Smlouva o spolupráci
při řešení výzkumného projektu č. 597/2017

uzavřená podle ustanovení § 1746 odst. 2 a souv. zákona č. 89/2012 Sb.,
občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník")

I.
Smluvní strany

CESNET, zájmové sdružení právnických osob
se sídlem: Zikova 4, 160 00 Praha 6
zapsáno: ve spolkovém rejstříku vedeném Městským soudem v Praze pod spis. značkou L 58848
IČ: 63839172
DIČ: CZ63839172
bankovní spojení: Komerční banka Praha 6, č. účtu: [redacted]
zastoupený: Ing. Janem Gruntorádem, CSc., ředitelem
(dále jen CESNET)

na straně jedné

a

Vysoká škola báňská – Technická univerzita Ostrava, Centrum informačních technologií
se sídlem: 17. listopadu 15, Ostrava-Poruba, 708 33
IČ: 61989100
DIČ: CZ61989100
bankovní spojení: ČSOB, č.ú.: [redacted]
zastoupená: prof. Ing. Ivo Vondrákem, CSc., rektorem
(dále jen Organizace)

na straně druhé

uzavírají níže uvedeného dne, měsíce a roku tuto smlouvu o spolupráci:

II.
Cíl spolupráce

1. Cílem spolupráce smluvních stran je zefektivnění evidence přístupů do počítačové sítě.
2. Tato spolupráce vychází z právního vztahu mezi CESNETem, jako sdružením a Organizací, jako řádným členem tohoto sdružení.

III.

Předmět smlouvy

1. Předmětem této smlouvy je spolupráce smluvních stran v rámci řešení projektu č. 597/2017, jehož hlavním cílem je umožnit rychlejší komunikaci a řešení opakujících se uživatelských problémů souvisejících s připojením vlastních zařízení do sítě (WiFi, VPN, pevné zásuvky s ověřováním přes IEEE 802.1x), se kterými se lze setkat při poskytování uživatelské podpory.
2. Výsledky a výstupy projektu budou prezentovány v závěrečné zprávě řešení projektu. Zpráva bude umístěna na stránkách organizace.
3. Technická zpráva bude po ukončení projektu publikována na webových stránkách pracoviště řešitele projektu.

IV.
Práva a povinnosti smluvních stran

1. Hlavním řešitelem za organizaci je Ing. Martin Pustka, Ph.D., který je v Organizaci v pracovním poměru.
2. Organizace zajistí pro řešení projektu institucionální zabezpečení a finanční prostředky ve výši 94.000,- Kč (slovy devadesátčtyřitisíc korun českých) bez DPH.
3. CESNET poskytne na řešení projektu finanční prostředky v celkové výši 177.000,- Kč, (slovy stosedmdesátsedmtisíc korun českých) bez DPH.
4. Výše finančních prostředků stanovených v odstavci 3 nesmí být překročena.
5. CESNET uhradí Organizaci ostatní neinvestiční náklady spojené s řešením projektu v celkové výši 177.000,- Kč bez DPH, a to na základě faktur – daňových dokladů vystavených Organizací. Tato úhrada bude provedena po úspěšném ukončení projektu.
6. Dokumentace Projektu č. 597/2017 je nedílnou součástí této smlouvy.
7. Výsledky spolupráce, včetně jejich publikace a prezentace, mají právo užívat obě smluvní strany při dodržení ustanovení autorského zákona č. 121/2000 Sb., v platném znění, zejména § 58 cit. zákona o zaměstnaneckém díle.

V.
Způsob platby a platební podmínky

1. Čerpání finančních prostředků poskytnutých CESNETem je možné zahájit po podpisu této smlouvy oběma smluvními stranami.
2. Lhůta splatnosti faktury – daňového dokladu je 14 dnů od doručení CESNETu. Daň z přidané hodnoty bude účtována v zákonem stanovené výši.
3. Pokud nebude naplněn cíl projektu, zavazuje se Organizace vrátit zpět na účet CESNETu finanční prostředky poskytnuté dle čl. IV. odst. 5.

VI.
Závěrečná ustanovení

1. Tato smlouva se uzavírá na dobu určitou, a to od podpisu smlouvy oběma smluvními stranami do ukončení řešení Projektu č. 597/2017. Navrhovaná doba trvání projektu je maximálně 12 měsíců. V případě uzavření dohody o prodloužení doby trvání projektu se automaticky prodlužuje o stejnou dobu i platnost a účinnost této smlouvy. Platnost a účinnost této smlouvy je dána dnem podpisu obou smluvních stran.
2. Tato smlouva může být ukončena vzájemnou dohodou smluvních stran nebo odstoupením od smlouvy v případě závažného porušení povinností stanovených touto smlouvou, nebo z důvodů uvedených v občanském zákoníku. Odstoupení od smlouvy nabývá účinnosti dnem doručení písemného oznámení o odstoupení druhé smluvní straně.
3. Změny a doplňky této smlouvy mohou být prováděny pouze formou písemných číslovaných dodatků, odsouhlasených oběma smluvními stranami.
4. Smluvní strany se zavazují řešit případné spory vzájemnou dohodou.
5. Výsledky projektu posoudí hodnotící komise a smluvní strany se zavazují její rozhodnutí respektovat.
6. Tato smlouva je vyhotovena ve dvou stejnopisech s platností originálu, každá strana obdrží jedno paré.
7. Smluvní strany prohlašují, že si text smlouvy přečetly, s jejím obsahem bezvýhradně souhlasí a na důkaz toho připojují podpisy svých oprávněných zástupců.

V Praze dne 01. 06. 2017

[redacted]

.....

[redacted]

za Organizaci

FOND ROZVOJE CESNET, z.s.p.o. LIST A

Agentura Rady Fondu rozvoje CESNET, z.s.p.o., Zikova 1903/4, 166 35 Praha 6
tel. 234 680 236, e-mail: agentura-fr@cesnet.cz

PODACÍ LIST PROJEKTU

Název projektu:
Evidence přístupů do počítačové sítě.

Č. j. fondu 594 /2017

Oblast: I.

Tematický okruh: A.

Celkový počet řešitelů:

Navrhovaná délka trvání projektu (počet měsíců) : 12

Finanční prostředky požadované z FR CESNET (v tis. Kč bez DPH):

IV: NIV: 177 Celkem: 177

Hlavní řešitel:

Příjmení, jméno, titul: Ing. Martin Pustka, Ph.D.

Název člena sdružení: Vysoká škola Báňská - Technická univerzita Ostrava

Ústav AV / org. součást VŠ: Centrum informačních technologií

Sídlo: 17.listopadu 15, Ostrava-Poruba, 708 33

Telefon:

E-mail: [redacted]

Anotace projektu (česky i anglicky):

Cílem projektu je umožnit rychlejší komunikaci a podporu při řešení uživatelských problémů souvisejících s připojením vlastních zařízení do sítě (WiFi, VPN, pevné zásuvky s ověřováním přes IEEE 802.1x).

Pro tyto účely budou vytvořeny programové prostředky, které budou integrovány do námi provozovaných RADIUS serverů (Radiator, FreeRadius). Data budou ukládána a zpracovávána v SQL databázi a zpřístupňována technických pracovníkům IT podpory (bezpečnostní tým, IT Helpdesk apod.).

he project goal is to enhance speed of communication and user support when troubleshooting internet onnection secured by IEEE 802.1x. For this purpouse we want to develop software which will be tegrated into our RADIUS servers (Radiator, FreeRadius). The collected data will be saved in SQL tabase which IT personnel can access (security team, IT helpdesk etc.).

FOND ROZVOJE CESNET, z.s.p.o. **LIST B**

Agentura Rady Fondu rozvoje CESNET, z.s.p.o., Zikova 1903/4, 166 35 Praha 6

PROHLÁŠENÍ STATUTÁRNÍHO ZÁSTUPCE AV ČR NEBO VŠ - ČLENA SDRUŽENÍ CESNET

Název projektu
Evidence přístupů do počítačové sítě.

Č. j. fondu 597 /2017

Hlavní řešitel: Ing. Martin Pustka, Ph.D.

Název člena: Vysoká škola Báňská - Technická univerzita Ostrava

Ústav AV / org.součást VŠ: Centrum informačních technologií

Finanční prostředky požadované z FR CESNET (v tis. Kč. bez DPH):

IV:	NIV:	177	Celkem:	177

Vyjádření statutárního zástupce VŠ nebo AV ČR - člena sdružení CESNET :

Prohlašuji, že řešitel je v hlavním pracovním poměru v naší organizaci a že pro řešení projektu poskytne (název organizace) Vysoká škola Báňská - Technická univerzita Ostrava. institucionální zabezpečení a finanční příspěvek ve výši 94000 Kč.

7. 2. 2017

Datum

[redacted]

FOND ROZVOJE CESNET, z.s.p.o. LIST C

Agentura Rady Fondu rozvoje CESNET, z.s.p.o., Zikova 1903/4, 166 35 Praha 6

IDENTIFIKAČNÍ LIST SPOLUŘEŠITELE - ČLENA SDRUŽENÍ

Název projektu:
Evidence přístupů do počítačové sítě.

Č. j. fondu 597 /2017

Hlavní řešitel: Ing. Martin Pustka, Ph.D.

Spoluřešitel:

Příjmení, jméno, titul:	Ing. Pavel Jeníček
Název člena sdružení:	Vysoká škola Báňská - Technická univerzita Ostrava
Ústav AV / org. součást VŠ:	Centrum informačních technologií
Sídlo:	17.listopadu 15, Ostrava-Poruba, 708 33

PROHLÁŠENÍ SPOLUŘEŠITELE:

Souhlasím, aby uvedený hlavní řešitel řídil práce na projektu a disponoval přidělenými finančními prostředky.

Prohlašuji, že jsem uvedl úplné a pravdivé údaje a beru na vědomí, že v opačném případě nebo při porušení obecně uznávaných zásad vědeckopedagogické etiky nebo pro hrubé závady při řešení projektu a hospodaření s přidělenými finančními prostředky a při kontrole výsledků podle čl.15 e) Konkurzního řádu Rady Fondu rozvoje CESNET, z.s.p.o. mohu být vyloučen z účasti na výběrovém řízení.

Souhlasím s tím, aby Rada fondu rozvoje CESNET používala osobní údaje uvedené v této žádosti při zpracování a evidenci mého projektu ve výběrovém řízení vypsaném pro rok 2017.

[redacted]

7. 12. 2017
Datum

VYJÁDŘENÍ VEDOUCÍHO PRACOVNÍKA SPOLUŘEŠITELE:

Souhlasím s účastí spoluřešitele na projektu a poskytnu mu institucionální zabezpečení.

[redacted]

7.12. 2017
Datum

Podpis vedoucího pracovníka

FOND ROZVOJE CESNET, z.s.p.o. **LIST C**

Agentura Rady Fondu rozvoje CESNET, z.s.p.o., Zikova 1903/4, 166 35 Praha 6

IDENTIFIKAČNÍ LIST SPOLUŘEŠITELE - ČLENA SDRUŽENÍ

Název projektu:
Evidence přístupů do počítačové sítě.

Č. j. fondu 594 /2017

Hlavní řešitel: Ing. Martin Pustka, Ph.D.

Spoluřešitel:

Příjmení, jméno, titul:	Ing. Jiří Grygárek
Název člena sdružení:	Vysoká škola Báňská - Technická univerzita Ostrava
Ústav AV / org. součást VŠ:	Centrum informačních technologií
Sídlo:	17.listopadu 15, Ostrava-Poruba, 708 33

PROHLÁŠENÍ SPOLUŘEŠITELE:

Souhlasím, aby uvedený hlavní řešitel řídil práce na projektu a disponoval přidělenými finančními prostředky.

Prohlašuji, že jsem uvedl úplné a pravdivé údaje a beru na vědomí, že v opačném případě nebo při porušení obecně uznávaných zásad vědeckopedagogické etiky nebo pro hrubé závady při řešení projektu a hospodaření s přidělenými finančními prostředky a při kontrole výsledků podle čl.15 e) Konkurzního řádu Rady Fondu rozvoje CESNET, z.s.p.o. mohu být vyloučen z účasti na výběrovém řízení.

Souhlasím s tím, aby Rada fondu rozvoje CESNET používala osobní údaje uvedené v této žádosti při zpracování a evidenci mého projektu ve výběrovém řízení vypsaném pro rok 2017.

7. 2. 2017
Datum

[redacted]
Podpis spoluřešitele

VYJÁDŘENÍ VEDOUCÍHO PRACOVNÍKA SPOLUŘEŠITELE:

Souhlasím s účastí spoluřešitele na projektu a poskytnu mu institucionální zabezpečení.

7. 2. 2017
Datum

[redacted]
Podpis vedoucího pracovníka

FOND ROZVOJE CESNET, z.s.p.o. **LIST C**

Agentura Rady Fondu rozvoje CESNET, z.s.p.o., Zikova 1903/4, 166 35 Praha 6

IDENTIFIKAČNÍ LIST SPOLUŘEŠITELE - ČLENA SDRUŽENÍ

Název projektu:
Evidence přístupů do počítačové sítě.

Č. j. fondu 597 /2017

Hlavní řešitel: Ing. Martin Pustka, Ph.D.

Spoluřešitel:

Příjmení, jméno, titul:	Jakub Kalnik
Název člena sdružení:	Vysoká škola Báňská - Technická univerzita Ostrava
Ústav AV / org. součást VŠ:	Centrum informačních technologií
Sídlo:	17.listopadu 15, Ostrava-Poruba, 708 33

PROHLÁŠENÍ SPOLUŘEŠITELE:

Souhlasím, aby uvedený hlavní řešitel řídil práce na projektu a disponoval přidělenými finančními prostředky.

Prohlašuji, že jsem uvedl úplné a pravdivé údaje a beru na vědomí, že v opačném případě nebo při porušení obecně uznávaných zásad vědeckopedagogické etiky nebo pro hrubé závady při řešení projektu a hospodaření s přidělenými finančními prostředky a při kontrole výsledků podle čl.15 e) Konkurzního řádu Rady Fondu rozvoje CESNET, z.s.p.o. mohu být vyloučen z účasti na výběrovém řízení.

Souhlasím s tím, aby Rada fondu rozvoje CESNET používala osobní údaje uvedené v této žádosti při zpracování a evidenci mého projektu ve výběrovém řízení vypsaném pro rok 2017.

7.2.2017
Datum

[redacted]
Podpis spoluřešitele

VYJÁDŘENÍ VEDOUCÍHO PRACOVNÍKA SPOLUŘEŠITELE:

Souhlasím s účastí spoluřešitele na projektu a poskytnu mu institucionální zabezpečení.

7.2. 2017
Datum

[redacted]
Podpis vedoucího pracovníka

FOND ROZVOJE CESNET, z.s.p.o. **LIST D**

Agentura Rady Fondu rozvoje CESNET, z.s.p.o., Zikova 1903/4, 166 35 Praha 6

CHARAKTERISTIKA CÍLE PROJEKTU A JEHO PŘEDPOKLÁDANÉHO PŘÍNOSU

Název projektu:
Evidence přístupů do počítačové sítě.

Č. j. fondu 597 /2017

Hlavní řešitel: Ing. Martin Pustka, Ph.D.

KONKRÉTNÍ VÝSTUPY

Výstupem projektu bude funkční systém vč. rozhraní pro jeho obsluhu a také návody, které by měly být aplikovatelné v jiných institucích, zejména pak připojených do infrastruktury sítě CESNET.

V ČEM SPOČÍVÁ PŘÍNOS PROJEKTU

Cílem projektu je postavit takové technické řešení, které nebude výrazně měnit stávající systém autentizace uživatelů v sítích s využitím protokolu 802.1x a zároveň jej bude vhodně doplňovat. Zároveň poskytne možnosti pro omezování přístupů do sítě univerzitnímu CSIRT týmu a také prostředky pro dohled např. pro operátory IT helpdesku.

Uveďte, zda předpokládáte, že výsledkem projektu/jedním z výsledků projektu může být předmět způsobilý ochrany právem duševního vlastnictví (např. vynález, užitný vzor, autorské dílo, počítačový program). Pokud ano, uveďte v návrhu projektu předpokládaný způsob ochrany takového výsledku a zda bude nutné omezení závěrečné zprávy projektu.

VLASTNÍ ROZVOJOVÝ PROJEKT JE PŘIPOJEN (min. 3 strany)

Osnova:
a) Současný stav řešeného problému
b) Cíle řešení
c) Způsob řešení
d) Prezentace výsledků
e) Charakteristika řešitelského kolektivu,
odborný životopis řešitele a spoluřešitelů
f) Navrhovaná doba trvání projektu (počet měsíců) - navrhovaná délka trvání
g) Konkretizace a zdůvodnění jednotlivých požadavků řešitele - položky dlouhodobého majetku (investiční) doložte nabídkou, ostatní položky (neinvestiční) rozepište po jednotlivých položkách v souladu se strukturou na listu E, není třeba dokládat nabídkou

PROHLÁŠENÍ

Uveďte, zda se na financování podaného projektu podílejí další subjekty.

	Zdroj financování	Výše fin. prostředků

FOND ROZVOJE CESNET, z.s.p.o.

LIST E

Agentura Rady Fondu rozvoje CESNET, z.s.p.o., Zikova 1903/4, 166 35 Praha 6

ROZPOČET NÁKLADŮ S PŘIPOJENOU DOKUMENTACÍ

Název projektu:
Evidence přístupů do počítačové sítě.

Č. j. fondu 594 /2017

Hlavní řešitel: Ing. Martin Pustka, Ph.D.

	Spoluúčast nositele	Požadováno z Fondu rozvoje	Náklady celkem (**)
(*) Dlouhodobý hmotný a nehmotný majetek - doložte nabídkou			
Náklady na dlouhodobý hm.a nehm.majetek celkem:	94		94
(*) Ostatní náklady			
Mzdy			
Odměny řešitelům a spoluřešitelům		120	120
Ostatní osobní výdaje (Ostatní mzdové náklady)			
Sociální a zdravotní pojištění		42	42
Knihy, učební pomůcky, odborná dokumentace			
Drobný hmotný majetek			
Drobný nehmotný majetek			
Materiál			
Pronájem zařízení			
Cestovné tuzemské			
Cestovné zahraniční			
Školení			
Ostatní služby			
Režie		15	15
Ostatní (neivestiční) náklady celkem			
Náklady celkem			
Náklady celkem	94	177	271

Veškeré finanční údaje uvádějte v tis. Kč. bez DPH

PROHLÁŠENÍ ŘEŠITELE

Prohlašuji, že jsem uvedl úplné a pravdivé údaje a beru na vědomí, že v opačném případě nebo při porušení obecně uznávaných zásad vědeckopedagogické etiky nebo pro hrubé závady při řešení projektu a hospodaření s přidělenými finančními prostředky a při kontrole výsledků podle čl.15 e) Konkurzního řádu Rady Fondu rozvoje CESNET, z.s.p.o. mohu být vyloučen z účasti na výběrovém řízení.

Souhlasím s tím, aby Rada fondu rozvoje CESNET používala osobní údaje uvedené v této žádosti při zpracování a evidenci mého projektu ve výběrovém řízení vypsaném pro rok 2017.

6.2.2017
Datum

[redacted]
Podpis

(*) Přesně rozepište v návrhu projektu podle jednotlivých položek v částkách bez DPH a včetně DPH

(**)Včetně příspěvku VŠ či fakulty nebo ústavu AV ČR, ale bez případných příspěvků z jiných zdrojů

Evidence externích přístupů do počítačové sítě

Současný stav řešeného problému

V současné době jsou přístupy uživatelů přes WiFi, VPN a také přístupy uživatelů do pevné sítě ověřovány na centrálních RADIUS serverech.

Radius servery jsou provozovány v univerzitním datovém centru VŠB-TUO a jsou integrovány do infrastruktury *eduroam*.

WiFi síť VŠB-TUO obsahuje cca 450 přístupových bodů. Ve špičkách bývá do této sítě současně připojeno okolo 5000 zařízení. Unikátní počet zařízení pak dosahuje 13300 zařízení a unikátní počet uživatelů je cca 7200.

Služby VPN připojení využívají řádově jednotky tisíc uživatelů. Obvykle využívá a na VPN koncentrátor bývá připojeno současně 150-200 uživatelů.

Ověřování uživatelů v pevné síti je realizováno v pokojích univerzitních kolejí. Zde se mohou připojit jak studenti VŠB-TUO, tak i studenti jiných institucí zapojených do projektu *eduroam*. Celkový počet uživatelů je v současné době cca 6000.

Centrální RADIUS servery jsou tvořeny dvěma servery s komerčním open-source systémem RADIATOR a jedním volně dostupným open-source FreeRADIUS serverem. Ověřování uživatelů probíhá na univerzitních LDAP serverech, popř. na národních eduroam radius serverech v případě ne-VŠB uživatelů.

Mezi nejčastější úlohy, které správa sítě řeší, je dohledávání bezpečnostních incidentů a také dohledávání technických problémů souvisejících s připojováním do sítě. Podkladem pro dohledávání jsou především informace zaznamenáváné všemi RADIUS servery.

Zdrojem incidentů bývají externí hlášení nebo interní IDS/IPS systémy univerzity. U bezpečnostních incidentů jsou obvykle zaznamenány IP adresy a časy, ve kterých byl

incident detekován. Vzhledem k redundancím RADIUS serverů je potřeba často tyto údaje dohledávat na více místech.

Při pozitivně ověřených bezpečnostních incidentech přistupují členové CSIRT týmu po zvážení také k blokacím uživatelů nebo konkrétních zařízení, která jsou v síti identifikována MAC adresou. Uživatele v takových případech informujeme o realizovaných krocích a v součinnosti s nimi řešíme konkrétní případ. Po jeho vyřešení dochází k opětovnému povolení provozu. Blokace jsou realizovány v konkrétním zařízení (např. Wireless kontroler, RADIUS server, firewall).

Většina funkčních problémů je uživateli hlášena prostřednictvím IT Helpdesku. Základní diagnostiku mohou provádět již operátoři IT helpdesku, Ti však nejsou v současné době ve výše uvedených případech schopni přímo získat ani analyzovat údaje v logovacích souborech serverů.

Centrum informačních technologií VŠB-TUO provozuje helpdeskové pracoviště, kde je v pracovní dobu 7-17h dostupný minimálně jeden pracovník. Operátoři mají přístup do některých základních agend (ověření hesla a jeho platnosti, identity, vztahů atd.). Incidenty v oblastech výše popsaných v současné době nemohou řešit, ale při nasazení vhodného nástroje by byli schopni ověřit, popř. rovnou vyřešit některé základní situace sami už při prvotní komunikaci s uživateli.

CSIRT tým VŠB-TUO byl založen v r.2008 a jeho členy jsou převážně pracovníci síťového oddělení doplnění o některé další technické pracovníky Centra informačních technologií. V uvedených oblastech jsou však v současné době schopni dohledávat a blokovat pouze síťoví specialisté a ne všichni členové CSIRT týmu.

Centralizované WiFi řešení je postaveno na technologiích Cisco, kde jsou využívány řídicí wireless moduly. Tyto řídicí moduly komunikují přímo s Radius servery.

Pro VPN přístupy jsou využívány prvky Cisco ASA. Podporujeme přístup k VPN prostřednictvím protokolu IPv6 a uživatelům jsou v rámci VPN propojení přidělovány také IPv6 adresy, což není v současnosti není ještě zcela běžně poskytovaná služba.

Uživatelé na kolejích jsou připojeni prostřednictvím přístupových FE přepínačů, směrování sítí pak probíhá na centálním L3 přepínači. Ověřování uživatelů na radius serverech zprostředkovávají přístupové přepínače, kterých je na kolejích VŠB nasazeno celkem cca 100.

Cíle řešení

Hlavním cílem projektu je umožnit rychlejší komunikaci a řešení opakujících se uživatelských problémů souvisejících s připojením vlastních zařízení do sítě (WiFi, VPN, pevné zásuvky s ověřováním přes IEEE 802.1x), se kterými se lze setkat při poskytování uživatelské podpory.

Hlavní cíle řešení jsou následující:

- minimalizovat nutnost participace specialistů při řešení přímé uživatelské podpory
- realizovat systém, který nám zajistí rychlé vyhledání uživatele nebo zařízení
- zajistit podporu automatizace, která nám v budoucnu umožní párovat automaticky incidenty (IP adresa a čas) s identitou uživatele
- realizovat webové rozhraní, které mohou využívat techničtí pracovníci a které umožní jednoduše blokovat zařízení nebo uživatele v počítačové síti
- realizovat webové rozhraní, které mohou využívat operátoři Helpdesku, popř. správci na fakultách, a ve kterém mohou ověřit, zda uživatel není blokován
- realizovat webové rozhraní, kterou mohou využívat operátoři bezpečnostního týmu k dohledání uživatelů a zařízení a které mohou využít pro blokaci zařízení bez asistence síťových nebo IDM administrátorů
- systém musí podporovat v maximální možné míře i protokol IPv6
- systém musí být otevřen a musí do budoucna umožnit snadnou integraci do jiných aplikací (např. pro provázání s IDS/IPS; pro kontrolu přístupů do IS, zda jsou realizovány opravdu uživateli z jejich zařízení apod.)

Budeme se snažit o vývoj dostatečně obecného řešení, které bude možno aplikovat po mírných úpravách i v jiném prostředí a nebude vysloveně vázané na konkrétní výrobce.

Celé řešení chceme zdokumentovat i publikovat tak, aby bylo použitelné i v jiných institucích a sítích.

Způsob řešení

Plánujeme vyvinout programový kód, které lze integrovat do RADIUS serverů. V programovém balíku Radiator je možno využít tzv. *account hooků*, resp. systém FreeRadius podporuje tzv. *SQL moduly*.

Využitím těchto API budeme schopni přebírat údaje autentizačních serverů a vkládat je do centrální databáze.

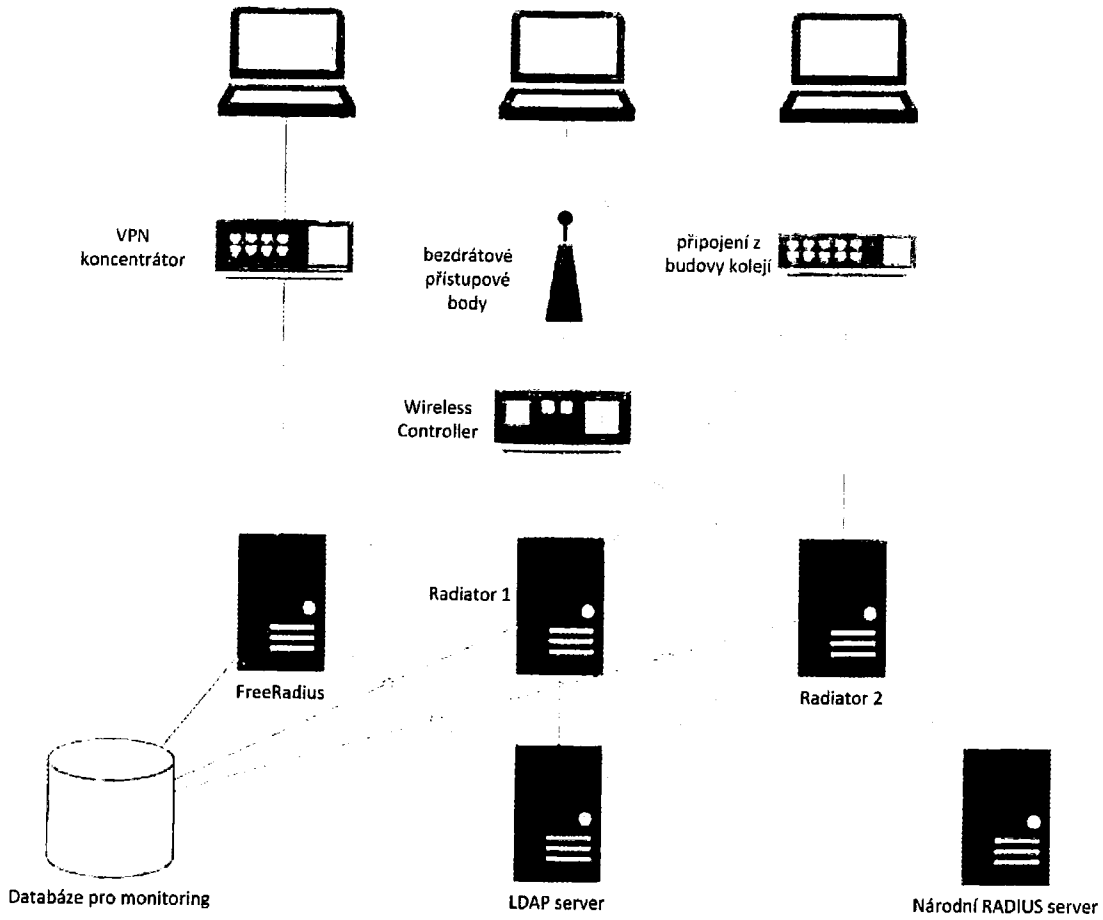
Krom toho lze podobná API využít i pro realizaci tzv. *blacklistů*. Plánujeme tak už v procesu ověřování přístupu uživatele explicitně ověřovat, zda příslušné zařízení nebo uživatel není v síti blokován.

Pro tyto účely bude zřízena dedikovaná databáze, která bude realizována ve virtualizovaném systému. Samotné webové rozhraní a obslužné utility budou realizovány ve druhém virtualizovaném systému.

Očekáváme poměrně velký datový tok informací do/z databáze. Proto nechceme sdílet výkon této databáze s jinými projekty. Vzhledem k poměrně velkému množství záznamů předpokládáme, že budeme pravidelně tyto záznamy agregovat a optimalizovat jejich uložení. To zejména proto, že jedno uživatelské sezení obsahuje v průběhu několik záznamů a nás pro výše uvedené účely zajímá zejména kdy započalo, kdy skončilo a případně sumarizované údaje vztahující se k celému sezení).

Není ve všech případech snadné získat informace o používané IPv6 adrese uživatele. Proto předpokládáme vývoj utilit, které budou z prvků sítě získávat informace o IPv6 a MAC adresách a bude naší snahou tyto informace korelovat s IPv4 a konkrétními uživateli.

Pro řešení předpokládáme využití open-source prostředků, zejména pak OS Debian GNU/Linux, PostgreSQL, web server Apache, programové prostředky Bash/Perl/Python.



Obr.: Schéma vazeb a komunikace jednotlivých prvků systému.

Pro účely projektu bude pořízen fyzický server, který bude integrován do univerzitního datového centra, na něm budou zprovozněny centralizované prostředky virtualizace (VMWARE, zálohovací systém Veeam) a všechny další potřebné prvky realizovaného systému. Předpokládáme, že bude obsahovat 1xCPU, 32 GB RAM, cca 1TB lokálních diskových kapacit v HW RAIDu. Níže uvedená přesná specifikace serveru je pro doložení ceny, při nákupu bude proveden nediskriminační výběr napříč trhem se zachováním ceny nakupovaného serveru.

Pro řešení bude pořízen následující HW a licence:

- server s výše popsanými parametry v celkové ceně 66 tis. Kč bez DPH; přiložená cenová nabídka je sestavou serveru SuperMicro, která byla generována prostřednictvím konfigurátoru serveru,

- licence VMWARE (https://www.senetic.cz/product/VS6-STD-A) v celkové ceně 15 tis. Kč bez DPH
- licence Veeam (https://www.senetic.cz/product/E-VBRSTD-VS-P0000-00) v celkové ceně 13 tis. Kč vč. DPH

(ceny platné k 6.2.2017).

Kategorie	Produkt	Ks
Procesor	Intel Xeon E5-2603v4 - 1,7GHz@6,4GT 15MB cache, 6core, 5W,LGA2011	[redacted]
Základní deska	X10DRi 2S-R3,3PCI-E16(g3)3PCI-E8,2GbE, 10sATA3,16DDR4-2400,IPMI	
Paměť	8GB 2400MHz DDR4 ECC Registered 1R×4, LP(31mm), Samsung	
Ethernet	Síťová karta Intel i350 2× GbE na zákl. desce	
VGA on board	Aspeed AST2400 with 16MB VRAM	
Management	IPMI 2.0 modul s KVM-over-LAN na základní desce	
Slot #1	Supermicro AOC-SAS2LP-H8iR-16DD(2108) SAS2RAID(0/1/5/6/10) 2×8087,exp:16HD,512MB,PCI-E8 g2,LP +5 500	
Raid - baterie	Supermicro BTR-0018L - baterie (BBU) pro SAS H4iR/H8iR (LSI2108) (1 rok záruka) +5 262	
HDD/SSD #1	Intel® SSD DC S3510 Series 80GB SATA3 6Gbps 2,5" 68/8kIOPS 0,3DWPD	
DVDRW	DVD±R/±RW/RAM LG GTC0N - SLIM interní mechanika	
Skříň	SC213A-R900LP 2U eATX13 16SFF(4×SFF-8087),5,25",slimCD,LP,rPS 900W,černý	
Chladič	SNK-P0048AP4 Aktivní 2U pro 1P/2P LGA2011 čtvercový i úzký ILM (52dBA,8500rpm,4pin) + (CAS BK	
SLA pro HW	Zásah 3r NBD v autorizovaném servisním středisku	
Montáž	Montáž serveru	

Celková cena sestavy: 65941 Kč bez DPH / 79789 Kč vč. DPH

(cena sestavy z http://www.abacus.cz, ze dne 6.2.2017)

Fáze projektu

1.-2. měsíc od započetí projektu

V tomto prvním období započaty práce na realizaci projektu, proběhne nákup HW vybavení a instalace SW částí.

Odhadovaná časová náročnost je 10 dní.

3.-9. měsíc od započetí projektu

V této fázi projektu budou realizovány práce v následujících oblastech:

- vývoj programových balíků
- provozní testování
- optimalizace využití prostředků

Odhadovaná časová náročnost je 40 člověkodní.

10.-12. měsíc od započetí projektu

V této fázi projektu budou probíhat finální práce, rutinní provoz a také tvorba dokumentace a závěrečné zprávy.

Odhadovaná časová náročnost je 15 člověkodní.

Prezentace výsledků

Výsledky a výstupy projektu budeme prezentovat v závěrečné zprávě řešení projektu, která bude veřejně dostupná na WWW stránkách fondu i na našich webových stránkách, kde bude umístěna i technická zpráva. Zpráva bude umístěna na stránkách VŠB-TU Ostrava.

Po ukončení projektu předpokládáme využití našich poznatků i dalšími organizacemi zapojenými do sdružení CESNET.

Zdrojové kódy budou publikovány na některém ze serverů určeným k publikování zdrojových kódů (např. github, gitlab).

Charakteristika řešitelského kolektivu

Ing. Martin Pustka, Ph.D.

Zaměstnanec Centra informačních technologií VŠB-TUO, kde působí jako vedoucí oddělení IT infrastruktury. Profesně se zabývá správou počítačové sítě TUONET a správou unixových systémů a technických prostředků datového centra. Je členem bezpečnostního týmu VŠB-TUO.

Ing. Pavel Jeníček

Zaměstnanec Centra informačních technologií VŠB-TUO, kde působí jako správce počítačové sítě a SAN infrastruktury. Je členem bezpečnostního týmu VŠB-TUO a působí také v Cisco akademii při VŠB-TUO.

Ing. Jiří Grygárek

Zaměstnanec Centra informačních technologií VŠB-TUO, kde působí jako správce počítačové sítě a SAN infrastruktury. Je členem bezpečnostního týmu VŠB-TUO a působí také v Cisco akademii při VŠB-TUO.

Jakub Kalník

Zaměstnanec Centra informačních technologií VŠB-TUO, kde působí jako administrátor počítačové sítě. Je členem bezpečnostního týmu VŠB-TUO.

Navrhovaná doba řešení projektu

Navrhovaná doba trvání projektu je 12 měsíců.

Konkretizace a zdůvodnění požadavků řešitele

Projekt předpokládá využití stávající technické infrastruktury VŠB-TUO, pro potřeby projektu budou pořízeny níže uvedené položky. Pokud není uvedeno jinak, tak ceny jsou uváděny

bez DPH.

Ceny investičních nákladů jsou použity z cenové nabídky nebo průzkumu trhu platné v době podání projektu. Ceny neinvestičních nákladů jsou použity z běžně dostupných cen.

Investiční náklady

Z prostředků VŠB-TU Ostrava budou pořízeny:

- 1 ks serverového systému, vč. licence pro VMWARE a 1-roční licence pro zálohovací systém Veeam

v celkové výši 94 tis. Kč bez DPH.

Neinvestiční náklady

Z prostředků FR CESNETu budou hrazeny náklady:

- Odměny řešitelům v celkové výši 120 tis. Kč a zdravotní a sociální pojištění ve výši 42 tis. Kč, které budou vyplaceny po úspěšné obhajobě projektu (celkem 162 tis. Kč).

- Režijní náklady v celkových nákladech 15 tis. Kč. Budou použity zejména na administrativu projektu, společné schůzky řešitelů a případné další projektové náklady.

Z prostředků FR CESNETu budou hrazeny náklady v celkové výši 177 tis. Kč.

Náklady na jeden pracovní člověkoden vč. odvodů odhadujeme na 2500 Kč, tj. 65 člověkodní. Časová náročnost řešení je uvedena u rozpisu jednotlivých částí projektu.

Vypořádání majetku pořízeného v rámci projektu

Investiční náklady budou plně hrazeny z prostředků VŠB-TU Ostrava.