  V procesu nebo postupu použijte minimální počet kroků potřebných k dosažení cílů. Přestože se tato zásada může zdát zřejmá, je často ignorována, což vede k příliš složitým pracovním metodám, které zřídka maximalizují výsledek nebo minimalizují náklady. [6]

4 Vlastní práce

Autor práce působí v IT oddělení výzkumné instituce na pozici systémového inženýra. V rámci instituce se zabývá správou a rozvojem infrastruktury. Pro rozvoj testuje nové technologie v oblastech, které mají potenciál k rozšíření nových služeb vědeckým pracovníkům.

Instituce je společným projektem dvou fakult veřejné vysoké školy a dalších veřejných výzkumných institucí. K prvnímu kvartálu 2019 působí v instituci přes 440 vědců a studentů. Téměř třetina z nich pochází ze zahraničí. Jejich společným cílem je detailní poznání organismů na molekulární úrovni, které bude inspirací pro aplikovaný výzkum, vývoj nových léků a léčebných postupů.

Počet zahraničních zaměstnanců a návštěvníků organizace v kombinaci s otevřenou bezdrátovou sítí neumožňoval poskytování zabezpečeného přístupu k sdíleným službám poskytovaným v rámci centra. Na základě výstupu z helpdeskového systému, kde byly zadávaným požadavky na zpřístupňování sdílených služeb na stávající otevřené sítí pro cizince nebo návštěvníky centra bylo zapotřebí projektově implementovat způsob hostovského přístupu.

4.1 Projekt „bezdrátová síť pro přístup hostů“:

Hlavním cílem bylo umožnit bezpečné připojení hostů a na základě identity jim případě nabízet možnost využít BYOD. Projekt byl realizován v průběhu roku 2018 a nyní je úspěšně ukončen.

- Očekávaný rozpočet projektu a jeho finanční vyhodnocení
    1. Investiční

    Investiční náklady jsou vyčísleny v: globální ceníkové ceně v USD, bez slev z rozsahu zakázky, daně z přidané hodnoty a individuální slevy vyjednané zákazníkem např. z důvodu dlouhodobé spolupráce s dodavatelem.

Katalogové číslo	Popis	Podpora v měsících	Ceníková cena	Počet ks	Cena za n ks
R-ISE-VMS-K9=	Cisco ISE Virtual Machine Small	---	6 700	1	6 700
L-ISE-BSE-PLIC	Cisco ISE Base License	---	5,7	1750	9 975
L-ISE-PLS-5Y-S1	Cisco ISE Plus License, 5Y	60	25,93	100	2 593
Celkem v USD a bez DPH					**19 268**

Tabulka 4: Investiční náklady projektu bezdrátová síť pro přístup hostů (vlastní zpracování)

Pro vyčíslení investičních nákladů byl použit průměrný kurz USD/CZK v roce 2018 dle ČNB, 1 USD = 21.735 Kč. Při použití zmíněného kurzu lze předpokládat investiční náklady ve výši 418 789,98 Kč bez DPH.

2. Provozní

Pro výpočet nákladů byla použita pozice „System Administrator“ pro kterou je typická hrubá mzda 75 000 Kč. Měsíční mzda je uváděna v českých korunách pro pozici při plném úvazku a měsíčním fondu 160 hodin. Pro výpočet provozních nákladů je kalkulováno se superhrubou mzdou 100 500 Kč. Data převzata z MZDOVÝ PRŮZKUM 2019 TRENDY NA PRACOVNÍM TRHU V ČESKÉ REPUBLICE Hays Czech Republic s.r.o.

Položka	Počet hodin	Cena za hodinu v Kč	Cena za n hodin v Kč
Analýza současného stavu	2	628,125	1 256,25
Drátový mode portálu	5	628,125	3140,625
Výběr produktu pro portál	15	628,125	9 421,875
Instalace ISE	2	628,125	1 256,25
Napojení ISE na infrastrukturu	3	628,125	1 884,375
Tvorba portálu	12	628,125	7 537,5
Nastavení ISE pro CWA	1	628,125	628,125
Nastavení síť. prvků	2	628,125	1 256,25
Řešení programátorských chyb	8	628,125	5 025
Celkem	**50**	628,125	**31 406,25**

Tabulka 5: Provozní náklady projektu bezdrátová síť pro přístup hostů (vlastní zpracování)

- Předpokládané organizační zajištění projektu

  pracovníkem IT oddělení ve spolupráci s dodavateli celého řešení, v rámci řešení projektu nebylo požadováno zvýšení úvazků dotčeného pracovníka. Předpokládaná potřeba zdrojů (lidé, technologie, informace, infrastruktura atd.)

- Očekávané dopady projektu

1. Dopady na současný stav organizace, na běžící projekty a na vše ostatní
    a. Možnost poskytovat bazální konektivitu hostům areálu a usnadnit tak hostům přístup k bezdrátové síti pomocí webového portálu.

2. Přínosy (finanční i nefinanční)
    a. Zrychlení poskytování IT služeb pomocí využití sítí pro hosty areálu a jednotlivé servisní organizace

- Možné negativní dopady projektu

Zvýšení závislosti na jednom výrobci infrastruktury

- Časový harmonogram

Předpokládáme kompletní realizaci v průběhu 6 měsíců:

1. příprava výběrového řízení – 1 měsíce
2. realizace výběrového řízení – 3 měsíce
3. zkušební provoz a akceptace – 2 měsíce

- Hlavní rizika projektu nebo jiná omezení
    1. Vznik technologického dluhu
    2. Nutnost zvýšení kvalifikace IT personálu v oblasti Hostovských portálů a automatizace

4.2 Analýza současného stavu technologie v organizaci

Síťové technologie nasazené v organizaci lze zhodnotit jak z pohledu roku 2013 tak na základě zkušeností po více než 5 letech provozu.

V letech 2013/2014 společnost Cisco uvedla do prodeje novou generaci prvků, založených na inovativním čipu UADP 1.1. Tento čip nazývaný též jako čip, jenž přináší inteligenci do přepínačů pro připojený Svět na základě jednoho operačního systému pro drátová i bezdrátová zařízení.

Tato specifická technologie umožnila rychlý rozvoj a nasazení v nově vybudovaném kampusu. V rámci nasazení byl využit produkt, jenž zjednodušuje správu drátových a bezdrátových zařízení v síti, a to Prime Infrastructure. Díky konfiguračním šablonám pro síťová zařízení, možnosti řízení rádiového spektra přístupových bodů v celém kampusu a dalším funkcím následné správy a řešení problémů byl nově vystavěný kampus v roce 2015 uveden do provozu s progresivními technologiemi, které umožnili poskytovat nové služby pro vědecké pracovníky, které na jiných technologií nebylo možné využívat.

	3650	3850	4K / Sup8-E	CT5760
	Podporováno/ Doporučeno	Podporováno/ Doporučeno	Podporováno/ Doporučeno	Podporováno/ Doporučeno
Mobility Kontrolér mód	ano	ano	ano	ano
Počet podporovaných AP	25	50	50	1000 / 600
Počet podporovaných klientů	1000	2000	2000	12000 / 7000
Počet MC v mobility doméně	8 / 2	8 / 2	8 / 2	72 / 2
Počet MA v sub doméně	16 / 8	16 / 8	16 / 8	350 / 32
Počet AP per doménu	250 / 50	250 / 100	250 / 100	7200 / 1200

Tabulka 6: Škálovatelnost technologie (vlastní zpracování)

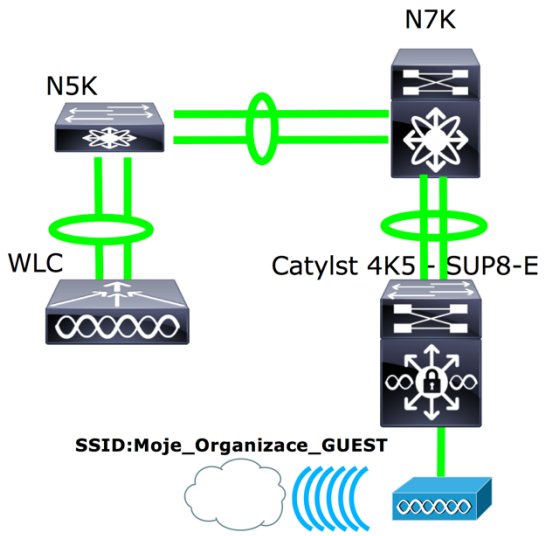
Po nasazení v těchto prostředích se objevily problémy s roamingem klientů. Ti si v rámci roamingu mezi jednotlivými MA vytvořili své datové CAPWAP tunely na přepínači, kde proběhla jejich první asociace do bezdrátové sítě – Point of Atachement (PoA), které je při prvotní asociaci stejné jako Point of Presence (PoP). Při následné migraci klienta mezi AP na různých přepínačích dojde ke změně PoP, ale nezmění se PoA. Klient naváže PoP u přepínače, na který provedl roaming a následně se tvoří CAPWAP tunel na původní MA, kde dojde k terminaci datového provozu klienta.

Problematiku lze názorně ilustrovat na posluchárně vysoké školy, kdy pro konci přednášky proběhne roaming několika stovek studentů. Z technického pohledu pak mají studenti PoA

na přepínači, jenž skrze svá AP obsluhuje posluchárnu, ale studenti pokračují dále po budově a díky kvalitnímu pokrytí bezdrátovým signálem nedojde k re-asociaci klienta, ale pouze ke změně PoP. Datový provoz klientů je tedy skrze CAPWAP tunely terminován na přepínači prvotní asociace a tím dochází k výraznému zatížení páteřních spojů mezi bezdrátovými řadiči.

4.2.1 Řešení hostovského přístupu

Hostovský přístup je realizován pomocí otevřené bezdrátové sítě. Na základě požadavků zadávaných do interního helpdeskového systému byla zpracována analýza potřeby změny řešení hostovského přístupu. Výsledkem byl požadavek na změnu řešení přístupu se zaměření na identifikaci koncového uživatele a vyžadováním jeho souhlasu s UAP organizace.



Obrázek 8: Logická topologie sítě před nasazením ISE (vlastní zpracování)

Organizace využívá tradiční hierarchický model sítě, tedy Jádro (Core), Distribuční vrstva (Distribtion) a přístupová vrstva (Access). Architektura je postavena na jednom výrobci, a to konkrétně Cisco Systems. Kde jednotlivé vrstvy jsou řešeny následovně: Core vrstva je řešena dvojící přepínačů řady Nexus 7000 na kterou je přímo napojena přístupová vrstva

tvořena přepínači řady Catalyst 4500 osazenými dvojící Supervisoru 8 v redundantním módu SSO. Distribuční vrstva slouží k připojení dvojice bezdrátových řadičů 5760 v redundantním režimu Statefull Switchover (SSO), dále pak k připojení jednotlivých prvků data centra.

4.3 Nasazení ISE

V této kapitole bude popsán postup, jehož cílem je postup zavedení hostovského portálu pomocí ISE v prostředí Converged Access. Bude provedena Instalace virtuální serveru pro ISE, nastavení produktu ISE, konfigurace síťových prvků a jejich následné napojení na ISE. Samotný produkt bude zaveden do KVM klastru proběhne nastavení požadované funkcionality. Bude vytvořen hostovský portál a kustomizován tak, aby odpovídal jednotné grafické identitě organizace. Zavádění produktu bude probíhat nejprve formou ostrovního systému. Daná bezdrátová síť bude nejprve přístupná pouze v prostorech IT oddělení, kde proběhne otestování všech požadovaných funkcionalit. Po ověření funkčnosti a chování služby budou rozšířeny potřebná nastavení na ostatní přepínače v roli MA v sítí, to pomocí funkce konfigurační šablony, která je součástí funkcí Prime Infrastructure.

4.3.1 Instalace do virtuálního prostředí

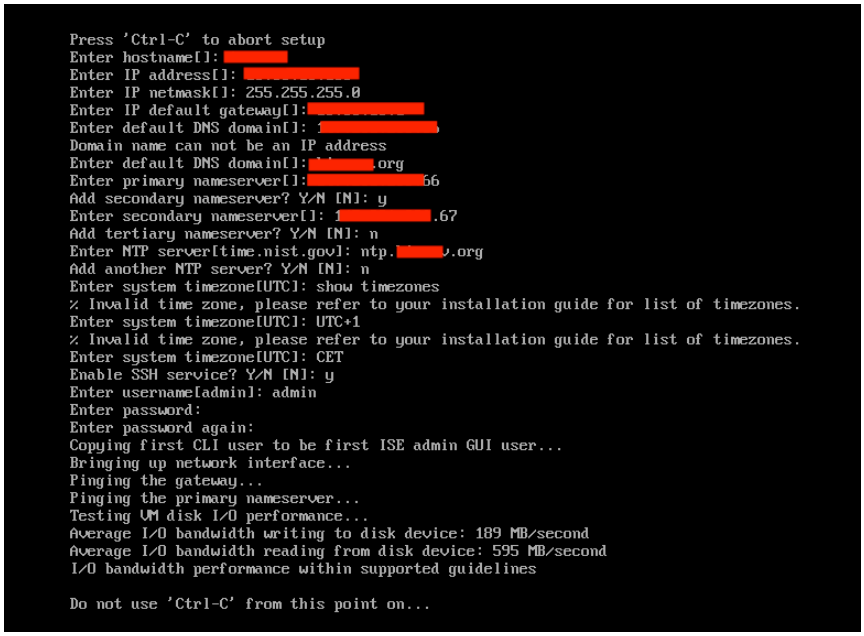
Prvním krokem je vytvoření nové instance virtuálního stroje ve webovém rozhraní vitalizačního prostředí. Při vytváření nového virtuální stroje vytvoříme daný stroj dle vlastních parametrů. Při prvním zpuštění je využita vestavěná konzole virt-manageru.

4.3.2 Instalace ADE-OS

Instalace byla provedena připojením ISO obrazu do virtuální mechaniky. Při prvním spuštěním proběhne boot z ISO obrazu. Výrobce také nabízí řešení produktu ve formě samostatného fyzického serveru a instalačních souborů pro VMWare ESX/ESXi 5.x/6.0 /KVM/Hyper-V.

4.3.3 Základní nastavení CLI

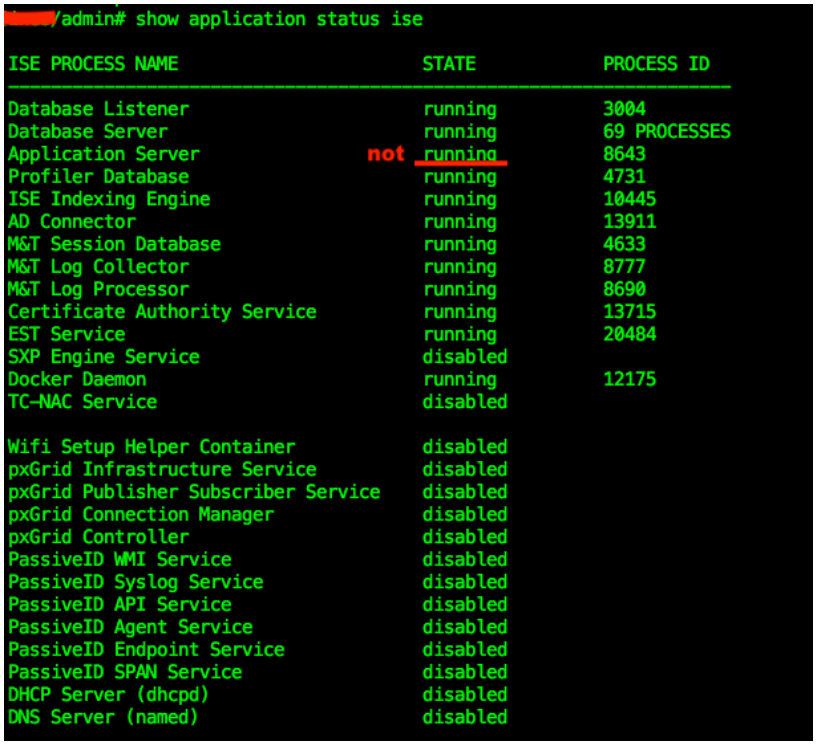
Základním nastavení CLI je nastaveno pomocí instalačního procesu. Nastavení lze dále upravovat po dokončení instalace pomocí příkazů v privilegovaném módu.



Obrázek 9: Průběh instalace serveru (vlastní zpracování)

4.4 Základní nastavení pro webového rozhraní

Po dokončení instalace dojde k restartování ADE-OS. Po restartování není webové rozhraní dostupné okamžitě, ale se zpožděním několika minut, rychlost zpuštění je ovlivněna přiřazenými systémovými prostředky. V ojedinělých případech se serveru nepodaří nastartovat aplikační server a je proto nutné se přihlásit pomocí SSH do CLI rozraní.



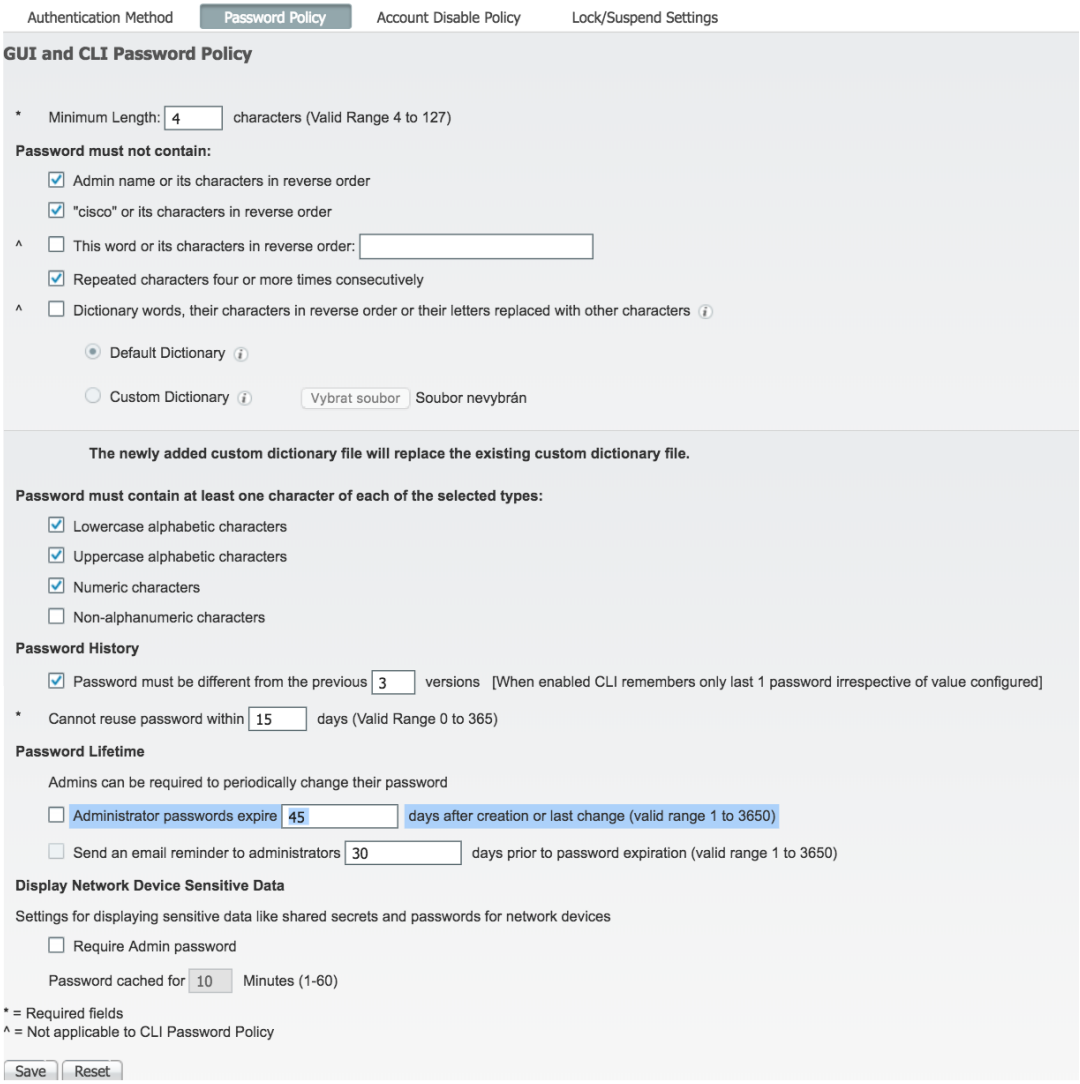
Obrázek 10: Výpis stavu procesů aplikace (vlastní zpracování)

Pokud aplikační server nezmění svůj stav na running do 10 minut je řešením zastavit službu a následně ji nastartovat pomocí sady instrukcí z instalačního manuálu, v některých případech je dokonce nutný restart serveru.

Přístup do webového rozhraní je realizován zadání IP adresy, nebo doménového jména stroje (je-li mu přiřazeno) do webového prohlížeče. Přihlášení je ve very 2.3 Patch 1 omezeno na následující webové prohlížeče: Mozilla Firefox (52.x, 53.x, 54.x) nebo Microsoft Internet Explorer (10.x a 11.x) nebo Google Chrome. Pro přihlášení použijeme uživatelské jméno a heslo zadané při instalaci.

4.4.1 Správa a generování hesel

Přístup k aplikaci byl zpracován na základě vnitřního předpisu organizace, který se věnuje úrovni zabezpečení pro jednotlivé služby. Řízení přístupu do vnitřní sítě organizace je dle předpisu chápána jako kritický prvek. Pro takové prvky platí vnitřní předpis, jenž definuje minimální počty znaků, speciálních znaků, číslovek a tak dále.



Obrázek 11: Nastavení politiky hesel (vlastní zpracování)

Při nastavení byl objeven nedokumentovaný bug, který bude popsán v kapitole Nalezené dokumentované a nedokumentované programátorských chyb věnující se programátorským chybám.

Obecně by heslo mělo obsahovat: malá a velká písmena, číslice atd. Dále je třeba zmínit problematiku změny hesla, obecné doporučení je měnit heslo každých 6 měsíců. Dle americké organizace NIST je přílišný tlak na změny hesel kontraproduktivní a vede k obcházení pravidel [7]. Zvýrazněné vypršení hesla po 45 dnech po vytvoření se v tomto případě ukázala jako problematická. Díky neprovedení tohoto nastavení došlo po uplynutí 45 dní k uzamčení administrátorského přístupu do webového rozhraní.
Resetování hesla je dostupné pouze z CLI rozhraní.

Další možností zabezpečení je suspendace nebo zablokování účtu po n počtu neplatných přihlášení. Zde záleží na bezpečnostní politice a vnitřních předpisech dané organizace.

4.4.2 Uživatelé, uživatelské skupiny a externí zdroje identit

Vytváření nových uživatelů je realizování pomocí vnitřních uživatelských účtů a jejich klasifikací do skupiny. Často je přístup realizován pomocí napojení systému na externí zdroj identit jako například Microsoft Active Directory nebo open source řešení LDAP.

Obrázek 12: LDAP a jeho skupiny (vlastní zpracování)

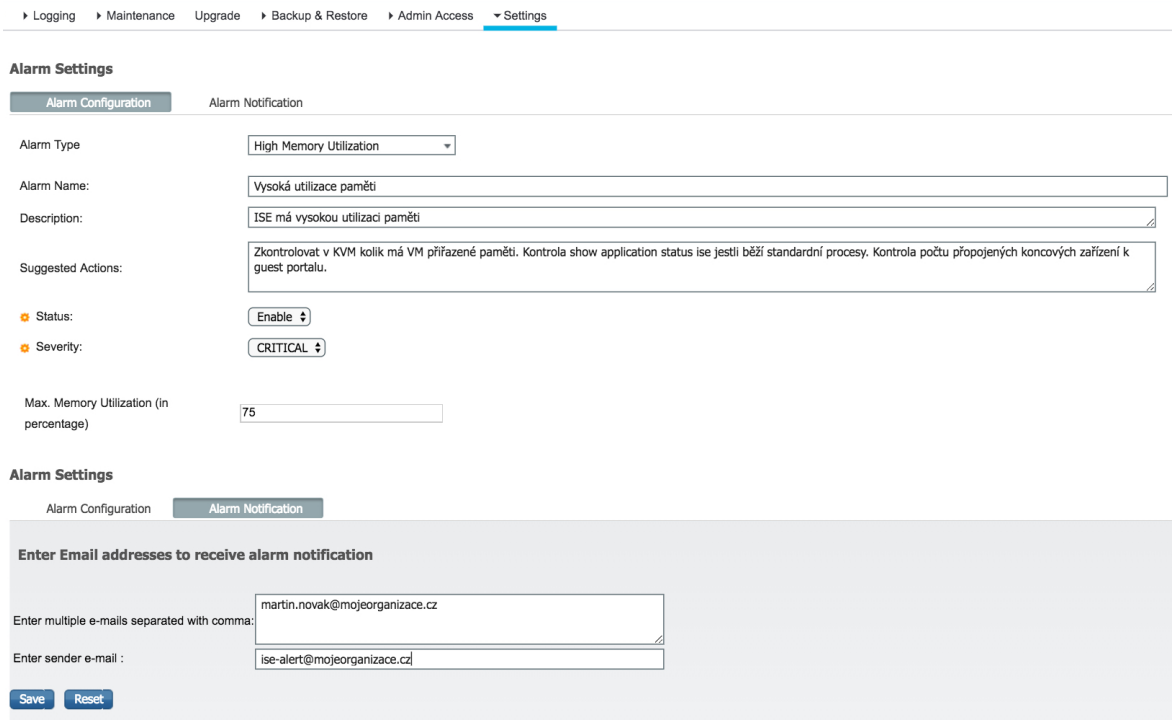
Vytváření nových uživatelů a jejich klasifikace do skupiny je pak řízena centrálně.

4.4.3 Notifikace uživatelů a správců

Odesílání notifikačních emailů je realizování pomocí SMTP serveru, kde je potřeba vydefinovat ISE a nastavit další parametry. SMTP je zkratka pro Simple Mail Transfer Protocol. Konfiguraci SMTP serveru provádí správce daného serveru a není součástí práce.

4.4.4 Alarmy a jejich využití pro správu

K monitorování systémových zdrojů a jednotlivých sužeb/procesů, které systém využívá. Nastavení je velké množství od utilizace volného místa na disku až po upozornění na vypršení platnosti licence. Následně lze vybrané alarmy zasílat pomocí služby SMTP.



Obrázek 13: Nastavení individuálního reportu (vlastní zpracování)

Na Obrázek 13 je ukázka vytvoření vlastního alarmu, jehož úkolem je monitorovat Množství utilizované paměti RAM daného virtuálního stroje. Alarm má nastavenou rozhodnou úroveň na 75 % přidělení paměti. Při dosažení této úrovně je automaticky odeslán e-mail s upozorňující na kritickou úroveň využití paměti RAM.

Globálně pak probíhá konfigurace emailů, na které jsou dané notifikace zasílány.

Při nastavování alarmů je třeba pozornost rozhodovací úrovni, kdy je notifikace zaslána.

4.4.5 Databáze stavu zařízení

Profilování a stav zařízení umožňují přiřazovat uživatelům, klientům a koncovým bodům atributy, které slouží k jejich identifikaci a k přiřazení do správné skupiny. Příkladem může být profilování zařízení jednoho výrobce na základě prvních tří oktetů MAC adresy jenž je vyhražená pro výrobce daného zařízení. Pomocí tohoto jednoznačného identifikátoru lze aplikovat více nebo méně specifické politiky, ať již zajišťující přístup k sdíleným službám sítě nebo jen k bazální konektivitě do internetu.

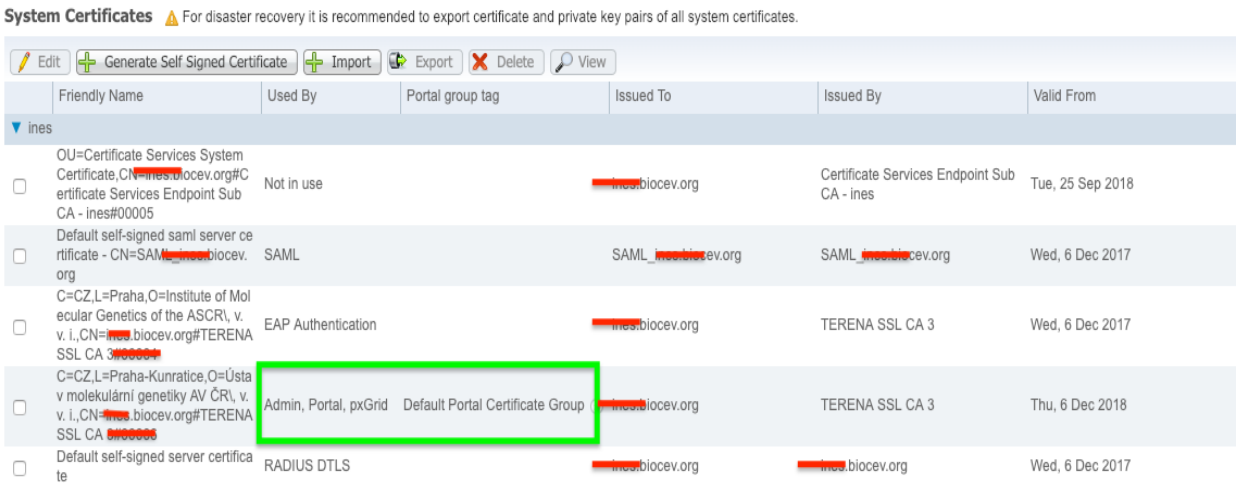
4.4.6 Certifikát a jeho instalace

Certifikáty se často v sítí objevují při implementaci zabezpečeného přístupu. Jsou používány mimo jiné pro identifikaci ISE a koncových bodů k zabezpečení komunikace mezi koncovém bodem a ISE. Certifikát je použit pro HTTPS komunikaci stejně jako pro EAP komunikaci [1, 8]

V rámci nasazení ISE má administrátor několik možností voleb použití jednoho certifikátu pro všechny identity nebo použití několika rozdílných certifikátu. Každý ISE server může používat mnoho rozdílech certifikátů.

V tomto případě je použit jeden certifikát zahrnující Admin identitu, tedy FQDN pro admin portál a druhé alternativní FQDN pro identitu pro Hostovský portál. [1, 8]

- Admin identita – ISE server se musí identifikovat vzhledech k dalším ISE serverům. Tuto identitu využívá administrátor při připojení k administrátorskému portálu ISE. [1, 8]
- Identita Hostovského portálu – Může být jeden nebo více portálů pro hostovský příštím a Centrální Webovou Autentizaci (CWA). Každý portál se musí identifikovat a chránit komunikaci od i k portálu pomocí certifikátu. [1, 8]

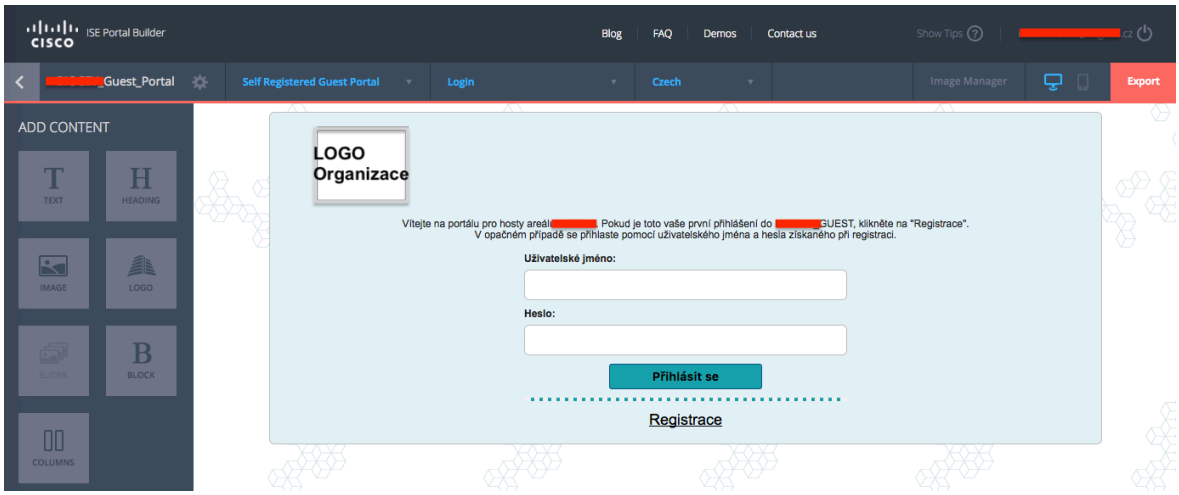


Obrázek 14: Certifikát a jeho funkce (vlastní zpracování)

Jako poslední krok po přidání certifikátu je provést restart serveru pro prvotním vytvoření portálu používající identitu hostovského portálu. Po restartu proběhne přidání portálu do skupiny základních portálů, na kterou se přidaný certifikát vztahuje, neučíme-li jinak.

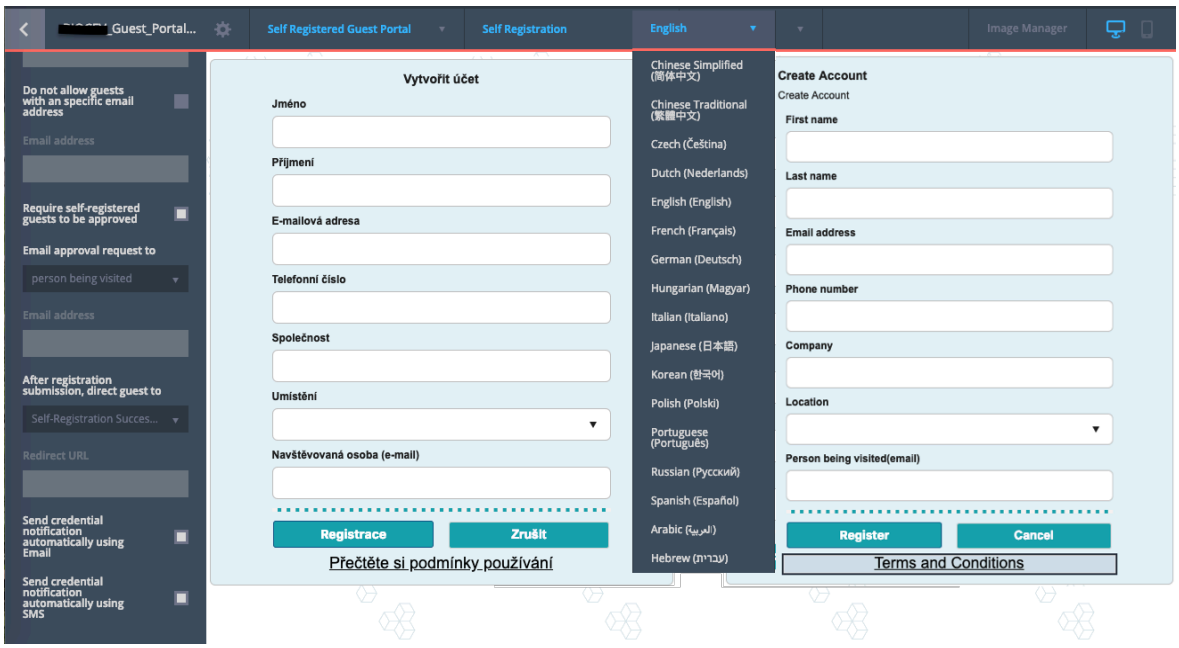
4.5 Vytvoření hostovského portálu

Vytvoření portálu je realizováno pomocí nástroje Cisco ISE Portal Builder (ISEpb) a to výběrem požadovaného typu portálu v tomto případě portálu se samoregistrací (Self-registred portal). Vytvoření portálu je dostupné na webové stránce https://isepb.cisco.com. Po přihlášení je možné nahrát obrázky dle logotypu organizace a zvolením Create New začít vytvářet vlastní portál, dle jednotné grafické indenty dané organizace. Webová aplikace nabízí předpřipravené šablony anebo tvorbu portálu pomocí vlastní šablony. Samotná aplikace pak pracuje v režimu WYSIWYG editoru, česky „co vidíš, to dostaneš“, což umožňuje vytvářet nebo upravovat celý portál a jeho součásti bez nutnosti exportu a importu do ISE.



Obrázek 15: Tvorba úvodní stránky vlastní portálu pomocí ISEpb (vlastní zpracování)

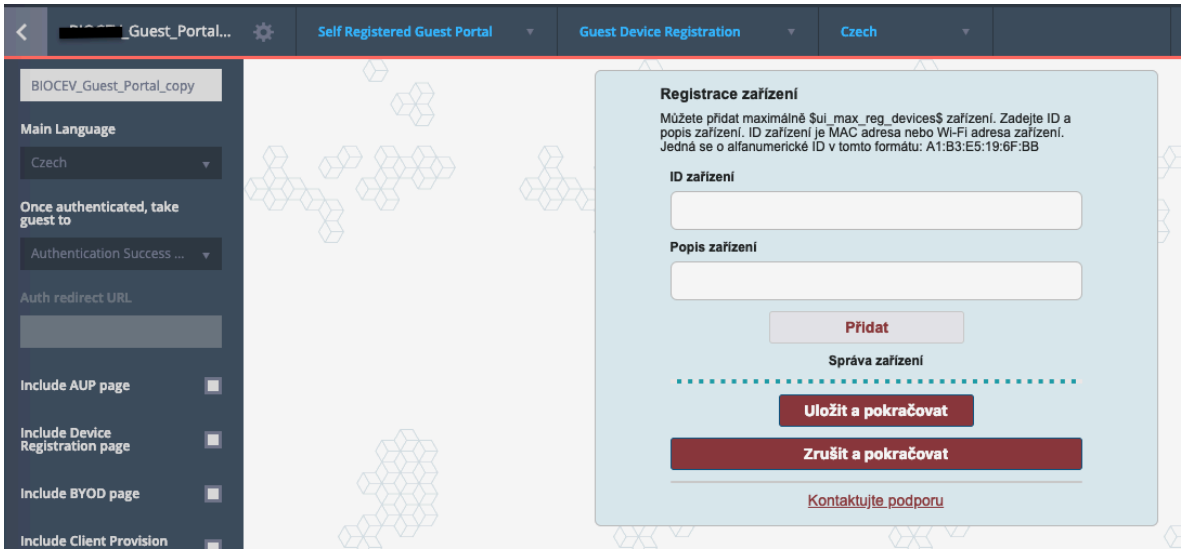
Aplikace poskytuje možnosti upravovat vzhled a podobu jednotlivých oken a podoken. Dále lze při tvorbě portálu nastavit, zda se bude jednotlivá pole jsou povinná a bez jejich vyplnění nelze pokračovat v registračním formuláři. Při nevyplnění daných polí a pokusu o pokračování v registraci je uživatel upozorněn na nutnost vyplnění. S ohledem na uživatelskou přívětivost je vhodné v textu registrace upozornit na požadavek na vyplnění požadovaných polí. Povinnost vyplnit pole se zobrazí pouze pokud je označeno a není do něj vepsána žádná informace.



Obrázek 16: Registrační formulář portálu pomocí ISEpb (vlastní zpracování)

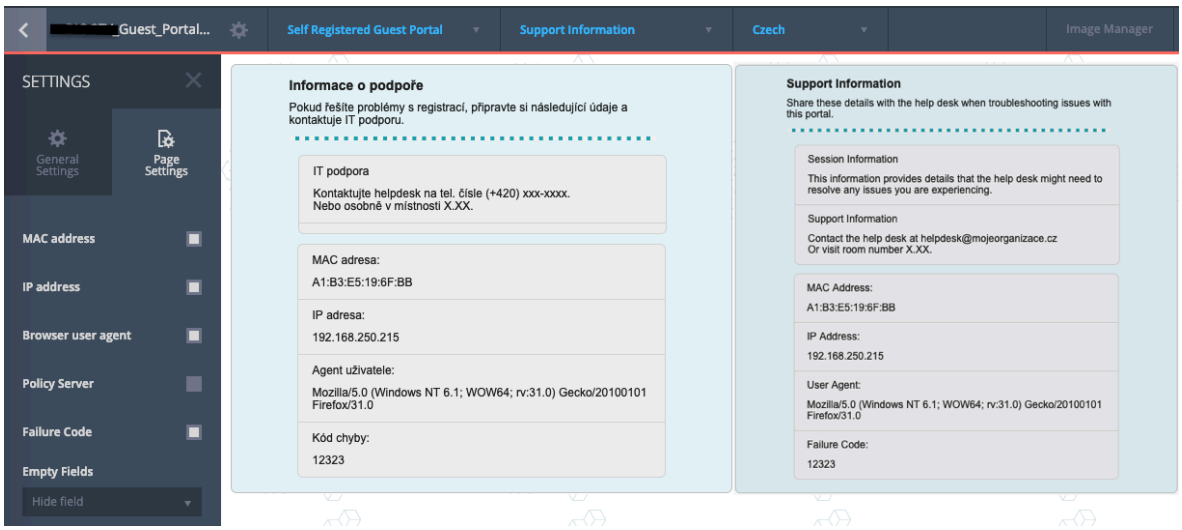
Aplikace umožňovala v 3. kvartálu 2018 vytvořit portál najednou až v 17 jazykových mutacích. Nastavením daného portálu v ISE umožňuje správce používat vybrané jazyky a využít funkce volby jazyka, který bude použit v případě, že prohlížeč hosta využívá jazyk, který není v portále podporován.

Chce-li host využívat připojení na více zařízeních současně, provede registraci zařízení pomocí MAC adresy Wi-Fi karty daného zařízení a připojí krátký popis o jaké zařízení se jedná např. notebook. Maximální počet registrovaných zařízení je určen pomocí proměnné $ui_max_reg_devices$ jejíž hodnota je importována z nastavení portálu v ISE.



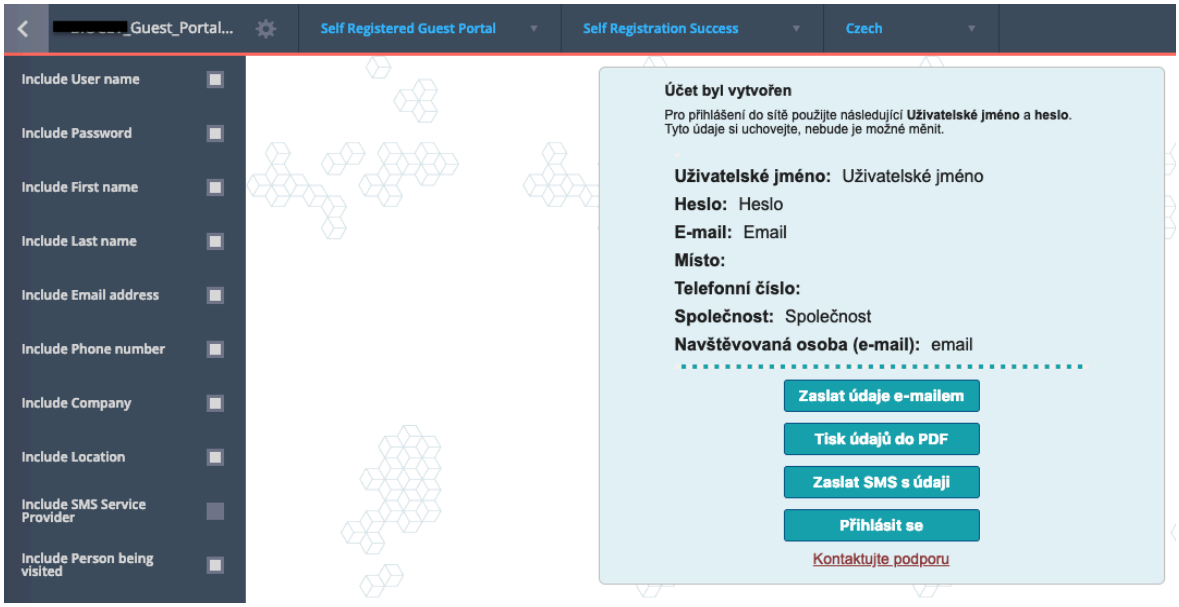
Obrázek 17:Registrace dodatečných zařízení pomocí ISEpb (vlastní zpracování)

Technologicky funkční a z uživatelského pohledu intuitivně ovládatelný portál je předpokladem pro bezproblémovou registraci ze strany hosta. Reálná prostředí přinášejí reálné situace ať již na straně klientského zařízení hosta nebo na straně infrastruktury, která zajišťuje připojení do otevřené bezdrátové sítě, přesměrování klienta na portál, jeho registraci a zaslání nebo zobrazení jeho uživatelských údajů. Pro urychlení řešení problémů s připojení a registrací byla vytvořena stránka obsahující informace, které pomohou administrátorovi při řešení problémů hostů, ať již při registraci nebo i v případě chyby na straně infrastruktury.



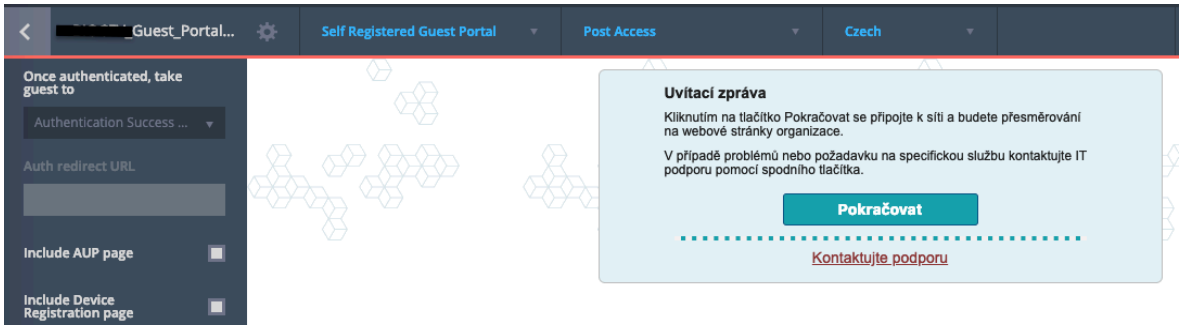
Obrázek 18: Podpůrné informace pro řešení problémů portálu pomocí ISEpb (vlastní zpracování)

Po úspěšné registraci je host přesměrován na webovou stránku obsahující informace, které zadal uživatel při registraci. Host může využít také možnost zaslání údajů pomocí e-mailu nebo SMS, podporovaný je také tisk údajů do PDF. Navštěvovaná osoba je informována pomocí e-mailu o návštěvě zmíněné osoby. Tato funkcionalita je využívaná zejména v případě pořádání konferencí, kdy pořádající tým získává informace o hostech, kteří jsou již v areálu.



Obrázek 19: Vytvoření účtu hosta portálu pomocí ISEpb (vlastní zpracování)

Po přihlášení je host informován o přesměrování na stránku organizace, která obsahuje speciálně pro hosta důležité informace jako jsou např. telefonní a e-mailové kontakty.
Dále jsou zde informaci o možnosti poskytnutí specifických služeb hostů se spolupráce IT podpory jako např. často žádaná možnost poskytnutí seminární místnosti.



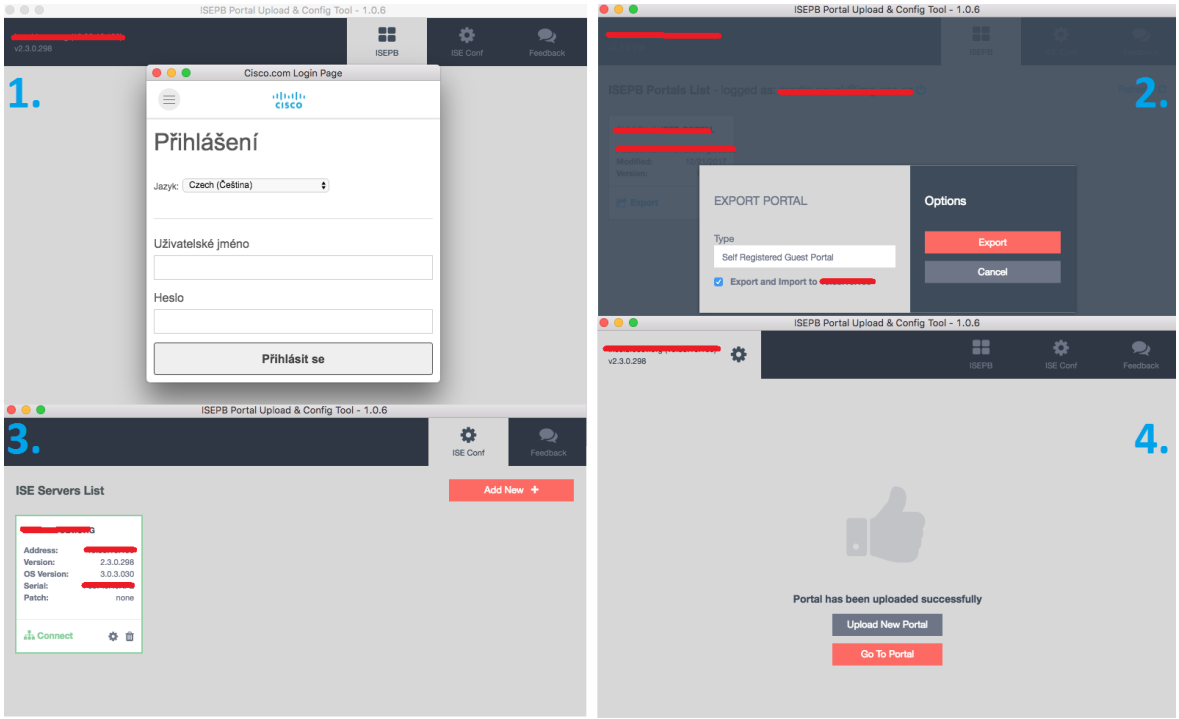
Obrázek 20: Uvítací zpráva po přihlášení do portálu pomocí ISEpb (vlastní zpracování)

Vyhodnocení bylo rozděleno na dvě úrovně, a to Výhody a Nevýhody tvorby portálu v ISE Portal Builder.

- Výhody tvorby portálu v ISE Portal Builder
  - Rozsáhlé možnosti grafických úprav
  - Vytváření portálu ve více jazykových mutacích najednou
  - Individuální grafický výsledek pro různé jazykové mutace
  - Kompatibilita portálu s starší nebo novou verzí ISE
  - Řešení problémů a individuálních úprav s ISEpb týmem

- Nevýhody tvorby portálu v ISE Portal Builder
  - Grafické úpravy pouze dle možností aplikace
  - Specifické úpravy pouze po konzultaci s ISEpb týmem

Export vytvořeného portálu a jeho import do ISE je možno provádět manuálně, a to pomocí tlačítka export v ISEpb a následném importu ve vytvořeném hostovském portálu. Nebo automaticky pomocí proprietárního nástroje ISEPB Portal Upload & Config Tool.



Obrázek 21: Import portálu pomocí ISEPB nástroje (vlastní zpracování)

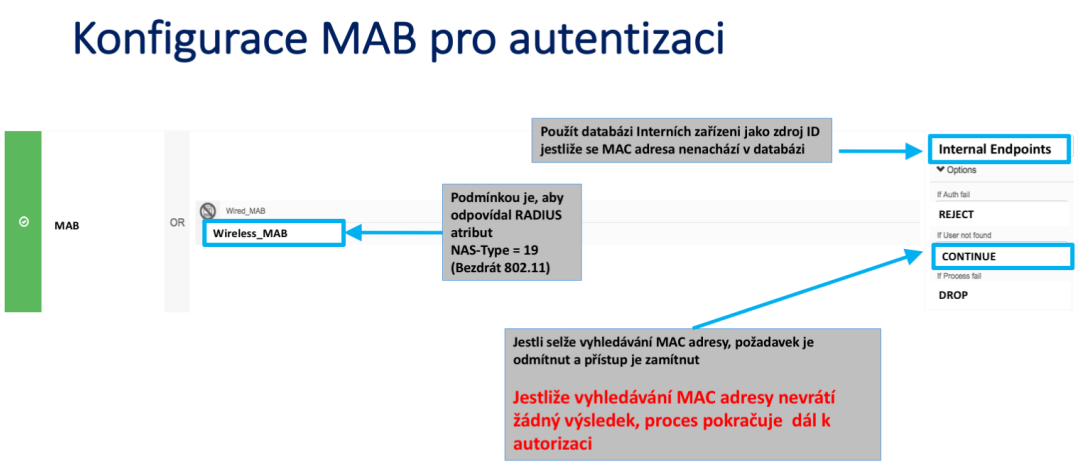
Nástroj je dostupný pro OS Microsoft Windows 7, 8, 8.1 a 10 a Mac Os X 10.13.1 High Sierra k datu 29. 1. 2018.

4.6 Nastavení ISE pro Centrální Webovou Autentizaci

Po správné konfiguraci sítových zařízení je třeba provést klíčové změny v autentizační politice.

- Konfigurace Mac Access Bypass (MAB) pro autentizaci

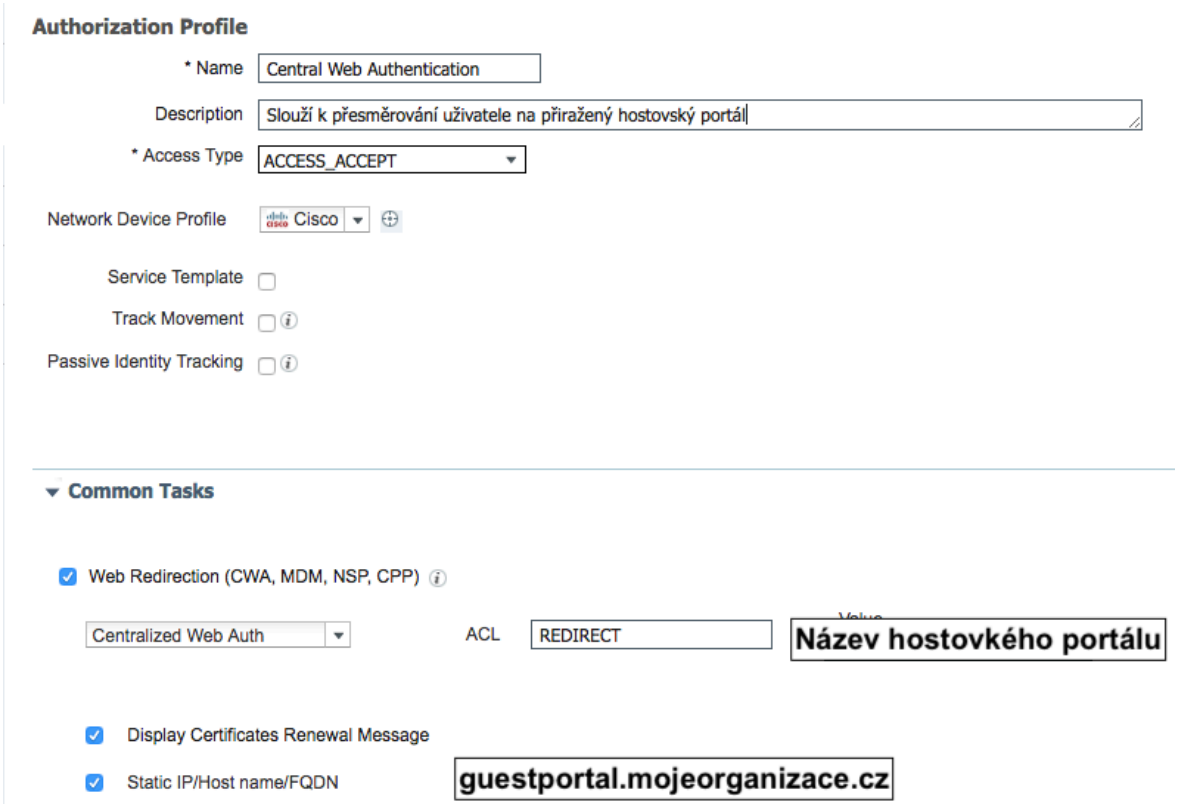
Webová autentizace je využívána pro hostovský přístup, což znamená, že koncové zařízení nebude pravděpodobně známé ISE, když se host připojí k síti. Z toho důvodu je důležité provést taková nastavení, aby proces autentizace pokračovala dále i když není MAC adresa serveru známá. [1, 9, 11, 12]



Obrázek 22: Nastavení MAB v ISE (vlastní zpracování)

- Vytvoření autorizační profilu CWA

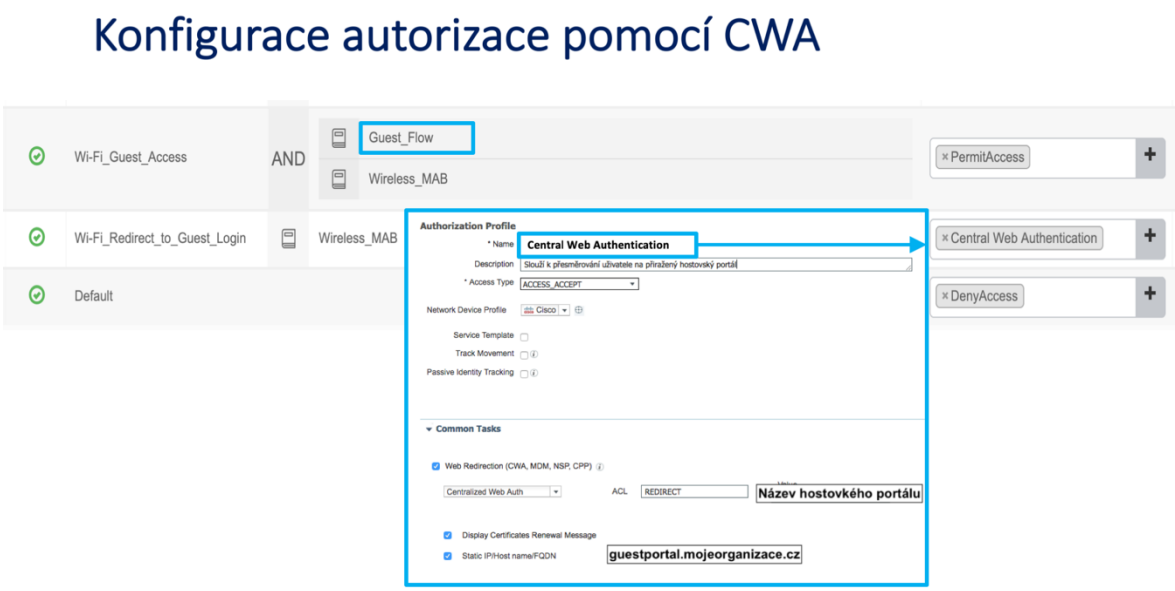
Vytvořením autorizační profilu umožníme koncovým uživatelům přístup do sítě, aplikujeme na ně URL přesměrování na hostovský portál pomocí URL přesměrujícího přístupového listu REDIRECT. [1, 9, 11, 12]



Obrázek 23: Nastavení autorizační profilu CWA (vlastní zpracování)

- Autorizace pomocí CWA

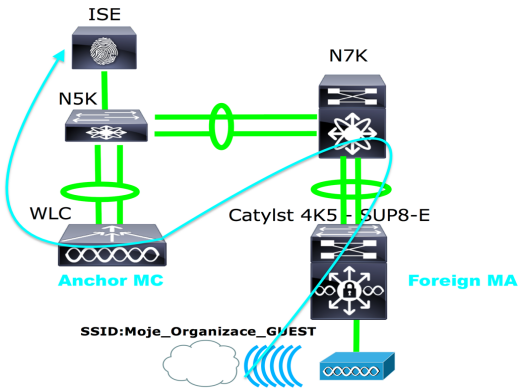
Existují tedy dvě autorizační pravidla pro přístup hostů. Pravidlo „***Wi-Fi_Redirect_to_Guest_Login***“, pomocí kterého jsou neznámé koncové body přesměrovávány na webový portál pomocí autentizační profil „***Central Web Authentication***“. Zadá-li uživatel přihlašovací údaje („Guest_Flow“) do hostovského portálu je použito pravidlo „***Wi-Fi_Guest_Access***“ pomocí kterého získá přístup do sítě („**PermitAccess**“)



Obrázek 24: Nastavení autorizačního pravidla (vlastní zpracování)

4.6.1 Řešení hostovského přístupu pomocí ISE

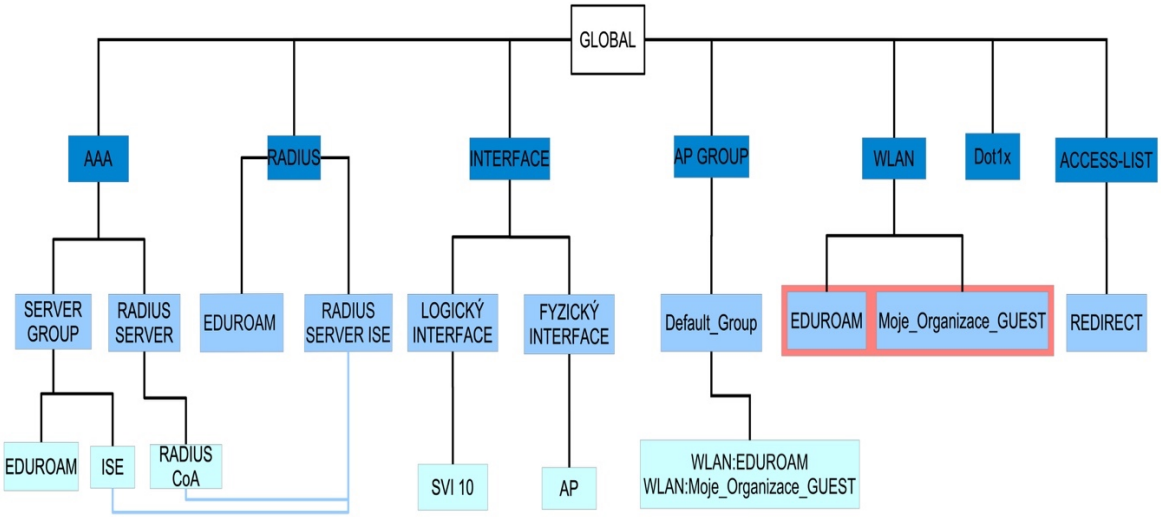
Kotvení hostů mezi WLC, který se je v módu Mobility Kontrolér a druhým WLC běžícím na SUP8-E, který je v módu Mobility Agent. Přepínač pracuje v bezdrátovém módu Mobility Agent. Z pohledu řešení bezdrátu v technologie Converged Access je připojený klient přímo kotven (Anchored) na WLC. Pro přepínač je klient Cizí (Foreign) a provádí jeho kotvení na WLC. [9, 12]



Obrázek 25: Logické topologie s ukázkou kotvení klientů (vlastní zpracování)

4.7 WLC a jeho nastavení

Nastavení zařízení je reprezentováno pomocí funkčních bloků, které se zaměřuje na grafickou prezentaci funkce operační systému přepínače ve vztahu k řešení problematice.



Obrázek 26: Grafická reprezentace nastavení přepínače (vlastní zpracování)

- GLOBAL

Autentizační metoda pro instruování přepínače, aby používal příslušnou skupinu serverů k ověření u 802.1X autentizačních požadavků (uživatelské jméno, heslo, certifikát), v tomto případě skupinu serverů pojmenovanou ISE. [3, 5, 10, 11, 13]

Pomocí autorizace definujeme, že uživatel nebo zařízení je skutečně umožněno přistoupit k sítí a jakou úroveň přístupu má skutečně povolenou. V tomto případě tedy dochází k autorizaci k autorizaci síťových služeb pomocí skupiny serverů (SERVER GROUP) ISE. [3, 5, 10, 11, 13]

Autorizace síťových služeb je realizována pomocí autorizačního listu MACFILTER, který je přiřazen na rozhraní WLAN – Moje_Organizace_GUEST, skrze skupinu serverů (SERVER GROUP) ISE. [3, 5, 10, 11]

Definice skupiny serverů (SERVER GROUP) typu RADIUS obsahující jeden server s názvem eduroam a jeden server s názvem ISE. Doba, po které po které přepínač chápe server jako nedostupný/neodpovídající je nastavena na 10 minut. [3, 5, 10, 11, 13]

- RADIUS CoA

Definice RADIUS dynamického autorizačního serveru. Následuje specifikace klienta, od kterého bude přepínač přijímá zařízení Změnu Autorizace (CoA) a žádosti o odpojení. Nastaven je též RADIUS klíč, který je sdílený mezi přepínačem a klientem (ISE) RADIUS. [3, 5, 10, 11]

- RADIUS Server ISE

Specifikace jména RADIUS serveru. Nastavení ipv4 adresy RADIUS serveru ISE a jeho parametry pro autentizaci a účtování. [3, 5, 10, 11, 13]

- Dot1x

Povolíme kontrolu přístupu přes AAA a globální přihlašování pomocí 802.1X. [3, 5, 10, 11, 13]

- ACCESS-LIST REDIRECT

Funkcí rozšířeného přístupového listu je zejména zakázat veškerého provozu odcházejícího k službám DNS a DHCP, dále pak provoz směřující na rozhraní hostovského portálu ISE. Povolený je pouze provoz na porty 80, 443 a 8443. Rozhraní hostovského portálu je provozováno na portu 8443. [5, 9, 10, 11, 12]

- SVI 10

Virtuální rozhraní Switch Virtual Interface (SVI) je využíváno pro odpověď a poslání přesměrování na webový portál klientům. V Hostovských bezdrátových sítích firewall typicky blokuje provoz mezi klienty v rámci adresního rozsahu, který je těmto klientům přidělován, proto přesměrování provozu klienta na webový portál nemusí řádně fungovat. Takové chování lze obejít pomocí povolení tohoto chování na firewallu nebo vytvořením SVI, která má staticky přiřazenou ip adresu z adresního rozsahu používaném v Hostovské síti. [12]

- WLAN

Síť je provozována jako otevřená, a tedy bez zabezpečení, kdy samotný provoz klientů je po přihlášení do sítě přesměrován na hostovský portál a není možné dále pokračovat do internetu. Bezpečnost je realizována pomocí registrace a spárováním konkrétního uživatele ke zařízením. Osobní údaje požadované při registraci jsou určeny vnitřní bezpečností politikou organizace. Provoz asociovaných hostů je transportován skrze kampusovou síť ke kotvícímu bezdrátovému řadiči (Anchor WLC). [3, 5, 9, 10, 11, 12, 13]

wlan Moje_Organizace_GUEST 1 Moje_Organizace_GUEST

- AP GROUP

Vytvoření standardní skupiny do které, se AP asociuje. Této skupině AP jsou přiřazeny dvě bezdrátové sítě, a to akademická síť eduroam a síť navázaná na hostovský portál Moje_Organizace_GUEST [3, 5, 9, 10, 11, 12, 13]

5 Výsledky a diskuse

5.1 Nalezené dokumentované a nedokumentované programátorských chyb

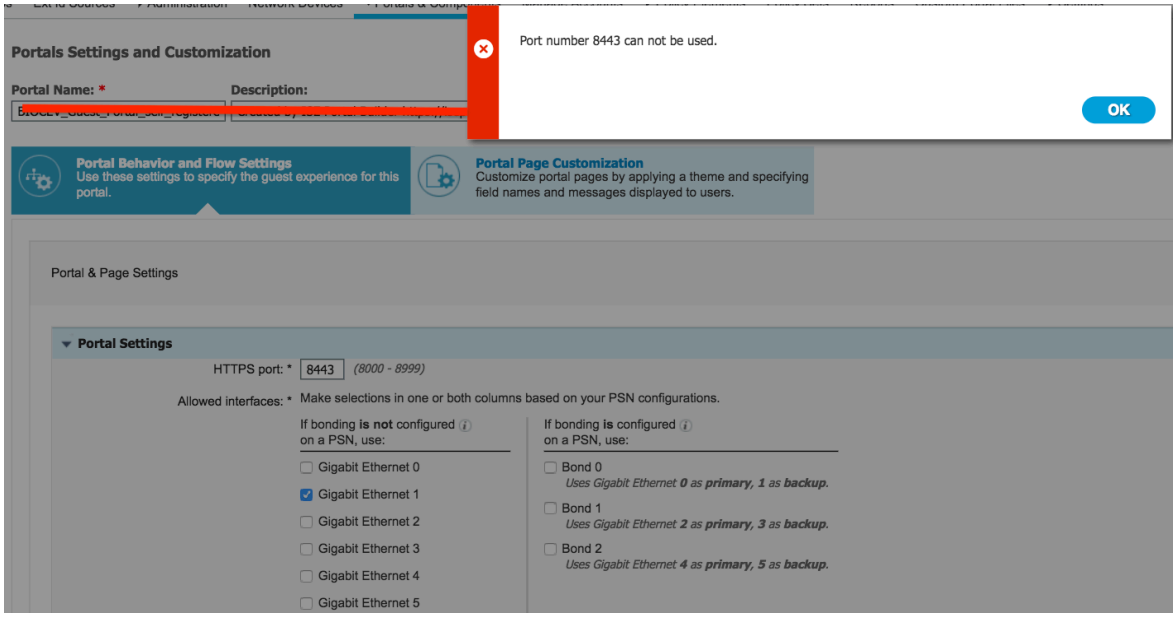
Zavádění produktu odhalilo 1 dokumentovaný, a tedy známý a 8 nedokumentovaných programátorských chyb (bug).

5.1.1 Nastavení politiky pro hesla do CLI a GUI

Chyba se projevuje při aktivaci zaškrtávacího okna v Obrázek 11 „Heslo nesmí obsahovat znaky "cisco" včetně znaků v opačném pořadí. Pokud bylo při instalaci do hesla administrátora přidány znaky ISE/ise dojde po odhlášení uživatele k uzamčení administrátorského účtu a nelze se pomocí něj přihlásit, jak do webového rozhraní, tak do CLI rozhraní pomocí SSH.
Řešením při uzamčením účtu je např. využití dalšího účtu administrátora nebo pomocí instalačního média, které při instalaci produktu nabízí resetovaného hesla administrátora.

5.1.2 Změna IP rozhraní portálu

Chyba se projevuje při změně rozhraní portálu z Gigabit Ethernet 0 na jiné rozhraní. V tomto případě na Gigabit Ethernet 1. Pokud je změna rozhraní portálu provedena v 1 kroku, tedy zakliknutí zaškrtávcího okna nového rozhraní a odkliknutí zaškrtávacího okna starého rozhraní a následné snaze uložit tuto změnu dojde k chybě zobrazené v Obrázek 27.

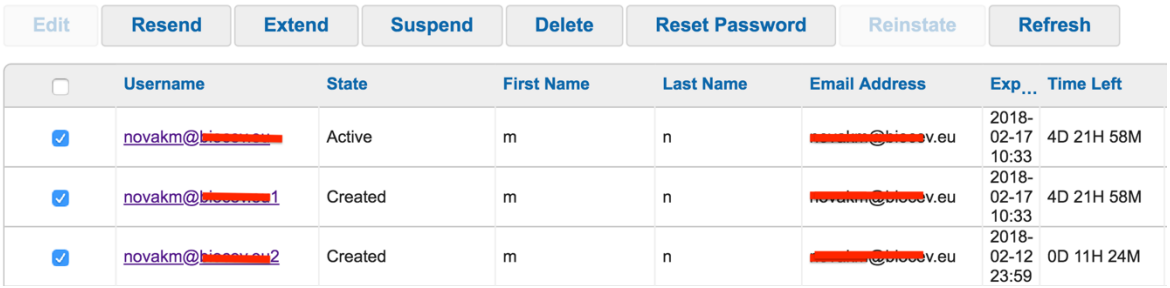


Obrázek 27: Chyba změny rozhraní portálu (vlastní zpracování)

Dočasným řešením tohoto problému do jeho odstranění je rozdělit proces na dva kroky. V prvním kroku odebrat rozhraní Gigabit Ethernet 0 a uložit změnu a následně v druhém kroku přidat rozhraní Gigabit Ethernet 1, které se portálu přiřáží dalším uložením. Chyba včetně dočasného řešení byla reportování skrze dodavatele až výrobci.

5.1.3 Vícenásobná registrace uživatele upravit obrázek

Chyba se projevuje při registraci hosta do sítě a jeho následné snaze o vícenásobnou registraci. ISE má zabránit vytvoření uživatelského účtu v případě, že e-mailová adresa je již zaregistrována. To v případě, že e-mail bude použit jako uživatelské jméno. ISE aktuálně umožňuje vytvářet a přidávat číslo na konci e-mailu, který je uživatelským jménem. Podle Cisco Bug Search Toolu je tato nefunkčnost nahlášena jako bug, a to již od veze 1.2, která byla zveřejněna v roce 2013. K 20.2.2018 byl skrze dodavatele.

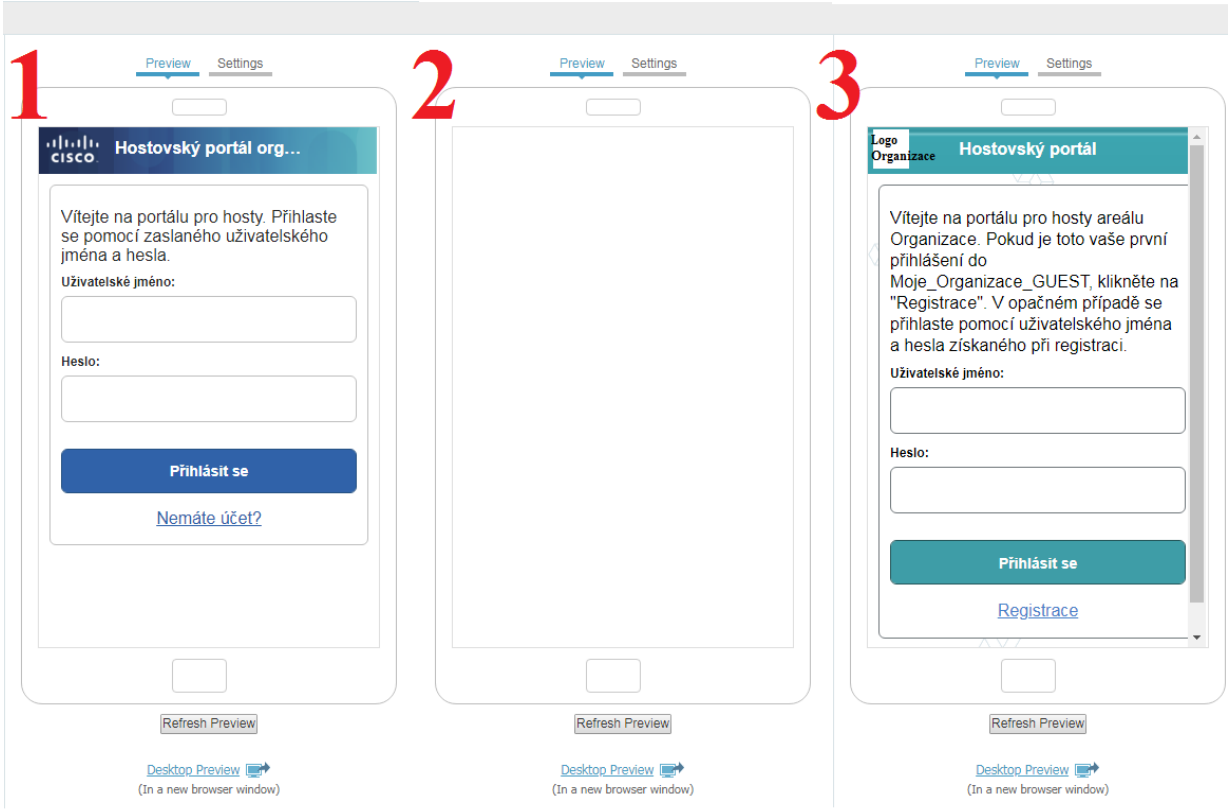


Obrázek 28: Vícenásobná registrace se stejným emailem (vlastní zpracování)

Dle vyjádření Cisco TAC týmu ze dne 21.2.2018 je tento postup standardní chování dle designu výrobce.

5.1.4 Nefunkční náhled hostovského portálu

Po importu portálu vytvořeném v ISEpb se nezobrazuje náhled a portál jde v češtině uložit pouze přes Internet Explorer 11 i přes to, že jako podporované prohlížeče uvádí výrobce: Mozilla Firefox (52.x, 53.x, 54.x) nebo Windows Internet Explorer (10.x a 10.x) nebo Google Chrome.



Obrázek 29: Náhled portálu (vlastní zpracování)

Problematiku ilustruje Obrázek 29 rozdělený do tří sekcí. První sekce zobrazuje standardní vestavěné téma portálu, druhá sekce zobrazuje vytvořené a importované téma portálu a třetí sekce obrázku zobrazuje portál vytvořený pomocí kustamizace portálu pomocí vestavěných funkcí ISE. Dle vyjádření ISEpb teamu bylo doplněno na https://isepb.cisco.com/#/blog/faq Why can't I use the small mobile preview pane in the ISE portal: dne 21.2.2018 je toto standardní projev po importu portálu z ISEpb [14]

5.1.5 Nefunkčnost napojení na externí STMP server

Nevýhodou produktu je nemožnost využít externího SMTP serveru. Dnes standardně využívaná služba externího řešení pošty např. implementací Office365 v organizace tedy neumožňuje napojit produkt na tento SMTP server. Organizace, v níž je produkt zaváděn má vlastní SMTP server. Podle Cisco Bug Search Toolu je tato nefunkčnost nahlášena jako bug, a to již od veze 1.2, která byla zveřejněna v roce 2013.

5.1.6 Import hostovského portálu

Dle vyjádření support centra výrobce ze dne 16.2.2018 je pro bezproblémový export/import portálu nutné provádět export/import pomocí nástroje ISEPB Portal Upload & Config Tool z OS Windows. Taktéž je nutné, aby Windows byly nainstalovány v českém jazyce.

Import/export pomocí nástroje ISEPB Portal Upload & Config Tool z Mac Os X nainstalovaném v českém jazyce tedy nelze doporučit.

5.1.7 Duplicitní import stejné jazykové instance

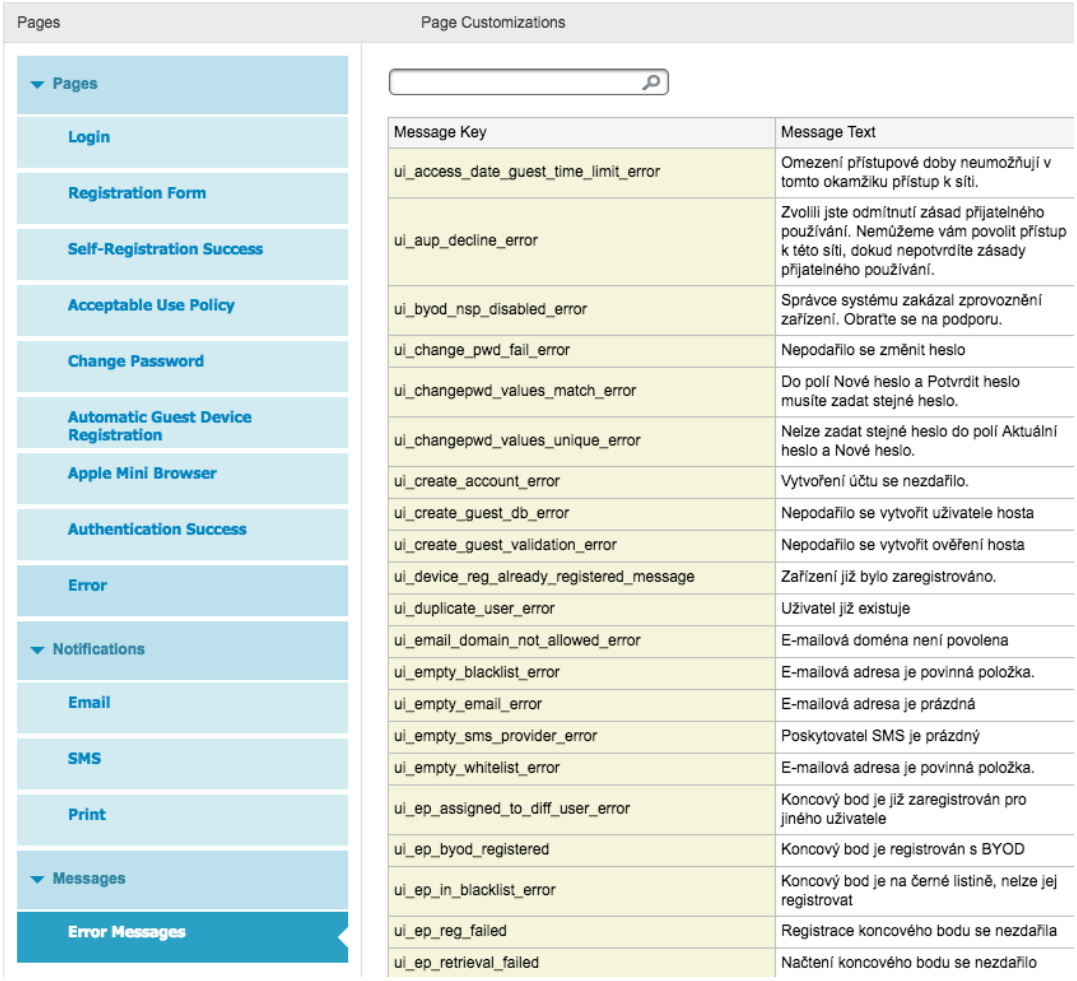
Produkt nabízí možnost exportu všech jazykových mutací portálu, úpravy původních chybových nebo informativních hlášek a zpětný import zpět do produktu. Nutnou podmínkou při individuálních úpravách je dodržení stejného názvu souboru, v tomto konkrétním případě jde o jazyk Czech. Tato informace byla na základě vyřešeného servisního incidentu doplněna do dokumentace.

13	9eb951e2-8c01-11e6-996c-525400b48521	Czech	cs,cs-cz
14	9eb9a000-8c01-11e6-996c-525400b48521	Dutch	nl,nl-nl,nl-be
15	9eb9c710-8c01-11e6-996c-525400b48521	ChineseSimplified	zh,zh-cn,zh-hk,zh-mo,zh-sg
16	aa1e4cb2-e4b7-11e7-a827-024215a6ab41	Hebrew	he
17	aa0b39e2-e4b7-11e7-a827-024215a6ab41	Arabic	ar,ar-dz,ar-bh,ar-eg,ar-iq,ar-jo,ar-kw,a
18	65677312-ef9a-11e7-a28b-525400efa2a8	Czech-[redacted]	cs,cs-cz

Obrázek 30: Chyba databáze při duplicitě jazykové mutace)

5.1.8 Nelze editovat chybové hlášky hostovského portálu

Po editaci chybové hlášky zobrazované portálem v případě předem definované chyby, nedochází k uložení této změny. Problém s editací byl reportován skrze dodavatele Cisco TAC týmu, před finálním vyjádřením ze strany TAC týmu byl tento problém odstraněn upgradem na verzi 2.4.



Obrázek 31: Chybové hlášky (vlastní zpracování)

5.2 Srovnávání očekávaného a dosaženého výsledku

Zavedením registrace a přihlašování pomocí webového portálu došlo koncovým uživatelům k snížení komfortu oproti připojení skrze otevřenou síť, to samo o sobě jde proti zásadě Navrhujte pro zkušenosti obsaženou v ITIL Practicioner. Nelze tedy jen maximalizovat „user experience“, ale je třeba brát v potaz další faktory jako je např. bezpečnost. Je důležité správně vybalancovat potřeby koncových uživatelů a bezpečnosti organice.

V rámci pořádání vědecké konferencí o několika stech účastnících ze zemí mimo EU, a tedy i bez eduroam účtu, ze svých domovských institucí se projevila problematika zmíněná v kapitole 4.2, došlo k nárůstu vytížení páteřních spojů, a to desítky procent oproti stejnému časovému úseku dne bez pořádání konference.

5.3 Návrh technologického vývoje organizace

Z důvodu ukončení možnosti zakoupit daný produkt ke 14.4.2017 a ukončení prodeje podpory ke 14.4.2018 a to na zařízení, které neměla dříve uzavřenou servisní smlouvu.

Dle předpovědi společnost Gartner bude softwarově-definované sítě využívat v roce 2020 více než 1000 rozsáhlých (kampusových) sítí. [15]

Na základě vývoje nových a kombinací již prověřených technologií společnost Cisco uvedla v 3. kvartálu roku 2017 na trh produkt Digital Network Architecture Center (DNA-C). DNA přináší softwarově-definovaný přístup k automatizaci a dohledu na službami napříč celým kampusem. DNA je založena na otevřené a rozšiřitelné platformě umožňující vytvářet sítě řízené záměrem.

Jedná se systém softwarově-definované sítě (SDN) pro kampusové sítě. Název DNA reprezentuje Digital Network Architecture, nejedná se tedy pouze o jeden produkt, ale o systémové řešení v oblasti kampusových sítí.

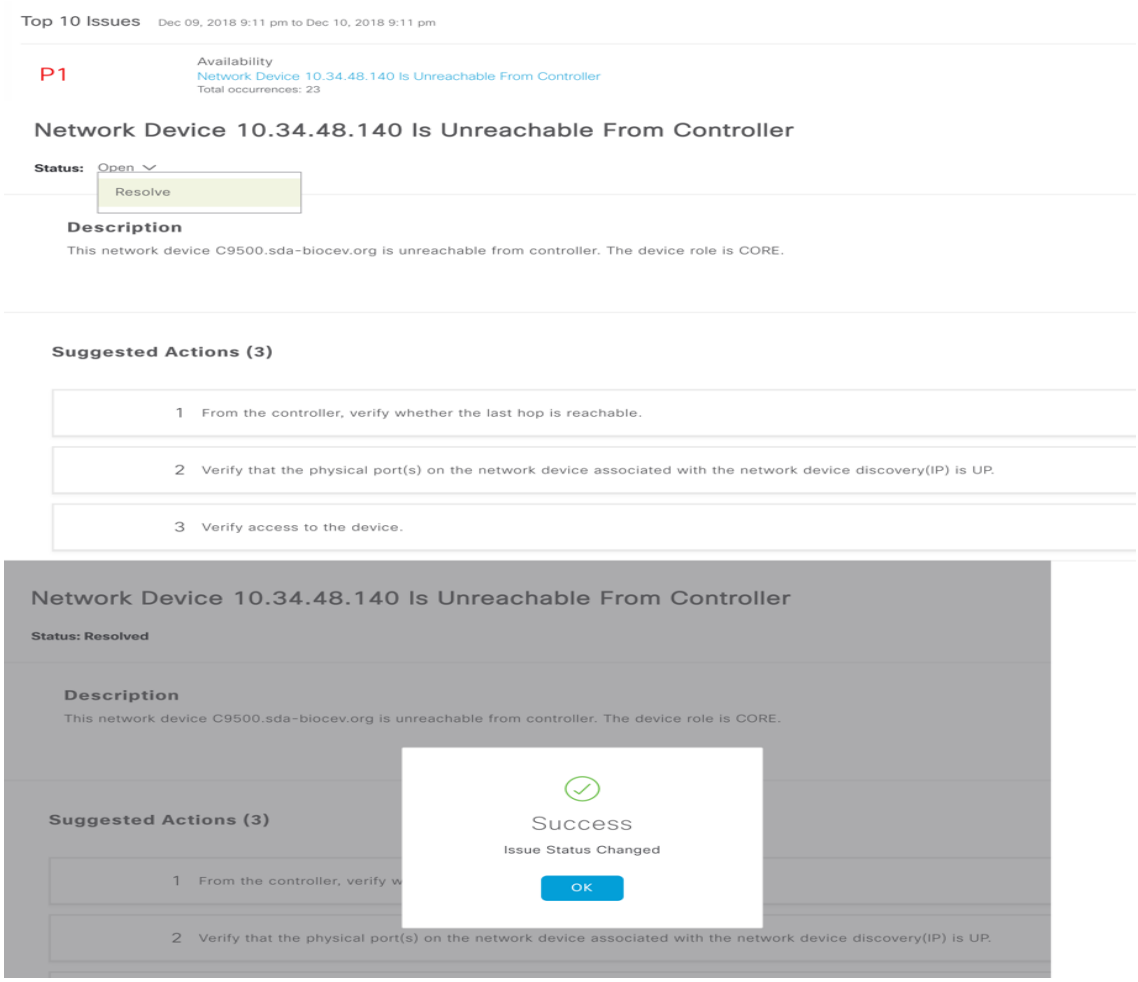
Systémové řešení Cisco DNA kombinuje nejen jednotnou drátovou a bezdrátovou síť, ale umožňuje i například oddělit sebe datový provoz konkrétních uživatelů nebo skupin uživatelů (segmentace) pomocí virtuálních sítí. Díky tomu může administrátor například oddělit datový provoz hostů využívajících připojení pomocí webového portálu od datového provozu zaměstnanců, kteří přistupují ke sdíleným službám poskytovaných v rámci organizace. Pomocí mikro segmentace lze v dané virtuální sítí řídit přístupy jednotlivých uživatelů. Vysoká mobilita uživatelů při jejich roamingu mezi přístupovými body je z pohledu koncového zařízení (smartphone, tablet atd.) realizována tak, že zařízení je stále připojeno ke stejnému logickému rozhraní, nehledě na pohyb zařízení nebo změnu fyzického umístění.

Softwarově-definovaný přístup ke správě sítě lze demonstrovat na příkladu vytvoření nové bezdrátové sítě. Kdy skrze administrátorského rozhraní orchestračního nástroje vydefinujeme parametry bezdrátové sítě jako jsou zejména služby dostupné pro uživatele dané sítě a lokalita ve které se bude nová bezdrátová síť vysílat. Jednotlivá nastavení napříč síťovou infrastrukturu pak provede orchestrační nástroj v podobě DNA Centra sám.

Administrátor tedy definuje, ČEHO chce dosáhnout, nikoliv způsob JAK toho dosáhnout. Díky této změně tak dochází zejména k významné úspoře času při implementaci ve velkých sítích a minimalizaci chyb.

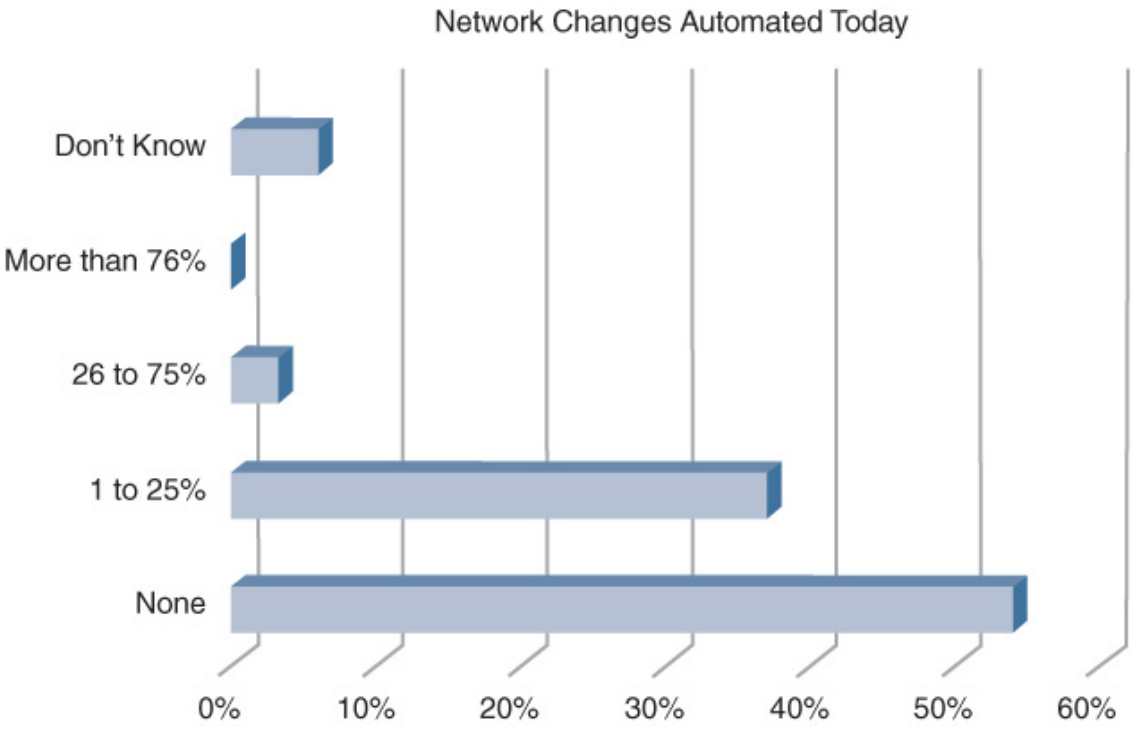
Orchestrační nástroj sám nastavuje to, ČEHO chce administrátor dosáhnou, způsob, JAKÝM je toho dosáhnuto je na DNA Centru. Pomocí automatické konfigurace je zaručeno, že jednotlivá nastavení jsou v souladu s validovaným designem výrobce. Významnou změnou v konceptu SDN je zejména zpracovávání informací získávaných ze sítě, kdy administrátor již nemusí trávit množství času na zpracováním a korelací těchto dat, aby odhalil nebo vyřešil daný problém.

V tradičnímu konceptu tyto data musí analyzovat člověk, což při v počtu tisíců událostí je velmi obtížní, nebo až zcela nemožné. Výhodou DNA Centra je zpracování, analýza a korelace těchto dat a jejich interpretace do jednotlivých incidentů.



Obrázek 32: DNA Assurance – testování proaktivní správy sítě (vlastní zpracování)

Hlavním rozdílem v sítích řízených záměrem, nebo chceme-li softwarově-definovanými sítěmi a počítačovými sítěmi, jak je známe a běžně užíváme v roce 2019 je způsob jakým přestupujeme ke správně sítě. V konceptu softwarově-definovaného přístupu je pro správce v dané organizaci důležité vědět ČEHO chce dosáhnout to, JAK je daný úkol splněn je úkolem orchestračního nástroje DNA Center.



Source: http://blogs.gartner.com/andrew-lerner/2016/12/20/network-resolutions-for-2017/

Obrázek 33: Úroveň automatizace v podnikových sítích (převzato z Gartner Network Resolutions for 2017)

V rámci přípravy návrhu technologického vývoje v organizaci se autor od února 2018 účastnil projektu Proof of Concept (PoC) softwarově-definovaných sítí. Projekt byl spuštěn v polovině 3. kvartálu 2018 a jeho hlavním cílem bylo ověřit koncept SDN v reálném kampusovém prostředí vědecké výzkumné organizace.

Bylo otestováno řešení hostovského přístupu k bezdrátové síti pomocí ISE (Identity Service Engine) a enterprise 802.1x bezdrátové sítě jako je akademická síť eduroam.
Dílčím cílem bylo ověřit reálné chování bezdrátových klientů při roamingu mezi AP, které byly zakončeny na přepínačích, umístěných v různých lokalitách, a to jak fyzických, tak logických a zároveň tak otestovat vysokou mobilitu bezdrátových uživatelů. Všechny provozované bezdrátové sítě byly provozovány v režimu Fabric-enabled Wireless.

Vyhodnocení PoC bylo rozděleno na dvě úrovně, a to Pozitivní a Negativní zkušenosti.

- Pozitivní zkušenosti:

Automatizovatelné update zařízení s nastavením času startu updatu. Reakce na „Make a Wish“ ze strany vývojářů a přidávání nových vlastností dle požadavků uživatelů.
Modul Assurance, jenž přináší nové možnosti v proaktivní správě sítě, kde upozornění na události nejsou zobrazovány jednotlivě jako je tomu v Cisco Prime Infrastructure, ale na základě analýzy dat.
Rychlost výstavby Underlay datové přenosové sítě pomocí vestavěné funkcionality LAN Automation, kdy funkční síť o rozsahu desítky přepínačů byla vybodována v řádu jednotek hodin. Vynikající podpora ze strany Cisco TAC. Intuitivní práce s fabrikou a jejími prvky. Propracované, dobře dokumentované a vylepšované rozhraní pro programování aplikací, které umožňuje vysokou míru automatizace

- Negativní zkušenost:

Nová verze DNA Centra neznamená vždy lepší, v rámci aktualizace, kdy během několika hodin po zveřejnění došlo k opravě jednoho z balíčku, který se určen pro automatizaci. V rámci testování jsme nahráli novou verzi a až po několika hodinách neúspěšného procesu LAN Automation došlo k vydání nové verze opraveného balíčku ke stažení v rozhraní DNA Centra. Nový balíček řešil chybu v procesu LAN Automatiation. Při obnově nastavení po reinstalaci DNA Centra lze používat zálohy pouze na stejnou verzi.

5.3.1 Přínos PoC softwarově-definovaných sítí

V rámci dílčího cíle byly otestovány nové možnosti na poli poskytování, monitorování a analýze služeb vědeckým pracovníkům. Na základě podkladů získaných z PoC, kde byla potvrzena vhodnost sítí řízených záměrem pro kampusové sítě a prostředí vědeckých institucí byla zahájena přípravná fáze pro projekt obnovy infrastruktury.

5.3.2 Shrnutí, důvody pro jeho existenci a cíle projektu

Cílem projektu „Intuitivní síť“ je:

- zvýšení úrovně kybernetické bezpečnosti počítačové sítě
- zvýšení flexibility při poskytování služeb počítačové sítě, možnost nabídnout zcela nové služby
- zkrácení doby obnovy funkčnosti služeb počítačové sítě prostřednictvím přechodu z převážně reaktivního modelu dohledu sítě na proaktivní
- zkvalitnění a rozšíření pokrytí Wi-Fi sítě

5.3.2.1 Očekávaný rozpočet projektu, jeho finanční vyhodnocení a dopady projektu

- Investiční

  Investiční náklady jsou vyčísleny v: globální ceníkové ceně v USD, bez slev z rozsahu zakázky, daně z přidané hodnoty a individuální slevy vyjednané zákazníkem např. z důvodu dlouhodobé spolupráce s dodavatelem.

Katalogové číslo	Popis	Podpora v měsících	Ceníková cena	Počet ks	Cena za n ks
R-ISE-VMS-K9=	Cisco ISE Virtual Machine Small	---	6 700	1	6 700
L-ISE-BSE-PLIC	Cisco ISE Base License	---	5,7	4000	22 800
L-ISE-PLS-5Y-S1	Cisco ISE Plus License, 5Y	60	25,93	1000	25 930
DN1-HW-APL	DNA Center Appliance	60	95 000	3	285 000
L-C4500E-IP-ES	Catalyst 4500E IP Base to Enterprise Services software upgrade license	---	12 000	10	120 000

C4500E-DNA-A-5Y	C4500E DNA Advantage 5 Year Term license	60	22 000	10	220 000
C9800-40-K9	Cisco Catalyst 9800-40 Wireless Controller	60	50 000	2	100 000
AIR-DNA-A-5Y	CISCO DNA for Wireless	60	900	200	180 000
C9500-24Y4C-A	Catalyst 9500 24-port 25 + 4x100G uplink, Advantage	60	30 000	2	60 000
C9500-DNA-L-A-5Y	DNA Advantage 5 Year License	60	18 000	2	36 000
Celkem v USD a bez DPH					**1 056 430**

Tabulka 7: Investiční náklady projektu Intuitivní síť (vlastní zpracování)

Pro vyčíslení investičních nákladů byl použit průměrný kurz USD/CZK v roce 2018 dle ČNB, 1 USD = 21.735 Kč. Při použití tohoto kurzu lze předpokládat investiční náklady ve výši 22 961 506,05Kč bez DPH.

- Provozní

*Pro výpočet nákladů byla použita pozice „System Administrator“ pro kterou je typická hrubá mzda 75 000 Kč. Měsíční mzda je uváděna v českých korunách pro pozici při plném úvazku a měsíčním fondu 160 hodin. Pro výpočet provozních nákladů je kalkulováno se superhrubou mzdou 100 500 Kč.

** Pro výpočet nákladů byla použita pozice „Network Security Engineer“ pro kterou je typická hrubá mzda 80 000 Kč. Měsíční mzda je uváděna v českých korunách pro pozici při plném úvazku a měsíčním fondu 160 hodin. Pro výpočet provozních nákladů je kalkulováno se superhrubou mzdou 107 200Kč.

Data převzata z MZDOVÝ PRŮZKUM 2019 TRENDY NA PRACOVNÍM TRHU V ČESKÉ REPUBLICE Hays Czech Republic s.r.o.

Položka	Počet hodin	Cena za hodinu v Kč	Cena za n hodin v Kč
Analýza současného stavu	20	628,125*	12 562,5
Analýza požadavků na politiky	25	670**	16 750
Implementace politik	40	670**	26 800
Instalace ISE	2	628,125*	1 256,25
Napojení ISE na infrastrukturu	10	628,125*	6 281,25
Instalace, nastavení a sestavení DNA clusteru	20	628,125*	12 562,5
Nastavení firewallu pro nový koncept	50	628,125*	31 406,25
Instalace a nastavení nových bezdrátových řadičů	20	628,125*	12 562,5
Ostatní nastavení	30	628,125*	18 843,75
Celkem			**139 025**

Tabulka 8: Provozní náklady projektu bezdrátová síť pro přístup hostů (vlastní zpracování)

5.3.2.2 Dopady na současný stav organizace, na běžící projekty a vůbec na vše ostatní

- Vyšší efektivita a úspora času pomocí využít nových technologií – např. možnost využití IoT (Internet of Things) řešení při výměně výzkumných dat, ať už v rámci jedné laboratoře nebo více laboratoří v celém areálu, přičemž různá IoT řešení jsou vzájemně bezpečně izolována.

5.3.2.3 Přínosy (finanční i nefinanční)

- Zrychlení poskytování IT služeb pomocí využití automatizace, programovatelnosti a virtualizace síťové infrastruktury umožní zefektivnění a zrychlení práce odd. IT, a to umožní dosažení vyšší efektivity zaměstnanců při využívání nabízených služeb. Rozšíření pokrytí bezdrátové Wi-Fi sítě v areálu

6 Závěr

Hlavním cílem této práce bylo vytvořit webového portálu pro přístup hostů do bezdrátové sítě, a to v pomocí Identity Service Engine. Byly provedena instalace Identity Service Engine, nastavena bezpečnostní opatření a též došlo k napojení produktu na produkční infrastruktur organizace.

Hlavním cílem diplomové práce bylo vytvořit webový portál pro návštěvníky veřejné výzkumné instituce v prostředí Converged Access, hlavní cíl byl rozdělen do tří částí. V první části byla provedena instlace produktu Identity Service Engine, nastavena bezpečností opatření a produkt byl napojen na infrastrukturu organizace. Druhá část popisuje topologii sítě se zaměřením na kotvení klientů na bezdrátový řadič a nastavení zařízení. K vypracování této části bylo použito blokového schéma, kde jednotlivé bloky reprezentují nastavení přepínače. V třetí části byl popsán proces vytvoření hostovského portálu, možnosti jeho kustomizace, nastavení Identity Service Engine pro Centrální Webovou Autentizaci. Tato část byla rozdělena na nastavení pravidel pro autentizaci a autorizaci. Hlavní cíle práce se podařilo splnit i přes nalezené dokumentované a nedokumentované programátorské chyby. Chyby byly zejména kosmetického charakteru nebo nebránili dokončení projektu.

Tato práce je doplněna o nalezené nedokumentované programátorských chyby, které byly nalezeny během zavádění, testování a provozu webového portálu. K chybám dochází zejména z důvodu nedostatečně otestovaného kódu, nedostatečném propojení komponent jako v případě nástroje Portal Builder anebo chybou v databáze, jako v případě import pomocí nástroje výrobce.

Práce dále rozpracovává tři dílčí cíle. První z dílčích cílů je analýzu současného stavu technologií v organizaci, který popsal specifika a inovativnost technologie v době jejího vzniku. Druhým dílčím cílem bylo vybrat vhodného výrobce technologie pro nasazení webového portálu pro hosty, který byl zpracován s návazností možnou obnovu infrastruktury po zakončení udržitelnosti projektu. Návrh dalšího technologického vývoje organizace byl rozpracován v posledním dílčím cíli. V rámci dílčího cíle byl proveden

Proof of Concept softwarově-definované sítí, který zkoumal vhodnost nasazení nového přístupu ke správně sítě a způsobu poskytování služeb vědeckým pracovníkům a specifika jejich koncových zařízení Dílčí cíle práce se podařilo splnit a první z dílčích cílů posloužil jako podklad pro další rozvoj.

Z pohledu návštěvníka areálu jakožto uživatele je nutné mít tzv. chytré zařízení s připojení na Wi-Fi a vlastní e-mailovou adresu, kterou návštěvník použije při registraci a na ní následně obdrží kopii registračních údajů.

Pro úspěšné zvládnutí této práce bylo využito odborné publikace, dokumentace výrobce a konzultace s odborníky v zmíněné oblasti. Získané poznatky jsou popsány v kapitole Teoretická východiska. Kapitola popisuje zejména technologii Converged Access, možnosti webové autentizace klientů, samotný projekt a zásady pomocí kterých bylo dosaženo předpokládaných výsledků a cíle projektu. Podpory výrobce bylo využito v oblasti nedokumentovaných programátorských chyb a jejich následného řešení.

Vypracování této práce pro mě bylo velkým obohacením v oblasti práce s elektronickými zdroji zabývajícími se odbornou stránkou předkládané diplomové práce. Z profesního hlediska zaměstnance vědecké výzkumné instituce jsem si rozšířil obzory v oblasti problematiky zpracování osobních údajů, aplikace ITIL a ITSM při přípravě, účasti a vedení projektů

7 Seznam použitých zdrojů

[1] WOLAND, Aaron a Jamey HEARY. *Cisco ISE for BYOD and Secure Unified Access*. Second Edition. Indianapolis, Indiana 46240 USA: Cisco Press, 2017. ISBN 978-1-58714-473-8.

[2] Converged Access – Wired / Wireless System Architecture, Design, and Operation [online]. 1. USA: Cisco Systems, 2013 [cit. 2018-03-25].

[3] *Converged Access Deployment Guide* [online]. 2016. USA: Cisco Systems, 2016 [cit. 2018-05-18]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-1/converged_access_deployement_guide/m_conAccess_deploy_guide.html

[4] *3850(MA) with 5760(MC)* [online]. 2014 [cit. 2018-03-25]. Dostupné z: https://mrncciew.com/2013/12/14/3850ma-with-5760mc

[5] WOLAND a Kevin REDMON. *CCNP Security SISAS 300-208 Official Cert Guide*. Indianapolis, Indiana, USA: Cisco Press, 2015, 928 s. ISBN 978-1-58714-426-4.

[6] *ITIL Practitioner Guidance*. London, United Kingdom: AXELOS, 2016. ISBN 9780113314874.

[7] Nový standard pro přihlašování: nenuťte uživatele měnit hesla. *Root* [online]. 2017 [cit. 2018-03-25]. Dostupné z: https://www.root.cz/clanky/novy-standard-pro-prihlasovani-nenutte-uzivatele-menit-hesla/

[8] Cisco ISE and Certificates: How to Implement Cisco ISE and Server Side Certificates. USA: Cisco Systems, 2012.

[9] *Central Web Authentication on Converged Access and Unified Access WLCs Configuration Example* [online]. In: . USA: Cisco Systems, 2017 [cit. 2018-03-25]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/wireless/5700-series-wireless-lan-controllers/117717-config-wlc-00.html

[10] *CCNA Wireless 200-355 Official Cert Guide*. Indianapolis, Indiana, USA: Cisco Press, 2016. ISBN 978-1-58714-457-8.

[11] WALLACE, Kevin. *CCNP Routing and Switching ROUTE 300-101 Official Cert Guide*. Indianapolis, IN 46240 USA: Cisco Press, 2015. ISBN 978-1-58720-559-0.

[12] DARCHIS, Nicolas. *Central Web Authentication with a Switch and Identity Services Engine Configuration Example* [online]. In: . 2016 [cit. 2019-01-07]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/113362-config-web-auth-ise-00.html

[13] Converged Access – Wired / Wireless System Architecture, Design, and Operation [online]. 1. USA: Cisco Systems, 2013 [cit. 2018-03-25].

[14] Why can't I use the small mobile preview pane in the ISE portal?. In: *ISE Portal Builder Blog* [online]. USA: Cisco Systems - ISEpb team, 2018 [cit. 2018-03-25]. Dostupné z: https://isepb.cisco.com/blog/faq

[15] Top 10 Technology Trends Impacting Infrastructure & Operations for 2018. Gartner [online]. Gartner, 2018, 2018, , [cit. 2019-1-02]. Dostupné z: https://www.gartner.com/smarterwithgartner/top-10-technology-trends-impacting-infrastructure-operations-for-2018/

8 Přílohy

Odkazovaný seznam příloh