FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Zadání bakalářské práce

Název:	Podpora Microsoft Windows Server pro českou federaci eduroam
Student:	Jan Čáslavský
Vedoucí:	Ing. Tomáš Čejka, Ph.D.
Studijní program:	Informatika
Obor / specializace:	Informační systémy a management
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	do konce letního semestru 2020/2021

Pokyny pro vypracování

1. Seznamte se s technickými a administrativními podmínkami zapojení organizace do federace eduroam.
2. Prozkoumejte technické možnosti platformy MS Windows Server 2019 (Windows Server) pro připojení do federace.
3. Ověřte možnosti různých typů připojení Windows Server do federace (např. umístěného za IPv4 NAT pomocí technologie IPsec dostupného na veřejné IPv4 nebo IPv6 adrese v transportním režimu).
4. Vytvořte virtuální infrastrukturu, na které vyzkoušíte i) nastavení Windows Serveru pro správu uživatelských účtů, ii) různé typy připojení do federace eduroam.
5. Rozšiřte existující dokumentaci eduroam pro nové správce o použití Windows Serveru a zaměřte se na přípravu podrobného návodu o správě účtů v ActiveDirectory, prozkoumejte možnost správy eduroam hesel.
6. Vzniklé návody ověřte v praxi u externích správců z vybraných institucí.
7. Proveďte ekonomicko-manažerské zhodnocení vašeho návrhu z hlediska nákladů a benefitů jeho realizace.

Elektronicky schválil/a Ing. David Buchtela, Ph.D. dne 12. února 2020 v Praze.

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Bakalářská práce

Podpora Microsoft Windows Server pro českou federaci eduroam

Jan Čáslavský

Katedra softwarového inženýrství
Vedoucí práce: Ing. Tomáš Čejka, Ph.D.

13. května 2021

Poděkování

Rád bych poděkoval svému vedoucímu bakalářské práce Ing. Tomáši Čejkovi, Ph.D. za to, že se ujal vedení mé práce a poskytl mi hodnotné rady. Poděkování patří Ing. Janu Tomáškovi za konzultace, podporu a čas strávený při realizaci práce. Také chci poděkovat Evě Cvrkové za pomoc při psaní práce. V poslední řadě děkuji sdružení CESNET, z. s. p. o. za poskytnutí příležitosti a příjemnou spolupráci.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 2373 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou a veškeré jejich dokumentace (dále souhrnně jen „Dílo"), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené.

V Praze dne 13. května 2021 . . . . . .

Odkaz na tuto práci

Čáslavský, Jan. *Podpora Microsoft Windows Server pro českou federaci eduroam*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2021.

Abstrakt

Práce *Podpora Microsoft Windows Server pro českou federaci eduroam* přispívá snažšímu použití platformy Windows Server jako RADIUS server v české federaci eduroam. Služba eduroam je celosvětový systém, který umožňuje uživatelům z akademických institucí připojení k Internetu především prostřednictvím Wi-Fi. Instituce připojující se do eduroam musejí provozovat vlastní RADIUS server. Cílem práce bylo provést analýzu požadavků pro připojení do eduroam a technických možností, které platforma Windows Server nabízí. Na základě analýzy byla vytvořena vituální infrastruktura, na které jsou otestována různé nastavení a připojení do eduroam. Po otestování nabytých zkušeností v praktické části práce byla rozšířena dokumentace na webu `eduroam.cz`.

Klíčová slova eduroam, Microsoft, RADIUS, IPsec, Network Policy Server, Windows Server, nastavení, analýza, CESNET

Abstract

The thesis *Support of Microsoft Windows Server in the Czech eduroam Federation* contributes to easily use platform Windows Server as a RADIUS server in the Czech eduroam federation. Service eduroam allows students,

researchers, and staff from participating institutions to obtain Internet connectivity by Wi-Fi mostly. An institution connecting to eduroam has to run its own RADIUS server. The goal of this thesis was to make an analysis of requirements for connecting an institution to eduroam and inspect the technical capabilities Windows Server offers. Base on these experiences was made a virtual infrastructure RADIUS servers. There were various types of connections and configurations tested. After testing gained experiences in the practical part of the thesis, I extended documentation on the website `eduroam.cz`.

Keywords eduroam, Microsoft, RADIUS, IPsec, Network Policy Server, Windows Server, configuration, analysis, CESNET

Obsah

Seznam obrázků

Úvod

Federace eduroam (education roaming) je akademický roamingový systém poskytující síťovou konektivitu pro své uživatele v připojených organizacích. [1] Studentům, výzkumníkům anebo zaměstnancům připojených institucí poskytuje eduroam připojení k internetu napříč všemi připojenými institucemi. eduroam je dostupný v různých místech ve více než 100 zemích světa, od studentského kampusu po kavárnu. V eduroam uživatel disponuje jedinou identitou (jeho údaje jsou uchovány v jeho domácí instituci), která jej opravňuje k přístupu ke všem participujícím sítím. Přístup je založen na zabezpečené autentizaci v domácí instituci.

Koordinaci eduroam v rámci české sítě národního výzkumu NREN[1] zajišťuje sdružení CESNET, které je současně provozovatelem této sítě v České republice.

CESNET zajišťuje technickou stránku i administrativní úkony pro připojení do české federace eduroam. Na počátku roku 2018 byla v rámci výzvy IROP[2] v oblasti základních a středních škol, zahrnuta podmínka k zajištění standardu konetivity, který má mezi svými kritérii povinné alespoň pasivní připojení do eduroam. [2]

Od vydání této výzvy počet středních ale i základních škol, které se připojovaly do eduroam, začal stoupat. [3] Střední a základní školy často využívají platformu Microsoft Windows Server, proto vznikl požadavek na zdokumentování této platformy a připravení řešení, na této platformě postavené.

Tato práce je zaměřená na prozkoumání nových možností a vytvoření dokumentace pro použití této platformy, což usnadní správcům institucí připojo-

[1] NREN (National Research and Education Network) je specializovaný poskytovatel internetového připojení a služeb, který se zaměřuje na podporu a rozvoj vzdělávacích a výzkumných komunit v rámci země.

[2] IROP (Integrovaný regionální operační program) je to jeden z operačních programů, prostřednictvím nichž se v Česku rozdělují prostředky poskytnuté z evropských fondů, konkrétně z Evropského fondu pro regionální rozvoj.

vání do eduroam a zároveň přinese nové možnosti a funkcionality pro rozšíření české federace eduroam.

V kapitole 2 se věnuji seznámení a prozkoumání možností připojení do federace eduroam. V kapitole 3 následuje podrobný popis testovací infrastruktury, kde v poslední podkapitole 3.4 porovnám výsledek práce z ekonomicko-manažerského pohledu.

Kapitola 1

Cíl práce

Cílem práce je podpořit použití platformy Microsoft Windows Server v české federaci eduroam. Výsledkem práce je vytvoření dokumentace pro účely připojování k eduroam a usnadnění práce správcům institucí, které tuto platformu používají. Tato dokumentace má za cíl ulehčit a zrychlit připojování k eduroam správcům institucí používajícím tuto platformu, ale také eliminovat část komunikace mezi správci institucí a správci federace eduroam při řešení problémů během připojování.

Na úvod je nutné v teoretické části práce prozkoumat podmínky připojení do federace eduroam, seznámit se možnostmi zapojení do eduroam, prostudovat základní pojmy a technologie používané v oboru. Dále je nutné prozkoumat možnosti platformy Microsoft Windows Server a komponent, které obsahuje.

V praktické části práce je cílem vytvoření virtuální infrastruktury postavené na platformě Microsoft Windows Server. V této infrastruktuře je cílem ověřit různé typy zapojení do federace eduroam, které simulují nejčastější situace z reality, a zároveň prozkoumat správu uživatelských účtů.

Kapitola 2

Analýza

Připojení instituce k eduroam.cz je komplexní úkon, správci instituce eduroam se musí předem seznámit s principy fungování eduroamu. Od správců se vyžaduje určitá znalost technologií používaných při připojování. Pokud organizace nedisponuje dostatečnými personálními nebo technickými zdroji, může využít pomoci implementačních firem, které mají s připojováním instituce do federace eduroam zkušenost. Připojení instituce do federace eduroam je prohlášeno za hotové, pokud připojovaná instituce splní všechny povinné náležitosti a požadavky. Prohlášení připojování instituce za hotové provádí správce federace eduroam. Požadavky na připojení lze rozdělit podle jejich povahy na administrativní a technické.

2.1 Administrativní požadavky pro připojení

Administrativní rámec české federace eduroam je zajištěn eduroam politikou. Roamingová politika upravuje chování jednotlivých členů a uživatelů eduroam.cz. Instituce připojené k síti CESNET[3] se mohou připojit bez dalších formálních administrativních úkonů. Připojení ostatních institucí je možné, pokud instituce splňuje AP[4] a AUP[5] sítě CESNET. Instituce nepřipojené do sítě CESNET, které se plánují připojit v režimu IdP+SP, musí dodat prohlášení žadatele o členství v české eduroam federaci. Instituce připojené v režimu SP se toto prohlášení netýká.

2.1.1 Režim připojení do eduroam

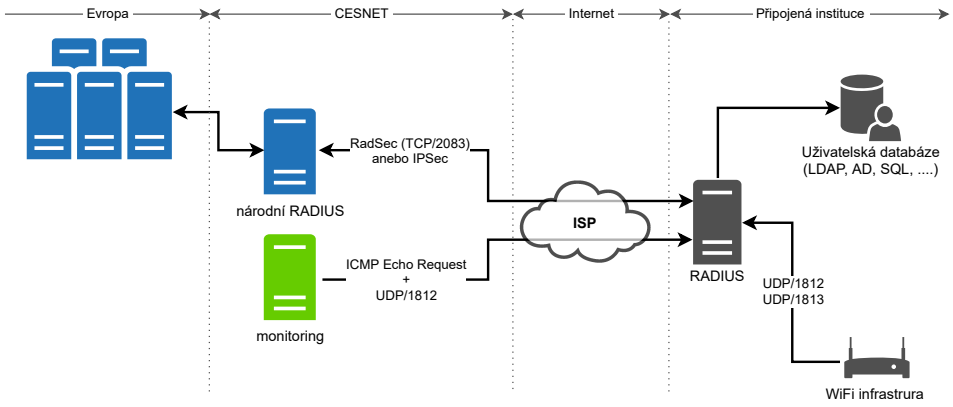
IdP+SP režim připojení znamená, že instituce poskytuje eduroam identity svým uživatelům a také poskytuje Wi-Fi konektivitu návštěvníkům. Naplňuje

[3]CESNET je vysokorychlostní počítačová síť, jejíž páteř propojuje okruhy s vysokými přenosovými rychlostmi největší univerzitní města České republiky a další oblasti.

[4]AP (Access Policy) jsou podmínky přístupu k infrastruktuře.

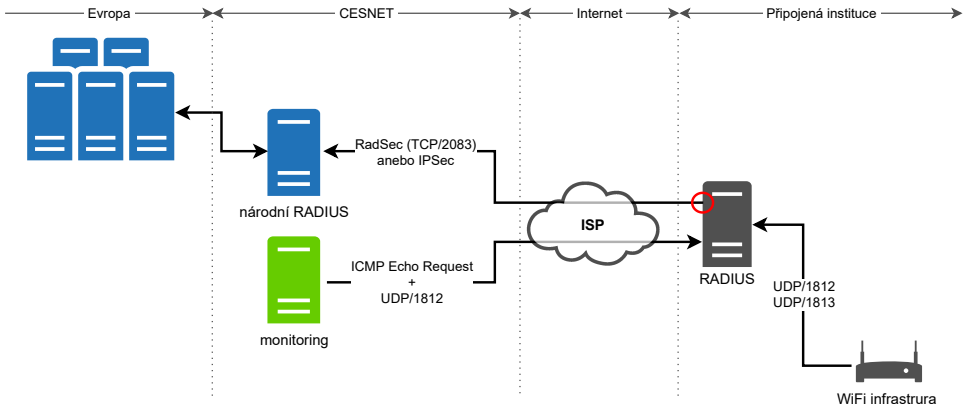
[5]AUP (Acceptable Use Policy) jsou zásady přijatelného užití infrastruktury.

tak princip reciprocity, na kterém je eduroam postaven. V terminologii podle IROP je instituce zapojena aktivním způsobem. Zapojení v režimu IdP+SP je znázorněno na obrázku 2.1.



Obrázek 2.1: Zapojení v režimu IdP+SP [4]

SP režim připojení instituce znamená, že instituce pouze poskytuje Wi-Fi konektivitu návštěvníkům. V terminologi podle IROP je takový typ zapojení nazvýván pasivní a je znáznorněn na obrázku 2.2. Tento režim zapojení má smysl pro letiště, nádraží, výstaviště, ...



Obrázek 2.2: Zapojení v režimu SP [5] Červený kroužek naznačuje jediný rozdíl u instituce zapojené v režimu SP. Národní RADIUS server neotvírá spojení směrem na RADIUS server instituce.

Úvodním krokem připojování je registrace do eduroam. Registrace se provádí v administrativní aplikaci. Tato aplikace běží na webové adrese `admin.eduroam.cz` a slouží ke správě organizačních a technických informací o instituci zapojené do eduroamu. Při registraci zástupce instituce vybere, v jakém režimu se instituce připojí, IdP+SP nebo SP. Způsob připojení může instituce

později změnit, je k tomu ale potřeba oprávnění a posouzení správce federace eduroam. Dále se v administrativní aplikaci při registraci definuje realm, RADIUS[6] server a může být jmenován další správce. V době registrace musí být doménové jméno RADIUS serveru zanesené v DNS[7]. Poslední položkou při registraci je typ protokolu připojení. Jde o typ protokolu, který se bude používat pro komunikaci mezi RADIUS serverem instituce a národním RADIUS serverem. Typ protokolu připojení si může správce samovolně později kdykoliv změnit.

Pokud se instituce připojuje v režimu IdP+SP, definuje svého testovacího uživatele. Testovacího uživatele využívá monitoring pro testování na ostatních institucích. Monitoring je zajišťován ze serveru `ermon.cesnet.cz`. Pro testování se používají testovací účty všech zapojených institucí, jedná se o testování každého s každým, tedy o end2end monitoring.

Povinností každé instituce je také vyplnit údaje o pokrytých lokalitách. Informace o pokrytí se zadávají prostřednictvím webové aplikace, která běží na `pokryti.eduroam.cz`. V první řadě jde o základní informace o instituci. Dále následuje seznam správců a v poslední řadě to jsou informace o tom, kde a v jakém rozsahu instituce eduroam vysílá. Souhrné informace o institucích zapojených do eduroamu se předávají do centrální evropské databáze. Tam slouží pro účely eduroam CAT, případné další podpůrné služby a také pro statistické účely.

eduroam CAT (Configuration Assistant Tool) je nástroj, který pomáhá uživatelům správně nastavit jejich zařízení pro připojení k eduroamu.

2.2 Technické požadavky pro připojení

Každá instituce zapojená do eduroamu má definovaný svůj realm a RADIUS server, který dokáže ověřit uživatele z této instituce. Uživatelské účty jsou vedeny v systému správy identit instituce a RADIUS k nim přistupuje pomocí standardizovaného protokolu. RADIUS servery institucí jsou v rámci dané země připojeny k národnímu RADIUS serveru (`radius1.eduroam.cz`), který zajišťuje předávání požadavků na ověřování mezi institucemi. RADIUS server pro Českou republiku zajišťuje CESNET.

Autentizace uživatele probíhá pomocí protokolu IEEE 802.1x[8] a je založena na schopnosti AP[9]. Klient se připojí na port zařízení, který je ve stavu zavřeno.

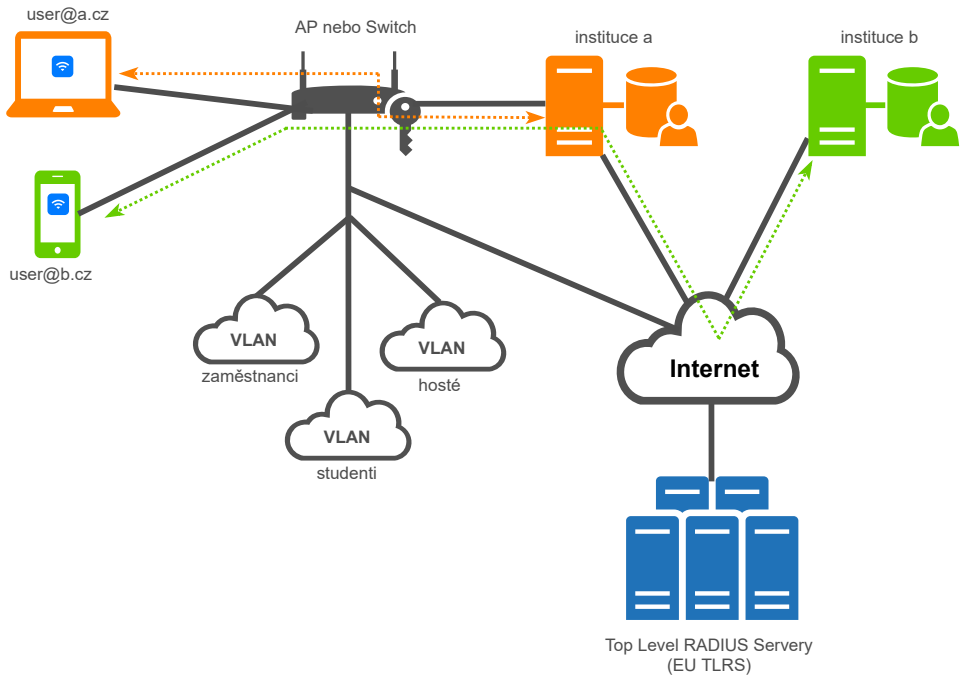
[6]RADIUS (Remote Authentication Dial In User Service) je síťový protokol, který umožňuje centrální ověřování, povolování a evidenci uživatelů připojujících se k síti. Protokol RADIUS je definován v RFC 2865.

[7]DNS (Domain Name System) je hierarchický, decentralizovaný systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace.

[8]IEEE 802.1x je protokol, který umožňuje zabezpečení přístupu do počítačové sítě. Protokol 802.1x je definován v RFC 3579 a 3580.

[9]AP (Access-Point) je síťové zařízení, které slouží k bezdrátovému připojení k síti.

Je povolen pouze autentizační protokol EAP[10]. Program běžící na straně klienta zahájí ověření přes EAP protokol. Klient vyšle na AP žádost o autentizaci, AP naváže spojení na RADIUS server a zprostředkuje ověření klienta vůči RADIUS serveru. Pokud je uživateů lokální, proběhne ověření přímo na RADIUS serveru, se kterým komunikuje AP. Pokud jde o návštěvníka, bude autentizační požadavek transportován přes strukturu RADIUS serverů až na domácí síť uživatele. Tento mechanismus je zachycen na obrázku 2.3, autentizační provoz je vizualizován tečkovanou čarou.



Obrázek 2.3: Autentizace na bázi protokolu 802.1x [6]

2.2.1 Realm

Při definici jména realmu a RADIUS serveru se eduroam opírá o systém DNS. Federace eduroam je založena na hierachické struktuře propojených RADIUS serverů znázorněné na obrázku 2.4.

Realm musí odpovídat doméně, kterou organizace spravuje. V případě realmů s koncovkou „.cz“ vše funguje podle hierachické struktury, evropské Top Level RADIUS servery posílají veškerý autentizační provoz na český národní RADIUS server. Do eduroamu je možné zapojit i organizace, které používají

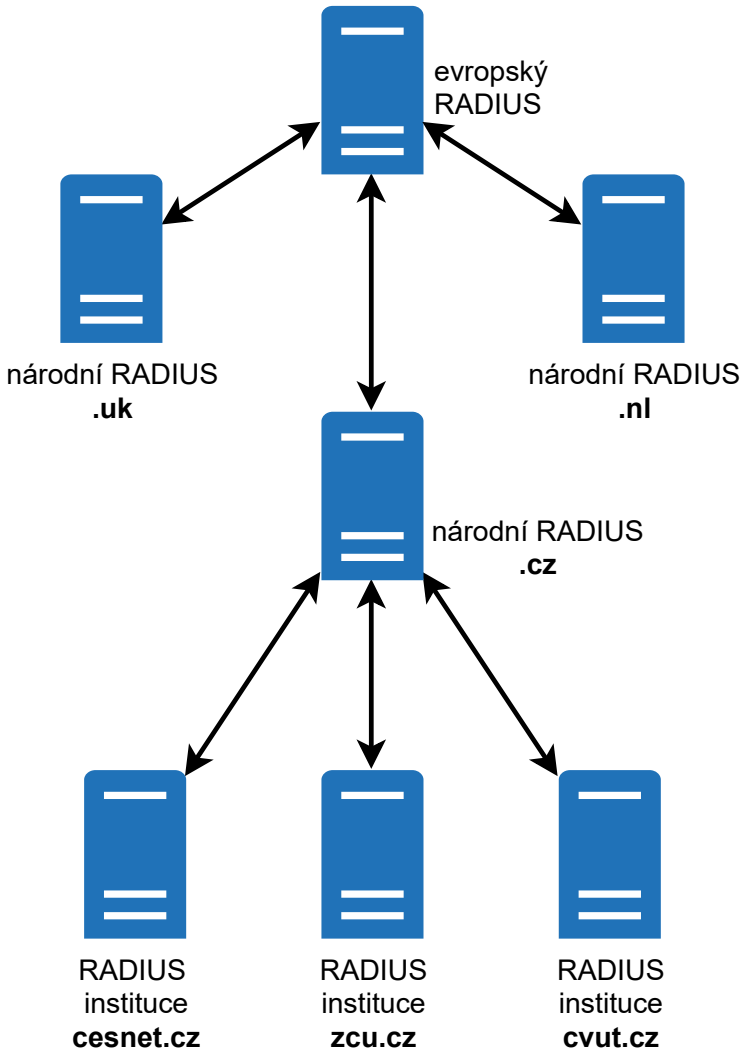
[10]EAP (Extensible Authentication Protocol) je autentizační konstrukce zprostředkující přenos a používání klíčů. Protokol EAP je definován v RFC 3748.

doménu mimo „.cz“ TLD[11]. Do DNS domény je třeba zanést speciální záznam, který zajistí směrování autentizačních požadavků na český národní RADIUS server, ten pak zajistí přenos jako u realmů z „.cz“ TLD.

Do DNS záznamu domény použité pro realm je třeba zanést NAPTR záznam:

```
DOMENA.eu. IN NAPTR 100 10 "s" "x-eduroam:radius.tls" \
    "" _radsec._tcp.eduroam.cz.
```

[11]TLD (Top Level Domain) je internetová doména na nejvyšší úrovni stromu internetových domén.



Obrázek 2.4: Hierachická infrastruktura RADIUS serverů [7]

2.2.2 RADIUS server

Při registraci instituce do eduroam musí být jméno RADIUS serveru registrováno ve veřejném DNS. Funkci RADIUS serveru lze zajistit pomocí různých implementací. Implementace RADIUS serveru musí splňovat technické požadavky:

- **RFC 2865; RADIUS** — podpora základního RADIUS protokolu
- **RFC 3580; EAP** — podpora protokolu EAP, ověřování uživatelů pomocí IEEE 802.1X (platí pouze pro IdP roli)
- **proxy** — RADIUS je schopen předávat požadavky na nadřazený RADIUS server na základě obsahu User-Name
- **filtrování atributů** — možnost odfiltrovat testovací účty podle hodnoty atributu, odstranit přiřazení VLAN z cizí sítě, ...

Každá instituce připojená v režimu IdP+SP poskytuje testovací účet, který je použit pro monitoring. Současně je nutné zpřístupnit RADIUS server organizace monitoringu. Zpřístupnit monitoring znamená povolit komunikaci z domény `ermon.cesnet.cz`. Kromě toho je nutné definovat monitoring v konfiguraci RADIUS, aby přijímal autentizační požadavky od monitoringu.

Pro Wi-Fi infrastrukturu instituce je třeba, aby vysílala essid „eduroam“, ověřovala uživatele protokolem IEEE 802.1X a používala šifrování. Vysílaný tvar essid musí být všude stejný, častou chybou bývají tvary „Eduroam“ nebo „EduRoam“.

2.2.3 Šifrování provozu

K zabezpečení provozu mezi národním RADIUS serverem a RADIUS serverem instituce se používá protokol RadSec nebo IPsec. Při použití systému unixového typu je doporučeno použít protokol RadSec, protože je součástí implementací RADIUS protokolu, jako je například SW Radiator nebo SW FreeRADIUS verze 3. Naopak při provozování RADIUS serveru na systému Microsoft Windows Server se doporučuje použít protokol IPsec.

IPsec

IPsec (IP security) definuje přidání bezpečnostního mechanismu do standardní IP vrstvy. Bezpečnostní mechanismy, které definuje IPsec, jsou dva:

1. **Ověřování** - Definuje původ dat. Příjemce si může ověřit, že právě přijatý IP paket pochází opravdu od toho, kdo paket vyslal.
2. **Šifrování** - Všechno kromě vlastní hlavičky IP paketu je zašifrováno pomocí předem domluveného algoritmu. Příjemce musí umět tento paket dešifrovat. Před vlastním přenosem dat se musí obě komunikující strany domluvit na způsobu šifrování dat.

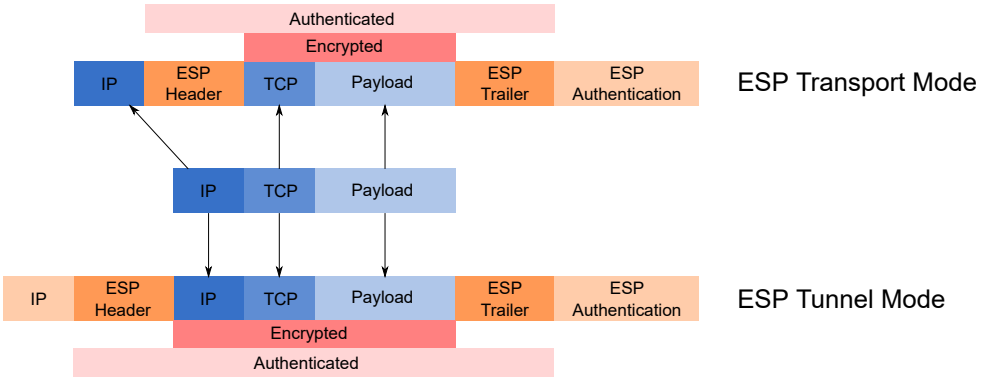
Základní protokoly:

- **AH (Authentication Header)** — Ověřuje autenticitu a původ dat.
- **ESP (Encapsulating Security Payload)** — Zajišťuje šifrování a ověření původu dat a ověřuje jejich integritu.
- **ISAKMP (Internet Security Association and Key Management Protocol)** — Automaticky domlouvá parametry spojení a vyjednává výměnu klíčů pomocí IKE (Internet Key Exchange)

Princip

Protokol ISAKMP má dvě fáze. První fáze stanovuje, aby byl chráněn proces výměny a dohod. Bezpečnost v první fázi je zaručena pomocí šifrovacího algoritmu a certifikátu. V této fázi existují dvě metody, main mode a aggresive mode. Aggresive mode se od main mode liší tím, že zaručuje přenost SA (security association), klíče a důvěryhodnost informace vztahující se k datům v jedné zprávě. V druhé fázi si obě strany vymění potřebná data a dohodnou se na vzájemně akceptovatelných podmínkách SA. Tajný symetrický klíč je vyměněn za použití Diffiho-Hellmanova schématu pro výměnu klíče.

IPsec může fungovat ve dvou režimech. První z nich je transport mode, který je vhodný pro propojení dvou uzlů. Druhý režim je tunnel mode. Tunnel mode se hodí pro propojení dvou sítí, například propojení mezi VPN[12] bránami. Rozdíly mezi módy jsou patrné z obrázku 2.5.



Obrázek 2.5: IPsec — Tunnel a Transport mode [8]

V tunnel mode je paket plně zapouzdřen včetně IP hlavičky uzlu. V transport mode jsou zapouzdřena jenom data z IP datagramu, a to tak, že se vloží hlavička ESP nebo AH mezi hlavičku IP a payload.

[12]VPN (virtual private network) je způsob zapouzdření a přenosu dat skrz jinou síť.

2.2.4 Certifikáty

RADIUS server potřebuje certifikát pro dva různé účely. Prvním je bezpečné propojení s národním RADIUS serverem a druhým účelem je EAP server, který slouží pro zabezpečení komunikace mezi uživatelským zařízením a RADIUS serverem instituce.

Pro RadSec anebo IPsec musí správci připojované organizace získat certifikát od uznávané certifikační autority:

- **TCS** - pro instituce připojené k síti CESNET
- **eduroam CA** - pro instituce nepřipojené k síti CESNET
- **CESNET CA4** - používá národní RADIUS server

V případě výběru certifikační autority, která podepíše certifikát pro EAP server, má každá instituce v eduroam mnohem větší volnost, ale také odpovědnost. Klíčové je, aby zařízení uživatelů ověřovalo, že RADIUS server má certifikát na předem nakonfigurované jméno a že certifikát je od jedné konkrétní CA. Porušení jednoho nebo druhého bodu nezajistí dostatečnou ochranu přihlašovacích údajů.

2.3 Technické možnosti Windows Server 2019

Windows Server 2019 je aktuální serverová verze operačního systému z řady Windows NT od společnosti Microsoft. Jako operační systém nabízí velké množství funkcí. Pro účely eduroam je stěžejní implementace RADIUS serveru.

Platforma Microsoft Windows Server obsahuje implementaci RADIUS serveru od verze 2003. Implementace se nazývá Network Policy Server (NPS). NPS je od verze 2008 součástí komponenty nazvané Network Policy and Access Services (NPAS). [9]

2.3.1 Podpora technických požadavků RADIUS

NPS je implementace RADIUS protokolu od Microsoft podle standardu definovaného v RFC 2865 a 2866. NPS může fungovat jako RADIUS server, který poskytuje ověření požadavků, povolení přístupu a určuje politiku pro bezdrátovou síť, virtuální privátní síť nebo běžnou síť. Alternativně lze NPS nakonfigurovat jako RADIUS proxy, který bude směřovat autentizační požadavky na jiný RADIUS server.

U autentizačních metod nabízí NPS na výběr méně bezpečné protokoly jako MS-CHAP (Challenge-Handshake Authentication Protocol), MS-CHAP v2 nebo PAP (Password Authentication Protocol). Dále ale nabízí specifikovat autentizační protokol EAP, ve kterém zahrnuje typ Protected EAP (PEAP),

zabezpečení heslem (EAP-MSCHAP v2) a použití autentizace na bázi certifikátu.

NPS ověřuje požadavky podle politik, ve kterých umožňuje filtrovat podle hodnot atributů.

2.3.2 Ostatní požadavky

V operačním systému Microsoft Windows Server není podpora protokolu RadSec. Alternativou pro šifrování provozu mezi servery je použití protokolu IPsec, který je součástí operačního systému Microsoft Windows Server.

Kapitola 3

Realizace

V praktické části bakalářské práce bylo mým úkolem vytvořit virtuální infrastrukturu, na které bude možné otestovat různé typy připojení do federace eduroam. Zároveň jsem ve virtuální infrastruktuře vyzkoušel uživatelskou správu účtů na platformě Microsoft Windows Server. Po otestování všech možností a zdokumentování postupů, jsem vytvořil dokumentaci o této platformě na informační web české federace eduroam.cz. Vytvořenou dokumentaci jsem otestoval se skupinou správců a ověřil její použitelnost v praxi. Na závěr jsem provedl ekonomicko-manažerské shrnutí. V tomto shrnutí porovnávám, co práce přinesla pro stranu správců federace eduroam a zároveň, jaký užitek měla pro správce z institucí.

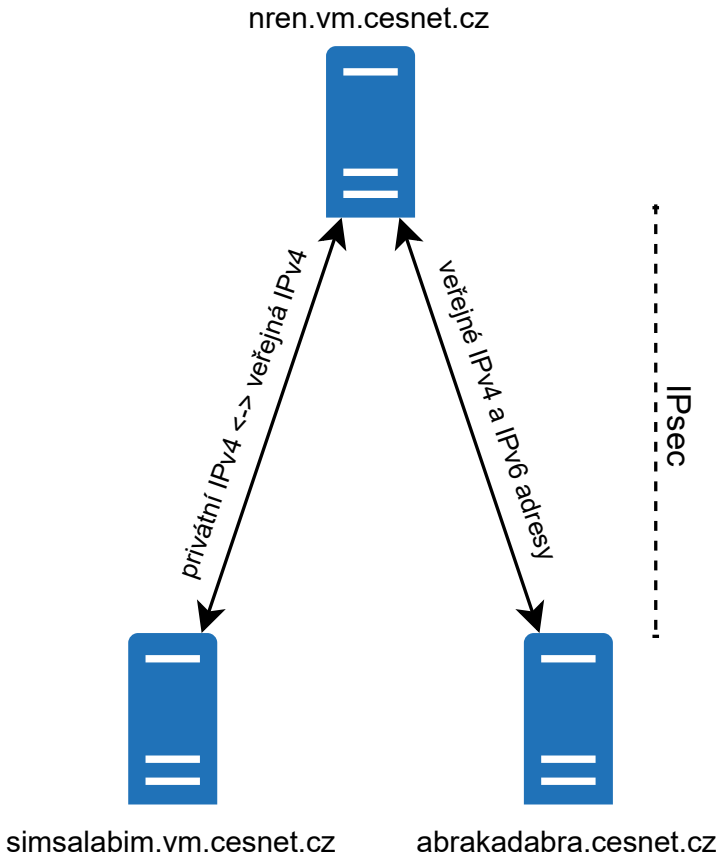
3.1 Virtuální infrastruktura

Produkční infrastruktura české federace eduroam je rozsáhlá síť RADIUS serverů. Samotný národní RADIUS server se skládá ze dvou fyzických serverů. Každý z nich je v jiné lokalitě, jeden je v aktivním stavu a druhý je ve stavu stand-by. Služby jsou řízeny HA clusterem[13]. Všechny RADIUS servery institucí jsou připojeny k národnímu a ten je připojen k evropskému RADIUS serveru, jak bylo patrné na obrázku 2.4.

Pro účely závěrečné práce jsem vytvořil zmenšenou virtuální infrastrukturu, která je znázorněná na obrázku 3.1.

Virtuální infrastruktura se skládá z nadřazeného RADIUS serveru (`nren.vm.cesnet.cz`), který simuluje národní RADIUS server, a dvou k němu připojených RADIUS serverů (`abrakadabra.cesnet.cz`, `simsalabim.vm.cesnet.cz`), které slouží jako vzorové RADIUS servery institucí. Všechny tři servery fyzicky běží ve virtualizaci CESNET. [10]

[13] HA cluster (High-Availability cluster) je seskupení více serverů.



Obrázek 3.1: Schéma virtuální infrastruktury

3.1.1 nren.vm.cesnet.cz

Server má roli národního RADIUS serveru ve virtuální infrastruktuře. Konfigurace serveru je podobná produkčnímu národnímu RADIUS serveru, jde o jeho zjednodušenou verzi. Při instalaci jsem vycházel z produkční konfigurace, aby podmínky testovacího prostředí byly srovnatelné s těmi v produkčním prostředí. Běží na operačním systému Debian 9, na stejném systému jako produkční verze. O sestavování IPsec spojení se stará SW Racoon a funkci RADIUS serveru zajišťuje SW Radiator. Rozdíl oproti produkční verzi je, že kromě veřejné IPv4 adresy má testovací `nren.vm.cesnet.cz` nakonfigurovanou i IPv6 adresu.

3.1.2 Virtuální RADIUS servery institucí

Na obou serverech běží operační systém Microsoft Windows Server 2019. Každý z nich simuluje server připojené instituce. Pro šifrovanou komunikaci mezi servery je nutné použít protokol IPsec, který je v Microsoft Windows Server nativně podporován.

abrakadabra.cesnet.cz

Server `abrakadabra.cesnet.cz` je provozován v datovém centru v Brně a má přidělenou veřejnou IPv4 a IPv6 adresu.

simsalabim.vm.cesnet.cz

Server `simsalabim.vm.cesnet.cz` je provozován v datovém centru v Praze a veřejné adresy jsou ukončeny na posledním síťovém prvku před tímto serverem. Síťový prvek překládá veřejnou adresu na privátní síť 10.10.20.5/24.

3.1.3 Nastavení firewallu

Komunikace mezi servery probíhá pomocí IPsec. Pro správné fungování komunikace mezi servery je nutné povolit příslušné protokoly a porty pro příchozí i odchozí provoz. V Microsoft Windows Server 2019 se firewall řídí podle pravidel, která se v grafickém rozhraní dají ovládat v komponentě zvané Windows Defender Firewall with Advanced Security. [11] Tato pravidla lze upravovat i pomocí příkazu *netsh advfirewall firewall* v příkazovém řádku *Windows PowerShell* s administrátorským oprávněním. Pro účely dokumentace jsem zvolil nastavení prostřednictvím příkazové řádky.

Příklad syntaxe příkazu pro přidání pravidla:

```
$ netsh advfirewall firewall add rule \
    name=<string> \
    dir=in|out \
    action=allow \
    protocol=icmpv4:any,any \
    localip=any|<IPv4 address>|<IPv6 address> \
    remoteip=any|<IPv4 address>|<IPv6 address> \
    localport=any|0-65535 \
    remoteport=any|0-65535 \
    protocol=0-255|icmpv4|icmpv6|tcp|udp|any
```

Pro komunikaci s národním RADIUS serverem je potřeba povolit protokol ICMP (č. 1), který se používá pro zjištění fuknčnosti IPsec spojení. Dále pro navazování IPsec spojení je třeba povolit protokol ESP (č. 50), protokol

AH se nepoužívá. V poslední řadě je nutné povolit protokol IPv4 (č. 4) a protokol UDP (č. 17) na portu 1812, na kterém RADIUS ověřuje požadavky.

Kromě povolení příslušných pravidel pro komunikaci s národním RADIUS serverem je potřeba povolit komunikaci s monitoringem. Pro něj je nutné povolit, obdobně jako pro `radius1.eduroam.cz`, protokoly ICMP, IPv4 a UDP na portu 1812.

Pro manipulaci s pravidly v příkazovém řádku lze použít stejný příkaz *netsh advfirewall firewall* s klíčovým slovem *show*, *set* nebo *delete*.

3.1.4 Instalace certifikátů

Práce s certifikáty na Microsoft Windows Server 2019 se provádí v grafickém rozhraní pomocí nástroje *Microsoft Management Console* v modulu *Certificates*. Analogicky lze použí příkazovou řádku *Windows PowerShell* s administrátorským oprávněním a příkazem *certutil*.

Pro účely práce je relevantní certifikát pro bezpečné propojení s národním RADIUS serverem.

Certifikát od eduroamCA nebo TCS certifikát, které lze použít pro IPsec spojení, je třeba naimportovat ve formátu *.pfx* nebo *.p12*. V tomto formátu obsahuje soubor kromě certifikátu i klíč.

Po naimportování certifikátu pro bezpečnou komunikaci s národním RADIUS serverem následuje import certifikátu, který používá protější strana. Národní RADIUS server používá ceritifkát od CESNET CA4, jeho import provedeme příkazem *certutil -addstore*.

Příklad syntaxe příkazu pro manipulaci s certifikáty:

```
$ certutil \
    -importPFX  -- Import certificate and private key
    -MergePFX   -- Merge PFX files
    -decode     -- Decode Base64-encoded file
    -addstore   -- Add certificate to store
    -delstore   -- Delete certificate from store
    -store      -- Dump certificate store
```

Pro manipulaci s certifikáty v příkazovém řádku lze použít stejný příkaz *certutil* s přepínači *-delstore*, *-store* nebo *-decode*.

3.1.5 Konfigurace IPsec

V produkční infrastruktuře se IPsec používá v transportním režimu za použití protokolu ESP. Dále probíhá komunikace pouze na IPv4 adresách a není podporován překlad adres. V této konfiguraci musí být IPsec spojení ukončené na veřejných adresách.

V testovací virtuální infrastruktuře je cílem rozšířit tyto možnosti. Kromě provozu na IPv4 adresách lze provozovat IPsec i na IPv6 adresách. Další možností je spojení mezi privátními IPv4 adresami za užití technologie NAT-T[14]. Nastavení IPsec spojení se provádí pomocí dvou pravidel:

Mainmode pravidlo

Mainmode pravidlo zajišťuje parametry pro vyjednávání SA mezi servery. [12]

Příklad syntaxe příkazu pro manipulaci s certifikáty:

```
$ netsh advfirewall mainmode add rule \
    name=<string> \
    mmsecmethods=dhgroup1|dhgroup2:3des|des|
aes256-md5|sha1|sha256|sha384|default \
    mmforcedh=yes|no \
    mmkeylifetime=<num>min,<num>sess \
    endpoint1=any|<IPv4 address>|<IPv6 address> \
    endpoint2=any|<IPv4 address>|<IPv6 address> \
    auth1=computerkerb|computercert|computerpsk|anonymous \
    auth1ca="<CA Name> [catype:root|intermediate]"
```

Consec pravidlo

Pravidlo consec specifikuje zabezpečení IPsec spojení. [13]

Příklad syntaxe příkazu pro manipulaci s certifikáty:

```
$ netsh advfirewall consec add rule \
    name=<string> \
    endpoint1=any|<IPv4 address>|<IPv6 address> \
    endpoint2=any|<IPv4 address>|<IPv6 address> \
    action=RequireInRequestOut|RequestInRequestOut|
 RequireInRequireOut|RequireInClearOut|NoAuthentication \
    mode=transport|tunnel \
    localtunnelendpoint=any|<IPv4 address>|<IPv6 address> \
    remotetunnelendpoint=any|<IPv4 address>|<IPv6 address> \
    port1=0-65535|<port range>[,...]|any \
    port2=0-65535|<port range>[,...]|any \
    protocol=0-255|tcp|udp|any \
```

[14]NAT-T (NAT-Traversal) je způsob navázání a správy spojení pomocí IP protokolu přes síťové prvky, které provádějí překlad síťových adres.

```
    auth1=computerkerb|computercert|computerpsk|anonymous \
    auth1ca="<CA Name> [catype:root|intermediate]" \
    qmpfs=dhgroup1|dhgroup2|mainmode|none \
    qmsecmethods=authnoencap:<integrity>+[valuemin]+ \
[valuekb]|ah:<integrity>+esp:<integrity>-<encryption>+ \
[valuemin]+[valuekb]
```

3.1.6 Instalace Network Policy Server (NPS)

Komponenta, která obsahuje Network Policy Server, se nazývá NPAS. Ve výchozím nastavení není součástí Microsoft Windows Server 2019 a musí být doinstalována prostřednictvím aplikace *Server Manager* nebo pomocí příkazu

```
$ Install-WindowsFeature NPAS -IncludeManagementTools
```

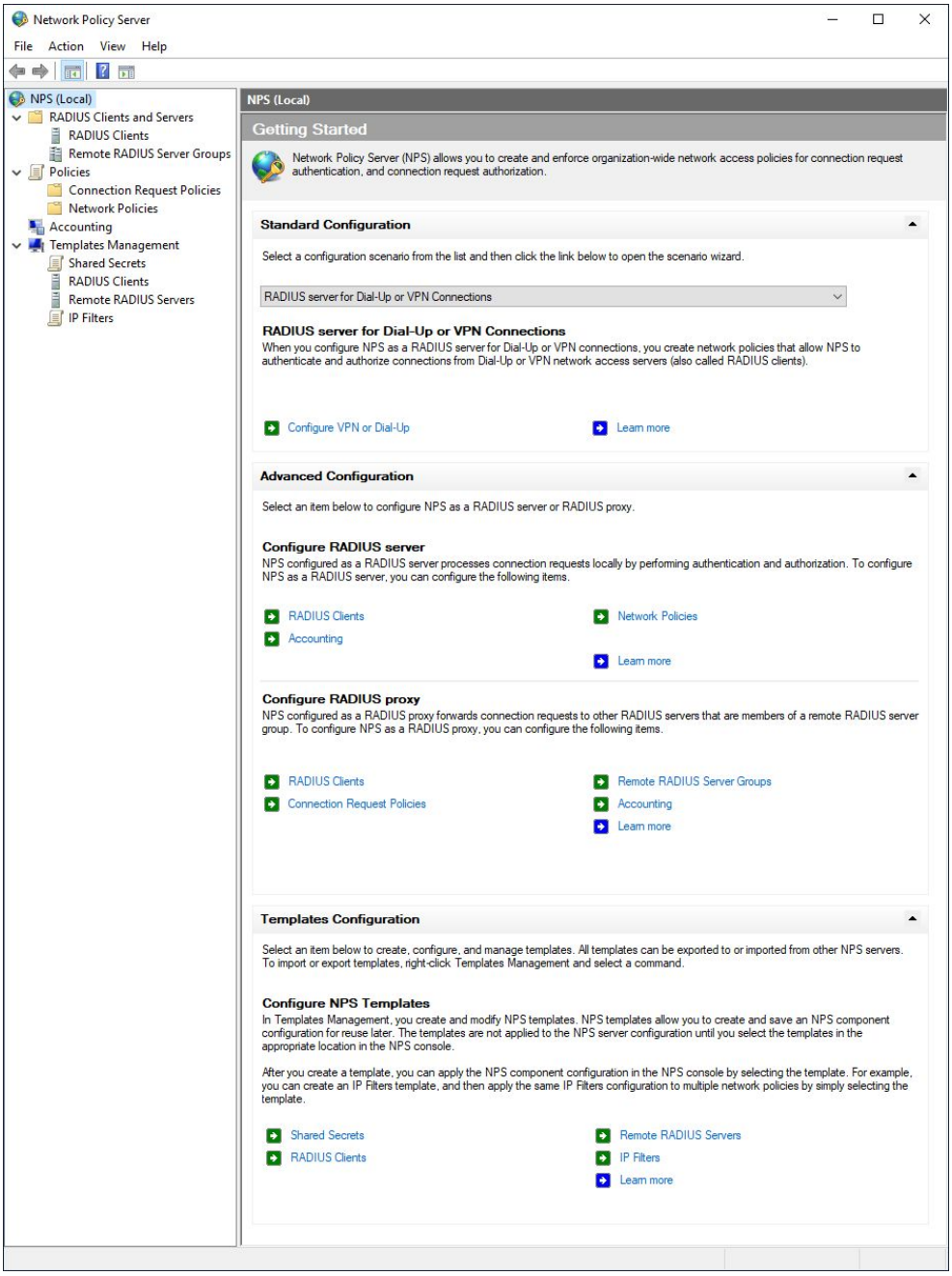
Konfigurace NPS se provádí v grafickém rozhraní ukázaném na obrázku 3.2.

Služba, která řídí NPS, se nazývá *Internet Authentication Service (IAS)*. Před spuštěním této služby je nutné registrovat realm v AD[15]. Každý vzdálený bod je třeba definovat. K tomu slouží sekce *RADIUS Clients*, kde definujeme náš národní RADIUS server, v produkčním prostředí monitoring a také všechny přístupové body nebo jejich řídící prvek. Pro národní RADIUS server je třeba vytvořit skupinu v sekci *Remote RADIUS Server Groups*. Na tuto skupinu budou přesměrovány požadavky na připojení od uživatelů cizích realmů. Řízení NPS mají na starost politiky *Connection Request Policies* a *Network Policies*. Při zpracovávání požadavku se prvně ověřuje proti sadě politik z *Connection Request Policies*. Zde se rozhoduje, jestli se požadavek bude ověřovat lokálně, nebo bude odeslán k ověření na vzdálený RADIUS server. Rozhodování se provádí na základě realmu v uživatelském jméně. Cizí realm se odešle ke zpracování na národní RADIUS server a realm domácí instituce bude dále zpracován podle *Network Policies*. V této sadě politik se požadavek ověří proti uživatelské databázi Active Directory.

V každé sadě politik, jsou pravidla seřazena podle pořadí, v jakém se budou vyhodnocovat, tedy záleží na jejich pořadí.

Celou konfiguraci Network Policy Server lze pomocí příkazu importovat a exportovat pro účely zálohy do souboru ve formátu XML.

[15] AD (Active Directory) je název adresářových služeb LDAP implementované firmou Microsoft pro řadu systémů Windows.



Obrázek 3.2: Rozhraní Network Policy Server

3.1.7 Různé způsoby zapojení

První možností zapojení serverů mezi sebou je přes veřejné IPv4 adresy. Tento způsob je aktuálně jediné možné zapojení při použití IPsec spojení v pro-

dukčním prostředí. Konfigurace IPsec na straně `nren.vm.cesnet.cz` je stejná jako na `radius1.eduroam.cz`. Ve virtuální infrastruktuře jsem toto zapojení testoval mezi `nren.vm.cesnet.cz` a `abrakadabra.cesnet.cz`. Veřejnou IPv4 adresu na serveru je bohužel v některých institucích nemožné získat, proto je na místě prozkoumání jiných zapojení.

Mezi stejnými servery jsem ladil zapojení na IPv6 adresách. Konfigurace SW na `nren.vm.cesnet.cz` vyžadovala rozšíření o definice IPv6 adres a přepsání IPsec politik. Na druhé straně na `abrakadabra.cesnet.cz` bylo potřeba přidat podmínku do firewallu, přepsat pravidla pro IPsec spojení a definovat RADIUS klienty na IPv6 adresách.

Při zapojení RADIUS serveru s privátní IPv4 adresou je konfigurace odlišná. Toto zapojení jsem nastavil mezi RADIUS servery `nren.vm.cesnet.cz` a `simsalabim.vm.cesnet.cz`. Pro správnou konfiguraci bylo potřeba zvolit tunnel mode a v pravidlech na obou stranách definovat privátní IPv4 adresu.

3.1.8 Logování

V systému Microsoft Windows Server jsou logy zaznamenávány a shromažďovány do komponenty zvané Windows Event Viewer. Do této komponenty se zaznamenají aktivity prováděné systémem, uživatelem nebo procesy aplikací v různých formátech. Nástroj Windows Event Viewer kategorizuje a ukládá logy, které umí následně filtrovat, exportovat, čistit či v nich vyhledávat. Logy řadí do pěti kategorií:

- **Application** — logování aplikací
- **Security** — zaznamenávání pokusů o ověření uživatelů, oprávnění aplikací
- **Setup** — logy instalace a aktualizace systému
- **System** — systémové logy
- **Forwarded Events** — sběr logů z podřazených serverů

Logování Network Policy Serveru spadá do kategorie Security. Ve výchozím stavu po instalaci NPS není logování zapnuté. Zapnutí logování NPS se provádí v nastavení NPS a je zde možnost logovat úspěšné a neúspěšné požadavky. NPS podporuje i vlastní accounting logování. Obsahuje detailnější nastavení logů. Informace lze ukládat do souboru nebo na SQL server do databáze.

3.2 Správa uživatelských účtů

Na platformě Microsoft Windows Server 2019 má správu uživatelských účtů na starost komponenta Active Directory. Active Directory (AD) je implementace adresářových služeb pro práci s objekty v síti. Objekty v síti mohou být servery, počítače, tiskárny, ale především uživatelské účty. Všechny objekty

jsou uspořádané ve stromové struktuře, nad kterou lze pracovat, nastavovat politiky a instalovat či aktualizovat software.

Pro instalaci Active Directory je třeba instalovat komponentu s názvem *Active Directory Domain Services*. Lze ji pohodlně instalovat z příkazové řádky Windows PowerShell příkazem:

```
$ Add-WindowsFeature AD-Domain-Services
```

Pro účely RADIUS serveru je nutné instalovat systém DNS (Domain Name Services). Tím se zvýší úroveň serveru na řadič domény a registruje se doména ve stromové struktuře příkazem:

```
$ Install-ADDSForest -DomainName domena.cz -InstallDNS
```

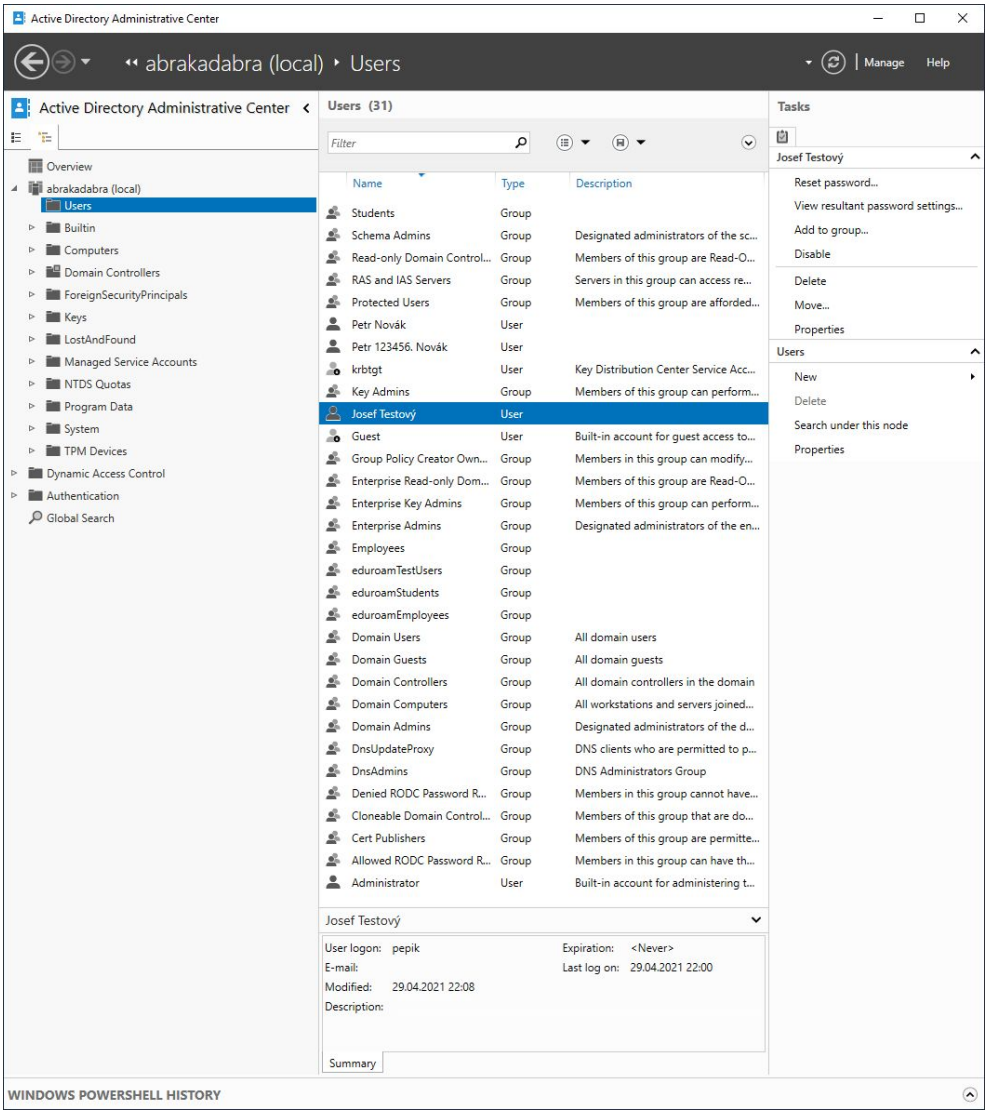
Rozhraní Active Directory pro správu uživatelských účtů je na obrázku 3.3.

3.2.1 Správa eduroam hesel

Uživatel získá při vzniku vztahu vůči instituci uživatelský účet. Jeho účet může sloužit k přístupu do interních systémů, emailu a také pro eduroam identitu. Myšlenka jednoho stejného hesla pro všechny služby přináší zjednodušení pro uživatele i správce. Zároveň může být stejné heslo do interních systémů instituce a heslo pro eduroam potenciálním bezpečnostním rizikem. Pro správné nastavení zařízení uživatele se doporučuje použít nástroj eduroam CAT. Při nekorektním nastavení zařízení může dojít ke zkopírování uživatelských údajů a ke zneužití identity. Toto doporučení bohužel značné množství uživatelů ignoruje. Někteří správci institucí berou toto riziko na vědomí, a proto dle doporučení upřednostňují použití alternativního hesla pro eduroam identity. Myšlenka alternativních hesel dává pro eduroam smysl, protože se jedná o službu, kterou uživatel využívá i v cizím a neznámém prostředí. Pokud má například uživatel stejné heslo do systému v instituci jako k eduroam, vystavuje se většímu riziku kompromitování přihlašovacích údajů a zneužití účtu. Přístup do interních systémů provádí uživatel vědomě, zatímco připojování k síti eduroam provádní zařízení uživatele na pozadí samovolně. Cizí síť může být napadená nebo může eduroam hesla útočník odchytávat cíleně.

Mým úkolem bylo prozkoumat možnost alternativních hesel na platformě Microsoft Windows Server. V systému Microsoft Windows Server se při výchozím nastavení NPS používají stejná přístupová hesla pro eduroam, jako se používají k doménovým účtům.

První možností bylo přidání alternativního hesla každému uživateli, které by sloužilo pro ověření požadavků do sítě eduroam. Heslo k uživatelskému účtu je z pohledu Active Directory hodnota atributu u objektu uživatelského účtu. Nástroj zvaný Active Directory Schema umožňuje přidat potřebný atribut k objektu uživatelských účtů. Po přidání alternativního hesla pro eduroam



Obrázek 3.3: Rozhraní Active Directory

k uživatelskému účtu je potřeba nastavit NPS, aby používal toto alternativní heslo. Bohužel takové nastavení NPS neumožňuje. NPS je uzavřená komponenta a nepodporuje tuto možnost, ani způsob, jakým by šel proces ověřování změnit.

Druhou možností, jak oddělit eduroam hesla, je vytvoření sekundárního účtu v AD každému uživateli. S tímto krokem nabývá větší režie na správu uživatelských účtů v instituci, ale je to způsob, jak oddělit heslo pro eduroam identitu od hesla do interních systémů. Pro lepší orientaci při správě účtů mohou být doménové účty a účty pro eduroam spárovány pomocí atributů.

Sekundární účet pro eduroam musí mít odlišný tvar od doménového účtu. Tím se vytvoří možnost anonymizovat eduroam účet.

3.3 Ověření návodů v praxi

Informační web o české federaci eduroam.cz obsahuje obecné informace o projektu eduroam. V první řadě jsou na webu základní informace a myšlenka eduroam, dále jsou zde dostupné mapy a seznam připojených organizací, roamingová politika, která upravuje chování jednotlivých členů a uživatelů, a kontaktní informace. V druhé řadě web eduroam.cz obsahuje dokumentaci. Dokumentace je dvojího druhu, pro uživatele a pro správce institucí. Uživatelská dokumentace slouží ke správnému obecnému nastavení koncových zařízení. Dokumentace pro správce institucí napomáhá ke správné konfiguraci technické stránky připojení do federace eduroam i ke splnění všech potřebných administrativních kroků.

Právě část této dokumentace, která popisuje připojení k eduroam při použití technologie postavené na platformě od firmy Microsoft, nebyla do této doby zdokumentována. Získané informace o této platformě jsem využil a vytvořil dokumentaci, která popisuje připojení do federace za použití SW Microsoft Windows Server a jeho příslušných technologií. Vytvořená dokumentace má svoji veřejnou část i zatím nepublikovanou privátní část.

3.3.1 Veřejná dokumentace

Veřejná část dokumentace umístěná do sekce *PRO SPRÁVCE » Připojení k eduroam.cz » RADIUS* nese název *NPS*. Hlavní sekce dokumentace NPS popisuje krok za krokem nastavení Network Policy Server v podobě snímků obrazovky. Každý snímek obsahuje doprovodný komentář se stručným vysvětlením daného kroku.

Pod hlavní kategorií jsou umístěny dílčí prerekvizity, které jsou potřeba před samotnou konfigurací NPS. Úvodním krokem je umožnit RADIUS serveru komunikaci v nastavení firewallu Windows Server. Je zde popsáno, jaké protokoly a na jakých portech je nutné povolit. Pravidla jsou rozdělena na příchozí a odchozí i podle cílových serverů, se kterými daná komunikace probíhá. Zároveň je zde popsána manipulace s pravidly, vše za pomocí příkazů z důvodu snažší udržitelnosti a aktuálnosti dokumentace. Tato pravidla lze analogicky převzít pro nastavení případného externího firewallu. Za předpokladu, že jej daná instituce nebo její poskytovatel připojení používá na hranici sítě instituce.

Další sekcí je část dokumentace věnující se instalaci certifkátů. Instituce mají na výběr ze dvou uznávaných vydavatelů certifikátů *eduroamCA* nebo *TCS*. Je zde uvedeno, jak se certifikáty importují a konvertují do potřebného formátu. Zároveň jsou níže uvedeny postupy pro import certifikátů certi-

fikačních autorit spolu s odkazy pro jejich stažení. Na konci je ukázka manipulace s cerifikáty.

Poslední prerekvizitou před konfigurací NPS je navázání IPsec spojení. K tomu jsou popsána dvě pravidla *consec* a *mainmode*. U každého je komentář s informací, jaké hodnoty atributů se mají upravit a kde tyto hodnoty najít. Uvedeno je zde také, jakým způsobem pravidla vypisovat, smazat a jak si ověřit funkčnost IPsec spojení. Pro účely hledání chyby či ladění popisuje dokumentace aktivování logování IPsec a jak s logy pracovat.

3.3.2 Privátní dokumentace

V interní sekci dokumentace existuje zatím nepublikovaná část. Je zde rozšířená dokumentace konfigurace IPsec spojení. V té se uvažuje více způsobů zapojení RADIUS serveru. Kromě zapojení pomocí veřejné IPv4 adresy je dále možnost použití IPv6 adresy nebo privátní IPv4 adresy. Tento způsob musí být prvně podporován na straně národního RADIUS serveru. Pak je zde uvedeno, v jakém režimu a pomocí jakých pravidel nakonfigurovat IPsec spojení ve způsobech zapojení. Sekce není ještě uveřejněna z důvodů nekompatibility na straně národního RADIUS serveru. Ten zatím umožňuje IPsec spojení pouze na veřejných IPv4 adresách.

Poslední částí vytvořené dokumentace je sekce týkající se Active Directory. Zde je na úvod popsáno, jakým způsobem se AD instaluje a konfiguruje. Poté je zde soupis nejčastějších příkazů, které se používají na denní bázi. Od vytváření objektů, hledání, mazání či vypisování jsou zde také ukázané operace mezi nimi. Instituce připojující se v režimu IdP+SP mají povinnost definovat testovacího uživatele. Část dokumentace popisující práci v Active Directory je pojata na příkladu operací s testovacím uživatelem. Operace v Active Directory se dají provádět v grafikém rozhraní, ale pro názornější a přesnější zdokumentování jsou použity příkazy do příkazové řádky Windows PowerShell.

3.4 Ekonomicko-manažerské shrnutí

V této kapitole shrnuji přínos, který pro českou federaci eduroam tato práce má. Nejlépe je přínos vidět z pohledu správce instituce, pro které je určena vytvořená dokumentace. Zároveň je zde značný přínos i pro správce federace eduroam.

3.4.1 Správce insituce

Práce má přínos pro správce, kteří se chystají připojit svoji instituci do federace eduroam. Za předpokladu, že významný podíl institucí používá systém nebo řešení na bázi Microsoft. Do doby vytvoření práce neexistovala dokumentace popisující použití této platformy pro připojení do eduroam. Správci museli

připojení realizovat za použití jiné, zdokumentované platformy. Mohli ale narazit na potíž, např. s jinou platformou neměli žádné zkušenosti a realizace připojení pro ně byla obtížná. Větší instituce s IT zázemím nemají obvykle s připojením problémy, u menších organizací se může vyskytnout nedostatek vlastních zdrojů. V takovém případě mají instituce možnost využít pomoc externích firem. [14] Na webu eduroam.cz existuje seznam implementačních firem, které již mají zkušenost s připojením instituce do eduroam a nabízejí své služby dalším institucím.

Volba implementace externí firmou přináší správcům instituce značnou úsporu času, do jisté míry zbavení odpovědnosti. V některých případech jde o jedinou možnost, jak se k eduroam instituce dokáže připojit. Nejen v těchto případech nastává otázka udržitelnosti. Připojení k eduroam není pouze jednorázová záležitost. Pokud se instituce připojí k eduroam, měla by nadále udržovat připojení ve funkčním stavu. Po dokončení připojování musí instituce být schopna reagovat na případné problémy. Může dojít k technickým problémům se spojením mezi RADIUS servery. Častým problémem jsou expirované certifikáty nebo změny IP adres RADIUS serverů. I z druhé strany, ze strany národního RADIUS serveru může dojít ke změně nebo aktualizaci a je potřeba aktivita nebo úprava konfigurace od správců institucí na jejich straně. Pokud tedy instituce využije služeb externí firmy, měla by pamatovat i na následný servis. Zároveň s použitím externí firmy se instituce vystavuje bezpečnostnímu riziku po stránce ochrany osobních údajů. Externí firma může mít přístup k uživatelské databázi, a tím i k osobním údajům uživatelů instituce.

Proto je žádoucí pro instituce implementovat připojení k eduroam primárně vlastními zdroji. Výstupy této bakalářské práce slouží jako významná podpora varianty připojení instituce vlastními silami a zdroji.

3.4.2 Správce federace

Na druhou stranu má práce přínos i pro správce federace. V první řadě dokumentace platformy Microsoft delší dobu chyběla a podpora při použití této platformy byla komplikovanější. Správcům federace se zjednodušila komunikace se správci institucí během připojování. Zároveň určitá část komunikace byla eliminována a to ušetřilo velké množství času správcům federace.

Z vytvořené dokumentace čerpají i externí firmy. Pokud ale instituce díky vytvořené dokumentaci implementuje připojení vlastními zdroji, vyhne se implemetaci externí firmou. Pro správce federace to znamená odstranění komplikací v situaci, kdy firma rozváže s připojovanou institucí vztah, nebo když firma není vázána následnou správou připojení a dojde k technickým problémům.

Závěr

eduroam je celosvětový roamingový systém, který zajišťuje uživatelům z akademických institucí transparentní přístup k Internetu bez ohledu na to, v jaké participující organizaci se uživatel nachází. V eduroamu uživatel disponuje jedinou identitou, která jej opravňuje k přístupu ke všem participujícím sítím. Údaje o uživateli jsou uchovány v jeho domácí instituci.

Záverečná práce vznikla ve spolupráci mezi Fakultou informačních technologií Českého vysokého učení technického v Praze a zájmovým sdružením právnických osob CESNET. Smyslem práce bylo podpořit používání platformy Microsoft Windows Server pro účely eduroam. Dokumentace české federace eduroam umístěná na webu `eduroam.cz` dosud neobsahovala dostatečné informace týkající se platformě Windows Server. Během připojování k eduroam má každá instituce povinnost zprovoznit a udržovat RADIUS server. Práce se zabývá možnostmi, jestli a jakým způsobem použít platformu Widnows Server jako RADIUS server instituce.

Po důkladné analýze podmínek pro připojení a technických možností jsem ve virtuální infrastruktuře otestoval různé typy připojení RADIUS serveru pomocí technologie IPsec. Zde se ukázalo, že všechny typy připojení serverů (umístění za IPv4 NAT, na veřejné IPv4 nebo IPv6 adrese) jsou dosažitelné. Ovšem zapojení RADIUS serveru umístěného za IPv4 NAT pomocí tzv. „tunnel mode“ technologie IPsec se po důkladném posouzení nedá doporučit pro nasazení v reálné produkční infrastruktuře. Tento způsob zapojení vyžaduje podrobnější konfiguraci ze strany národního RADIUS serveru, což není v produkčním prostředí udržitelné. Připojení na veřejných IPv4 a IPv6 adresách je ze závěru práce použitelné rešení pro tuto platformu. V produkčním prostředí je ale doposud možné pouze připojení na veřejné IPv4 adrese. Národní RADIUS server zatím nepodporuje IPv6 adresy. Doporučení ze závěru práce pro správce české federace eduroam je nasazení IPv6 adres v produkčním prostředí.

Dalším přínosem práce je významná úspora času a práce pro správce nově se připojujících institucí. Instituce, zejména střední a základní školy, provozují

často své IT řešení na bázi Microsoft. Dokumentace jim umožní vyhnout se experimentování během implementace. Stejně tak si nemusí správci osvojovat a provozovat jiné technologie (např. řešení na bázi Linuxu), která by byla alternativou.

Dokumentace přinesla úsporu i pro správce federace eliminací podstatné části komunikace se správci institucí. Současně práce doplnila dokumentaci eduroam.cz, a tím zvýšila úroveň této služby. Dokumentace po vytvoření prošla zkušebním provozem s vybranými správci a před publikováním byla upravena, aby její obsah byl ucelený a srozumitelný pro nejširší spektrum správců s různými znalostmi a zkušenostmi.

V budoucnu může vytvořená dokumentace posloužit jako základ pro zdokumentování nové verze Windows Server.

Literatura

[1] eduroam.cz [eduroam.cz] [online]. [cit. 2020-10-19]. Dostupné z: https://www.eduroam.cz/

[2] IROP - Ministerstvo pro místní rozvoj ČR - Informace k eduroam v rámci výzev IROP [online]. [cit. 2020-10-28]. Dostupné z: https://irop.mmr.cz/cs/ostatni/web/novinky/informace-k-eduroam-v-ramci-vyzev-irop/

[3] eduroam - zvětšení pokrytí díky projektům IROP [online]. [cit. 2020-10-28]. Dostupné z: https://konference.cesnet.cz/prezentace2019/sal3/1_JanTomasek.pdf

[4] eduroam.cz [eduroam.cz] [online]. [cit. 2020-11-14]. Dostupné z: https://www.eduroam.cz/_media/cs/spravce/pripojovani/typicke-zapojeni-org-do-eduroamu.png

[5] eduroam.cz [eduroam.cz] [online]. [cit. 2020-11-14]. Dostupné z: https://www.eduroam.cz/_media/cs/spravce/pripojovani/sponly_zapojeni.png

[6] eduroam.cz [eduroam.cz] [online]. [cit. 2020-10-20]. Dostupné z: https://www.eduroam.cz/_media/cs/spravce/autentizace_802_1x.png

[7] eduroam.cz [eduroam.cz] [online]. [cit. 2020-10-21]. Dostupné z: https://www.eduroam.cz/_media/cs/spravce/hierachicka_infrastruktura.png

[8] Ipsec-esp-tunnel-and-transport.svg [Wikipedia] [online]. [cit. 2021-04-08]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/6/64/Ipsec-esp-tunnel-and-transport.svg

[9] Network Policy Server (NPS) — Microsoft Docs [online]. [cit. 2020-11-28]. Dostupné z: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top

[10] Virtualizace CESNET [Virtualizace] [online]. [cit. 2021-03-29]. Dostupné z: https://virtualizace.cesnet.cz/

[11] Windows Defender Firewall with Advanced Security (Windows 10) - Windows security [online]. [cit. 2021-04-14]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security

[12] Netsh AdvFirewall MainMode Commands [online]. [cit. 2021-04-28]. Dostupné z: https://winintro.ru/netsh_technicalreference.en/html/742524e0-a905-4188-8f8e-db13a0ff95ab.htm

[13] Netsh AdvFirewall Consec Commands [online]. [cit. 2021-04-28]. Dostupné z: https://winintro.ru/netsh_technicalreference.en/html/8975bcb7-4046-418b-9183-0edce4fb6c60.htm

[14] Seznam implementačních firem pro eduroam [eduroam.cz] [online]. [cit. 2021-05-05]. Dostupné z: https://www.eduroam.cz/cs/spravce/pripojovani/seznam_implementatoru

Příloha **A**

Seznam použitých zkratek

CESNET Czech Education and Scientific NETwork

IdP Identity Provider

SP Service Provider

XML Extensible markup language

NPS Network Policy Server

MS Microsoft

SW Software

CA Certifikační autorita

TCS Trusted Certificate Service

Příloha **B**

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `doc` ..... adresář s vytvořenou dokumentací
  - `Instalace certifikátů [eduroam.cz].pdf`
  - `Nastavení Firewall [eduroam.cz].pdf`
  - `Konfigurace IPsec - rozšířená [eduroam.cz].pdf`
  - `Konfigurace IPsec [eduroam.cz].pdf`
  - `Active Directory [eduroam.cz].pdf`
  - `Microsoft Network Policy Server pro eduroam [eduroam.cz].pdf`
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF
  - `thesis.ps` ..... text práce ve formátu PS