Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Zabezpečený přístup k lokální počítačové síti

Bc. Jan Kočiš

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Jan Kočiš

Informatika

Název práce

Zabezpečený přístup k lokální počítačové síti

Název anglicky

Secure access to local area network

Cíle práce

Hlavním cílem práce je souhrn a porozumění principů, na kterých jsou založeny autentizační metody, jejich využití k řízenému přístupu k lokální počítačové síti a aplikace získaných poznatků v praxi.
Dílčí cíle diplomové práce jsou:
- vysvětlit a popsat základní terminologii autentizace a procesů s ní souvisejících
- osvětlit teoretické principy, na kterých autentizace funguje a její využití
- analyzovat obecné požadavky na zabezpečení přístupu k lokální síti
- implementace vlastního řešení pro autentizaci a autorizaci přístupu k lokální síti s využitím aktuálních technologií

Metodika

Metodika řešené problematiky diplomové práce je založena na studiu a analýze odborných informačních zdrojů. Vlastní řešení je realizováno formou návrhu a implementace konkrétního zabezpečeného přístupu k lokální počítačové síti. Na základě syntézy teoretických poznatků a výsledků vlastního řešení budou formulovány závěry diplomové práce.

Doporučený rozsah práce

50 – 60 stran

Klíčová slova

bezpečnost, AAA, autentizace, autorizace, accounting, autentizační metody, zabezpečený přístup, 802.1x

---

Doporučené zdroje informací

BALLAD, B., BALLAD, T. a BANKS, E. K. Access control, authentication, and public key infrastructure: the definitive guide to firewalls, VPNs, routers, and intrusion detection systems. Sudbury, MA : Jones. 2011. str. 391. ISBN 978-0-7637-9128-5.

DOUCEK, P. *Řízení bezpečnosti informací : 2. rozšířené vydání o BCM.* Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

STEWART, J. M, MATTORD, H. J. a GREEN, A. Network security, firewalls, and VPNs: the definitive guide to firewalls, VPNs, routers, and intrusion detection systems. 2nd ed. Burlington, Mass: Jones. 2014. str. 346. ISBN 978-1-284-03167-6.

Předběžný termín obhajoby

2015/16 LS – PEF

Vedoucí práce

Ing. Čestmír Halbich, CSc.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 28. 10. 2015

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 02. 03. 2016

Čestné prohlášení

Prohlašuji, že svou diplomovou práci „*Zabezpečený přístup k lokální počítačové síti*“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce, s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury 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 30.3.2016 _____

Poděkování

Rád bych na tomto místě poděkoval vedoucímu diplomové práce panu Ing. Čestmíru Halbichovi, CSc. za vedení a cenné rady při vypracování diplomové práce. Zvláštní poděkování patří mým rodičům a partnerce, kteří mi byli velkou oporou v průběhu studia.

Zabezpečený přístup k lokální počítačové síti

Souhrn

Diplomová práce se zabývá problematikou zabezpečení přístupů k lokální počítačové síti. Práce si klade za cíl charakterizovat teoretická východiska řízeného přístupu k počítačové síti, mezi která patří bezpečnostní principy, doporučené praktiky, autentizační metody, síťové protokoly a procesy s nimi související. Nedílnou součástí práce je na základě těchto poznatků realizovat zabezpečení přístupu k lokální počítačové síti v reálném prostředí.

První část charakterizuje teoretické principy, na kterých je založen návrh a implementace celého sytému.

Praktická část práce se zabývá implementací konkrétního řešení zabezpečeného přístupu k lokální počítačové síti ve strojírenské společnosti. V první části je představen podnik, jeho prostředí a požadavky. Navazující pasáž zachycuje provedenou analýzu původního stavu a na základě získaných informací shrnuje navržené řešení. Implementace komplexního systému řízeného přístupu k lokální počítačové síti je podrobně popsána v další části. Součástí práce je popis procesu zavádění systému do produkčního provozu, definice akceptačních testů a doporučení pro řešení možných problémů. Závěr kapitoly obsahuje ekonomické aspekty řešení a možné dopady na provoz výpočetních systémů podniku.

Závěrečné zhodnocení shrnuje diplomovou práci, sumarizuje výhody implementovaného systému a rozebírá slabá místa s doporučením pro jeho další rozvoj. Zároveň shledává navržený zabezpečený přístup k lokální počítačové síti jako vhodný, bezpečný a praktický způsob řízeného přístupu k místním síťovým prostředkům.

Klíčová slova: bezpečnost, AAA, autentizace, autorizace, accounting, autentizační metody, zabezpečený přístup, 802.1X

Secure access to local area network

Summary

This master‘s thesis deals with the field of secure access to the local area computer network. The main aim of the thesis is to characterize theoretical background of controlled access to computer networks, which includes security principles, recommended practices, authentication methods, network protocols and related processes. This thesis also includes practical usage of acquired knowledge by implementing secure access to local area network in a real environment.

The first part characterize the theoretical principles underlying the design and implementation of the entire system.

The practical part deals with the implementation of specific secure access to the local area computer network solution in the engineering company. The first part introduces the company, its environment and requirements. The following section describes performed analysis of the original state and based on the obtained information summarizes the proposed solution. Implementation of the comprehensive system of the controlled access to the local area network is described in detail in the next section. Description of the system deployment into production operation process, the definition of acceptance tests and recommendations for solving of potential issues are part of this work as well. Conclusion chapter contains summary of the system’s economic aspects and the potential impacts on information systems operation in the company.

Final evaluation summarizes the thesis, highlights the benefits of the implemented system and analyses its weak points, with recommendations for further development. It finds the designed secure access to the local network as a suitable, secure and practical way to control access to local network resources.

Keywords: security, AAA, authentication, authorization, accounting, authentication methods, secure access, 802.1X

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍKLADŮ

1 ÚVOD

V současnosti je počítačová bezpečnost velmi důležitým oborem. Autentizace a autorizace jsou v tomto ohledu často zmiňovanými pojmy, kterým ale ne každý správně rozumí. Jen těžko nalezneme komplexní informační systém či technologii, pro kterou by nebyla autentizace základním stavebním kamenem. Bez spolehlivého ověření identity uživatelů nelze považovat jakýkoliv systém za bezpečný. V důsledku špatné implementace pak dochází k nežádoucím průnikům do počítačových systémů a následnému zcizení citlivých a soukromých dat tak, jak jsme tomu v poslední době svědky na globální úrovni.

Běžnou praxí je bohužel situace, kdy uživatelé mohou přistupovat ke zdrojům lokální počítačové sítě bez jakékoliv povinnosti se autentizovat. V takovém případě není možné zjistit, kdo a kdy k počítačové síti přistupoval, ani zamezit síťovým útokům či nežádoucímu přístupu k firemním datům a síťovým prostředkům.

Smyslem práce je souhrn a porozumění principů, na kterých jsou autentizační metody založeny a využití získaných poznatků v praxi při implementaci zabezpečeného přístupu k lokální počítačové síti.

2 CÍL PRÁCE A METODIKA

Diplomová práce je tematicky zaměřena na aktuální možnosti řízeného přístupu uživatelů a zařízení při používání lokálních síťových prostředků.

2.1 Cíl práce

Práce si klade za cíl charakterizovat základní terminologii autentizace, autorizace a procesů s nimi souvisejících. Hlavním cílem práce je souhrn a porozumění principů, na kterých jsou autentizační metody založeny, jejich využití k řízenému přístupu k lokální počítačové síti a aplikace získaných poznatků v praxi. Dílčí cíle diplomové práce jsou:

- Charakterizovat základní terminologii autentizace a souvisejících procesů.
- Osvětlit teoretické principy, na kterých autentizace funguje a její využití.
- Analyzovat obecné požadavky na zabezpečení přístupu k lokální síti.
- Implementace vlastního řešení pro autentizaci a autorizaci přístupu k lokální síti s využitím aktuálních technologií.

2.2 Metodika

Metodika řešené problematiky diplomové práce je založena na studiu a analýze odborných informačních zdrojů. Vlastní řešení je realizováno formou návrhu a implementace konkrétního zabezpečeného přístupu k lokální počítačové síti. Na základě syntézy teoretických poznatků a výsledků vlastního řešení budou formulovány závěry diplomové práce.

3 TEORETICKÁ VÝCHODISKA

3.1 Potřeba zabezpečení přístupů

V dnešní kybernetické době, kdy je Internet běžně využíván jako komunikační médium jednotlivců i společností všech velikostí, se stala bezpečnost mnohem důležitějším faktorem nejen pro uživatele, ale i pro poskytovatele telekomunikačních služeb. Potřeba silné a spolehlivé autentizace roste a s tím v posledních letech dochází k velkému rozvoji souvisejících informačních technologií. [1]

3.2 Potřeba autentizace

Při návrhu a realizaci počítačových sítí je nutné se ujistit, že jsou implementovány patřičné bezpečnostní opatření. Zejména v podnikovém prostředí jsou cenné informace uložené v systémech připojených k počítačové síti. Aby bylo možné je adekvátně chránit před útočníky a narušiteli, je nutné mít k disposici mechanismy, které využívají osvědčené metody ověřování. [2]

3.2.1 Autentizace

Autentizace je proces ověření a doložení totožnosti uživatele před zpřístupněním chráněného prostředí. Autentizace zajišťuje, že informace pochází z důvěryhodného, známého zdroje a zároveň že byla doručena správnému adresátovi. Přestože je nejrozšířenějším způsobem autentizace použití hesla, jedná se o nejméně bezpečnou metodu. Nejspolehlivějším způsoben je tzv. „více – faktorová“ autentizace, která využívá kombinaci několika metod současně. Mezi vhodné metody autentizace patří čipové karty, digitální certifikáty, jméno a heslo, jednorázová hesla tzv. OTP a v neposlední řadě i biometrické metody. [3; 4]

Autentizace může být zprostředkována dedikovanými autentizačními servery, které zajišťují nejen autentizaci, ale také autorizaci a tzv. účtování, tedy sledování aktivit a využívání prostředků, neboli accounting. Označujeme je zkratkou AAA technologie a patří mezi ně RADIUS, TACACS, 802.1X, LDAP nebo Active Directory.

3.2.2 Autorizace

Autorizace je kontrola nad tím, co je uživatel oprávněn provádět a co není. Je tak zajištěn přístup pouze tam, kam má uživatel právo přistupovat. Někdy je autorizace označena také jako kontrola přístupu a řídí se bezpečnostní politikou, viz 3.4.2. [3]

3.3 Autentizace a zabezpečení

Autentizace zajišťuje identifikaci uživatele. Pokud probíhá ověření identity v zabezpečeném prostředí, jsou chráněna i přenášená autentizační data. V případě autentizace ke vzdálenému systému jsou data přenášena nezabezpečeným prostředím a mohou být odposlechnuta a zneužita. Pro ochranu tohoto procesu určení identity uživatele a zabránění možnosti zneužití je nutné dodržet níže popsané principy zabezpečení. [5]

3.3.1 Požadavky na bezpečnost

Bezpečnostní požadavky jsou stanovené cíle, kterých je potřeba dosáhnout, pro zajištění nutné úrovně zabezpečení. V následující části jsou zmíněny nejdůležitější požadavky. [3]

3.3.1.1 Důvěrnost

Důležitým požadavkem zabezpečení je ochrana před neautorizovaným přístupem a současně zajištění potřebného přístupu autorizovaným uživatelům. Důvěrnost zajišťuje, že informace nejsou žádným způsobem prozrazeny nikomu bez oprávněné potřeby je znát. Důvěrnost může být definována také jako schopnost garantovat, že neexistuje neoprávněný uživatel, který by byl schopen nahlédnout do přenášených dat. [3; 4]

3.3.1.2 Integrita

Ochrana před nežádoucí a neoprávněnou změnou informací a umožnění legitimních úprav uživatelům autorizovaným, se nazývá zajištění integrity dat. Integrita zaručuje, že data v průběhu času zůstanou konzistentní. Integrita dat je dalším požadavkem, kterého dosahujeme pomocí šifrování dat. Integritou je zároveň ověřeno, že přijímané informace jsou ve stejném stavu, v jakém byly odeslány. V dřívějších dobách bylo integrity informací

dosahováno použitím pečetě a následnou kontrolou jejího neporušení. V současnosti se ke stejnému účelu využívá elektronický podpis a funkci hash. [3; 4]

3.3.1.3 Dostupnost

Dostupností se rozumí zabezpečení spolehlivosti služby a ochrana před výpadkem, ztrátou dat, nebo zablokováním přístupu. Dostupnost zajišťuje uživateli přístup k náležitým prostředkům a možnost dokončit tak jeho práci včas. [3]

3.3.1.4 Utajení

Pomocí utajení je chráněna důvěrnost, integrita a dostupnost osobních a citlivých dat. Mezi taková data například patří finanční nebo zdravotní záznamy. [3]

3.4 Způsoby zabezpečení

Pro zabezpečení autentizace se používají běžné principy počítačové bezpečnosti a složitější autentizační protokoly. Tyto protokoly umožnují ověření identity pomocí demonstrace sdíleného tajemství, aniž by případný útočník mohl zneužít jejich jednorázovou znalost. Využívá se kryptografických protokolů, principů tunelování a vlastností symetrického a asymetrického šifrování. [5]

3.4.1 Síťová bezpečnost

Síťová bezpečnost je obor zabývající se kontrolou a ochranou před nechtěným průnikem nebo zneužitím privátní sítě. Součástí je i proaktivní monitoring útoků, chyb protokolů, blokování nepovolených přenosů dat a přístupů k nim. V neposlední řadě pokrývá rychlou reakci na zjištěné problémy. Tento obor se také podílí na zajištění potřebné komunikace organizací i jednotlivců a jejich cílů, s ohledem na zamezení nežádoucího zneužití informačních zdrojů a zajištění integrity přenášených dat, tedy bezpečnostních požadavků, viz kapitola 3.3.1. [3; 6]

3.4.2 Bezpečnostní politiky

Efektivní bezpečnostní politiky musí jasně definovat bezpečnostní pravidla a omezení, současně korespondovat s cílem organizace, pro kterou jsou určené. Stejně jako

všechny bezpečnostní politiky, musí i tyto vycházet z důkladného ohodnocení a analýzy rizik. [3; 6]

3.4.3 Tunelování

Proces, při kterém je zapouzdřen jeden typ paketu do jiného za účelem přenosu, je nazýván tunelování. Jedním z příkladů může být přenos broadcast paketů napříč infrastrukturou se síťovými směrovači, nebo zabezpečení IP paketů šifrováním. [4]

3.4.4 Šifrování

Šifrování na aplikační vrstvě může být docíleno programy jako je například Pretty Good Privacy (PGP) nebo zabezpečenými kanály kterým je Secure Shell (SSH). Většina těchto programů pracuje přímo mezi hostiteli, což znamená, že nabízejí ochranu pouze pro přenášená data, nikoliv pro pakety samotné. Výjimkou je například SSH, které může být použito v port-forwarding módu k vytvoření tunelu. [4]

Na transportní vrstvě se používá k zabezpečení obsahu konkrétní síťové komunikace kryptografické protokoly jako je Secure Socket Layer (SSL) a jeho nástupce Transport Layer Security (TLS). Tyto protokoly mohou být použity i pro tunelování. Typické použití SSL a TLS je při komunikaci webového prohlížeče, kdy je opět chráněn pouze obsah paketu, nikoliv samotný paket. Více o SSL/TLS protokolu pojednává kapitola 3.6.1. [4]

Šifrováním, zapouzdřením ani tunelováním nelze učinit předávaná data nepřístupnými. Data je možné stále odchytit, získat a analyzovat. Dodržením aktuálních bezpečnostních doporučení, bezpečnostních politik, správné implementace a použití adekvátního šifrovacího algoritmu, zůstane přenášený obsah v bezpečí. [4]

3.4.5 Kryptografie

Kryptografie je vědecká disciplína zabývající se skrýváním informací před neoprávněným uživatelem. Kryptografie je praktikovaná pomocí vratných procesů nazývajících se šifrování a dešifrování dat. Šifrování je postup, při kterém jsou originální čitelná data převedena do nepoužitelné formy. Zpětný proces, kdy jsou data opět převedená do původní čitelné formy, je nazýván dešifrování. Jedná se o velmi rozsáhlý a komplikovaný obor. [3; 4]

Moderní kryptografie je založená na využívání složitých matematických algoritmů. Jedná se o soustavu pravidel a procedur, které definují, jak proces šifrování a dešifrování probíhá. Mnoho algoritmů je veřejných a je tak každému umožněno analyzovat jejich sílu a slabiny. Matematické algoritmy ke své funkci využívají klíče. Klíč je tajné a jedinečné binární číslo, které řídí proces šifrování a dešifrování. Bitová délka klíče je počet binárních čísel, ze kterých se klíč skládá. [3]

V oboru kryptografie se využívá tří hlavních typů algoritmů. Jedná se o symetrické šifrování, asymetrické šifrování a tzv. hašovací funkce, anglicky hashing. [3]

3.4.5.1 Symetrické šifrování

Sdílený klíč, někdy také nazýván sdílené tajemství, je využíván šifrovací metodou, která pro zašifrování i rozšifrování využívá stejný klíč. Jedná se o takzvané symetrické šifrování. Předpokladem je, že si všichni zúčastnění sdílený klíč sdělili s dostatečným předstihem a odpovídajícím zabezpečením tak, aby jej nezjistil nikdo neoprávněný. Tento způsob šifrování je pak velmi efektivní a rychlý, protože potřebné matematické operace nejsou tak složité jako v případě asymetrického šifrování. Při použití stejně dlouhého klíče a shodné výpočetní síly je symetrická kryptografie 10.000 krát rychlejší než asymetrická. Obecně platí, že čím delší je klíč použitý k šifrování, tím silnější a tedy bezpečnější je výsledná šifra. V současné době je šifrování využívající klíče kratší než 128 bitů považováno za nedostatečné. Doporučené jsou délky klíčů od 128 bitů výše. Klíče s délkou nad 256 bitů jsou označovány za velmi silné. Největší nevýhodou symetrického algoritmu je právě složitost bezpečné výměny klíčů na dálku a zároveň autentizace neznámého partnera. Existuje řada symetrických algoritmů. Nejznámější algoritmy symetrického šifrování jsou RC4, RC5, RC6, RC7, IDEA, DES, Triple DES, AES, ČÁST, Twofish a Blowfish. Výběr silného a bezpečného algoritmu je přinejmenším stejně důležité, jako délka použitého klíče. [3; 4]

3.4.5.2 Asymetrické šifrování

Způsob znečitelnění dat, kde je využito dvou různých klíčů, se nazývá asymetrické šifrování. V případě využití veřejného a privátního klíče se jedná o asymetrickou kryptografii veřejných klíčů. Veřejným klíčem se data zašifrují a dekódovány jsou klíčem

privátním. Velmi důležitý je vztah mezi těmito dvěma klíči, kdy veřejný klíč nemůže být využit ke zpětnému získání klíče privátního. Zašifrovat data může tedy kdokoliv pomocí kopie veřejného klíče a pouze vlastník klíče privátního je schopen data dešifrovat. Privátní klíč je tedy nutné zabezpečit a držet v tajnosti. V případě, že vlastník privátního klíče jej použije k zašifrování dat, mluví se o digitálním podpisu. Pomocí veřejného klíče lze tato data rozšifrovat a díky tomu je možné ověřit identitu odesílatele. [3; 4]

Matematické operace jsou při využití asymetrických algoritmů více komplexní než při symetrických a tím pádem i časově a výkonově náročnější. Tato náročnost je způsobena i délkou použitých klíčů, která se obvykle pohybuje v rozmezí od 1024 bitů do 8192 bitů. Z těchto důvodů se asymetrická kryptografie příliš nehodí pro šifrování souboru dat, ale je velmi vhodná pro ověřování identity a výměnu klíčů. [3; 4]

Nejvíce rozšířené algoritmy asymetrického šifrování jsou Diffie-Hellman, El Gamal a kryptografie eliptických křivek, které nevyužívají veřejných klíčů. Dále pak RSA algoritmus, založený na principu veřejných klíčů. Diffie-Hellman algoritmus je první existující algoritmus asymetrického šifrování. Vytvořila jej dvojice vědců, Whitfield Diffie a Martin Hellman, v roce 1976. [3; 4]

Asymetrické šifrování je díky svým vlastnostem využíváno informačními technologiemi pro zabezpečení výměny sdílených klíčů pro symetrické šifrování, autentizaci koncových bodů nebo uživatelů a k ověření zdroje a integrity přenášených dat. [3]

3.4.5.3 Hashing

Hašovací kryptografická funkce má na vstupu soubor nebo zprávu a výstupem je hodnota o konstantní délce tzv. otisk, hašovací hodnota nebo kontrolní součet. Délka výstupu je určena zvoleným algoritmem. Vstup může být libovolně velký a není nikterak v procesu hašovací funkce pozměněn. Obvyklou délkou výstupu je 128 bitů, při použití MD5 algoritmu, 160 bitů použitím SHA-1 nebo 512 bitů je-li použit algoritmus SHA-2, případně SHA-3. Pomocí porovnání dvou hodnot hašovací funkce je možné ověřit integritu dat. Pokud by byla data změněna, například přenosem nebo útočníkem, nově vypočtená hodnota kontrolního součtu bude výrazně odlišná. Hašovací funkce je pouze jednosměrná

a neumožňuje snadno z hodnoty výstupu zpětně získat vstupní data. V kombinaci s asymetrickým šifrováním se hašování využívá v elektronickém podpisu. [3]

3.5 SSL a TLS

SSL neboli Secure Socket Layer vyvinula firma NetScape. Primárním cílem SSL/TLS je bezpečně přenášet data a autentizovat uživatele. SSL/TLS spojení lze rozdělit na dvě fáze. První je ustanovení spojení a zabezpečená výměna klíčů (tzv. SSL handshake), druhá je následující šifrované spojení pomocí symetrické šifry. Bezpečný přenos symetrického klíče je zajištěn šifrováním asymetrickou šifrou za použití známého veřejného a utajeného privátního klíče. Zprávu zašifrovanou konkrétním veřejným klíčem lze dešifrovat jen příslušným privátním klíčem. Není tak potřeba zajistit výměnu klíče před přenosem, což je jedno z největších rizik symetrického šifrování. Vazbu veřejného klíče na konkrétní jméno a uživatele, tedy autentizaci, zajistí certifikát. Pokud jeden uživatel, případně server, předá svůj certifikát s veřejným klíčem druhému, je snadné si díky certifikátu u certifikační autority ověřit, kdo je skutečným vlastníkem tohoto klíče. Více o digitálních certifikátech pojednává kapitola 3.5.3. [7]

Secure Socket Layer (SSL) protokol a jeho následovník Transport Layer Security protokol se používají k zajištění silného šifrování přenášených dat. SSL podporuje 128 bitové šifrování, zatímco TLS podporuje AES protokol s možností šifrování použitím až 256 bitových klíčů. IETF standard definuje protokol v dokumentu RFC 5246 jako TLS. V praxi je ale často označován starším protokolem SSL, případně kombinací SSL/TLS. [3; 4]

Většina uživatelů si SSL protokol a zabezpečení přenosu dat ve webovém prohlížeči spojuje pouze s malým zámečkem, nebo podobným symbolem v jejich prohlížeči. Všechny nejběžnější prohlížeče webu jako například Microsoft Internet Explorer, Opera, Firefox a Chrome SSL/TLS protokol plně podporují. SSL/TLS se stal standardní metodou pro šifrování webového přenosu dat. Běžný HTTP provoz používá TCP protokol a port 80, SSL šifrovaný HTTP také známý jako HTTPS, funguje na portu 443 protokolu TCP. [4]

SSL/TLS protokol neumožňuje pouze zabezpečený přenos dat, ale také autentizaci koncových bodů. Typické použití SSL/TLS autentizace je jednosměrná při přístupu klienta na zabezpečený server. Server je takto autentizován tím, že klient porovná informace

uvedené v SSL certifikátu s adresou serveru, na který přistupuje, s platností a důvěryhodností certifikátu jako takovou. SSL/TLS může být použit i pro obousměrnou autentizaci použitím klientských certifikátů. [3]

Ačkoliv je SSL, resp. TLS protokol nejčastěji spojován s HTTP, může být použit i pro šifrování dalších protokolů, k nimž patří například SMTP(S), LDAP(S), POP3(S) nebo IMAP(S), EAP-TLS a PEAP. [4]

3.5.1 SSL na straně klienta

Pokud aplikace SSL/TLS protokol podporuje, je většinou pro uživatele velmi jednoduché tuto podporu využívat. Například téměř všechny webové prohlížeče mají podporu SSL/TLS zapnutou ve výchozím stavu a uživatel nemusí nic nastavovat, přestože jsou detailní nastavení týkající se SSL a TLS protokolu dostupná. Alternativní metodou, kterou lze použít pro aplikace, jež SSL/TLS nepodporují je výše zmíněné tunelování. [4]

3.5.2 SSL na straně serveru

Zapnutí podpory SSL/TLS protokolů na straně serveru, který to umožňuje, je přímočarý úkol. Takovým je například webový server. SSL a TLS využívají digitálně podepsané certifikáty, takže nejdůležitějším úkolem je získání a nainstalování těchto certifikátů. Při implementaci SSL/TLS v serveru je třeba vhodně zvolit kompromis mezi požadavky na sílu šifrovacího algoritmu a zpětnou kompatibilitou aplikací na straně klienta, například webových prohlížečů. V dnešní době je doporučené minimálně 256 bitové šifrování, které je již klienty běžně podporováno. [4]

3.5.3 Digitální certifikáty

Aby řešení autentizace založené na asymetrické kryptografii mohlo fungovat, je potřeba spravovat public key infrastrukturu, neboli infrastrukturu veřejných klíčů a certifikačních autorit vydávajících certifikáty [5]. Veřejný klíč, který je digitálně podepsaný důvěryhodnou třetí stranou, nazývanou certifikační autorita neboli CA, se nazývá digitální certifikát. Digitální certifikát v nejčastěji používaném formátu X.509 obsahuje také informace o vydavateli certifikátu, o vlastníkovi veřejného klíče, sériové číslo certifikátu a další. Úkolem certifikační autority je ověření identity osob nebo společností před tím, než

jim vydá digitální certifikát. Klienti uchovávají pouze podepsané veřejné klíče certifikačních autorit, kterým důvěřují. Při ověřování platnosti certifikátu se využívá principu přenosu důvěry a spoléhá se na to, že byl vydán důvěryhodnou CA. Dále se ověřuje platnost certifikátu, a zda není na seznamu odvolaných certifikátů (CRL), který si spravuje každá CA. Při použití digitálních certifikátů je k zašifrování zprávy odesílatele použit veřejný klíč získaný z digitálního certifikátu příjemce. Příjemce použije svůj privátní klíč k rozšifrování zprávy. Využitím digitálních certifikátů na místo obyčejného veřejného a privátního klíče je možné zvýšit spolehlivost autentizace. [3]

Pro získání digitálního certifikátu je nutné vytvořit žádost pro certifikační autoritu, neboli Certificate Signing Request (CSR). Současně se s žádostí vygeneruje privátní a veřejný klíč. Důvěryhodná certifikační autorita (CA) ověří žádost a její legitimitu. Pokud je vše v pořádku, vygeneruje digitální serverový certifikát a podepíše veřejný klíč, dodaný s CSR. [4; 8]

3.6 Rozdělení typů autentizačních metod

Variant a řešení autentizace je celá řada. Jednotlivé typy lze rozlišovat dle různých kritérií. Mezi tři základní faktory, které jsou při autentizaci využívány, se řadí:

- Něco, co uživatel zná.
- Něco, co uživatel vlastní.
- Něco, čím uživatel je, případně co dělá. [3]

Všechny tyto metody mají své klady a zápory. Zejména v případě citlivých a důležitých systémů je identitu uživatele vhodné ověřovat pomocí „více – faktorové“ autentizace. [8]

3.6.1 Něco, co uživatel zná

Něco, co uživatel zná, může být cokoliv, co si pamatuje a tím pádem to může napsat nebo sdělit v situaci, kdy je vyzván se autentizovat. Hesla jsou nejčastějším příkladem takovéhoto autentizačního faktoru. [3]

Výhodou takového způsobu ověření identity je fakt, že se jedná o znalost, kterou je možné lehce přenášet, předávat a zadávat do systému. Toto může být zároveň i nevýhodou z důvodu možné kompromitace a to i bez vědomí uživatele. Další nevýhodou je skutečnost, že lidská paměť má omezenou schopnost zapamatování si dat a následkem toho pak dochází ke zjednodušování hesel uživateli, případně užívání stejných hesel na více místech. [5]

3.6.2 Něco, co uživatel vlastní

Něco, co uživatel vlastní, může být cokoliv, co je potřeba nosit při sobě. V praxi se jedná o nějaké zařízení, nebo tzv. token, mezi které se řadí klíčenky pro uchování digitálních certifikátů, samotný certifikát, čipové karty, RFID čipy nebo elektronická zařízení známá jako jednorázové generátory hesel. Ta bývají často označována jako token. Jejich výhodou je, že je lze jen obtížně zkopírovat. Nevýhodou bývá vzájemná kompatibilita, možnost ztráty autentizačního předmětu a finanční náročnost řešení. Mnoho současných autentizačních metod a protokolů využívá již zmíněné principy asymetrické kryptografie, například protokolů SSL a TLS, digitálních certifikátů a klíčů. [3; 5]

3.6.3 Něco, čím uživatel je

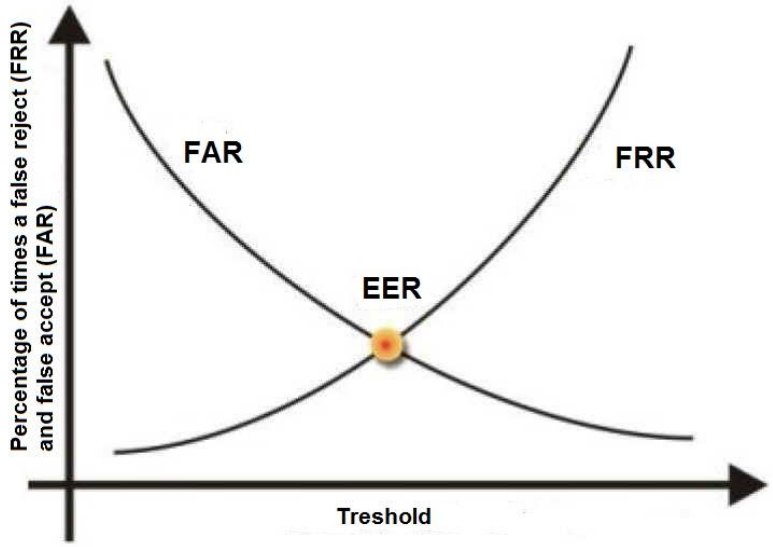
Něco, čím uživatel je, případně co dělá, je obecně označováno jako biometrika. Určité části lidského těla jsou zde využívány k ověření identity uživatele. Do biometriky se řadí nejen otisky prstů a snímky sítnice, ale například i analýza hlasu, stisku kláves, nebo podpisového vzoru. Zásadním rozdílem mezi biometrickým a předchozími způsoby ověření identity je ve způsobu odpovědi. Biometrické systémy nedávají odpověď ve tvaru ano či ne, ale v procentuální pravděpodobnosti shody. Pro každý takový systém je nutné určit vhodnou prahovou hodnotu určující, jak moc musí být biometrická data podobná, aby byl uživatel úspěšně autentizován. Existují dva druhy chyb, kterých se mohou biometrické systémy dopustit. Jedná se o „nesprávné odmítnutí“ (FRR) a „nesprávné přijetí“ (FAR). Čím nižší jsou tato čísla, tím je systém přesnější. [3; 5; 9]

Výhodou biometriky je, že uživatel nemá co zapomenout, ani ztratit. [10]

Nevýhodou je obtížnost měření biometrických faktorů. S tím souvisí různá přesnost jednotlivých biometrických autentizačních systémů, což může zásadně ovlivnit jejich bezpečnost. [10]

Graf závislosti FRR a FAR při nastavené bezpečnostní úrovni zobrazuje Obrázek 1. Místo, kde se křivky protínají, označujeme jako ukazatel přesnosti zařízení (EER). [9]

Obrázek 1: Závislost chybovosti biometrického systému



Zdroj: [9]

3.6.4 Jedno a více – faktorová autentizace

Pro zachování výhod jednotlivých řešení, minimalizaci jejich nedostatků a zvýšení celkové bezpečnosti a spolehlivosti, se doporučuje používat jejich vzájemné kombinace. [5]

3.6.4.1 Jedno – faktorová autentizace

Mezi „jedno – faktorovou“ autentizaci se řadí například autentizaci jménem a heslem. Její hlavní výhody jsou jednoduchost a tudíž i rozšířenost. Mezi nevýhody patří snížená možnost kontroly duplikátů, případně zcizení identity dalším subjektem. [5]

3.6.4.2 Dvou – faktorová autentizace

Do kategorie „dvou – faktorové“ autentizace se řadí kombinace autentizace něčím, co uživatel má, tedy „předmětem“, případně čím je, v kombinaci autentizace něčím co zná. Vhodný příklad je certifikát zabezpečený PIN kódem, jednorázové heslo generované po ověření tajným osobním heslem, atp. Teprve kombinace toho co uživatel má (vlastnictví certifikátu) a toho co ví (příslušné heslo/PIN) mu umožní prokázat svou identitu.

V současnosti je nejběžnějším případem asi ověřování při přístupu do internetových bankovnictví, kde se v první fázi uživatelé přihlašují jménem a heslem a v druhé jednorázovým kódem zaslaným přes SMS. [5]

Mezi výhody „dvou – faktorové“ autentizace patří vyšší odolnost proti záměrné i nechtěné duplikaci autentizačních předmětů. Nevýhodou může být finanční náročnost celého řešení a složitější podpora systémů. [5]

3.6.4.3 Více – faktorová autentizace

Maximálního zabezpečení můžeme dosáhnout pomocí „tří – faktorové“ autentizace. Tento způsob využívá jednu metodu ověření z každé ze tří výše zmíněných skupin. Vzorový postup autentizace lze popsat následovně. V první fázi uživatel vloží token do autentizačního zařízení spolu se zadáním PIN kódu nebo hesla. Token ověří PIN. V další fázi se uživatel ověří pomocí zadání své biometrické informace, například otiskem prstů. Ta je porovnána s již uloženou informací. Pokud se shoduje i tato, je uživatel úspěšně autentizován. [5; 11]

Výhodou je velká komplexnost a bezpečnost autentizace, která se hodí pro velmi citlivé systémy. Nevýhodou je finanční náročnost, složitost systémů a problémy vyplívající z přesnosti měření biometrických informací. [5]

3.7 Problematika řízení přístupu k lokálním počítačovým sítím

Majetek lidé chrání fyzickými bezpečnostními opatřeními. S daty a informacemi by to nemělo být jiné. Zcizení identity je v moderní společnosti velikou hrozbou, protože velké množství soukromých a citlivých informací je uchováváno v síťových databázích. Jedinou možnou ochranou je důsledná kontrola přístupů pomocí autentizačních metod. Řízení přístupu je metoda, která umožní přístup správným uživatelů k definovaným zdrojům, které potřebují ke své činnosti. Bez silné kontroly a řízeného přístupu k počítačovým sítím může ve společnostech docházet k obrovským finančním ztrátám. Jednou z metod, jak zabezpečit přístup k lokální síti, je využití standardu IEEE 802.1X. [8]

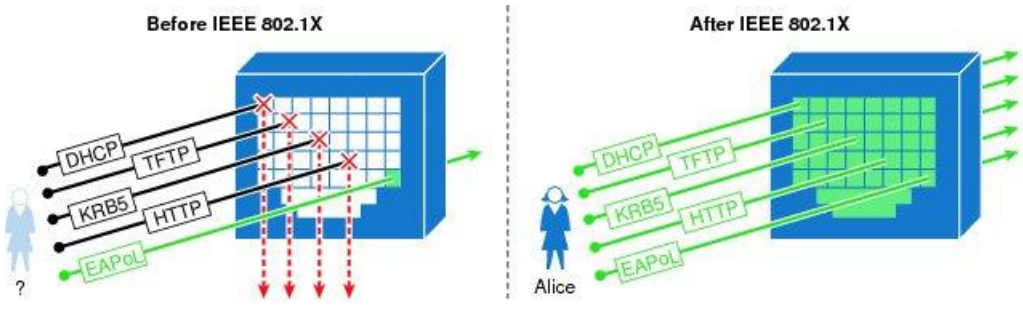
3.8 Standard IEEE 802.1X

Standard IEEE 802.1X, někdy také nazýván jako „autentizace síťových portů“, dále jen 802.1X, lze nazývat jazykem, který rozšiřuje „Extensible Authentication Protocol” (EAP) v lokálních počítačových sítích (LAN) procesem „Extensible Authentication Protocol over LAN” (EAPOL). Tento protokol řeší přenos autentizačních informací mezi dvěma zařízeními. [12]

Autentizace síťových portů neumožní neautorizovaným uživatelům a klientským zařízením přístup k chráněným síťovým zdrojům jako jsou servery, podnikové aplikace a databáze. Bez autentizace může útočník lehce získat přístup k počítačové síti připojením přenosného počítače do zásuvky počítačové sítě. Když má útočník přístup do sítě, může se soustředit na hledání bezpečnostních zranitelností a ty zneužít k proniknutí do jednotlivých systémů. Jakmile je jednou připojen, má takových možností celou škálu. Autentizace síťových portů tuto hrozbu znatelně redukuje. [2]

802.1X přináší řízený přístup síťových portů využitím autentizace. Takový síťový port může být dynamicky povolen, nebo zakázán v závislosti na identitě uživatele nebo zařízení, které se k němu připojuje. Před autentizací je identita koncového zařízení neznámá a všechen síťový provoz kromě protokolu EAP je blokován. Po autentizaci je již identita zařízení známa a všechen síťový provoz tohoto zařízení je povolen. Obrázek 2 znázorňuje chování síťového portu se zapnutou podporou IEEE 802.1X. [13]

Obrázek 2: Přístup k síti „před“ a „po“ ověření pomocí 802.1X



Zdroj: [13]

Standard 802.1X je důležitý, ale některé další standardy a specifikace jsou nezbytné pro řízený přístup k počítačové síti pomocí autentizace síťových portů. Mezi takové patří

EAP, EAP-Method, EAPOL a RADIUS protokol, které jsou rozebrány v dalších kapitolách. [2]

3.8.1 Komponenty 802.1X

Základními součástmi řešení založeného na 802.1X, jsou klient resp. tzv. „supplicant“, RADIUS klient neboli autentizátor a autentizační server. [12]

Supplicant je programové vybavení klientského zařízení, které umožňuje předávat autentizační údaje uživatele pro jeho ověření. Může to být samostatný software, může být součástí operačního systému, nebo integrován v samotném zařízení. Někdy tak bývá označován i klient, případně klientské zařízení. [2]

Autentizátor je zařízení pracující na druhé vrstvě OSI síťového modelu. Příkladem je síťový přepínač, označovaný jako switch, nebo přístupový bod bezdrátové sítě. V podnikové síti by všechny porty síťových přepínačů měli mít naimplementovánu podporu 802.1X. Autentizátor působí jako brána mezi klientem a chráněnou sítí. Zároveň funguje jako překladač mezi RADIUS klientem a autentizačním serverem. [2]

Autentizační server ověřuje uživatelské údaje zaslané k ověření klientem a přiřazuje definovanou úroveň přístupu k síti, jinými slovy autentizuje a autorizuje klienta. Dalo by se říci, že obecným standardem v oboru je používat jako autentizační server RADIUS server. V některých případech může být autentizační server zabudován v RADIUS klientovi. [2]

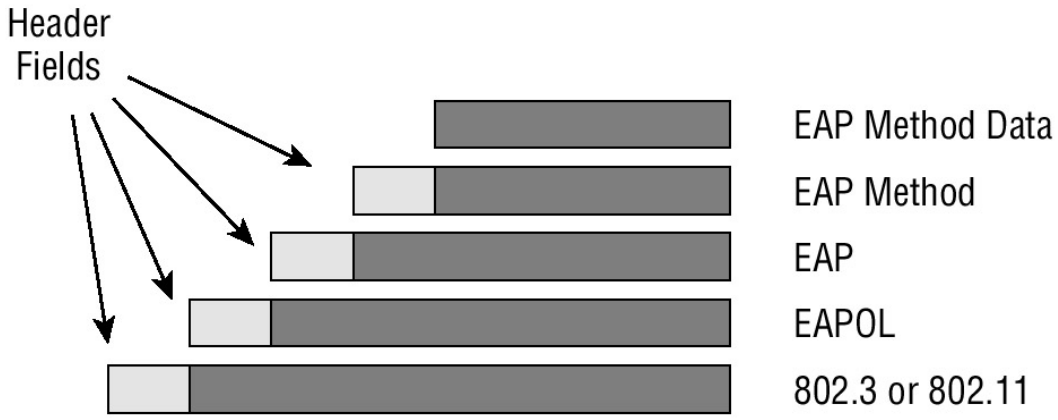
Další komponentou může být centrální databáze uživatelských identit, které se autentizační server dotazuje, aby ověřil uživatelské údaje. Běžnými představiteli jsou LDAP, Active Directory a Novell eDirectory. Pokud se při autentizaci využívá digitálních certifikátů, je nezbytnou součástí i infrastruktura veřejných klíčů (PKI). [13]

3.8.2 EAPOL

EAPOL neboli EAP over LAN je zapouzdřovací protokol definovaný standardem 802.1X pro přenos EAP protokolu mezi klientským zařízením a autentizátorem v lokálních sítích dle standardu IEEE 802. EAP protokol v žádosti (EAP-Request) a odpovědi (EAP-Response) nese způsob autentizace (EAP-Method) a autentizační data (EAP-Method-data).

EAPOL přidává další hlavičku k EAP datovým rámcům a vytváří speciální typ EAP datového rámce. Dále EAPOL přenáší EAP datové rámce jako data v těle EAPOL datového rámce. EAPOL protokol operuje na druhé vrstvě síťového OSI modelu, aby se zabránilo připojení klienta do počítačové sítě před autentizací. Protokol zároveň zajišťuje, že EAPOL data jsou první, která se po připojení k síťovému portu zasílají. Obrázek 3 znázorňuje zapouzdření jednotlivých vrstev mezi klientem a Autentizátorem. [2]

Obrázek 3: EAPOL zapouzdření



Zdroj: [2]

EAPOL přidává další tři pole do EAP datového rámce. První pole obsahuje verzi EAPOL protokolu, kterou odesílatel podporuje. V současné době ve všech implementacích 802.1X toto pole obsahuje hodnotu „0000 0002“. Ukládání verze umožňuje vývojářům udržet zpětnou kompatibilitu. Pole zvané „TYP“ identifikuje druh EAPOL zprávy, která je zasílána. Všechny hodnoty, které může v současné době nabývat, jsou v Tabulce 1. [2]

Tabulka 1: EAPOL pole TYP

TYP	**HODNOTA TYP POLE**
EAP-Packet	0000 0000 (Hex “00”)
EAPOL-Start	0000 0001 (Hex “01”)
EAPOL-Logoff	0000 0010 (Hex “02”)
EAPOL-Key	0000 0011 (Hex “03”)

Zdroj: [2]

Pole „délka“ ukládá délku těla datového rámce. Maximální délka je limitovaná druhem využívaného přenosového protokolu například IEEE 802.3 nebo 80.2.11. Tělo datového rámce obsahuje dat dle typu EAPOL. [2]

3.8.3 Průběh autentizace

802.1X může být inicializována buďto klientem nebo autentizátorem. Pokud je autentizace na portu zapnutá, po připojení zařízení do síťového portu přepínače, přepínač započne autentizaci zasláním „EAP-Request-Identity“ zprávy. Pokud přepínač neobdrží odpověď, posílá žádost opakovaně v nastavených intervalech. Klient může pomocí „Supplicant“ software začít autentizaci zasláním „EAPOL-Start“ zprávy. Tato funkce umožňuje urychlit celý autentizační proces. [13]

Následuje autentizační fáze, ve které autentizátor předává autentizační EAP zprávy mezi klientem a autentizačním serverem. Úkolem prostředníka je vybalovat a zabalovat EAP zprávy z a do EAPOL a RADIUS protokolu viz Obrázek 4. [13]

Obrázek 4: EAPOL a RADIUS protokol

Zdroj: [13]

Další způsob komunikace a výměny dat je závislý na zvolené metodě autentizace protokolu EAP (EAP-Method). V závislosti na metodě může klient předat jméno a heslo, digitální certifikát a další. Tyto údaje mohou být přenášeny umístěním do TLS šifrovaného tunelu jako „hash“ nebo jinou bezpečnou formou. [13]

V případě, že klient předá správné ověřovací údaje, autentizační server odpoví RADIUS zprávou „Access-Accept“ se zapouzdřenou „EAP-Success“ zprávou. Toto je povel pro síťový přepínač povolit přístup klientovi. Volitelně může zpráva obsahovat další informace formou atributů, například dynamicky přidělované číslo virtuální sítě (VLAN). V případě absence těchto parametrů switch povolí komunikaci na portu a ponechá jeho

nastavení. V případě bezdrátové sítě klienta autentizuje a umožní mu připojení k bezdrátové síti. [13]

Pokud klient předá nesprávné ověřovací údaje, nebo nesplní některé ze zásad pro připojení k počítačové síti, autentizační server odpoví RADIUS zprávou „Access-Reject“ se zapouzdřenou „EAP-failure“ zprávou. Toto indikuje, že klient nemá být autorizován pro přístup do sítě a v závislosti na nastavení se pokus o autentizaci opakuje, zkouší se alternativní metoda ověření, případně je klient umístěn do speciální oddělené VLAN, tzv. „Guest VLAN“. [13]

Součástí autentizačního procesu je i ukončení spojení. Aby byla zajištěna integrita oprávněných spojení, je nezbytné ukončit spojení okamžitě, když se autentizované zařízení, případně klient odpojí. Mechanismů jak toho docílit je více. Nejčastěji používané jsou detekce odpojení klienta od síťového portu, nebo definice maximálního času spojení. „EAPOL-logoff“ zpráva byla navržena pro možnost ukončení spojení na žádost klienta. [13]

3.9 EAP

Extensible Authentication Protocol (EAP) je nástroj, který podporuje různé autentizační metody. Funguje přímo na druhé vrstvě síťového modelu OSI a nevyžaduje Internet Protokol (IP). EAP disponuje vlastním řešením pro odstranění duplicitních požadavků a opakovaným zasíláním zpráv. Fragmentace datových rámců není podporována. EAP může být provozován na dedikovaných linkách, přepínaných okruhách, drátových i bezdrátových sítích. Jedna z výhod EAP protokolu je jeho architektura, která mu dává velkou možnost flexibility. EAP je používán k výběru konkrétního způsobu autentizace (EAP-Method). [14]

3.10 EAP Metody autentizace

EAP protokol ze své podstaty podporuje mnoho způsobů autentizace. Způsob autentizace EAP je nazýván „EAP-Method“. EAP-Method implementuje samotný autentizační proces mezi klientem a autentizačním serverem. Některé metody byly definovány v EAP specifikaci, ostatní jsou doplňkové a metody jednotlivých výrobců. Pro potřeby této práci budou rozebrány pouze ty nejdůležitější z nich. [2]

Volba konkrétní EAP metody je závislá na mnoha faktorech. Je ovlivněna bezpečnostní politikou, existující infrastrukturou, podporou a procesy spojenými s distribucí digitálních certifikátů, síťovými i serverovými zařízeními a klientskými stanicemi. [2]

3.10.1 EAP-MD5

Jedna z nejstarších metod autentizace EAP protokolu je EAP-MD5, metoda typu číslo „4“. K ověření používá kombinace jména a hesla zasílaného v podobě MD5 „hash“. Tato metoda by v praxi již neměla být využívána, protože je náchylná na odposlech ověřovacích údajů, slovníkový útok a další. [2]

3.10.2 EAP-TLS

Metoda EAP-TLS využívá TLS protokolu, infrastruktury veřejných klíčů, tedy digitálních certifikátů. Je to standard definovaný v RFC 2716, jedná se o „EAP-Method” typu č. „13“. Tato metoda vyžaduje, aby každý klient i autentizační server měli vlastní pár veřejného a privátního klíče. K ověření se používá veřejný klíč, který musí být podepsaný důvěryhodnou certifikační autoritou. Samotný přenos dat je tunelovaný protokolem TLS. Jedná se o nejbezpečnější aktuálně dostupnou metodu, která sebou nese nemalé požadavky na provozování a správu digitálních certifikátů. Proto není v praxi tolik rozšířená jako ostatní metody. EAP-TLS je metoda vhodná pro podnikové sítě, které mají infrastrukturu veřejných klíčů v provozu a vlastní digitální certifikáty používají. [2; 13]

Autentizační proces je následující. Síťový přepínač zašle „EAP-Request-Identity“ požadavek klientovi. Klient odpoví zasláním „EAP-Response-Identity“ zprávou obsahující uživatelský identifikátor přepínači. Přepínač zašle klientovu identitu autentizačnímu serveru. Autentizační server zašle „EAP-TLS-Start“ požadavek. Klient odpoví „EAP-Response“ žádostí s typem „EAP-TLS“. Datové pole datagramu obsahuje jeden nebo více TLS záznamů. Následuje odpověď autentizačního serveru ve stejné podobě. [2]

Jakmile se klient a server dohodnou na autentizaci pomocí „EAP-TLS“ metody, server zašle klientovi svůj digitální certifikát. Pokud je certifikát serveru ověřen, předloží klient serveru svůj klientský certifikát. Dále server validuje certifikát klienta, autorizuje jej k přístupu k síti. V případě, že v tomto procesu není některý z certifikátů ověřen, autorizace přístupu bude zamítnuta. [13]

3.10.3 EAP-TTLS

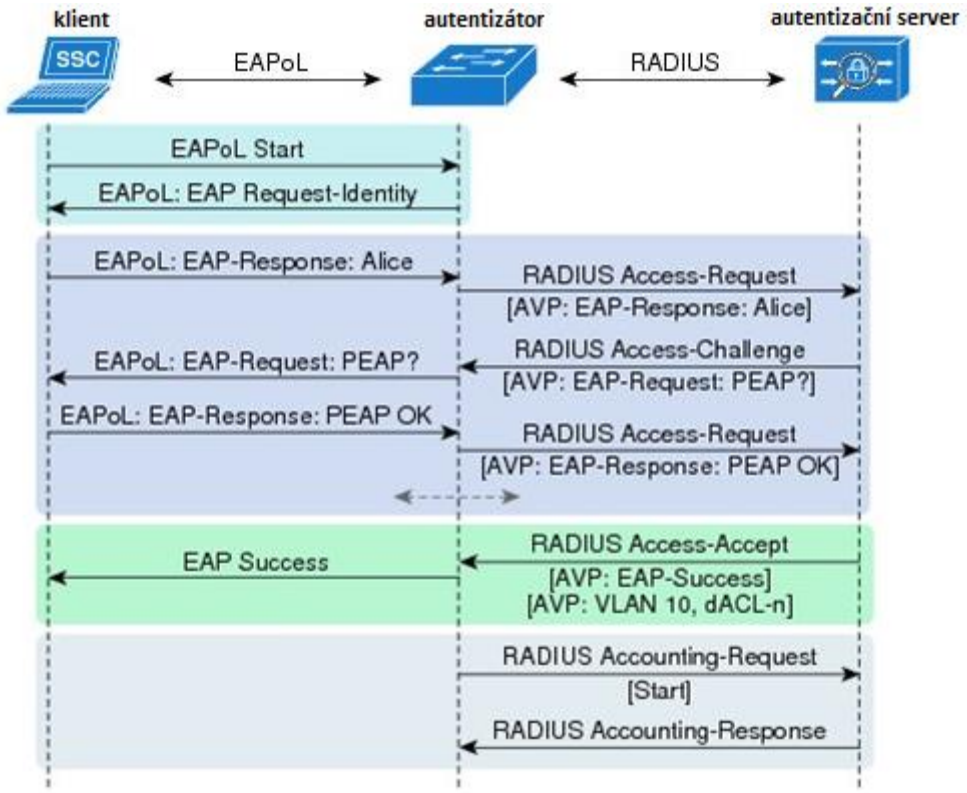
Odlehčenou alternativou je EAP-TTLS. Jedná se o „EAP-Method“ typ č. „21“. Byla vyvinuta společností Frunk Software jako rozšíření EAP-TLS. Funguje na stejném principu jako EAP-TLS. Rozdíl je pouze ve skutečnosti, že klient nepoužívá ke své autentizaci klientský digitální certifikát, ale jméno a heslo. To je opět chráněno tunelovaným přenosem protokolem TLS. Pro potřeby provozu EAP-TTLS je nutné nainstalovat aplikaci třetích stran. [2]

3.10.4 PEAP

Protected EAP (PEAP) metoda byla vyvinuta ve spolupráci společností Cisco Systems, Microsoft Corporation a RSA Security. Jedná se o EAP metodu typu č. „25“, která řeší bezpečnostní nedostatky ostatních metod tím, že vytváří šifrovaný tunel pomocí protokolu TLS a použitím digitálního certifikátu autentizačního serveru, který je zaslán na začátku ověřovacího procesu. Certifikát musí být nejprve úspěšně ověřen klientem, aby mohl být následně použit pro šifrování. V takto vytvořeném tunelu pak dochází k nové dohodě na EAP ověřovací metodě. Protože TLS tunel následně chrání autentizaci a přenos dat, je možné použít i jinak méně bezpečné metody jako je autentizace jménem a heslem. To umožňuje zavádět zabezpečený přístup k lokální počítačové síti i bez potřeby distribuce certifikátů na všechny klienty a bez správy PKI. MSCHAPv2 je běžně používanou druhotnou metodou EAP v rámci PEAP. Metoda je založena na autentizaci jménem a heslem a MD4 a DES algoritmy. Přestože samotný tento způsob již není považován za bezpečný kvůli objeveným zranitelnostem, použití v kombinaci s TLS protokolem je bezpečné. PEAP –MSCHAPv2 se obvykle používá v sítích s Active Directory infrastrukturou. [2; 13]

Autentizace probíhá v následujících krocích. Po té, co se klient a autentizační server dohodnou na metodě PEAP-MSCHAPv2, server odešle svůj digitální certifikát klientovi. Klient ověří platnost certifikátu serveru a poté co je úspěšně ověřena, vytvoří TLS šifrovaný tunel. Uvnitř tunelu zašle klient své přihlašovací jméno a heslo serveru s využitím standardu MSCHAPv2. Pokud server potvrdí správnost údajů, je klient ověřen. V opačném případě dojde k zamítnutí přístupu. Celý průběh je zřejmý z Obrázku 5. [13]

Obrázek 5: Znázornění procesu autentizace pomocí PEAP protokolu

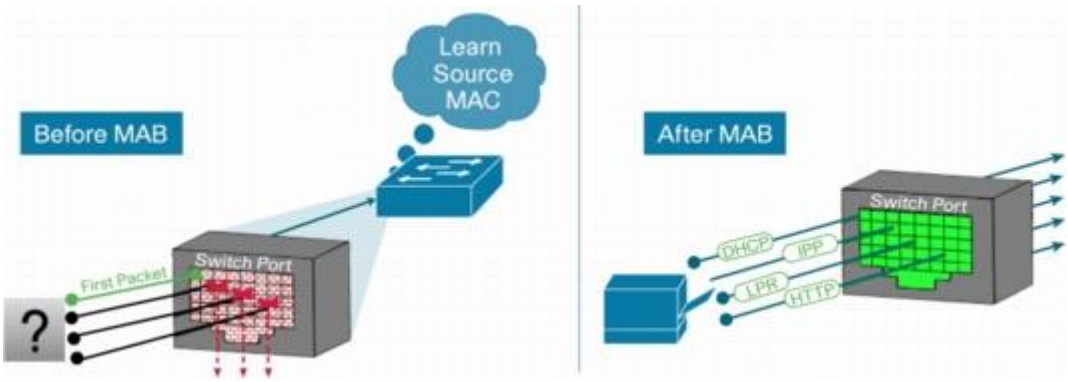


Zdroj: [13]

3.11 MAC Authentication Bypass (MAB)

Při implementaci 802.1X je nezbytné pamatovat i na zařízení, která neumožňují ověřování protokolem EAP, resp. standard 802.1X nepodporují. Mezi takové zařízení typicky patří tiskárny a multifunkční zařízení, IP telefony, stroje připojené do počítačové sítě a další. Pro všechny tyto klienty je nezbytné zprovoznit záložní metodu ověřování. Ideálním způsobem je „MAC authentication Bypass“ (MAB). Tato záložní metoda autentizace využívá MAC adresy zařízení, která je předávána jako uživatelské jméno i heslo. Autentizace probíhá stejným způsobem a řídí se obdobnými pravidly 802.1X standardu, EAP a RADIUS protokolu. Jediným rozdílem je využití MAC adresy pro ověření klienta na místo jména a hesla nebo digitálního certifikátu. Zapnutím a nakonfigurováním MAB na síťovém přepínači, resp. RADIUS klientovi, je po neúspěšné autentizaci klientem RADIUS získaná MAC adresa předána autentizačnímu serveru obdobným způsobem, jako by bylo předáno uživatelské jméno a heslo. [15]

Obrázek 6: MAC Authentication Bypass



Zdroj: [15]

3.12 RADIUS

RADIUS je protokol, který podporuje všechny tři moduly AAA, autentizaci, autorizaci i účtování (accounting). RADIUS byl vyvinut společností Livingston Enterprises, Inc. a je popsán v RFC 2865. Na rozdíl od jeho alternativ jako je například TACACS+ společnosti Cisco, se jedná o otevřeně podporovaný standard. RADIUS je IP protokol, který používá UDP pro svůj přenos. K ověřování se obecně využívá port UDP 1812 a k ověřování zpráv o účtování port UDP 1813. Zároveň je standardem IETF používaným pro AAA. RADIUS pracuje modelem klient, server. To znamená, že AAA klient posílá uživatelské údaje AAA serveru, v tomto případě skrze RADIUS protokol. RADIUS server odpovídá všemi potřebnými informacemi, které potřebuje AAA klient ke zpřístupnění síťového připojení koncovému zařízení. [16]

Při síťové autentizaci protokolem RADIUS, jsou některé části komunikace zašifrovány sdíleným heslem. Sdílené heslo v tomto případě není nikdy posíláno počítačovou sítí, což zajišťuje jeho integritu. RADIUS protokol neudržuje stav spojení a případné výpadky na trase a další s tím spojené problémy jsou řešeny zařízeními, které RADIUS protokol využívají. RADIUS protokol funguje ve dvou krocích. Přihlášení uživatele, případně připojení zařízení generuje požadavek AAA klienta „Access-Request“ na RADIUS server. Následuje odpověď serveru, která může nabývat hodnot „Access-Challenge“, „Access-Accept“, nebo „Access-Reject“. [16]

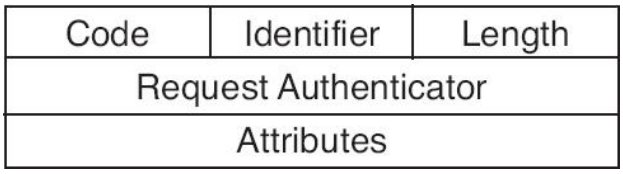
„Access-Request“ požadavek obsahuje uživatelské jméno, zašifrované heslo, IP adresu AAA klienta a číslo portu. Formát požadavku také obsahuje informace o typu spojení, které má být navázáno. Pokud je potřeba, RADIUS server si může vyžádat dodatečné informace zasláním „Access-Challenge“ zprávy. [16]

Každá RADIUS zpráva obsahuje tyto informace:

- Pole „kód“ (Code) může nabývat hodnot „Access-Request (1)“, „Access-Accept (2)“, „Access-Reject (3)“, „Accounting-Request (4)“, „Accounting-Response (5)“, „Access-Challenge (11)“, „Status-Server (12)“, „Status-Client (13)“, „Reserved (255)“. Je velikosti 8 bitů.
- Pole „identifikátor” (Identifier), které pomáhá RADIUS serveru spárovat požadavky a odpovědi a detekovat duplicitní zprávy a je délky 8bitů.
- Pole „délka“ o velikosti 16 bitů, (Length) udává délku vlastního datového rámce. Pole „Request Authenticator“ je použito pro samotný autentizační proces. Má délku 128 bitů.
- Poslední pole pro RADIUS atributy. [16]

Všechna pole zobrazuje Obrázek 7.

Obrázek 7: RADIUS datagram



Zdroj: [16]

Když RADIUS server obdrží „Access-Request“ požadavek o autentizaci od AAA klienta, prohledá nakonfigurovanou databázi. Databáze uživatelů může být lokální, případně vzdálená databáze uživatelů v adresářovém serveru LDAP, Active Directory a podobně. Pokud najde uživatelské jméno a zaslané heslo je správné, zašle zpět „Access-Accept“ odpověď s povolením přístupu. Pokud uživatelské jméno v databázi není, nebo se neshoduje heslo, odpoví zprávou „Access-Reject“ a přístup je zamítnut. Součástí „Access-Accept“ odpovědi jsou i již zmíněné atributy, které popisují další parametry připojení. [16]

Účtování RADIUS protokolu je docíleno zasíláním zpráv o začátku a konci spojení. Tyto zprávy obsahují informace o spojení, volitelně i čas. Pro tento účel se využívají RADIUS zprávy „Accounting-Request“ a „Accounting-Response“. [16]

Mezi aktuálně dostupné a hojně využívané RADIUS servery patří Cisco Access Control server, Microsoft Network Policy Server, Juniper Unified Access Control a další. Mezi zdarma dostupné patří především FreeRADIUS server.

4 VLASTNÍ PRÁCE

Jedním z hlavních cílů práce je realizace vlastního řešení zabezpečeného přístupu k lokální počítačové síti v praxi. Celý proces lze rozdělit do několika fází. Nejprve je nutné provést analýzu stávajícího stavu. Následuje návrh a volba konkrétního řešení, příprava a konfigurace celého prostředí, postupné zavádění do produkce, testování a produkční provoz.

Implementace celého systému bude provedena ve strojírenské výrobní společnosti ze středočeského kraje.

4.1 Stručná charakteristika podniku

Z bezpečnostních důvodů a z důvodu zachování obchodního tajemství si subjekt, ve kterém probíhala implementace, nepřeje být jmenován. Ze stejných důvodů jsou v následujících kapitolách záměrně vynechány, pozměněny nebo skryty některé technické detaily a informace osobního nebo obchodního charakteru, které nejsou pro vlastní práci důležité. V některých případech a schématech bylo také použito zjednodušení s cílem znázornit pouze relevantní a podstatné informace. Zde je základní charakteristika podniku:

- Strojírenská výrobní společnost,
- základní kapitál cca 50M Kč,
- obrat cca 200M Kč,
- cca 140 zaměstnanců celkem,
- z toho 56 zaměstnanců na administrativních pozicích,
- rozsáhlé výrobní a kancelářské prostory.

4.2 Požadavky na zabezpečení přístupu k síti

Podnik disponuje mnoha kancelářskými pracovišti, ale i rozsáhlými prostory určenými pro strojírenskou zakázkovou i kusovou výrobu. Ve všech těchto prostorech je nutné mít pro výkon činnosti podniku k disposici připojení k lokální počítačové síti. Veškeré podnikové prostory jsou tedy vybaveny rozvody kabelové počítačové sítě, i signálem bezdrátové sítě Wi-Fi. Kabelové rozvody jsou zakončeny zásuvkami s konektorem RJ45.

Protože pohyb osob po areálu a prostorách podniku má minimální omezení a vzhledem ke skutečnosti, že jednotlivé síťové zásuvky i bezdrátová síť jsou teoreticky přístupné komukoliv, bylo základním požadavkem omezit přístup neověřeným uživatelům a umožnit přístup k lokální počítačové síti pouze řádně autentizovaným uživatelům a síťovým zařízením. V případě bezdrátové sítě bylo požadavkem rozšíření sítě o virtuální WLAN, která bude dostatečně zabezpečená tak, aby v ní bylo možné zpřístupnit lokální serverové prostředky a informační systémy.

4.3 Analýza původního stavu

Společnost dlouhodobě vlastní, spravuje a rozvíjí síťovou infrastrukturu pro provoz výpočetní techniky. Spoléhá se na osvědčené a hojně rozšířené produkty renomovaných výrobců pro malé a střední podniky, tzv. sektor „Small Business“. Při volbě a výběru je kladen důraz nejen na cenu, ale i na spolehlivost a servisní, záruční i pozáruční podporu. Mezi hlavní patří společnost Microsoft, Cisco, Mikrotik, Ubiquity a DELL.

4.3.1 Bezpečnostní opatření

Stávající bezpečnostní opatření se řídí bezpečnostní politikou společnosti a lze je rozdělit na fyzické a logické.

Mezi použité opatření pro fyzické zabezpečení patří například přístupový a kamerový systém společně s oddělením fyzické ostrahy objektu. Objekt podniku je nepřetržitě monitorován a pod dohledem. Celý zabezpečovací systém je napojen na pult centrální ochrany externí společnosti. Přístup do objektu je umožněn pouze po autorizaci pomocí přístupového tokenu. Další pohyb v rámci prostor podniku již ale omezen není. Kritické části infrastruktury jsou uzamčeny, například místnost pro síťové rozvaděče tzv. „data-centrum“. Ta disponuje dvěma samostatnými přívody elektrické energie a záložními zdroji pro případ výpadku napájení elektrickým proudem. Ostatní síťové rozvaděče rozmístěné po budově jsou uzamčené. Zásuvky RJ45 počítačové sítě jsou volně přístupné nejen v kancelářích, ale i ve výrobních prostorech a odlehlých částech podniku.

Na logické úrovni podnik a jeho počítačové systémy chrání mnoho opatření. Mezi nejdůležitější patří zabezpečení celé sítě, stanic i serverů firewallem a celková segmentace

počítačové sítě. Dále pravidla pro vytváření a rušení jmenných uživatelských účtů, politika komplexnosti a složitosti hesel, zabezpečení jednotlivých aplikací a přístupu k nim, granulární nastavování přístupových práv pouze k prostředkům, které jednotliví uživatelé nezbytně potřebují k výkonu své práce, antivirové řešení s rozšířenou funkcionalitou a centrální správou, automatické zamykání OS počítačů při nečinnosti, stejně tak uživatelských účtů při opětovné neúspěšné autentizaci a mnoho jiných. Síťové přepínače mají ve většině případů nakonfigurované a zapnuté pouze porty, které jsou aktuálně využívány, ostatní jsou administrativně vypnuté. Důležitou součástí celkového řešení bezpečnosti je pravidelná aktualizace všech aplikačních součásti jednotlivých systémů, ale operačních systémů serverů i aktivních síťových prvků, dále monitoring a kontrola celé počítačové sítě.

4.3.2 HW

Základním stavebním kamenem sítě jsou síťové přepínače od společnosti Cisco. Všechny použité síťové přepínače podporují standard IEEE 802.1X, ale na žádném není použit. Jednotlivé síťové segmenty jsou propojeny pomocí směrovače s operačním systémem RouterOS od společnosti Mikrotik. Bezdrátová síť je provozována na technologii Unifi od výrobce Ubiquity s centralizovanou správou. Fyzické servery nesou značku DELL. Ve velké míře je využita virtualizace serverových OS pomocí technologie ESXi společnosti VmWare.

Seznam a typy nejdůležitějších HW zařízení:

- 16 ks síťových přepínačů Cisco, řada SG300 10-52 portů, celkem 502 portů
- 1 ks síťový přepínač Mikrotik RB450G
- 12 ks přístupových bodů sítě Wi-Fi
- 58 ks osobních a přenosných počítačů
- 51 ks telefonů Cisco SPA
- 16 ks síťových tiskáren různých výrobců
- 13ks výrobních strojů s připojením k počítačové síti (CNC, apod.)
- 2 ks server Dell pro Informační systém a pro virtualizaci

4.3.3 SW

Operační systém aplikačních serverů je Microsoft Windows server ve verzi 2008, ve většině případů virtualizovaný. Alternativně je pro některé účely použit unixový operační systém. Pro virtualizaci je použit operační systém VmWare ESXi verze 5.5.0.

V případě klientských stanic je předinstalovaný OS Microsoft Windows 7 professional.

Hlavními virtualizovanými servery jsou server provozující službu Active Directory, Exchange serveru, souborového serveru, tiskového serveru a serveru pro terminálové služby. Informační systém společnosti je instalován na samostatném HW serveru s vlastní instalací OS MS Windows Server 2008 a databázovým serverem SQL 2008 server. Doménový řadič s Active Directory server zároveň slouží jako lokální certifikační autorita pro své klienty.

Centrální správu Wi-Fi sítě řídí aplikace pro operační systém Linux, konkrétně Ubuntu LTS 12.04, jménem Unifi Controller verze 3.2.5.

Pro potřeby telefonních služeb je v provozu SW VoIP pobočková ústředna (PBX).

Další programové vybavení klientských počítačů i serverů se různí dle potřeb jednotlivých oddělení a uživatelů a není důležité pro potřeby této práce.

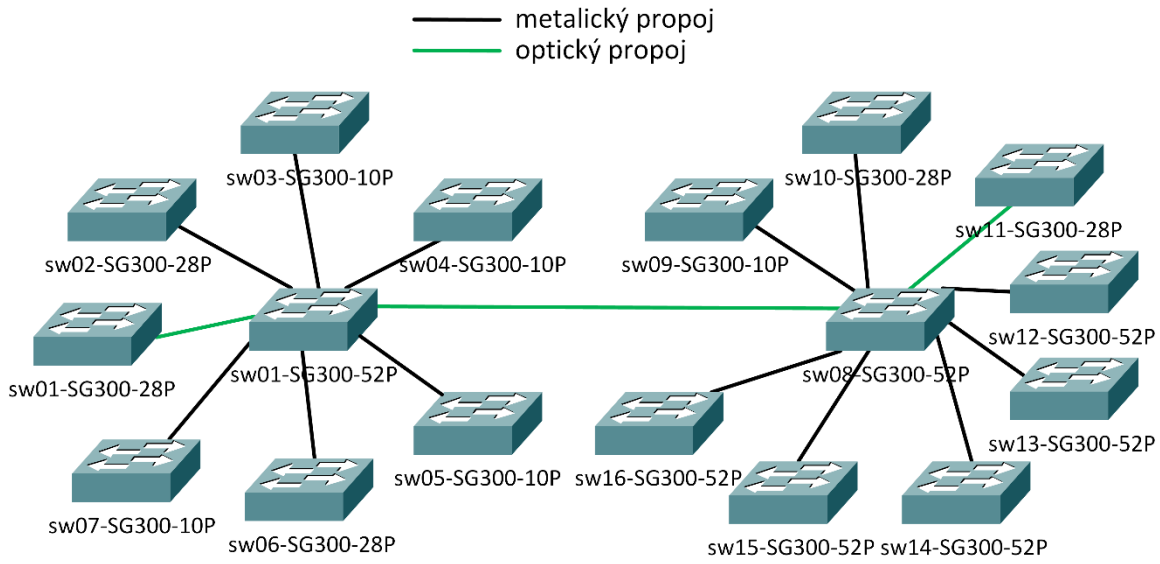
4.3.4 Topologie sítě

Detailní představu o struktuře sítě si lze udělat z pohledu fyzické a datové vrstvy OSI síťového modelu, případně síťové a vyšších vrstev.

4.3.4.1 Fyzická a datová vrstva

První a druhou vrstvu počítačové sítě tvoří síťové přepínače včetně strukturované kabeláže. Celá síť je zapojena do tzv. „hvězdy“ se dvěma centrálními přepínači. Ve většině případů je využita strukturované kabeláž typu CAT5e. Ve vzdálenějších místech provozovny jsou v některých případech síťové přepínače zřetězeny. Jednotlivé síťové segmenty jsou odděleny pomocí virtuálních sítí (VLAN). Schéma zapojení přepínačů je zřejmé z Obrázku 8.

Obrázek 8: Topologie počítačové sítě – L2



Zdroj: autor

4.3.4.2 Síťová a vyšší vrstvy

Centrálním prvkem pracujícím na třetí a vyšších vrstvách síťového OSI modelu je jeden hlavní směrovač, neboli router, značky Mikrotik. Na něm jsou nakonfigurovány síťová rozhraní pro jednotlivé VLAN. Síťová komunikace mezi jednotlivými sítěmi je chráněna integrovaným Firewallem s patřičnou uživatelskou konfigurací. Definované nastavení povoluje pouze nezbytné služby a síťové protokoly pro konkrétní zařízení a segmenty sítě.

Klientské stanice, serverové prostředky, tiskárny a multifunkční zařízení připojené kabelem jsou zapojené do stejné sítě. Klienti bezdrátové sítě jsou připojeny do oddělených VLAN, dle účelu bezdrátové sítě, bez přístupu k lokálním síťovým prostředkům. Například klienti bezdrátové sítě pro návštěvníky podniku mají přístup pouze do Internetu. Klienti Wi-Fi sítě pro VoIP telefonii mají přístup do Internetu a ke službám síťové pobočkové ústředny. Dalšími příklady oddělených sítí jsou například síť pro výrobní stroje, tzv. management síť pro potřeby správy a konfigurace síťových prvků a zařízení, atd. Nejpodstatnější sítě, jejich adresaci obsahuje Tabulka 2.

Tabulka 2: Seznam virtuálních sítí

název sítě	číslo VLAN	IP adresa sítě	výchozí brána	účel
vlan1	1	10.0.0.0/24	10.0.0.1	VLAN pro servery a PC
vlan20	20	10.0.20.0/24	10.0.20.1	telefonní VLAN
vlan30	30	10.0.30.0/24	10.0.30.1	veřejná Wi-Fi
vlan40	40	10.0.40.0/24	10.0.80.1	kamerová síť
vlan50	50	10.0.50.0/24	10.0.50.1	výrobní stroje CNC
vlan60	60	10.0.60.0/24	10.0.60.1	speciální zařízení
vlan70	70	10.0.70.0/24	10.0.70.1	tiskárny a multifunkční zařízení
vlan200	200	10.0.90.0/24	10.0.90.1	management VLAN

Zdroj: autor

4.4 Volba způsobu řešení

Návrh a konkrétní způsob realizace i implementace celkového systému zabezpečeného přístupu k lokální počítačové síti je podložen teoretickými poznatky z první části práce. Zároveň vychází z analýzy původního stavu celé infrastruktury. Zohledněny jsou požadavky na jednoduchost, stabilitu, efektivnost, bezpečnost a nízké náklady implementace i následného provozu celého sytému autentizace a autorizace uživatelů i zařízení při přístupu k počítačové síti.

4.5 Návrh řešení

Systém zabezpečení přístupu k lokální počítačové síti bude postaven na standardu IEEE 802.1X a protokolu EAP. Z analýzy vyplývá, že infrastruktura společnosti podporuje potřebný standard i protokoly a není tedy nutné volit některý z proprietárních nebo uzavřených řešení komerčních výrobců.

Způsobem autentizace bylo zvoleno ověřování uživatelů. Tato metoda má výhodu možnosti umístění různých uživatelů do pro ně speciálně určených VLAN, dle druhu jejich činnosti, nebo oprávnění. Prozatím bude autentizace umožněna pouze zaměstnancům společnosti, kteří mají aktivní účet v centrálním adresáři Active Directory. Všichni uživatelé pracující na firemních osobních počítačích budou sdílet společnou VLAN.

Z důvodu nedostatečně rozvinuté Infrastruktury veřejných klíčů v podniku a jednodušší správy a údržby bylo na základě analýzy zvoleno ověření uživatelským jménem a heslem. Citlivá data jsou v průběhu autentizace chráněna použitým protokolem PEAP, konkrétně variantou PEAP-MSCHAPv2.

Zařízením, která nezískají přístup k síti ověřeným uživatelem, se automaticky přiřadí návštěvnická sít, tzv. „Guest VLAN“. Zařízení, která potřebují přístup k lokálním síťovým prostředkům, ale standard IEEE 802.1X nepodporují, budou autentizovány s využitím záložní metody ověření pomocí MAC adresy. Jednotlivým skupinám budou přidělovány omezené a oddělené virtuální sítě, dle účelu jejich použití.

Nová bezdrátová síť bude shodně využívat standard 802.1X, někdy označovaný jako Enterprise autentizace, konkrétně protokol PEAP-MSCHAPv2 a šifrování WPA2. Každý uživatel bude ověřen a autorizován individuálně pomocí vlastního, centrálně spravovaného jména a hesla v adresáři Active Directory. To bude zabezpečeno přenosem šifrovaným TLS protokolem.

V následujícím textu se předpokládá, že lokální počítačová síť podniku je kombinace kabelové počítačové sítě označované LAN a bezdrátové Wi-Fi počítačové sítě označované WLAN.

4.5.1 HW

Pro potřeby sytému nebude nutné pořizovat další fyzické prostředky. Využijí se stávající prvky infrastruktury a již zakoupené licence aplikačního vybavení.

4.5.1.1 Infrastrukturní část

Autentizátorem, neboli klientem serveru RADIUS budou veškeré stávající síťové přepínače s nově a korektně nastavenou konfigurací. Bude využito existující podpory standardu 802.1X a protokolu PEAP. Veškeré přístupové porty budou nakonfigurovány pro vynucenou autentizaci přístupu k síti. Výjimku z povinné autentizace budou mít pouze porty pro serverovou a páteřní infrastrukturu, které jsou fyzicky ochráněné.

Pro autentizační server bude využito prostředků virtualizačního serveru.

4.5.1.2 Klientská část

Použitá klientská zařízení, která se budou ověřovat při přístupu k síti, budou aktuálně využívané osobní počítače, síťové periferie, výrobní stroje a IP telefonní přístroje.

4.5.2 SW

4.5.2.1 Infrastrukturní část

Služby autentizačního serveru zastane do nové virtuální instance nainstalovaný operační systém Windows Server 2008 R2 standard se službou „Network Policy Server“ tzv. „NPS“. Verze „Server 2008 R2“ byla zvolena z důvodu již zakoupených klientských licencí. Tato verze poskytuje srovnatelné funkce jako aktuální verze 2012 a zároveň je stále plně podporována výrobcem.

Network Policy Server umožnuje přijímat autentizační požadavky autentizátorů a předávat je k ověření doménovému řadiči s adresářovou službou Active Directory.

4.5.2.2 Klientská část

V operačním systému Windows 7 professional nainstalovaném na klientských stanicích je integrován „supplicant“ s podporou standardu 802.1X pro drátové i bezdrátové sítě. Proto není nutné pořizovat speciální aplikační vybavení na klientské počítače.

V případě ostatních síťových zařízení, která nepodporují potřebný standard, bude využito alternativního způsobu autentizace a autorizace s využitím MAC adresy zařízení tzv. MAC Authentication Bypass neboli MAB. Detailně o implementaci a konfiguraci MAB pojednává kapitola 4.10.

4.5.3 Topologie sítě

K realizaci práce bude potřeba provést konfigurační změny na úrovni druhé, třetí a vyšších vrstev síťového OSI modelu.

4.5.3.1 Fyzická a datová vrstva

Fyzické zapojení přepínačů zůstane zachováno. V serverové části sítě vznikne nový autentizační server. Pro novou bezdrátovou síť bude nutné vytvořit novou virtuální síť

VLAN 80 „Interní Wlan“. Schéma a detaily zapojení, včetně síťové adresace a potřebných pravidel na firewallu, jsou popsány níže.

4.5.3.2 Síťová a vyšší vrstvy

Adresní rozsahy nových sítí a prvků včetně celkové topologie přibližuje schéma na Obrázku 9 a Tabulky 3 a 4.

Tabulka 3: Seznam virtuálních sítí – nové sítě

název sítě	číslo VLAN	IP adresa sítě	výchozí brána	účel
vlan80	80	10.0.80.0/24	10.0.80.1	interní bezdr. síť – Wi-Fi-INT
vlan998	998	10.9.98.0/24	10.9.98.1	unauthenticated VLAN
vlan999	999	10.9.99.0/24	10.9.99.1	guest VLAN

Zdroj: autor

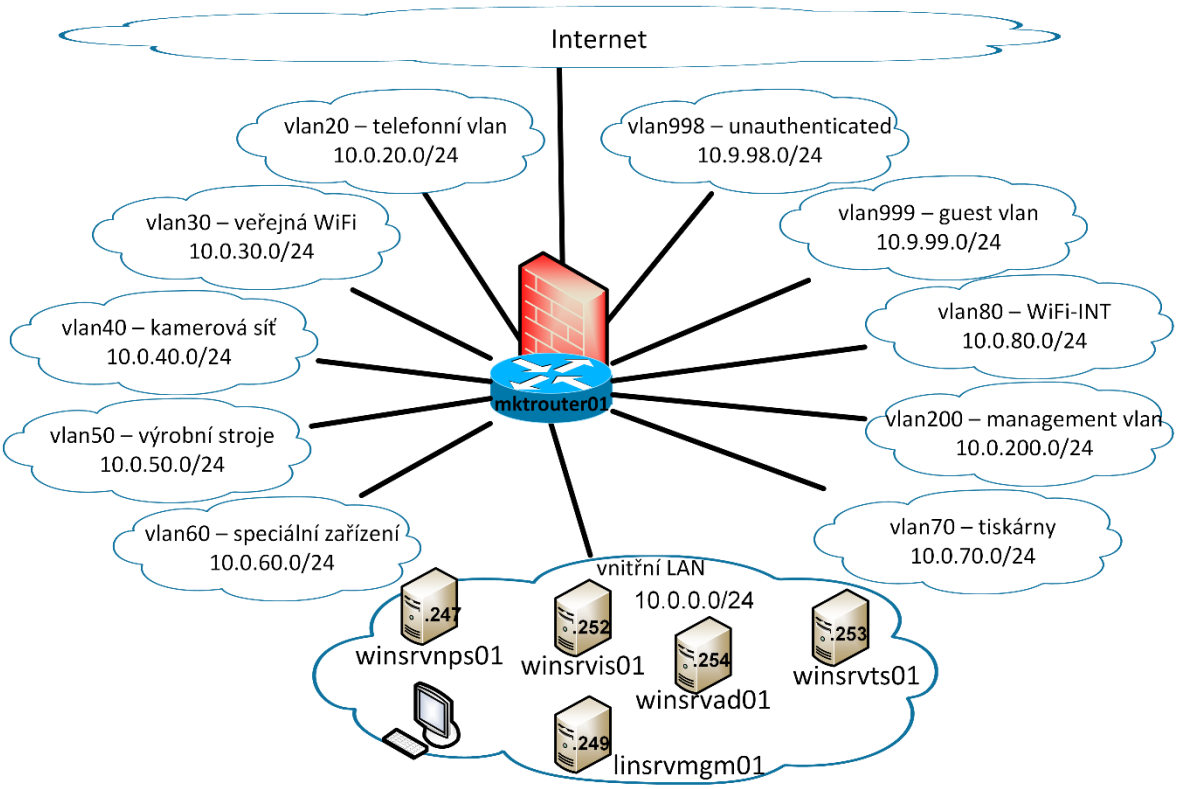
Tabulka 4 obsahuje seznam, adresaci a popis důležitých zařízení.

Tabulka 4: Seznam zařízení

IP adresa	název zařízení	operační systém	funkce
10.0.0.254	winsrvad01	Windows Server Standard 2008 R2	AD, CA, DHCP, DNS
10.0.0.253	winsrvts01	Windows Server Standard 2008 R2	Terminal Server
10.0.0.252	winsrvis01	Windows Server Standard 2008 R2	IS server
10.0.0.249	linsrvmgm01	Ubuntu LTS 12.04	řadič a správa Wi-Fi sítě
10.0.0.247	winsrvnps01	Windows Server Standard 2008 R2	Autentizační server
10.0.0.1	mktrouter01	Router OS 6.32.2	router, firewall, DHCP, DNS
10.0.200.2[31-46]	SW0[1-16]-SG300	Cisco	Autentizátory – switch – 16 ks
10.0.200.[18-26]	AP0[1-12]-WiFi	Ubiquity unifi firmware	Autentizátory – Wi-Fi AP – 12 ks

Zdroj: autor

Obrázek 9: Topologie počítačové sítě – L3

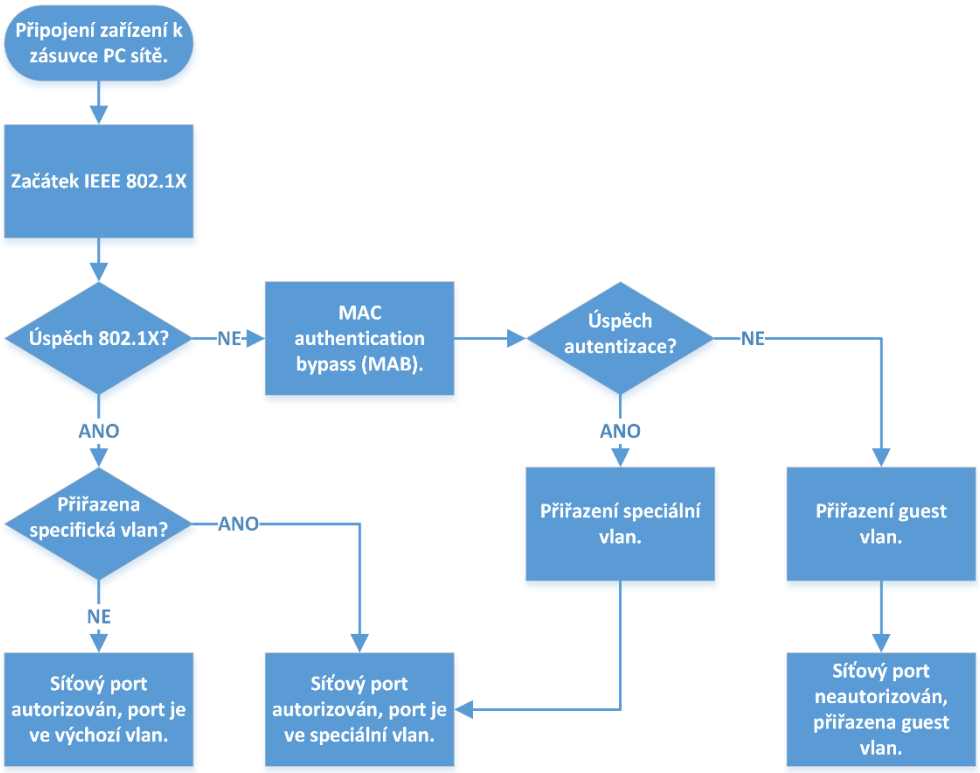


Zdroj: autor

4.5.3.3 Průběh autentizace a autorizace

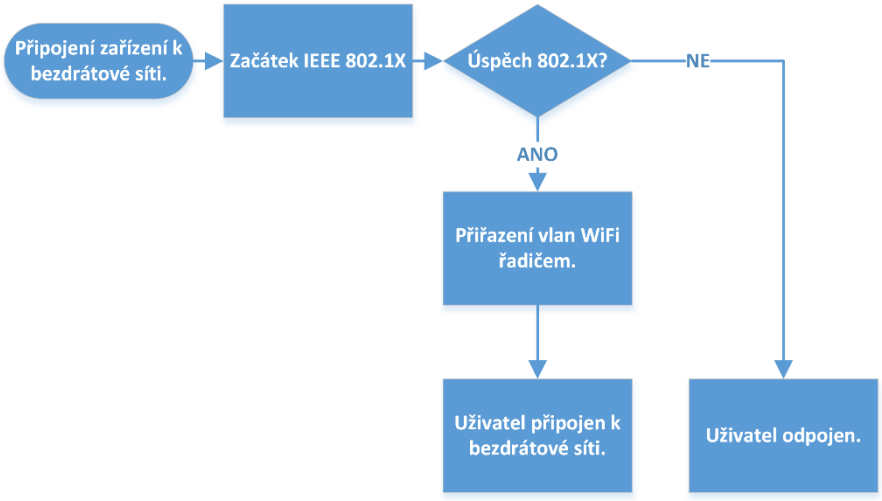
Průběh ověření uživatele pomocí standardu IEEE 802.1X bude následující. V případě kabelové počítačové sítě uživatel připojí své zařízení k zásuvce počítačové sítě. Po počáteční inicializaci síťového portu vyzve přepínač zařízení k autentizaci protokolem EAP. Pokud bude autentizace úspěšná, může nastat situace, kdy RADIUS server vrátí přepínači atribut s hodnotou VLAN, do které má být přiřazen následně autorizovaný síťový port. Když není atribut předán, přejde port do autorizovaného stavu a ponechá si své statické nastavení. Neúspěšná autentizace, ať již z důvodu špatných ověřovacích údajů, nebo chybějící podpory 802.1X na straně klienta znamená, že se přepínač pokusí o autentizaci pomocí MAC adresy. V případě úspěchu bude vždy RADIUS atributem přiřazena speciální VLAN, v ostatních případech dojde k umístění zařízení do tzv. „Guest VLAN“. Celý proces autentizace je zřejmý z diagramu na Obrázku 10. V případě bezdrátové počítačové sítě se uživatel se k síti autentizuje úspěšně a je připojen, nebo nikoliv, viz diagram na Obrázku 11.

Obrázek 10: Průběh autentizace LAN



Zdroj: autor

Obrázek 11: Průběh autentizace WLAN



Zdroj: autor

4.6 Příprava prostředí

V již existující infrastruktuře počítačové sítě bylo nutné zprovoznit a nakonfigurovat jednotlivé prvky pro využití standardu IEEE 802.1X. Následující kapitoly popisují postup a nastavení jednotlivých součástí v doporučeném pořadí jednotlivých kroků.

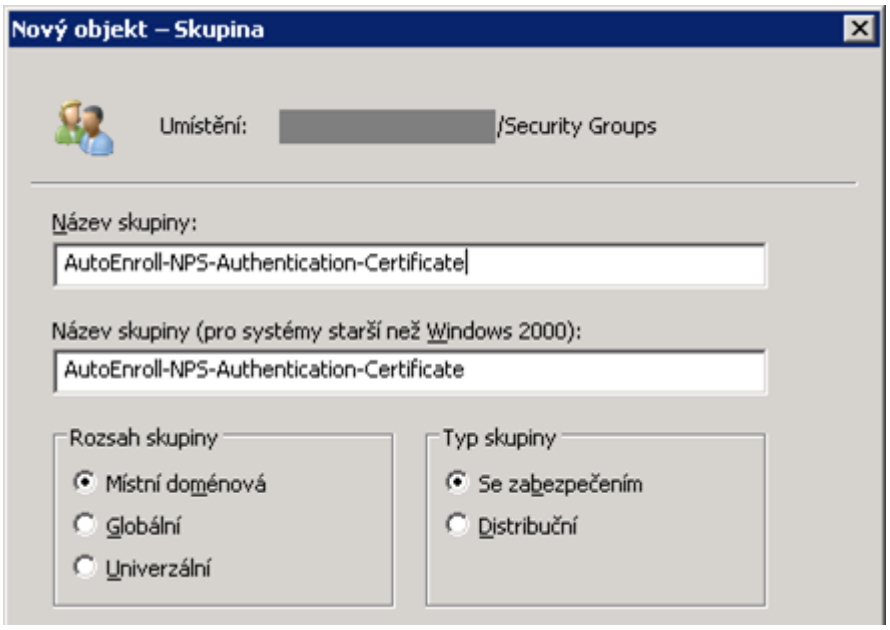
4.6.1 Konfigurace certifikátů

Pro zvolenou metodu ověřování PEAP-MSCHAPv2 bylo potřeba zajistit SSL/TLS serverový certifikát NPS serveru a jeho automatické vydávání. Zde je využito za tímto účelem vytvořené skupiny zabezpečení v AD.

4.6.2 Konfigurace skupin AD

Obrázek 12 znázorňuje konfiguraci nové skupiny zabezpečení v Active Directory se jménem „AutoEnroll-NPS-Authentication-Certificate“ pro automatické vydávání serverového certifikátu serveru NPS, který bude jejím členem. Členové této skupiny automaticky obdrží serverový certifikát podepsaný certifikační autoritou.

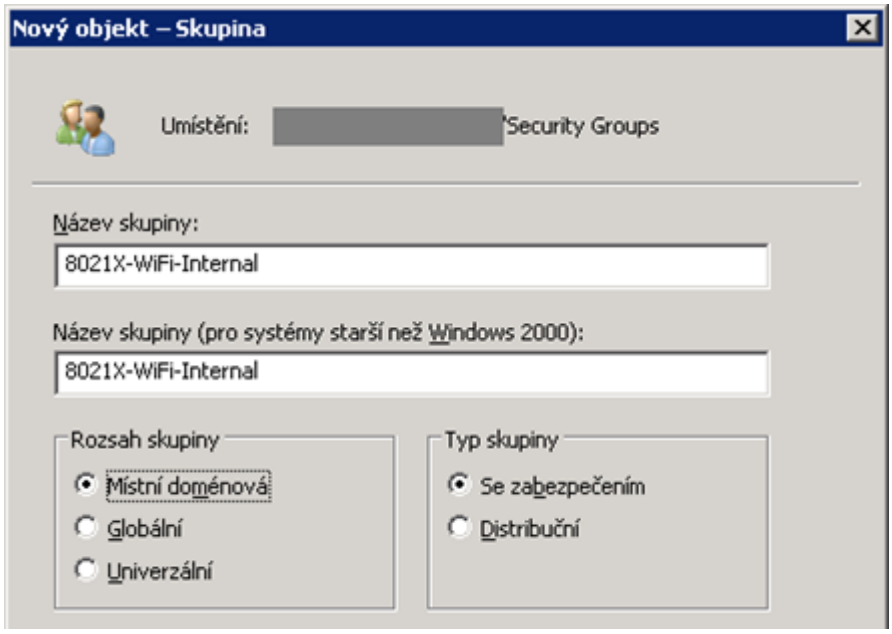
Obrázek 12: Vytvoření skupiny pro vydávání certifikátů NPS



Zdroj: autor

Pro potřeby bezdrátové sítě byla vytvořena dle Obrázku 13 skupinu zabezpečení „8021X-WiFi-Internal“. Vybraní uživatelé, členové této skupiny budou mít oprávnění připojit se k interní bezdrátové síti.

Obrázek 13: Vytvoření skupiny pro autentizaci uživatelů interní Wi-Fi sítě



Zdroj: autor

Dále pro každou plánovanou virtuální síť VLAN byla vytvořena skupina zabezpečení ve tvaru „8021X-vLAN-?“, kde otazník značí číslo VLAN. Například „8021X-vLAN-50“ pro VLAN určenou výrobním strojům. Členové, v tomto případě zařízení patřící do této skupiny budou po úspěšné autentizaci umístěny do patřičné virtuální sítě. Obdobným způsobem byla připravena skupina „8021X-MAB-Password-Policy“ pro autentizaci zařízení nepodporujících 802.1X.

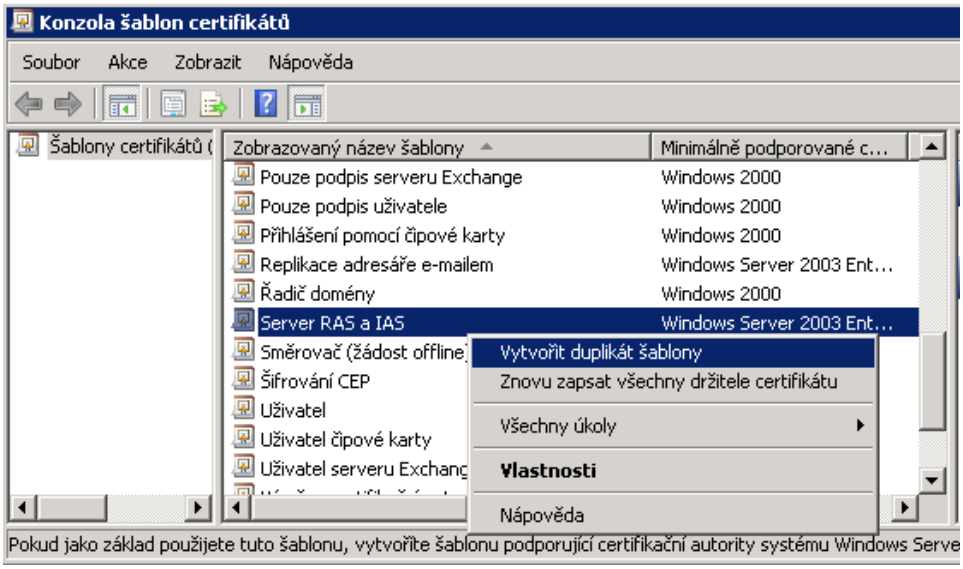
4.6.3 Konfigurace šablony certifikátů

Následující text zachycuje vytvoření jednoúčelové šablony certifikátů. Tato šablona je využita pro vydávání certifikátů sloužících pro autentizaci RADIUS serveru (NPS) klienty a vytvoření šifrovaného PEAP tunelu.

Na doménovém řadiči ve správci „Certification Authority“ byla vytvořena nová šablona pro ověření serveru, podpis a šifrování. Do konzole šablon certifikátů lze přistoupit

volbou „Spravovat“ po stisku pravého tlačítka myši. Název šablony byl zvolen „Server – autentizační certifikát“. Vytvořila se duplikováním již existující šablony „Server RAS a IAS“ viz Obrázek 14 a Obrázek 15.

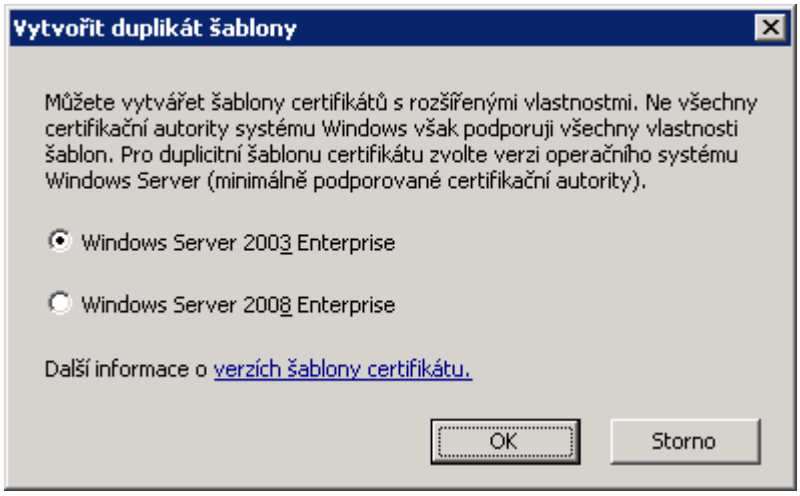
Obrázek 14: Šablona serverového certifikátu #1



Zdroj: autor

Při vytváření se z důvodů zpětné kompatibility volí verzi „Windows Server 2003 Enterprise“ dle Obrázku 15.

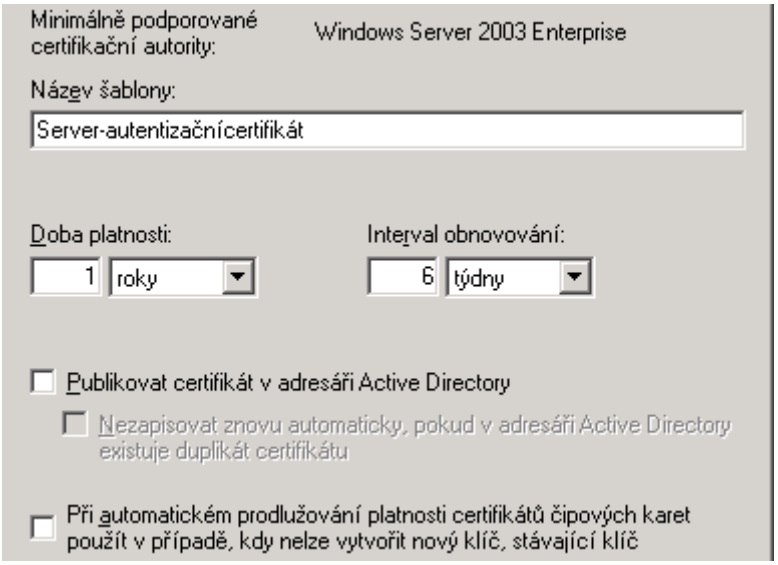
Obrázek 15: Šablona serverového certifikátu #2



Zdroj: autor

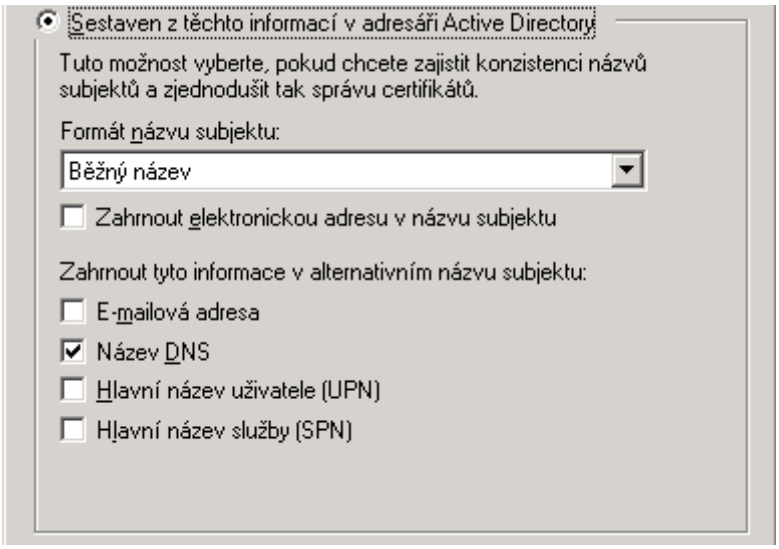
Doba platnosti certifikátů vydaných dle této šablony je 1 rok a interval obnovování 6 týdnů. Název subjektu je sestaven z informací v AD, konkrétně název DNS. V záložce zabezpečení má připravená skupina nastavena práva na registraci a automatický zápis. Parametry šablony jsou zřejmé z obrázků 16, 17 a 18.

Obrázek 16: Vlastnosti nové šablony #1



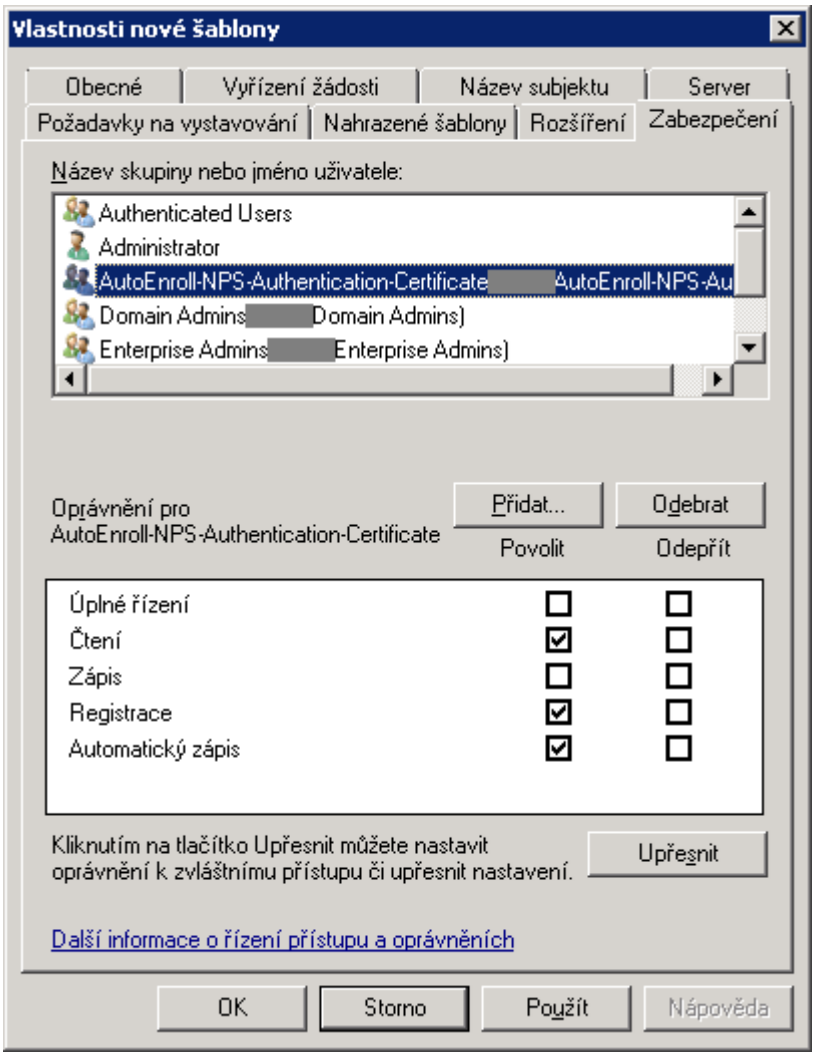
Zdroj: autor

Obrázek 17: Vlastnosti nové šablony #2



Zdroj: autor

Obrázek 18: Vlastnosti nové šablony #3



Zdroj: autor

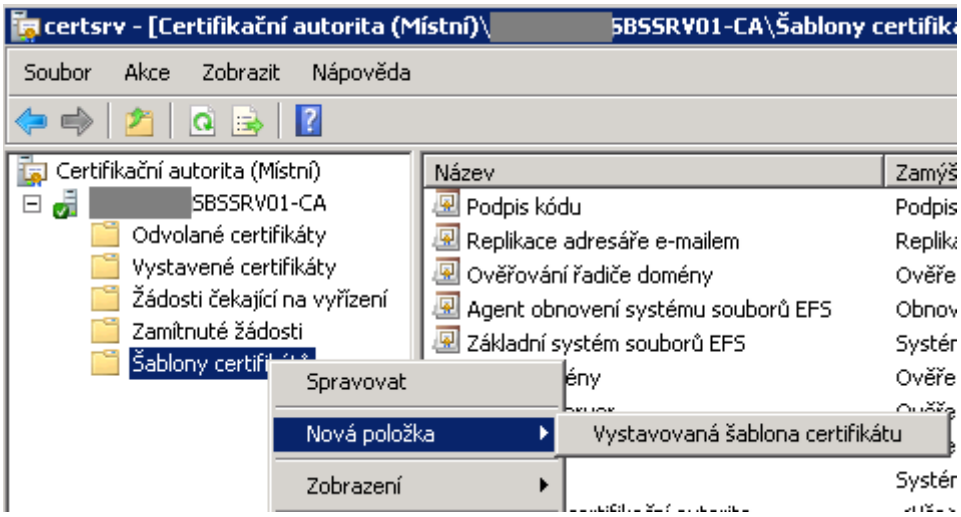
Obrázek 19 znázorňuje finální podobu nové šablony v seznamu konzole šablon certifikátů.

Obrázek 19: Nová šablona certifikátů pro NPS

Zdroj: autor

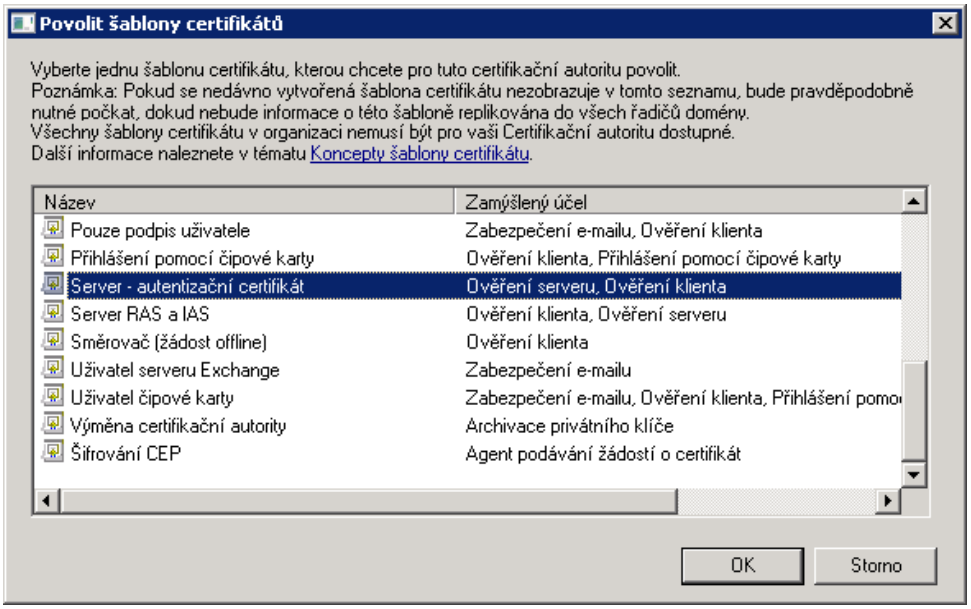
Dalším krokem bylo přidání vytvořené šablony do seznamu dostupných šablon certifikační autority. Toho lze docílit použitím pravého tlačítka myši na „Šablony certifikátů“, dále „Nová položka“ a volby „Vystavovaná šablona certifikátů“ viz Obrázek 20 a Obrázek 21.

Obrázek 20: Přidání šablony do certifikační autority #1



Zdroj: autor

Obrázek 21: Přidání šablony do certifikační autority #2

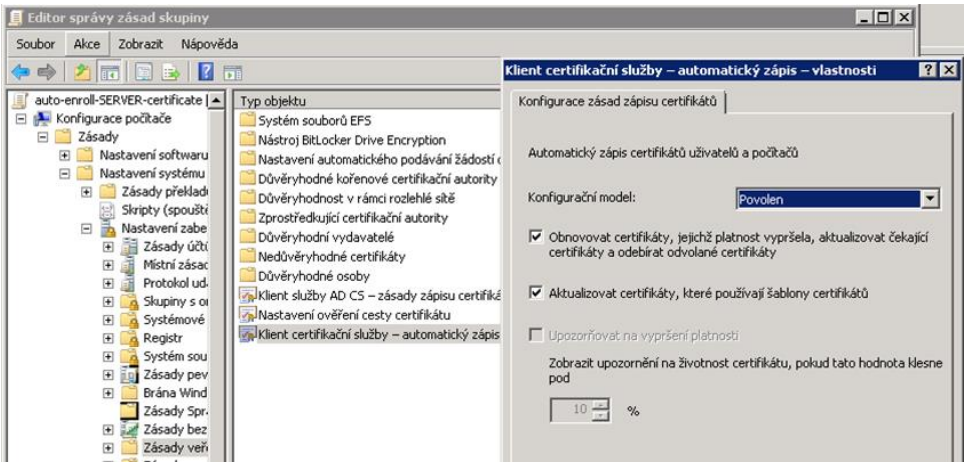


Zdroj: autor

4.6.4 Konfigurace automatického vydávání certifikátů

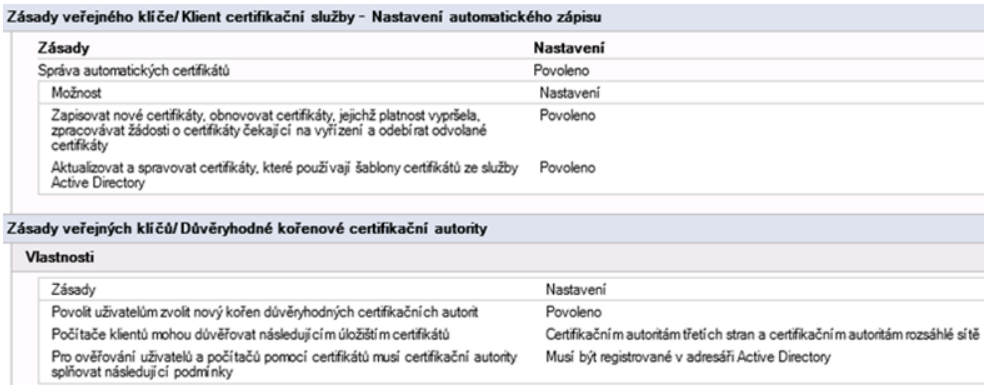
Automatického vydávání certifikátů bylo docíleno pomocí správy zásad skupiny NT domény, tzv. GPO. Za tímto účelem byla zřízena speciální organizační jednotka v AD pojmenovaná „server-with-certificate“. Pro novou jednotku se vytvořil propojený objekt zásad skupiny, jinými slovy konfigurační politika pojmenovaná „auto-enroll-SERVER-certificate“. Jedná se o zásadu „konfigurace počítače“, „nastavení systému“, „nastavení zabezpečení“, „zásady veřejných klíčů“. Konfiguraci a výsledné nastavení zásady znázorňuje Obrázek 22 a 23.

Obrázek 22: Konfigurace GPO – AutoEnroll Server Certificate



Zdroj: autor

Obrázek 23: Nastavení GPO – AutoEnroll Server Certificate



Zdroj: autor

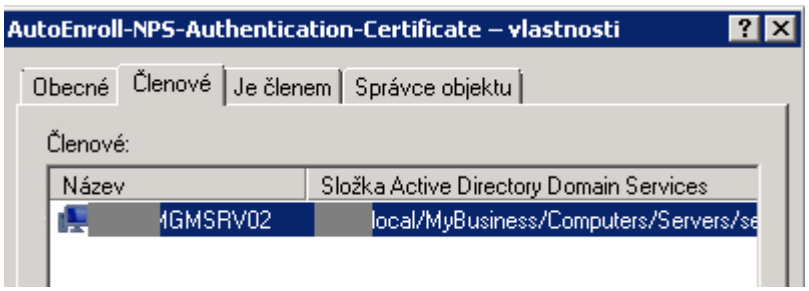
4.7 NPS server

Network Policy Server od společnosti Microsoft bude sloužit jako autentizační RADIUS server.

4.7.1 Instalace NPS serveru

Network Policy Server je provozován v OS Microsoft Windows serveru verze 2008 R2 standard. Server byl nainstalován obvyklým způsobem a připojen do existující NT domény. Nový Windows server musí být členem vytvořené skupiny zabezpečení pro automatické vydávání certifikátů. Obrázek 24 zobrazuje členství ve skupině.

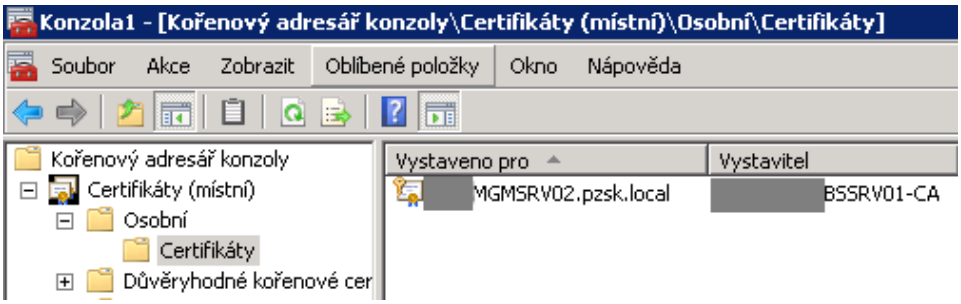
Obrázek 24: Členství NPS ve skupině zabezpečení



Zdroj: autor

Důležité je, aby server byl umístěn v připravené organizační jednotce v Active Directory „server-with-certificate“. Po přemístění serveru do správného místa v AD a opětovném načtení zásad skupiny, které lze vynutit příkazem „gpupdate /f“ nebo restartem operačního systému serveru, dojde k automatickému vydání a nahrání serverového certifikátu. Na certifikační autoritě můžeme ověřit úspěšné vydání, které lze vidět na Obrázku 25.

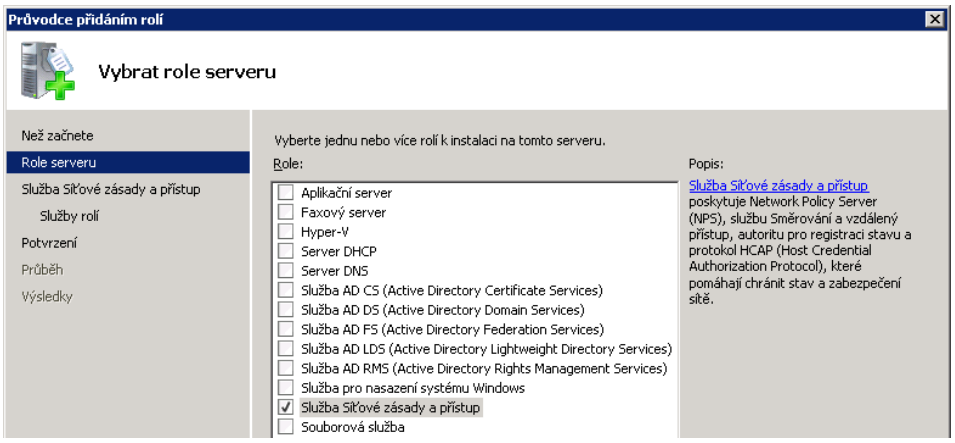
Obrázek 25: CA – vydaný certifikát pro NPS



Zdroj: autor

Po vydání certifikátů následuje instalace služby síťové zásady a přístup, tzv. Network Policy Server zkráceně NPS. Postup instalace role je zřejmý z obrázku 26.

Obrázek 26: Instalace NPS

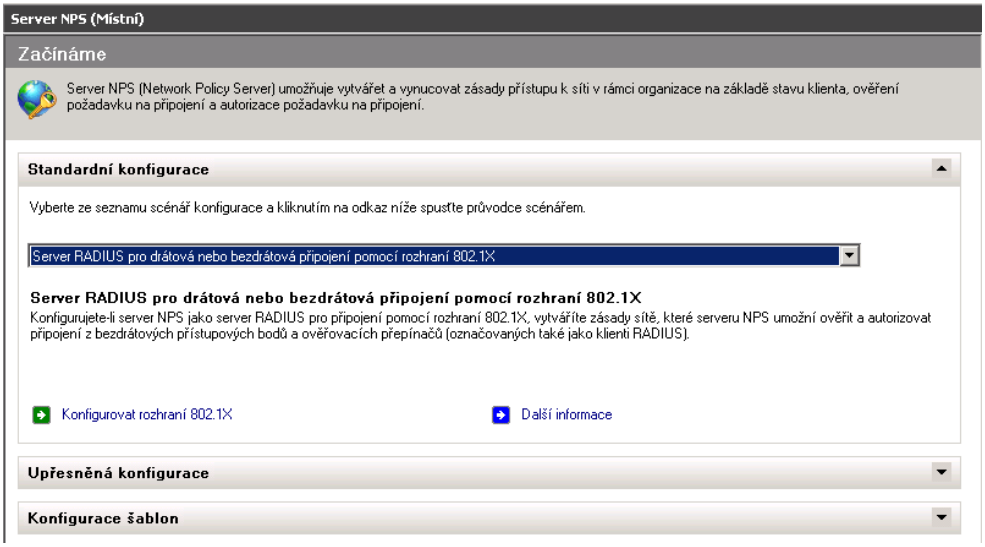


Zdroj: autor

4.7.2 Konfigurace RADIUS klientů

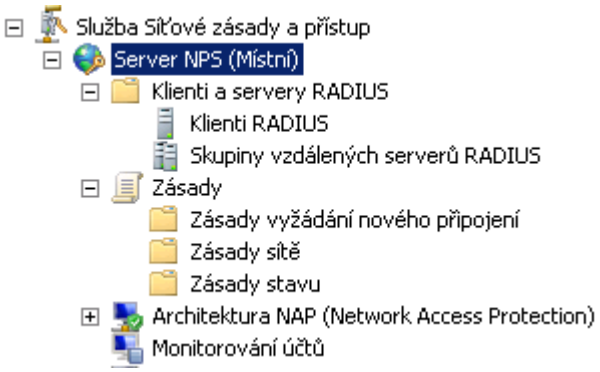
Na připraveném NPS serveru bylo nezbytné nastavit klienty RADIUS, způsoby a protokoly ověřování a další parametry zajišťující správnou funkčnost autentizace uživatelů při přístupu k počítačové síti, které popisují následující pasáže. Vzhled a organizace konfigurační konzole NPS serveru zobrazují Obrázek 27 a Obrázek 28.

Obrázek 27: Konzole serveru NPS #1



Zdroj: autor

Obrázek 28: Konzole serveru NPS #1



Zdroj: autor

Výslednou podobu konfigurace RADIUS klientů pro všechna síťová zařízení (autentizátory) lze vidět na Obrázku 29.

Obrázek 29: Klient RADIUS – výsledná konfigurace

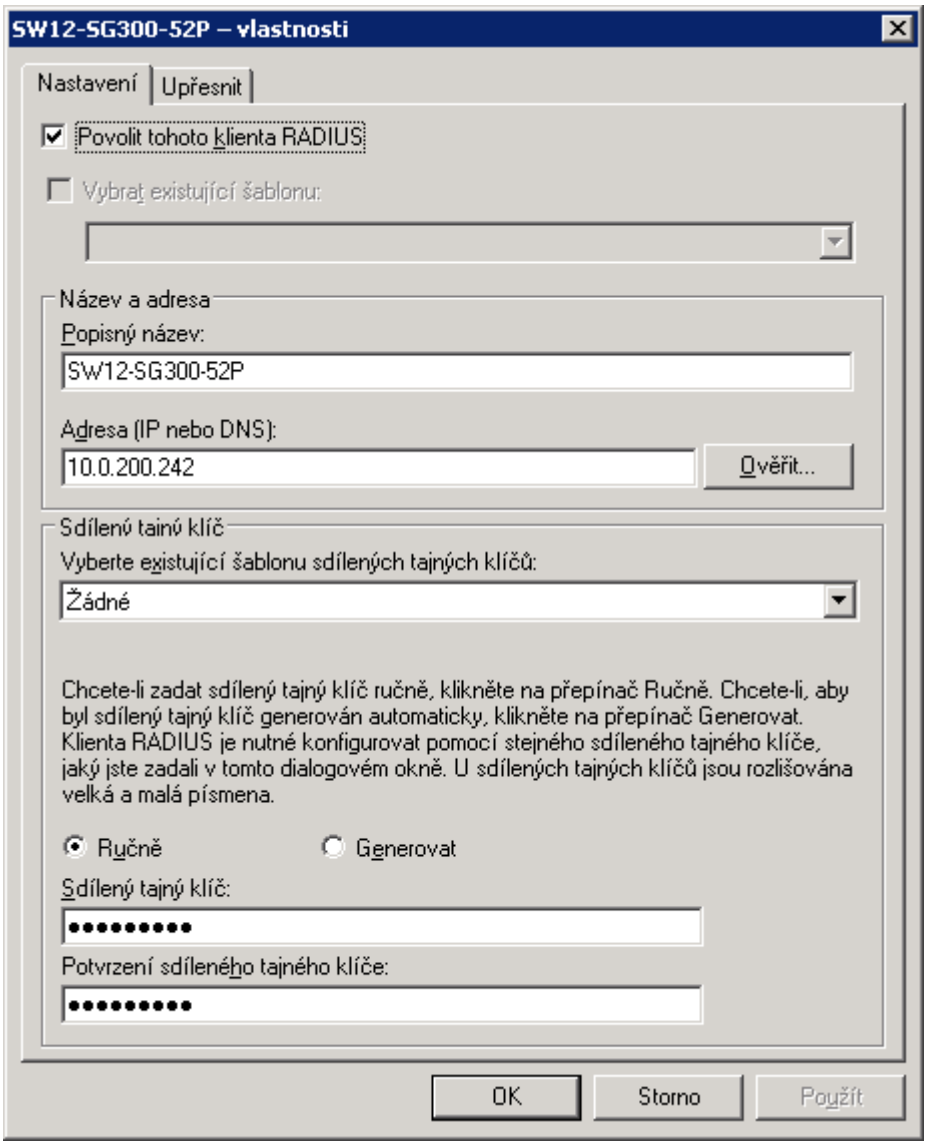
Popisný název	IP adresa	Výrobce zařízení	Podporující architekturu NAP	Stav
AP01-WiFi	10.0.200.18	RADIUS Standard	No	Povoleno
AP02-WiFi	10.0.200.19	RADIUS Standard	No	Povoleno
AP03-WiFi	10.0.200.20	RADIUS Standard	No	Povoleno
AP04-WiFi	10.0.200.21	RADIUS Standard	No	Povoleno
AP05-WiFi	10.0.200.22	RADIUS Standard	No	Povoleno
AP06-WiFi	10.0.200.23	RADIUS Standard	No	Povoleno
AP07-WiFi	10.0.200.24	RADIUS Standard	No	Povoleno
AP08-WiFi	10.0.200.25	RADIUS Standard	No	Povoleno
AP09-WiFi	10.0.200.26	RADIUS Standard	No	Povoleno
AP10-WiFi	10.0.200.27	RADIUS Standard	No	Povoleno
AP11-WiFi	10.0.200.28	RADIUS Standard	No	Povoleno
AP12-WiFi	10.0.200.29	RADIUS Standard	No	Povoleno
SW01-SG300-28P	10.0.200.231	RADIUS Standard	No	Povoleno
SW02-SG300-28P	10.0.200.232	RADIUS Standard	No	Povoleno
SW03-SG300-10P	10.0.200.233	RADIUS Standard	No	Povoleno
SW04-SG300-10P	10.0.200.234	RADIUS Standard	No	Povoleno
SW05-SG300-10P	10.0.200.235	RADIUS Standard	No	Povoleno
SW06-SG300-28P	10.0.200.236	RADIUS Standard	No	Povoleno
SW07-SG300-10P	10.0.200.237	RADIUS Standard	No	Povoleno
SW08-SG300-52P	10.0.200.238	RADIUS Standard	No	Povoleno
SW09-SG300-10P	10.0.200.239	RADIUS Standard	No	Povoleno
SW10-SG300-28P	10.0.200.240	RADIUS Standard	No	Povoleno
SW11-SG300-28P	10.0.200.241	RADIUS Standard	No	Povoleno
SW12-SG300-52P	10.0.200.242	RADIUS Standard	No	Povoleno
SW13-SG300-52P	10.0.200.243	RADIUS Standard	No	Povoleno
SW14-SG300-52P	10.0.200.244	RADIUS Standard	No	Povoleno
SW15-SG300-52P	10.0.200.245	RADIUS Standard	No	Povoleno
SW16-SG300-52P	10.0.200.246	RADIUS Standard	No	Povoleno

Zdroj: autor

4.7.2.1 LAN

Pro každý síťový přepínač musí být vytvořen RADIUS klient v konzoli NPS. V prvním kroku se konfigurují název klienta, IP adresa a sdílený tajný klíč pro RADIUS ověření klienta viz Obrázek 30.

Obrázek 30: LAN klient RADIUS – vlastnosti

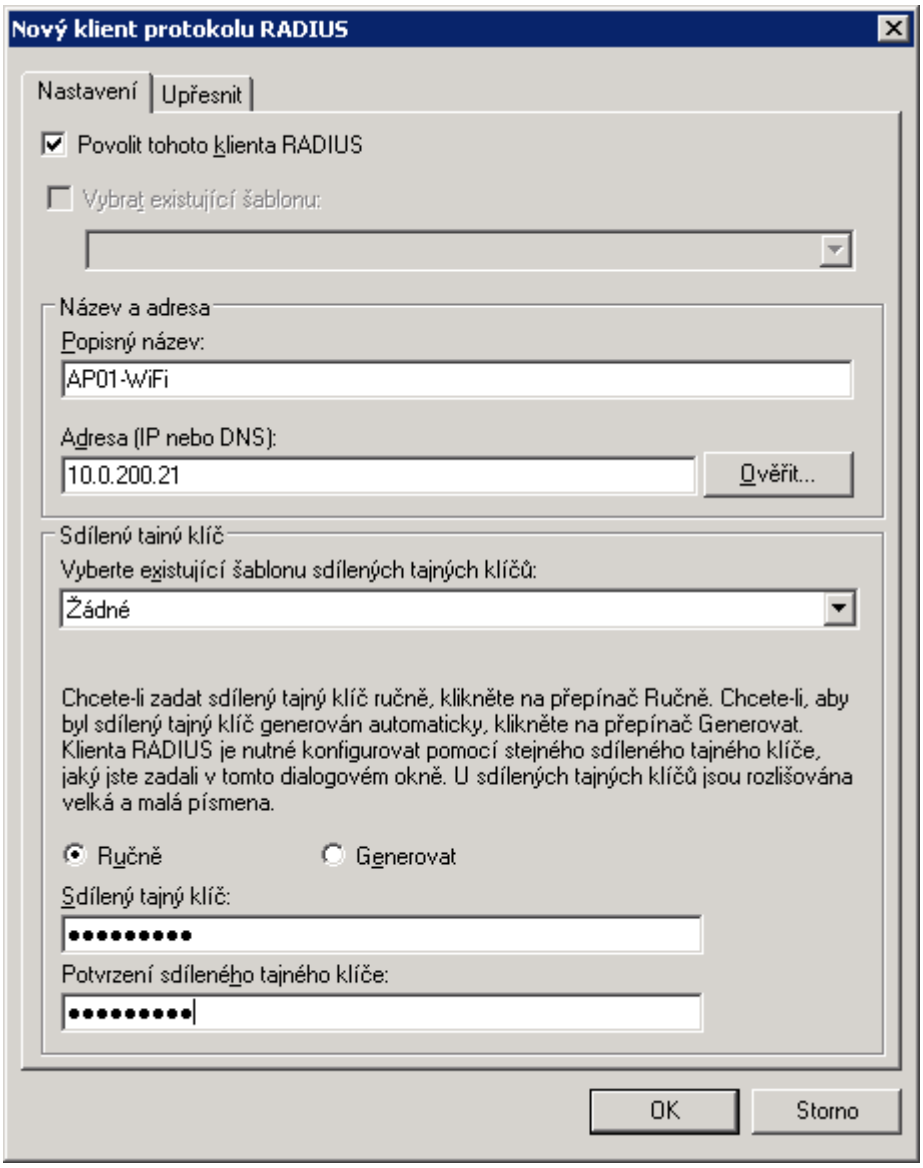


Zdroj: autor

4.7.2.2 WLAN

V případě bezdrátové sítě Wi-Fi dochází k ověřování přístupu z každého jednotlivého vysílače individuálně. Proto bylo nezbytné připravit RADIUS klientský profil pro všechny bezdrátové přístupové body. Postup nastavení je obdobný jako pro RADIUS klienty kabelové počítačové sítě. Konfiguraci vzorového případu znázorňuje Obrázek 31.

Obrázek 31: WLAN klient RADIUS – nový klient protokolu

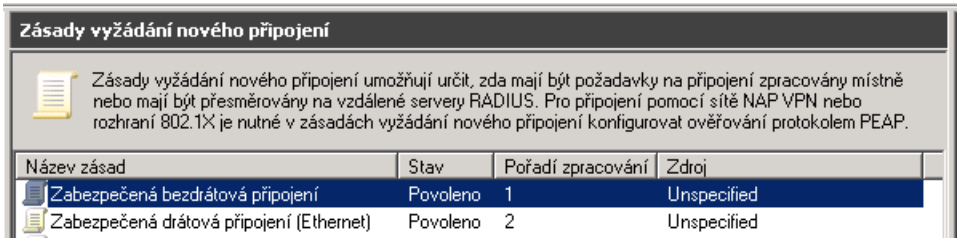


Zdroj: autor

4.7.3 Konfigurace zásad vyžádání nového připojení

Zásady vyžádání nového připojení, tzv. „Connection request policies“ definují sady podmínek a nastavení, které určuje, jaké RADIUS servery zajišťují autentizaci, autorizaci a monitorování požadavků připojení k síti [17]. Každá metoda přístupu k síti musí mít nakonfigurovánu „zásadu vyžádání nového připojení“. Výsledná podoba nastavení těchto zásad je zřejmá z Obrázku 32.

Obrázek 32: Zásady vyžádání nového připojení

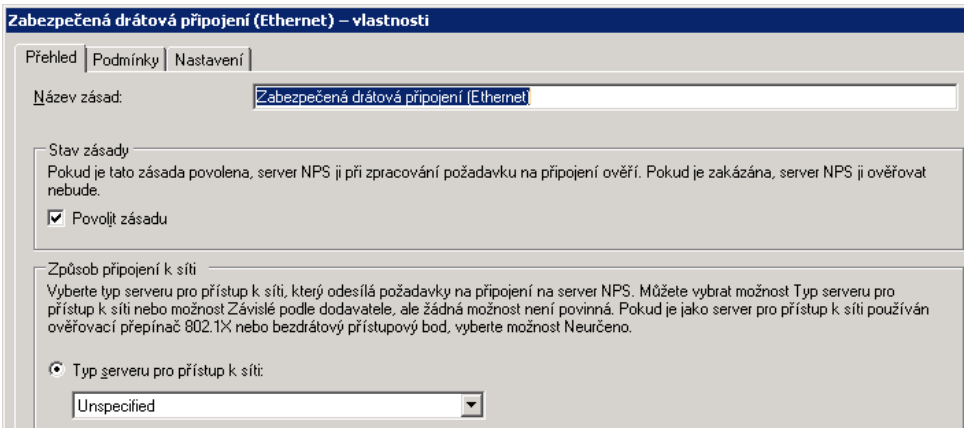


Zdroj: autor

4.7.3.1 LAN

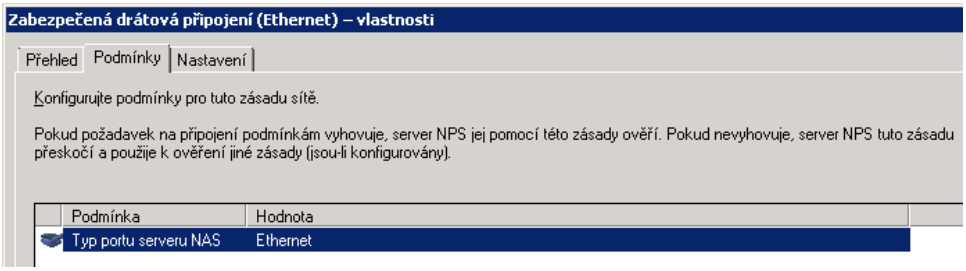
Pro potřeby kabelové počítačové sítě byla připravena zásada „Zabezpečená drátová připojení (Ethernet)“. Typ serveru pro přístup k síti není specifikovaný. Jediná podmínka této zásady je „Typ portu serveru NAS“ s hodnotou „Ethernet“. V záložce nastavení není třeba speciálních změn, většina nastavení bude řízena zásadami sítě. Všechny parametry jsou k vidění na Obrázcích 33, 34 a 35.

Obrázek 33: LAN zásada vyžádání připojení – přehled



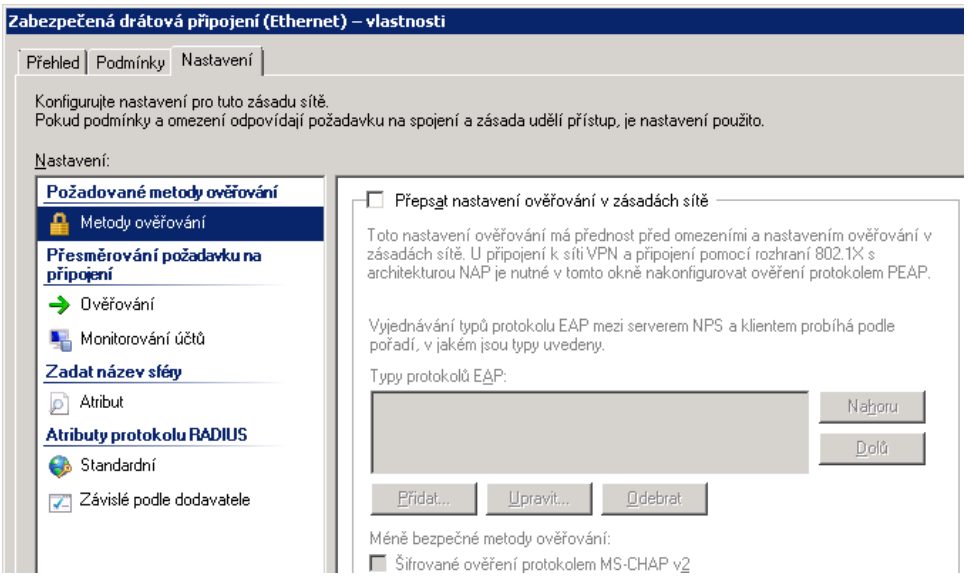
Zdroj: autor

Obrázek 34: LAN zásada vyžádání připojení – podmínky



Zdroj: autor

Obrázek 35: LAN zásada vyžádání připojení – nastavení

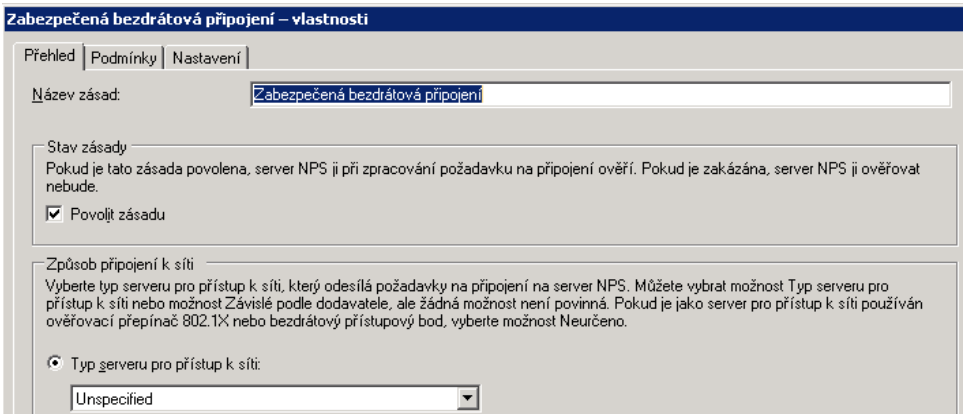


Zdroj: autor

4.7.3.2 WLAN

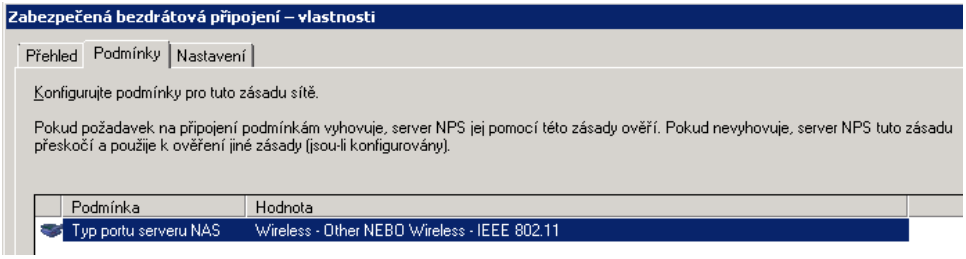
Obdobným způsobem byla přidána zásada vyžádání nového připojení pro bezdrátovou síť. Rozdíl je v podmínce zásady. Pro WLAN je nutné zvolit „Typ portu serveru NAS“ s hodnotou „Wireless – IEEE 802.11“. Graficky zachycují parametry Obrázky 36, 37 a 38.

Obrázek 36: WLAN zásada vyžádání připojení – přehled



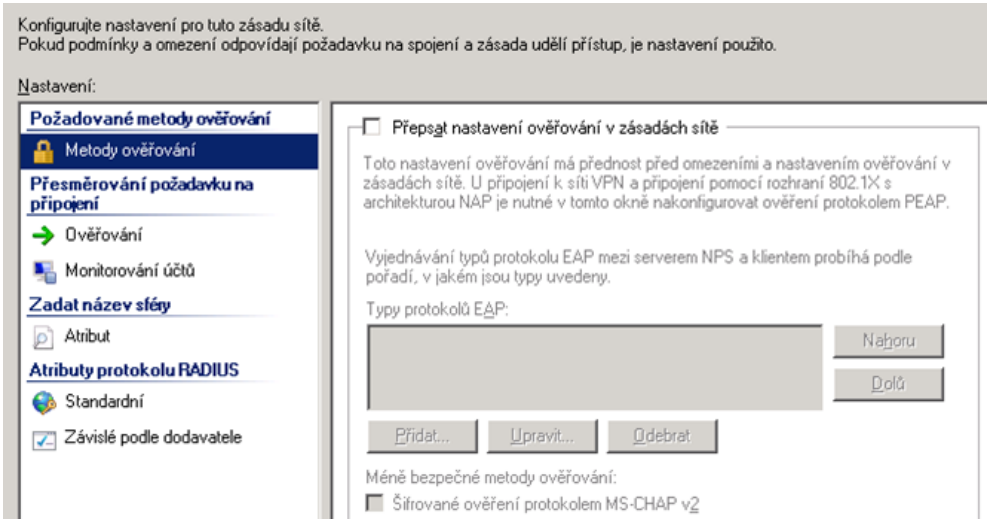
Zdroj: autor

Obrázek 37: WLAN zásada vyžádání připojení – podmínky



Zdroj: autor

Obrázek 38: WLAN zásada vyžádání připojení – nastavení



Zdroj: autor

4.7.4 Konfigurace zásad sítě

Zásady sítě, tzv. „Network policies“ jsou sady podmínek, omezení a nastavení, které určují, kdo se smí připojit k síti a jejich pravidla. Ke konfiguraci zásad sítě mohou být přiřazeny zásady stavu tzv. „Health policies“. Tyto zásady umožňují během procesu ověřování, aby NPS server prováděl kontrolu stavu nastavení a zabezpečení klientů. Zásady sítě umožňují definovat různé podmínky mnoha druhů, jako např. omezení na operační systémy, vlastnosti klientů RADIUS, časová omezení, předávat RADIUS atributy například číslo VLAN, atp. Důležité je pořadí jednotlivých zásad, které udržuje sled, ve kterém se zpracovávají. To znamená, že nejkonkrétnější a důležitější, musí být navrchu seznamu. [17]

Výslednou podobu zásad sítě pro všechny skupiny a virtuální sítě lze vidět na Obrázku 32.

Obrázek 39: LAN zásada sítě – výsledná konfigurace

Zásady sítě umožňují určit uživatele oprávněné připojit se k síti a okolnosti, za kterých se lze či nelze připojit.

Název zásad	Stav	Pořadí zpracování	Druh přístupu	Zdroj
Zabezpečená drátová připojení (Ethernet) - vlan70	Zakázáno	1	Udělit přístup	Unspecified
Zabezpečená drátová připojení (Ethernet) - vlan60	Zakázáno	2	Udělit přístup	Unspecified
Zabezpečená drátová připojení (Ethernet) - vlan50	Zakázáno	3	Udělit přístup	Unspecified
Zabezpečená drátová připojení (Ethernet) - vlan40	Zakázáno	4	Udělit přístup	Unspecified
Zabezpečená drátová připojení (Ethernet) - vlan30	Povoleno	5	Udělit přístup	Unspecified
Zabezpečená drátová připojení (Ethernet) - vlan20	Zakázáno	6	Udělit přístup	Unspecified
Zabezpečená drátová připojení (Ethernet) - vlan200	Zakázáno	7	Udělit přístup	Unspecified
Zabezpečená drátová připojení (Ethernet)	Povoleno	8	Udělit přístup	Unspecified
Zabezpečená bezdrátová připojení	Povoleno	9	Udělit přístup	Unspecified

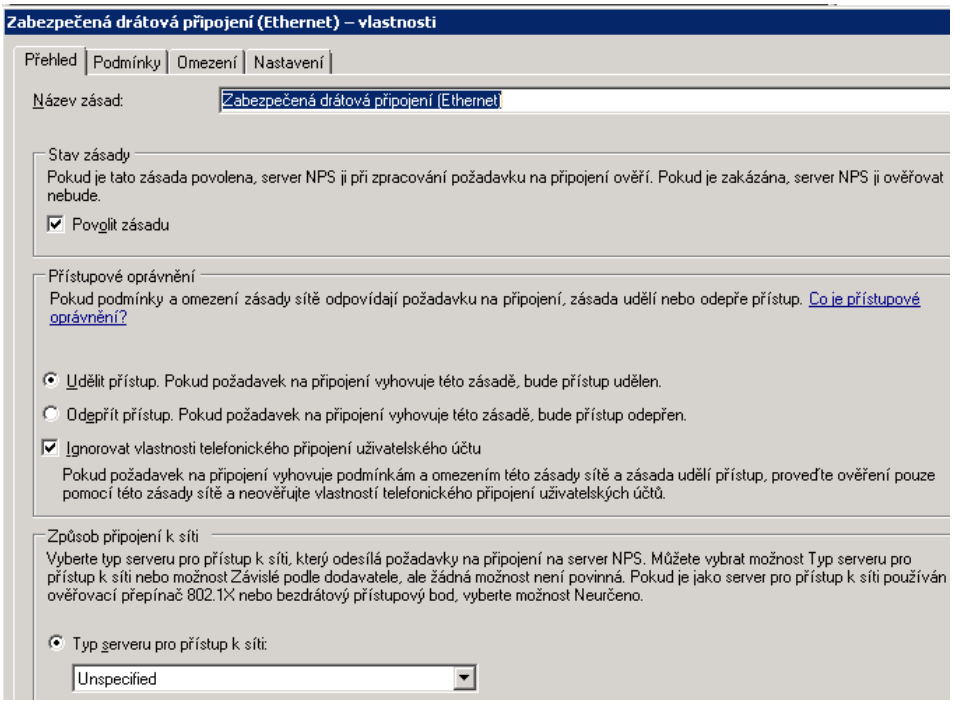
Zdroj: autor

4.7.4.1 LAN

V zásadách sítě pro kabelovou počítačovou síť byly použity podmínky „typ portu NAS“ na hodnotu „Ethernet“ a skupinu uživatelů „Domain Users“. To znamená, že každý uživatel NT domény společnosti, má oprávnění autentizovat se při přístupu k síti. V záložce omezení je nutné zvolit metodu ověřování, konkrétně PEAP protokol. V rozšířené konfiguraci se použije správný serverový certifikát, povolí rychlé obnovení připojení a zvolí typ EAP protokolu – „zabezpečené heslo (EAP–MSACHAP v2)“. V záložce nastavení

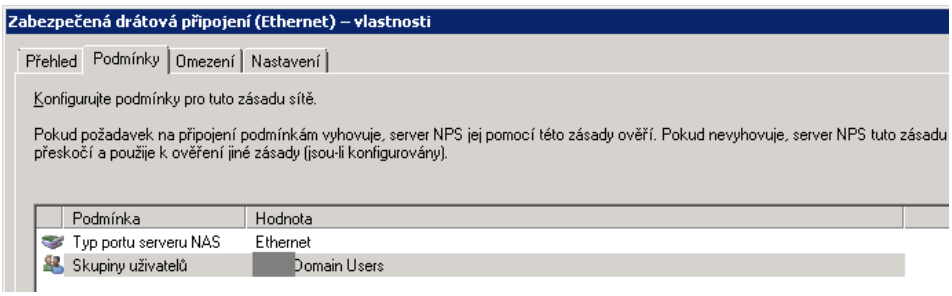
se zadají potřebné atributy protokolu RADIUS. Konkrétně atribut č. 65 jménem „Tunnel-Medium-Type“ s hodnotou „802 (includes all 802 media plus Ethernet canonical format)“. Pro zásady, které nastavují specifickou VLAN, bylo nezbytné konfigurovat atribut „Tunnel-Type“ č. 64 s hodnotou „Virtual LANs (VLAN) a atribut č. 81 s hodnotou konkrétní VLAN, například „10“. Konfigurace zásad sítě pro LAN je zřejmá z Obrázků 40, 41, 42, 43 a 44.

Obrázek 40: LAN zásada sítě – přehled



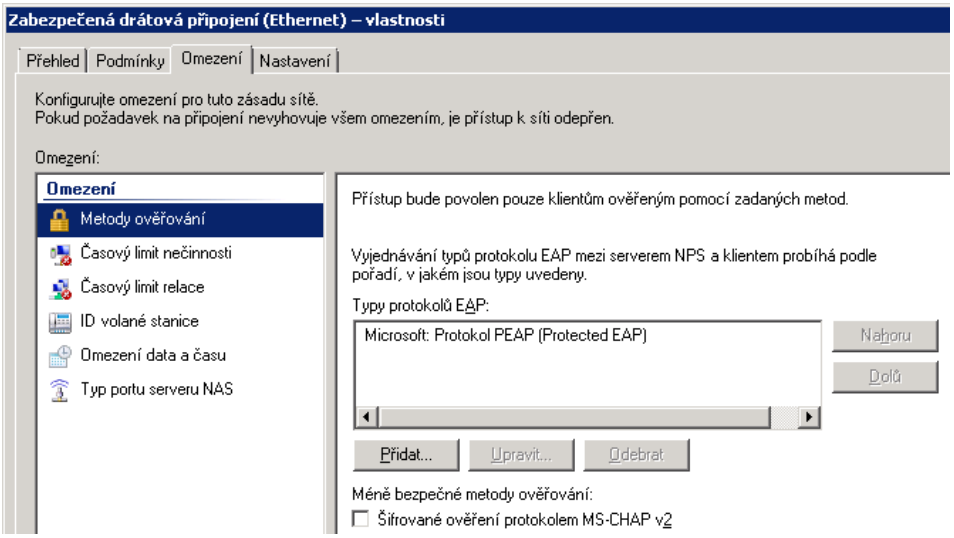
Zdroj: autor

Obrázek 41: LAN zásada sítě – podmínky



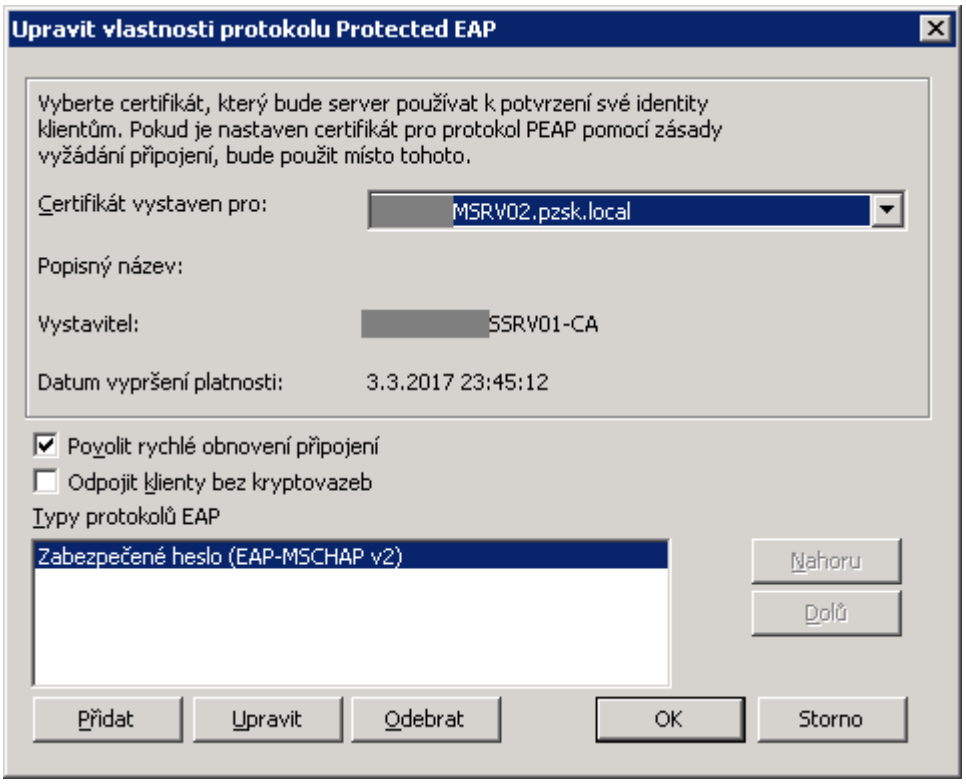
Zdroj: autor

Obrázek 42: LAN zásada sítě – metoda ověřování



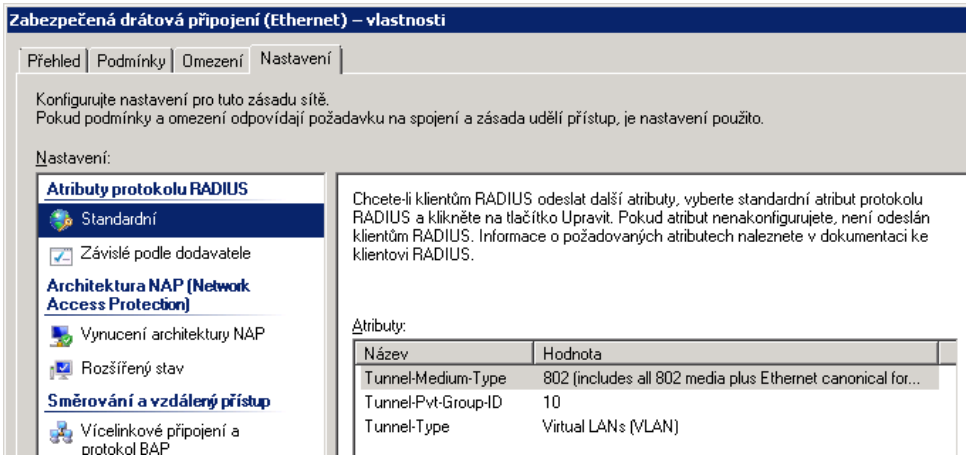
Zdroj: autor

Obrázek 43: LAN zásada sítě – vlastnosti PEAP protokolu



Zdroj: autor

Obrázek 44: LAN zásada sítě – nastavení atributů RADIUS

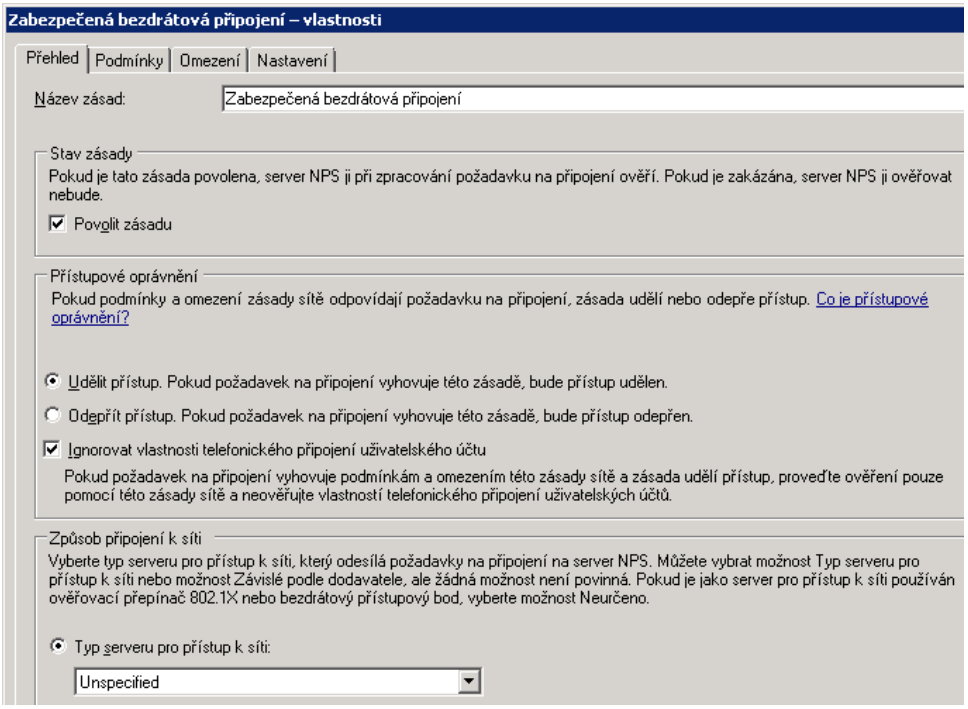


Zdroj: autor

4.7.4.2 WLAN

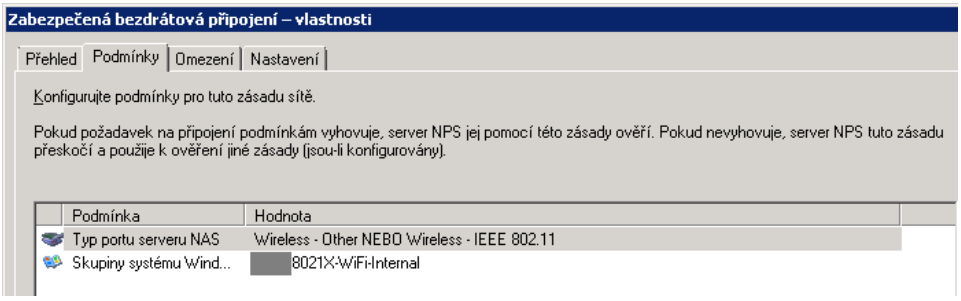
Zásada sítě pro bezdrátovou počítačovou síť byla potřeba pouze jedna. Konfiguruje se obdobným způsobem, jako pro LAN. Rozdíl je pouze v podmínkách zásady a RADIUS atributech. Pro WLAN byla použita připravená skupina zabezpečení v AD identifikující uživatele oprávněné používat interní bezdrátovou síť. Podmínka „typ portu NAS“ je nastavena na hodnotu „Wireless – IEEE 802.11“. Atributy pro WLAN nejsou potřeba žádné specifické. Vlan je v tomto případě řízena aplikací pro správu bezdrátových sítí. Vše znázorňují Obrázky 45, 46, 47, 48 a 49.

Obrázek 45: WLAN zásada sítě – přehled



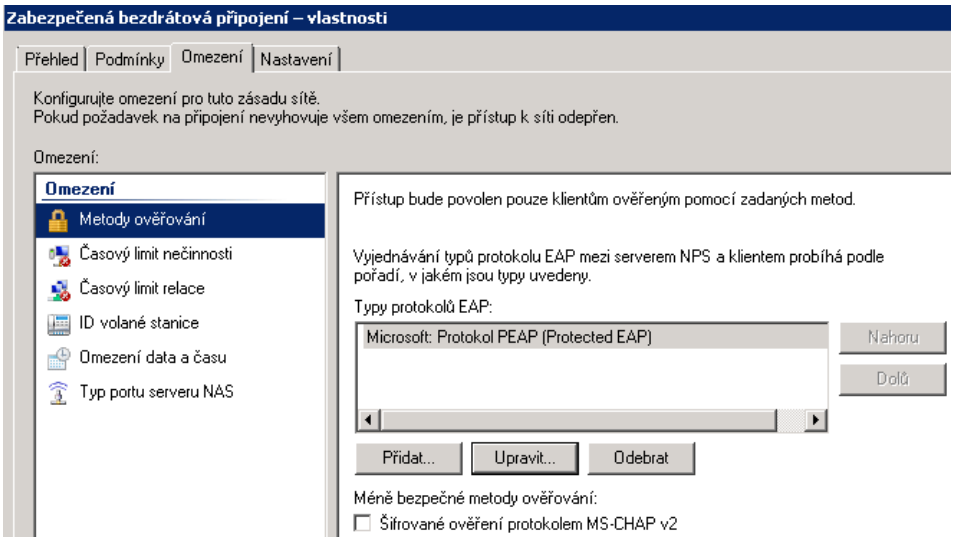
Zdroj: autor

Obrázek 46: WLAN zásada sítě – podmínky



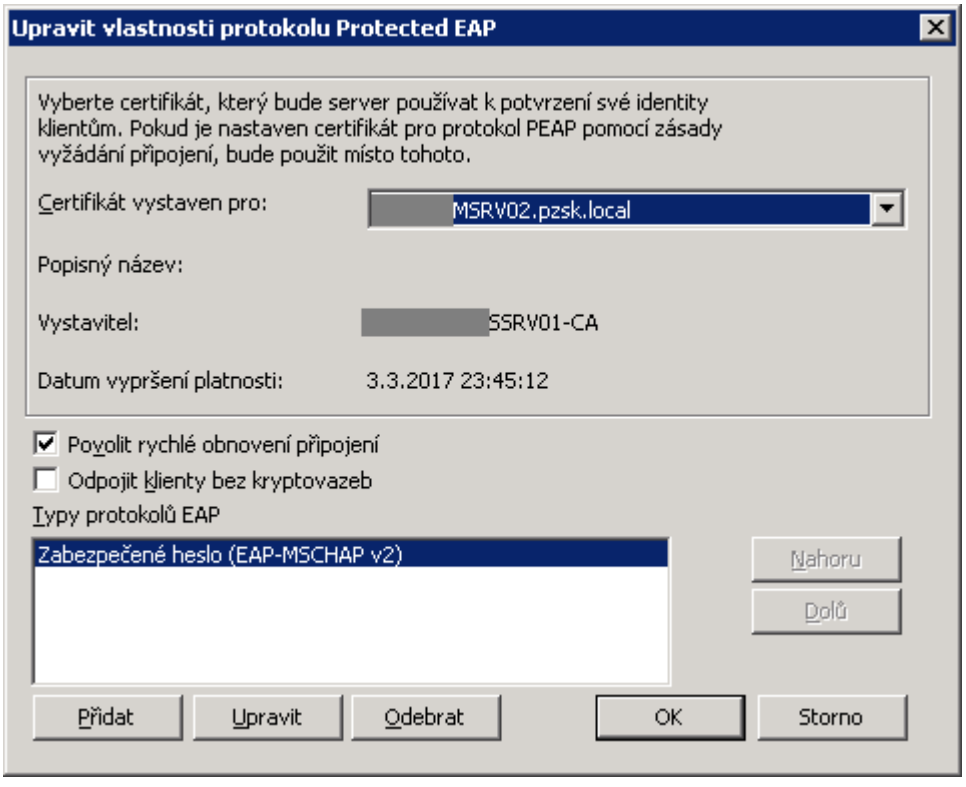
Zdroj: autor

Obrázek 47: WLAN zásada sítě – metoda ověřování



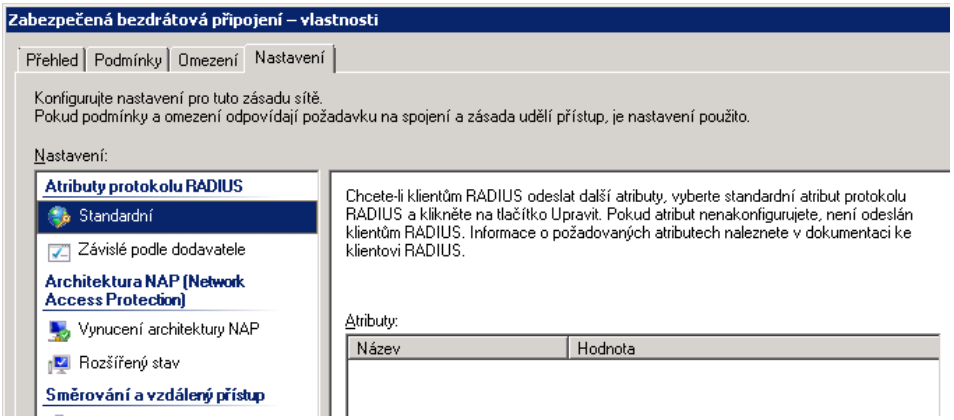
Zdroj: autor

Obrázek 48: WLAN zásada sítě – vlastnosti PEAP protokolu



Zdroj: autor

Obrázek 49: WLAN zásada sítě – nastavení atributů



Zdroj: autor

4.8 Síťové prvky

Správné nastavení aktivních síťových prvků je nedílnou součástí konfigurace zabezpečeného přístupu k lokální počítačové síti. Podpora standardu IEEE 802.1X musí být zapnuta a nastavena na všech síťových přepínačích, i přístupových bodech bezdrátové počítačové sítě.

4.8.1 Konfigurace síťových přepínačů

Nastavení síťových přepínačů obnáší povolení autentizace 802.1X, definici RADIUS serveru, konfigurace jednotlivých síťových portů pro podporu 802.1X s možnými způsoby autentizace, konfiguraci VLAN a dalších parametrů. Tyto změny se týkají portů, které slouží pro připojení klientských počítačů, zařízení a všech volně dostupných nepoužitých portů. Následující kapitoly popisují nastavení potřebných parametrů.

4.8.1.1 Vytvoření „Guest VLAN“

„Guest VLAN“ je výchozí virtuální síť, do které jsou automaticky přepnuté všechny neautorizované síťové porty přepínače, zároveň VLAN, přiřazená neautorizovaným klientům a zařízením [18]. Vytvoření a parametry pro konfiguraci VLAN na přepínači jsou zřejmé z Příkladu 1.

Příklad 1: Konfigurace „Guest VLAN“ – Cisco

```
sw12-SG300-52P#show running-config
…
vlan database
vlan 999
exit
interface vlan 999
 name guest
 dot1x guest-vlan
…
```

Zdroj: autor

Pro správnou funkčnost bylo nutné vytvořit a nastavit VLAN rozhraní virtuální sítě na centrálním směrovači a DHCP server pro tuto síť. Správné nastavení zobrazuje Příklad 12.

Příklad 2: Konfigurace „Guest VLAN“ – VLAN a DHCP – Mikrotik – CLI

```
/interface vlan
add comment="guest vlan" interface=ether2 l2mtu=1516 \
    name=vlan999 vlan-id=999
/ip address
add address=10.9.99.1/24 comment=guest-vlan-interface \
    interface=vlan999 network=10.9.99.0
/ip dhcp-server network
add address=10.9.99.0/24 gateway=10.9.99.1
/ip pool
add name=d dhcp_guestvlan ranges=10.9.99.18-10.9.99.254
/ip dhcp-server
add address-pool=dhcp_guestvlan disabled=no interface=vlan999 \
    name=dhcpVlan999
```

Zdroj: autor

Možnosti případného administrativního přístupu ke stanicím, které nezískali oprávnění přístupu do sítě, bylo docíleno povolením jednosměrné komunikace z administrátorských stanic do „Guest VLAN“ v síťovém firewallu dle Příkladu 3. Povolen byl protokol Remote Desktop, VNC a SSH pro vzdálené ovládání zařízení, protokol http a HTTPS pro možnost konfigurace pře webové rozhraní.

Příklad 3: Konfigurace „Guest VLAN“ – firewall – Mikrotik – CLI

```
/ip firewall filter
add chain=forward comment=\
    "POVOL ADMIN komunikaci do GUEST vlan" dst-address=\
    10.9.99.0/24 dst-port=22,80,443,3389,5900 protocol=tcp \
    src-address-list="Administratori"
```

Zdroj: autor

4.8.1.2 Vytvoření „unauthenticated VLAN“

Neautentizovaná VLAN je dostupná virtuální síť i bez ověření. Takto dostupných sítí může být nastaveno i více. Slouží například pro potřeby klientů, kteří nesplňují požadavky na autentizaci [18]. Postup přípravy této VLAN pro případné budoucí použití naznačuje Příklad 4 a Příklad 5.

Příklad 4: Konfigurace „unauthenticated VLAN“ – Cisco

```
sw12-SG300-52P#show running-config
…
vlan database
vlan 998
exit
interface vlan 998
 name unauthenticated-vlan
 dot1x auth-not-req
…
```

Zdroj: autor

Příklad 5: Konfigurace „unauthenticated VLAN“ – VLAN – Mikrotik – CLI

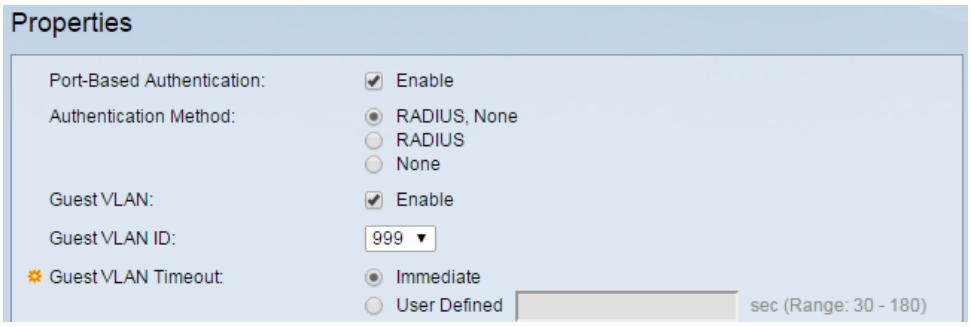
```
/interface vlan
add comment="unauth vlan" interface=ether2 l2mtu=1516 \
    name=vlan998 vlan-id=998
/ip address
add address=10.9.98.1/24 comment=guest-vlan-interface \
    interface=vlan998 network=10.9.98.0
```

Zdroj: autor

4.8.1.3 Povolení 802.1X

Na přepínačích je nezbytné mít aktivovanou metodu ověřování přístupů k síti, tzv. „Port-Based Authentication“. Jedná se o standard IEEE 802.1X. Autentizační metoda byla zvolena kombinace „RADIUS, NONE“. Ta zajišťuje, že autentizovaní uživatelé a zařízení získají přístup do sítě, neautentizovaní nikoliv. Zároveň řeší situaci nedostupnosti RADIUS serveru, který je v podniku v provozu pouze jeden. V takovém případě se bude přepínač chovat shodně jako před konfigurací 802.1X. Toto je volba, které mírně snižuje bezpečnost řešení a je náchylná například na DDOS síťový útok mířený na RADIUS server, ale zároveň zvyšuje schopnost podniku vykonávat svou činnost i při neočekávaném výpadku autentizačních serverů z důvodu poruchy. Při nastavené vynucení automatické opakované autentizace k síťovým portům a dalším bezpečnostním opatřením v infrastruktuře podniku, bylo toto riziko a řešení schváleno jako akceptovatelné. Způsob nastavení pomocí webového i příkazového rozhraní tzv. CLI, zobrazují Obrázek 50 a Příklad 6.

Obrázek 50: Konfigurace 802.1X – Cisco – web



Zdroj: autor

Příklad 6: Konfigurace 802.1X – Cisco – CLI

```
sw12-SG300-52P#show running-config
…
aaa authentication dot1x default radius none
…
```

Zdroj: autor

4.8.1.4 Nastavení RADIUS serveru

Dalším krokem instalace byla konfigurace RADIUS serveru na každém síťovém přepínači. Přidání RADIUS serveru obnáší nastavení především parametrů IP adresy serveru, tajného sdíleného klíče, dobu čekání na odpověď serveru, čísel portů protokolu RADIUS pro autentizaci a účtování, počet opakovaných pokusů ověření. Účel použití serveru byl zvolen ALL, aby bylo možné do budoucna použít server i pro autentizaci přístupu ke konfiguračnímu rozhraní přepínačů. Konkrétní hodnoty jsou k vidění na Obrázku 51 a Příkladu 7.

Obrázek 51: Konfigurace RADIUS – Cisco – web

Zdroj: autor

Příklad 7: Konfigurace RADIUS – Cisco – CLI

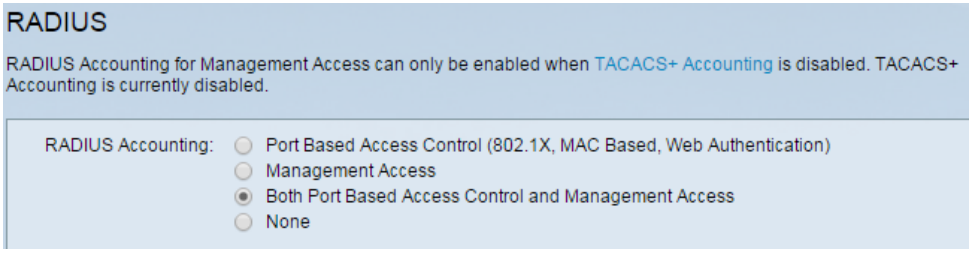
```
sw12-SG300-52P#show running-config
…
encrypted radius-server host 10.0.0.247 key ****** priority 1
usage all
…
```

Zdroj: autor

4.8.1.5 Nastavení RADIUS účtování

Accounting neboli účtování bylo výhodné povolit pro ověřování uživatelů při přístupu k síťovým portům i pro přístup k administrativní správě prvků. Obrázek 52 vyobrazuje nastavení těchto vlastností přes webové rozhraní, Příklad 8 pomocí příkazové řádky administrativní konzole.

Obrázek 52: Konfigurace účtování – Cisco – web



Zdroj: autor

Příklad 8: Konfigurace účtování – Cisco – CLI

```
sw12-SG300-52P#show running-config
…
aaa accounting dot1x start-stop group radius
…
```

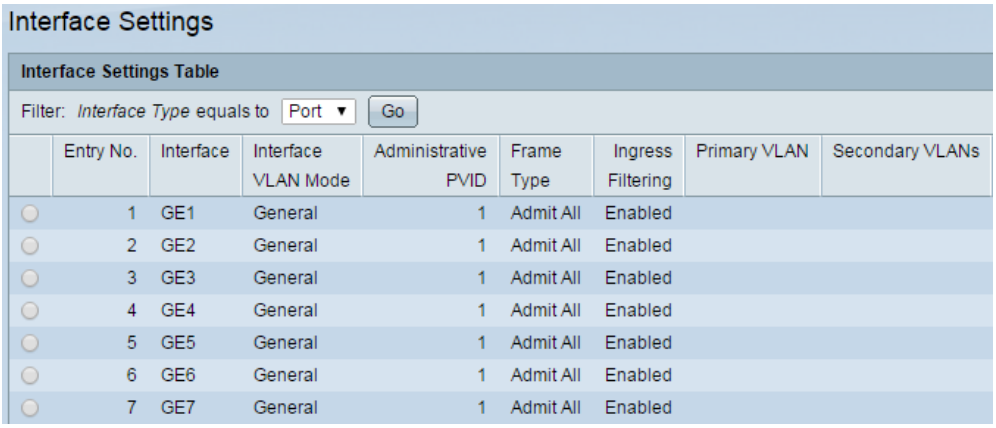
Zdroj: autor

4.8.1.6 Nastavení Ethernet portů

- Režim síťových portů (port mode)

Porty byly nakonfigurovány do módu „general“, aby bylo do budoucna možné využít více označkovaných, tzv. „tagged“ i neoznačkovaných, tzv. „untagged“ virtuálních sítí na jednom síťovém portu. Způsob nastavení je zřejmý z Obrázku 53.

Obrázek 53: Konfigurace režimu portů – Cisco – web



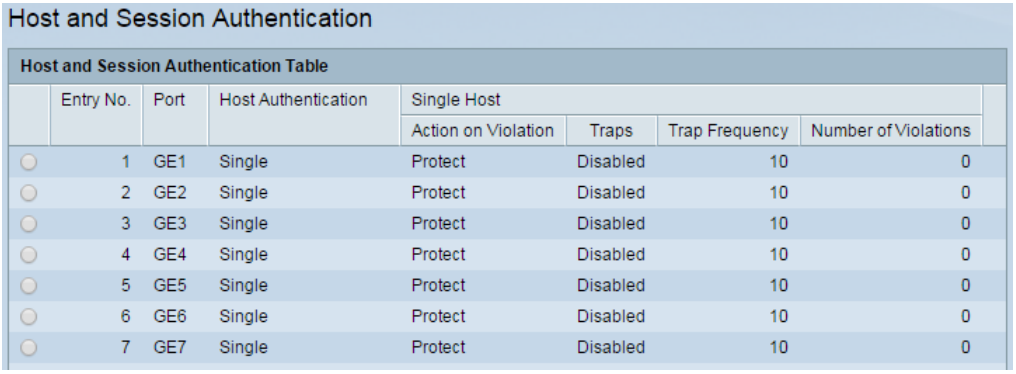
Entry No.	Interface	Interface VLAN Mode	Administrative PVID	Frame Type	Ingress Filtering	Primary VLAN	Secondary VLANs
1	GE1	General	1	Admit All	Enabled		
2	GE2	General	1	Admit All	Enabled		
3	GE3	General	1	Admit All	Enabled		
4	GE4	General	1	Admit All	Enabled		
5	GE5	General	1	Admit All	Enabled		
6	GE6	General	1	Admit All	Enabled		
7	GE7	General	1	Admit All	Enabled		

Zdroj: autor

- Režim 802.1X síťových portů

Režim 802.1X byl vybrán „single host“, který umožňuje připojit a ověřit pouze jedno zařízení na jednom síťovém portu. Zamezí se tak nežádoucímu a neoprávněnému připojování a rozšiřování sítě dalšími síťovými přepínači. Data z neautorizovaných zařízení na takovém portu jsou při nastavení akce „protect“ zahozena, viz Obrázek 54.

Obrázek 54: Konfigurace režimu 802.1X – Cisco – web

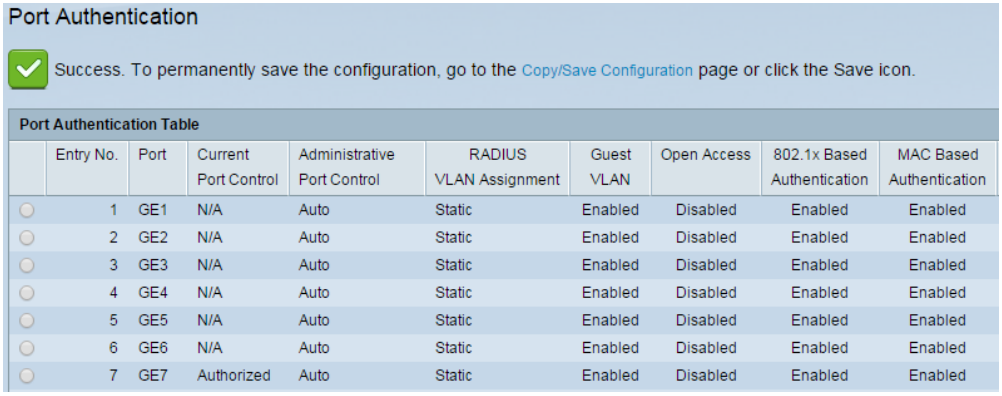


Zdroj: autor

- Autentizace síťových portů

Autentizace na jednotlivých portech se zapíná v sekci „port authentication“. Pro potřeby podniku bylo zapotřebí použít „Administrative Port Control“ možnost auto, kdy stav portu autorizovaný/neautorizovaný je závislý na výsledku ověření klienta či zařízení. Přiřazování konkrétních čísel VLAN je možné díky zapnutému parametru „RADIUS VLAN Assignment“. Přepínač „static“ říká, že v případě chybějícího nebo nesprávného atributu pro číslo VLAN, bude port po úspěšné autentizaci nastaven dle své statické konfigurace. „Guest VLAN“ byla povolena. „Open Accessů v produkčním provozu není žádoucí, viz kapitola 4.11. Dále bylo nezbytné povolit vlastní 802.1X autentizaci a záložní metodu autentizace pomocí MAC adres. MAC adres autentizaci se podrobně věnuje kapitola 4.10. Obrázek 55 zachycuje zmíněné parametry.

Obrázek 55: Konfigurace 802.1X autentizace – Cisco – web



Port Authentication

Success. To permanently save the configuration, go to the Copy/Save Configuration page or click the Save icon.

Port Authentication Table

	Entry No.	Port	Current Port Control	Administrative Port Control	RADIUS VLAN Assignment	Guest VLAN	Open Access	802.1x Based Authentication	MAC Based Authentication
○	1	GE1	N/A	Auto	Static	Enabled	Disabled	Enabled	Enabled
○	2	GE2	N/A	Auto	Static	Enabled	Disabled	Enabled	Enabled
○	3	GE3	N/A	Auto	Static	Enabled	Disabled	Enabled	Enabled
○	4	GE4	N/A	Auto	Static	Enabled	Disabled	Enabled	Enabled
○	5	GE5	N/A	Auto	Static	Enabled	Disabled	Enabled	Enabled
○	6	GE6	N/A	Auto	Static	Enabled	Disabled	Enabled	Enabled
○	7	GE7	Authorized	Auto	Static	Enabled	Disabled	Enabled	Enabled

Zdroj: autor

Celková konfigurace a všechny nezbytné parametry portu jsou k disposici v Příkladu 9.

Příklad 9: Konfigurace rozhraní – Cisco – CLI

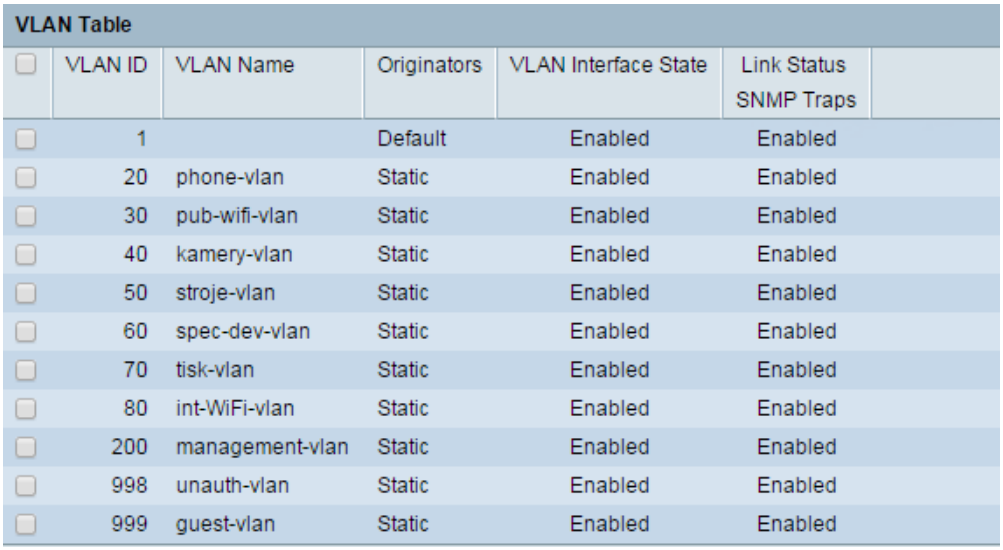
```
sw12-SG300-52P#show running-config interface GE 7

interface gigabitethernet7
 dot1x host-mode single-host
 dot1x violation-mode protect trap 10
 dot1x guest-vlan enable
 dot1x reauthentication
 dot1x authentication 802.1x mac
 dot1x radius-attributes vlan static
 dot1x port-control auto
 switchport mode general
!
```

Zdroj: autor

4.8.1.7 Nastavení potřebných VLAN

Dle topologie sítě byly vytvořeny potřebné VLAN. Výsledek je zachycen na Obrázku 56 a v Příkladu 10 a 11.

Obrázek 56: Konfigurace VLAN – Cisco – web



VLAN Table

VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps
1		Default	Enabled	Enabled
20	phone-vlan	Static	Enabled	Enabled
30	pub-wifi-vlan	Static	Enabled	Enabled
40	kamery-vlan	Static	Enabled	Enabled
50	stroje-vlan	Static	Enabled	Enabled
60	spec-dev-vlan	Static	Enabled	Enabled
70	tisk-vlan	Static	Enabled	Enabled
80	int-WiFi-vlan	Static	Enabled	Enabled
200	management-vlan	Static	Enabled	Enabled
998	unauth-vlan	Static	Enabled	Enabled
999	guest-vlan	Static	Enabled	Enabled

Zdroj: autor

Příklad 10: Konfigurace VLAN – Cisco – CLI #1

```
sw12-SG300-52P#show running-config
…
vlan database
vlan 20,30,40,50,60,70,80,200,998-999
exit
…
interface vlan 20
 name phone-vlan
!
interface vlan 30
 name pub-wifi-vlan
!
interface vlan 40
 name kamerova-vlan
!
interface vlan 50
 name stroje-vlan
!
interface vlan 60
 name spec-dev-vlan
!
interface vlan 70
 name tisk-vlan
…
```

Zdroj: autor

Příklad 11: Konfigurace VLAN – Cisco – CLI #2

```
sw12-SG300-52P#show running-config
…
interface vlan 80
 name int-WiFi-vlan
!
interface vlan 200
 name management-vlan
 ip address 10.0.200.242 255.255.255.0
!
interface vlan 998
 name unauth-vlan
!
interface vlan 999
 name guest-vlan
 dot1x guest-vlan
!
…
```

Zdroj: autor

4.8.1.8 Nastavení firewallu

Autentizační prvky a autentizační server jsou z bezpečnostních důvodů umístěny v různých sítích. Pro jejich komunikaci bylo nezbytné povolit RADIUS protokol na centrálním síťovém firewallu. RADIUS využívá protokolu UDP s číslem 1812 pro autentizaci a č. 1813 pro účtování. Konkrétní provedení konfigurace vystihuje Příklad 12.

Příklad 12: Konfigurace firewallu – Mikrotik – CLI

```
/ip firewall address-list
add address=10.0.200.0/24 list=management_network
add address=10.0.0.247 comment="NPS server" list=radius_servers

/ip firewall filter
add chain=forward comment=\
    "POVOL autentizaci RADIUS protokolem z MGM site" \
    dst-address-list=radius_servers dst-port=1812,1813 log=\
    yes log-prefix=ALLOW-LAN-RADIUS-TO-NPS protocol=udp \
    src-address-list=management_network
```

Zdroj: autor

4.8.2 Konfigurace bezdrátové sítě

Nově vytvořená bezdrátová síť má přidělen vlastní virtuální název sítě ESSID a samostatnou virtuální síť, které je od zbytku sítě oddělena síťovým firewallem. Z důvodu bezproblémového fungování v doménovém prostředí podnikové počítačové sítě bylo nezbytné i pro interní bezdrátovou síť použít DNS a DHCP servery provozované na doménovém řadiči. Odstavce níže popisují postup a parametry jednotlivých konfiguračních změn.

4.8.2.1 Nastavení WLAN

Ubiquity Unifi Controller provozovaný v podniku umožňuje nastavit virtuální bezdrátové sítě. Toho bylo využito pro novou bezdrátovou síť s názvem WiFI-INT. Z bezpečnostních důvodů bylo vysílání jejího názvu skryto volbou „Hide SSID“. Protokol pro autentizaci a autorizaci přístupů k Wi-Fi byl zvolen „WPA-Enterprise“. Jedná se o standard IEEE 802.1X. Do sekce RADIUS serveru bylo nutné vyplnit IP adresu NPS serveru, standardní port protokolu RADIUS a sdílené tajné heslo, dříve definované v RADIUS klientovi na serveru NPS. Konfigurace VLAN, i ostatním nezbytných parametrů je k disposici na Obrázku 57.

Obrázek 57: Konfigurace WLAN – Ubiquity – web

Zdroj: autor

4.8.2.2 Nastavení VLAN a rozhraní

Na centrálním síťovém směrovači bylo aktivováno rozhraní pro virtuální síť a nastavena IP adresa výchozí brány nové bezdrátové sítě dle Příkladu 13.

Příklad 13: Konfigurace VLAN rozhraní – Mikrotik – CLI

```
/interface vlan
add comment=Wi-Fi-INT interface=ether2 l2mtu=1516 name=\
    vlan80 vlan-id=80
/ip address
add address=10.0.80.1/24 comment=\
    "Wi-Fi internal defaul gateway" interface=vlan80 \
    network=10.0.80.0
```

Zdroj: autor

4.8.2.3 Nastavení přepínačů

Síťové porty, do kterých jsou připojeny jednotlivé bezdrátové přístupové body, bylo nezbytné nakonfigurovat tak, aby akceptovali označkované datové rámce číslem VLAN 80. Obdobně byla nová VLAN přidána do všech patřičných propojovacích, tzv. „trunk“ portů.

4.8.2.4 Nastavení firewallu

Autentizace 802.1X předpokládá možnost komunikace RADIUS protokolem mezi autentizátory, které jsou v tomto případě bezdrátové přístupové body a autentizačním serverem. Přístupové body mají servisní rozhraní zapojené do sítě provozované za tímto účelem. Odtud byla komunikace skrze firewall již povolena dle Příkladu 12.

Aby byla zajištěna dostupnost základních síťových služeb, bylo zapotřebí povolit síťovou komunikaci mezi klienty interní bezdrátové sítě a doménovým řadičem. Mezi takové služby patří DNS, Kerberos, NetBIOS, HTTPS, SMB, LDAP(s), SMTP, RPC, DCOM, SOAP a další. Konfiguraci naznačuje Příklad 14. [19]

Příklad 14: Konfigurace firewallu pro DC – Mikrotik – CLI

```
/ip firewall filter
add chain=forward comment=\
    "POVOL nezbytnou komunikaci Wi-Fi INT na DC" \
    dst-address=10.0.0.254 dst-port=\
    53,88,123,137,138,389,445,464 protocol=udp \
    src-address=10.0.80.0/24
add chain=forward comment=\
    "POVOL nezbytnou komunikaci Wi-Fi INT na DC" \
    dst-address=10.0.0.254 dst-port="25,53,88,135,443,44\
    5,464,389,636,3268,3269,5722,9389,49152-65535" \
    protocol=tcp src-address=10.0.80.0/24
```

Zdroj: autor

Pro potřeby běžné práce bylo nezbytné povolit přístup do oddělené sítě s tiskárnami, přístup na terminálový server, do databáze informačního systému, a další viz Příklad 15.

Příklad 15: Konfigurace firewallu obecná – Mikrotik – CLI

```
/ip firewall filter
add chain=forward comment=\
    "POVOL RDP komunikaci Wi-Fi INT na TS" dst-address=\
    10.0.0.253 dst-port=3389 protocol=tcp src-address=\
    10.0.80.0/24
add chain=forward comment=\
    "POVOL RDP komunikaci Wi-Fi INT na TS" dst-address=\
    10.0.0.253 protocol=udp src-address=10.0.80.0/24
add chain=forward comment=\
    "POVOL komunikaci Wi-Fi INT s tiskarnami" \
    dst-address=10.0.70.0/24 dst-port=\
    88,137,138,445,464 protocol=udp src-address=\
    10.0.80.0/24
add chain=forward comment=\
    "POVOL komunikaci Wi-Fi INT s tiskarnami" \
    dst-address=10.0.70.0/24 dst-port=\
    80,135,443,445,464 protocol=tcp src-address=\
    10.0.80.0/24
add chain=forward comment=\
    "POVOL komunikaci Wi-Fi INT s IS serverem" \
    dst-address=10.0.0.252 dst-port=88,137,138,445,464 \
    protocol=udp src-address=10.0.80.0/24
add chain=forward comment=\
    "POVOL komunikaci Wi-Fi INT s IS serverem" \
    dst-address=10.0.0.252 dst-port=\
    80,135,443,445,464,1433 protocol=tcp src-address=\
    10.0.80.0/24
```

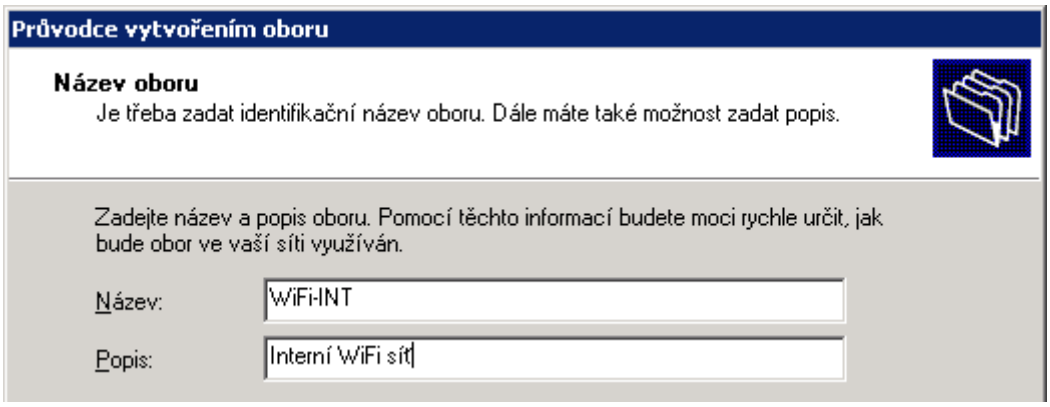
Zdroj: autor

Samozřejmostí je nutnost přístupu k síti Internet a dalším službám, které jsou řešeny dlouhodobě existujícími obecnějšími pravidly síťového firewallu.

4.8.2.5 Konfigurace DHCP a DNS na doménovém řadiči

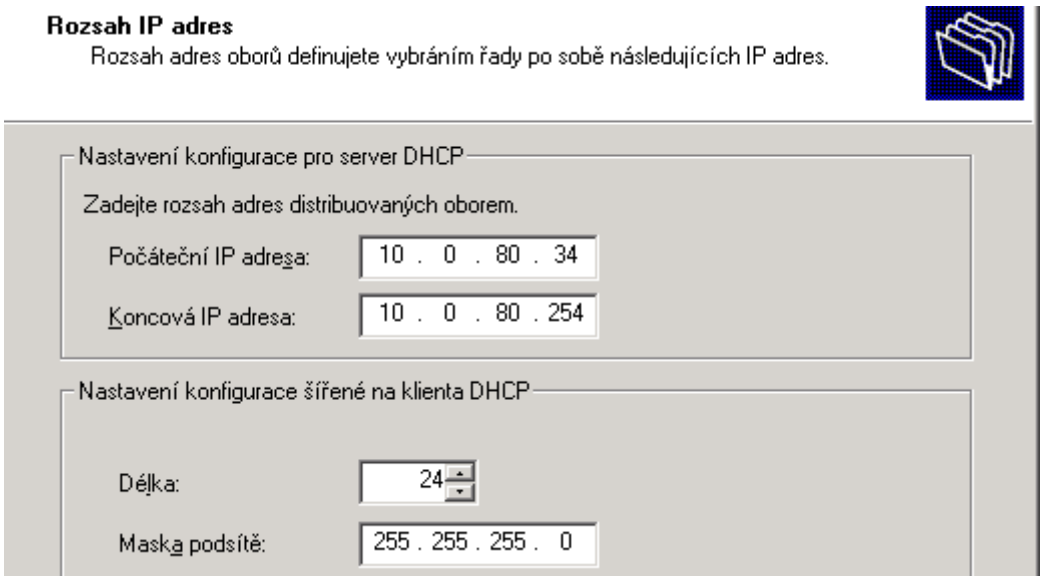
Přidělování IP adres klientům nové, interní bezdrátové sítě je dynamické. Pro tyto účely bylo nezbytné nastavit DHCP server spuštěný na doménovém řadiči. Průvodce přidáním a nastavením nového DHCP oboru zachycují Obrázky 58, 59, 60 a 61.

Obrázek 58: Konfigurace DHCP na DC #1



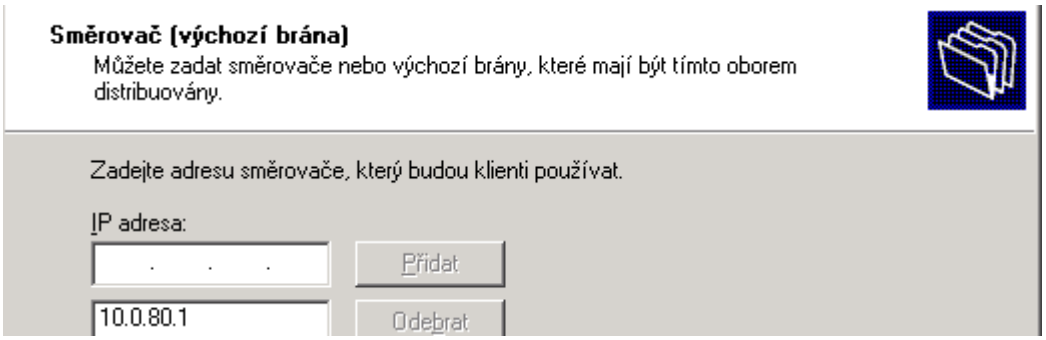
Zdroj: autor

Obrázek 59: Konfigurace DHCP na DC #2



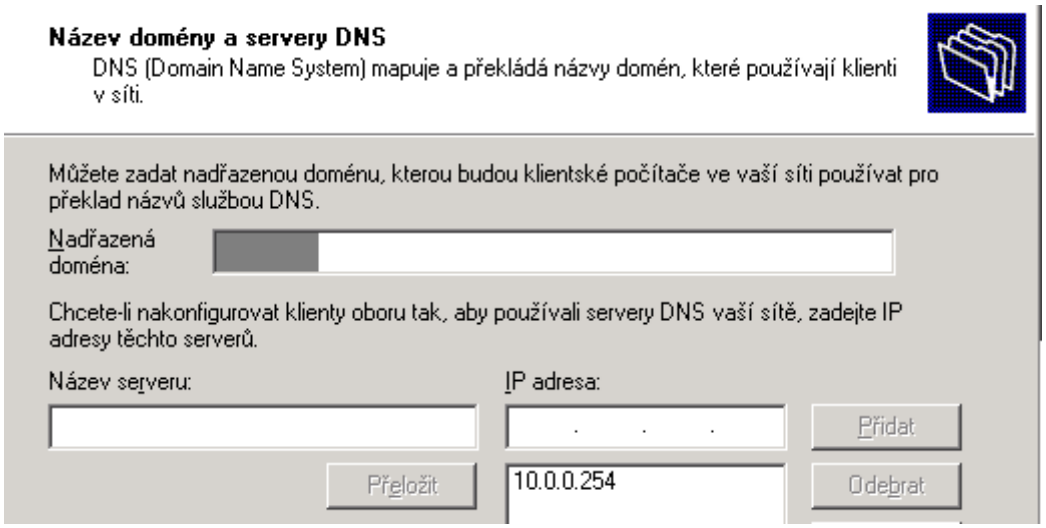
Zdroj: autor

Obrázek 60: Konfigurace DHCP na DC #3



Zdroj: autor

Obrázek 61: Konfigurace DHCP na DC #4



Zdroj: autor

4.8.2.6 Předávání požadavků DHCP

Autentizovaní a autorizovaní klienti bezdrátové sítě ihned po ověření žádají o IP adresu server DHCP. Tyto požadavky je nezbytné zachytit a předat doménovému řadiči, který slouží jako DHCP server pro interní síť kabelovou i bezdrátovou. Tato funkce se nazývá „DHCP relay" a její zprovoznění ilustruje Příklad 16.

Příklad 16: Konfigurace DHCP relay – Mikrotik – CLI

```
/ip dhcp-relay
add dhcp-server=10.0.0.254 disabled=no interface=vlan80 \
    name=WiFi-INT-DHCP-relay
```

Zdroj: autor

4.9 Konfigurace klientů

Stolní a přenosné osobní počítače potřebují k funkční autentizaci k síti standardem 802.1X a protokolem EAP programové vybavení, tzv. „Supplicant“. Operační systém Windows 7 professional, který je nainstalován na všech podnikových pracovních stanicích, je vybaven takovým programem, ale ve výchozím stavu je potlačen a není nakonfigurován pro připojení kabelové sítě.

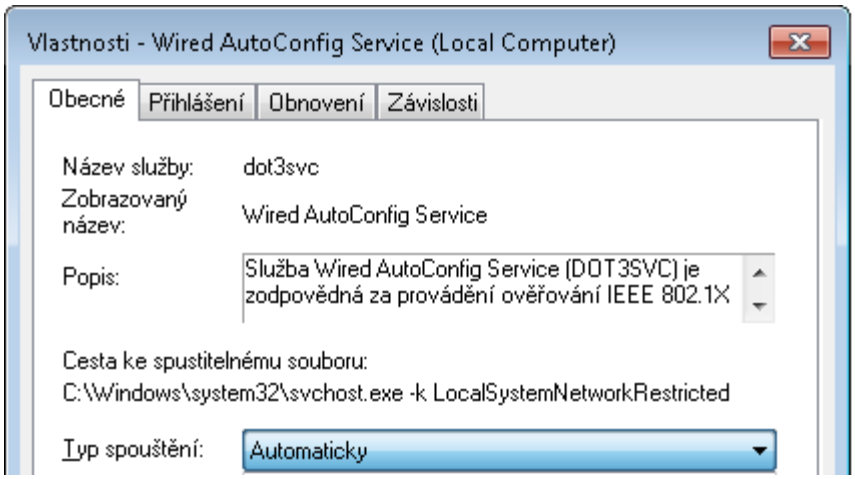
4.9.1 Připojení kabelem

Pro zprovoznění autentizace k počítačové síti při připojení kabelem lze v OS Windows 7 professional použít integrovanou službu „Wired AutoConfig Service“. Služba má na starosti ověřování standardem 802.1X v drátových sítích rozhraní Ethernet. V sítích, kde není vynucené toto ověřování, nemá na připojení k počítačové síti žádný vliv.

4.9.1.1 Manuální nastavení

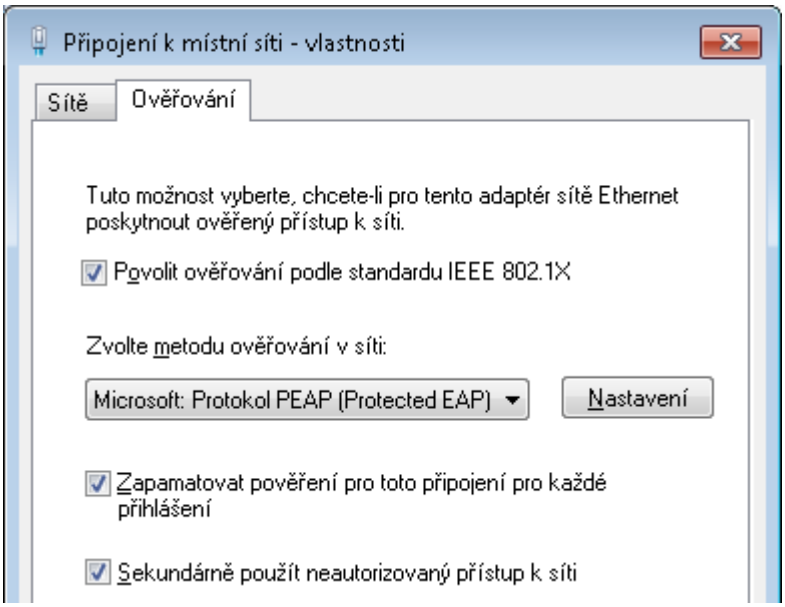
Manuální konfigurace obnáší zapnutí automatického spuštění zmíněné služby. Po spuštění služby, lze ve vlastnostech síťového připojení změnit parametry ověřování. Výchozí nastavení ověřování, kdy je povoleno „ověřování podle standardu IEEE 802.1X“, metodou „Microsoft: Protokol PEAP (Protected EAP) je správné. Stejně tak nastavení samotného protokolu PEAP se vynuceným ověřováním certifikátu serveru a metodou ověřování „Zabezpečené heslo (EAP-MSCHAP v2). V seznamu důvěryhodných certifikačních autorit musí být uveden server lokální certifikační autority. Použitá metoda je založena na ověřování uživatelů, proto je v upřesňujícím nastavení protokolu 802.1X nutné zvolit adekvátní volbu. Popsaná nastavení vystihují Obrázky 62, 63, 64, 65.

Obrázek 62: Konfigurace LAN klienta – služba pro 802.1X



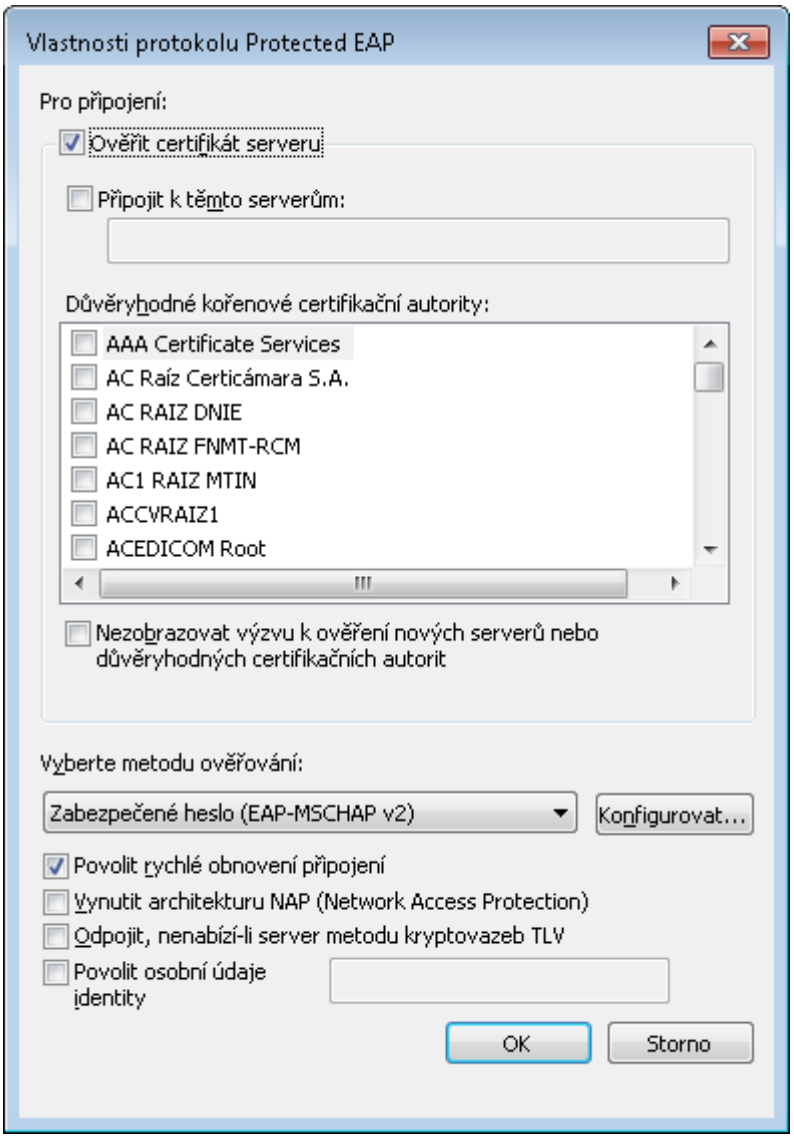
Zdroj: autor

Obrázek 63: Konfigurace LAN klienta – ověřování 802.1X



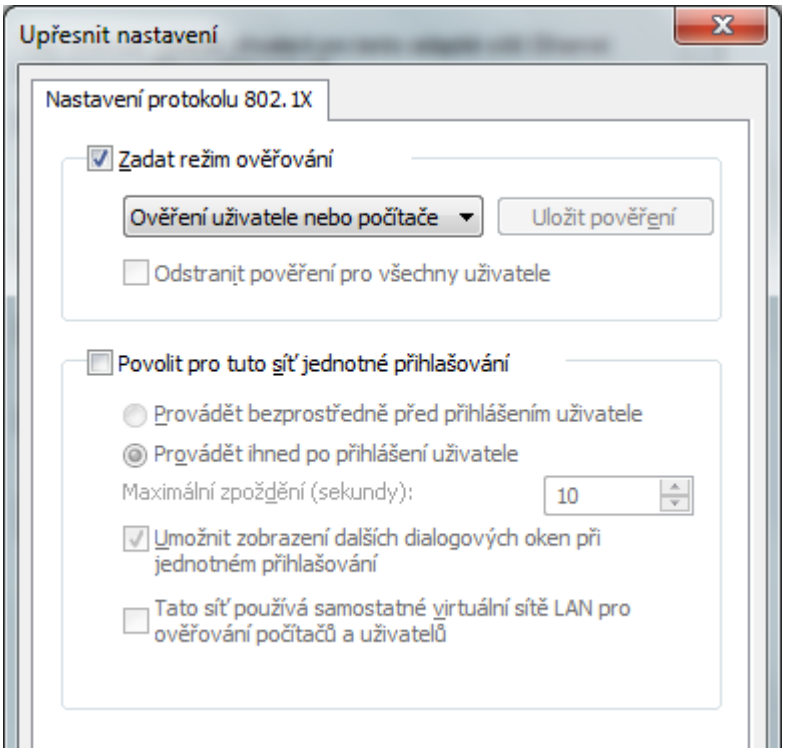
Zdroj: autor

Obrázek 64: Konfigurace LAN klienta – protokol EAP



Zdroj: autor

Obrázek 65: Konfigurace LAN klienta – upřesňující nastavení

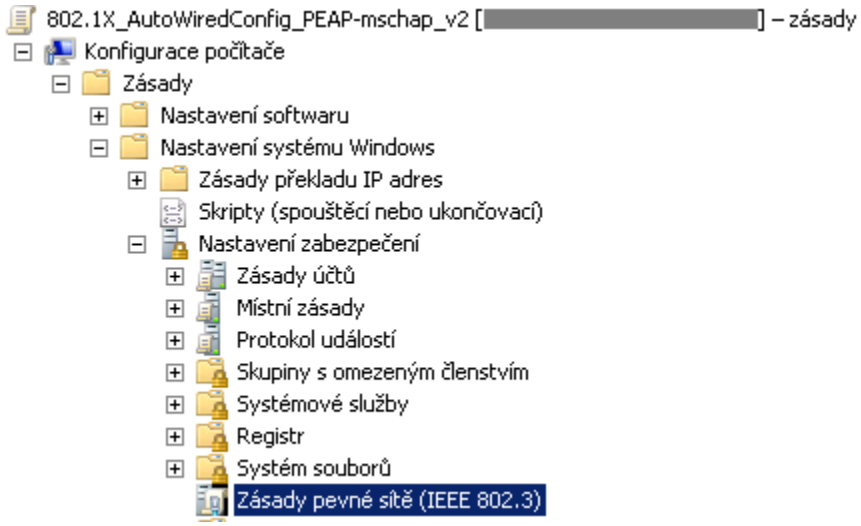


Zdroj: autor

4.9.1.2 Automatické nastavení – GPO

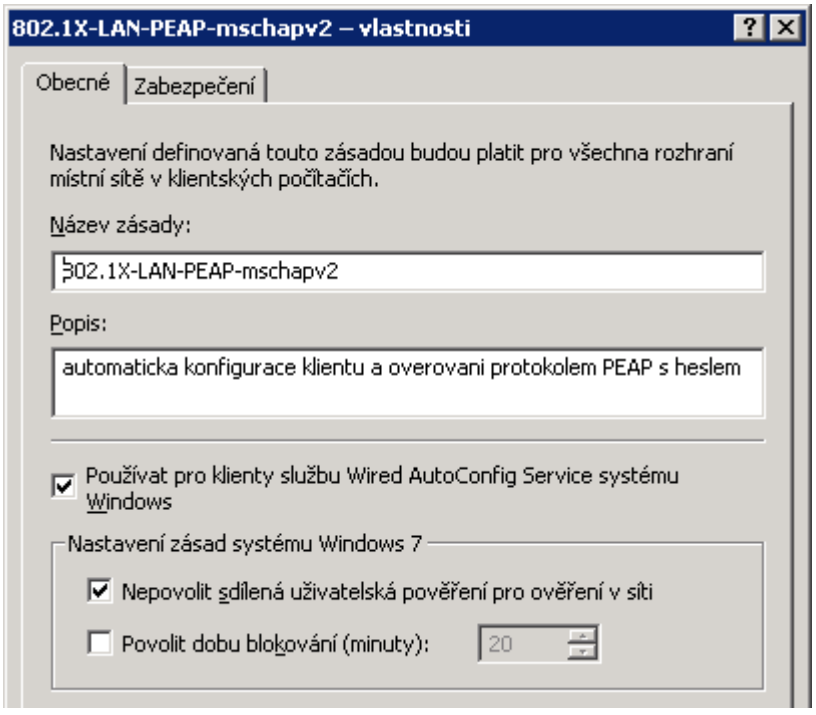
Výše popsané parametry byly z praktických důvodů konfigurovány pomocí nástroje na centrální správu klientů Active Directory, zásad skupiny nazývané zkratkou GPO. V administrační konzoli GPO bylo nutné vytvořit novou zásadu konfigurace počítače. Jedná se o „nastavení sytému Windows“, „nastavení zabezpečení“, konkrétně „zásady pevné sítě (IEEE 802.3)“. Vlastnosti a parametry konfigurované v této zásadě jsou shodné s manuální konfigurací výše. Znázorňují je Obrázky 66, 67, 68, 69, 71, 70 a 72. Vytvořená zásada byla aplikována na všechny klientské pracovní stanice.

Obrázek 66: Konfigurace LAN klienta – GPO



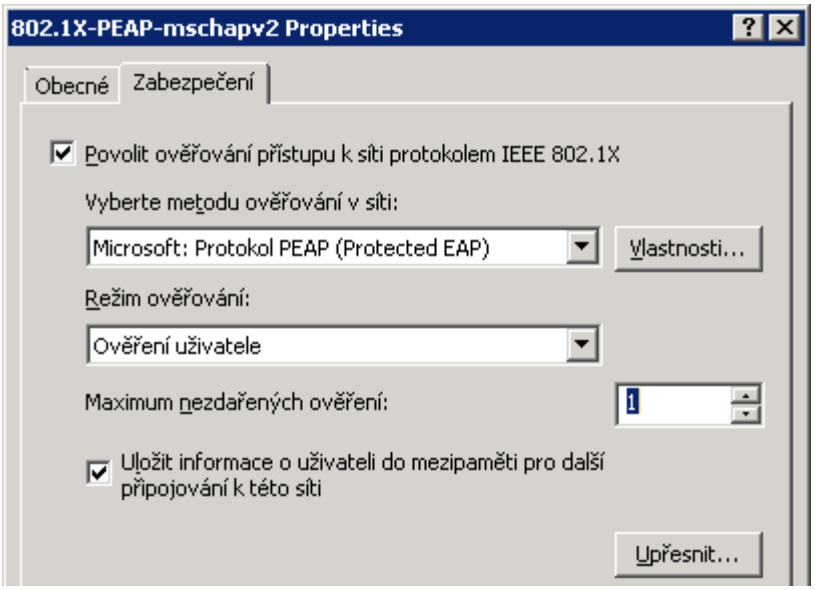
Zdroj: autor

Obrázek 67: Konfigurace LAN klienta – GPO – obecné



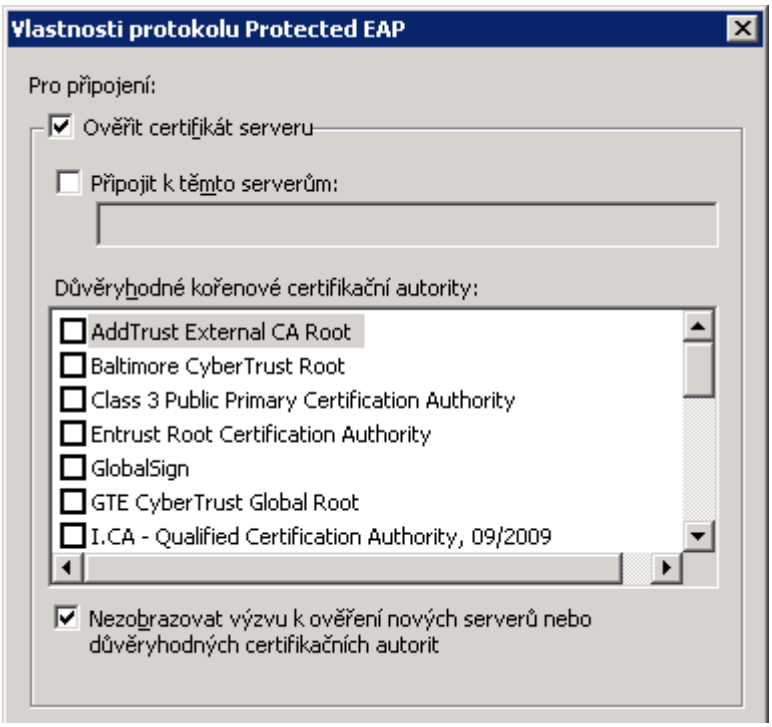
Zdroj: autor

Obrázek 68: Konfigurace LAN klienta – GPO – zabezpečení



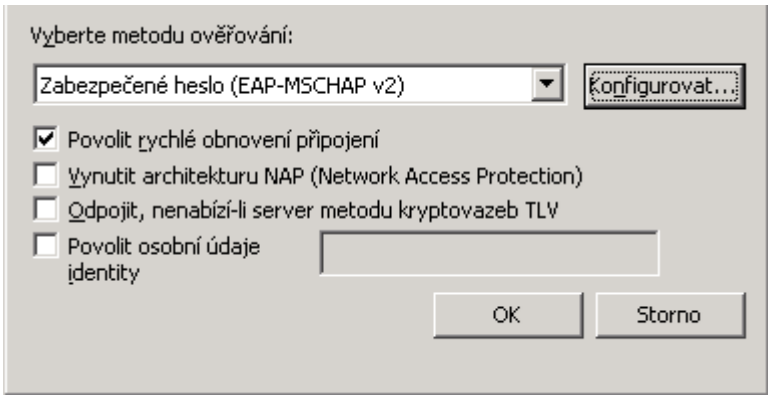
Zdroj: autor

Obrázek 69: Konfigurace LAN klienta – GPO – PEAP #1



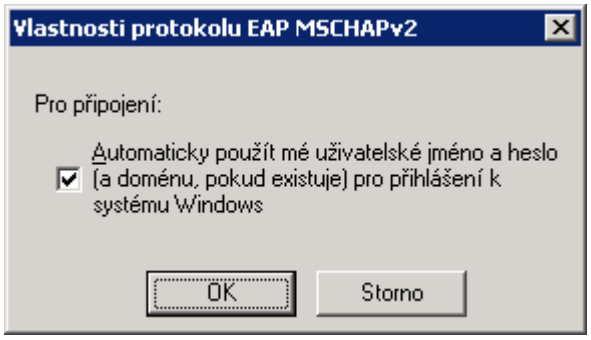
Zdroj: autor

Obrázek 70: Konfigurace LAN klienta – GPO – PEAP #2



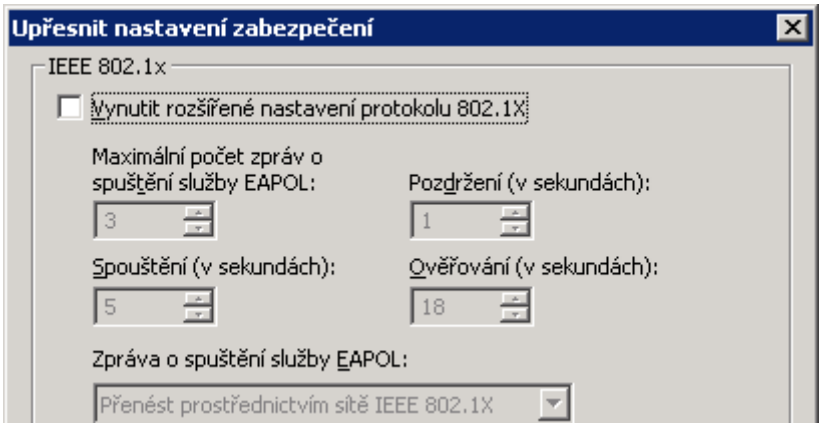
Zdroj: autor

Obrázek 71: Konfigurace LAN klienta – GPO – EAP MSCHAPv2



Zdroj: autor

Obrázek 72: Konfigurace LAN klienta – GPO – upřesňující



Zdroj: autor

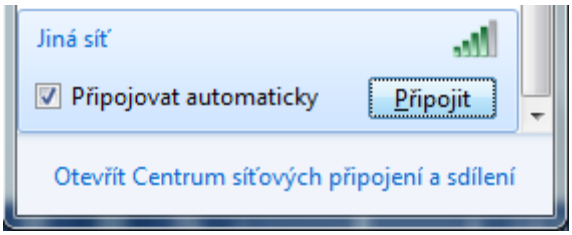
4.9.2 Připojení k bezdrátové síti

Pro autentizaci a připojení k bezdrátové počítačové síti se standardem IEEE 802.1X a protokolem EAP není v moderních operačních systémech Microsoft Windows zapotřebí programové vybavení, tzv. „Supplicant“. Některé externě vyvíjené softwarové alternativy přináší rozšířené funkcionality. Pro potřeby této práce a podniku byl použit integrovaný software v operačním systému klientských pracovních stanic, který je plně dostačující.

4.9.2.1 Manuální nastavení

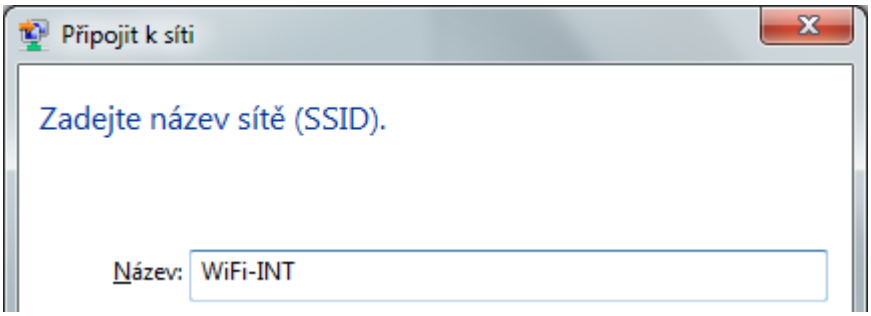
Manuální připojení spočívá v připojení k síti, která nepropaguje veřejně svůj název. Ten je nutné zadat manuálně, viz Obrázek 73 a 74. Následuje autentizace uživatele a připojení k síti, pokud ověření proběhlo v pořádku. Obojí je zřejmé z Obrázku 75 a 76. Předpokladem je stejně jako v případě autentizace ke kabelové síti důvěra v CA, která vydala certifikát NPS serveru a jeho aktuálnost a platnost.

Obrázek 73: Konfigurace WLAN klienta



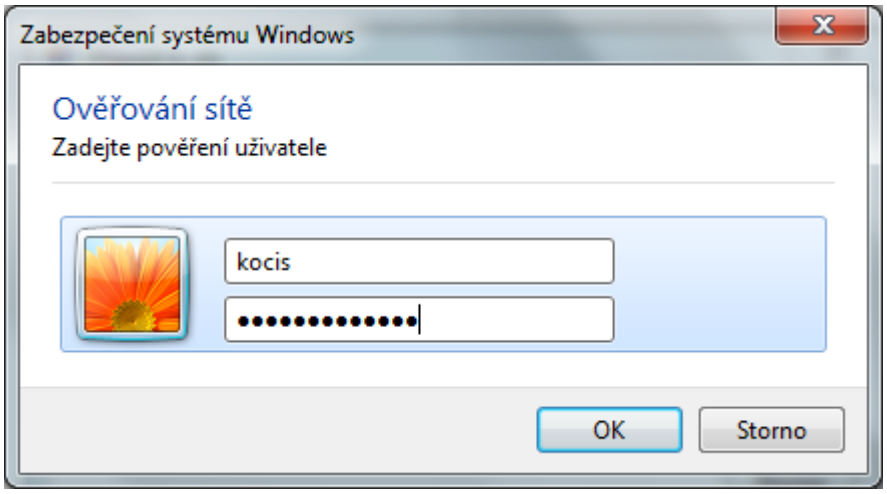
Zdroj: autor

Obrázek 74: Konfigurace WLAN klienta – SSID



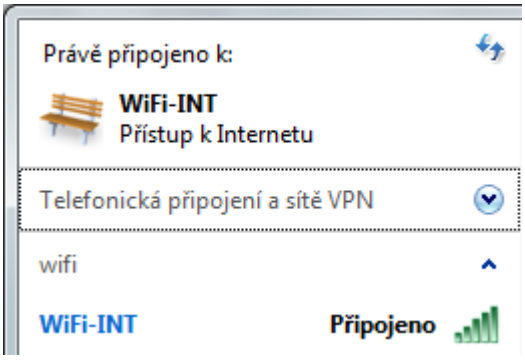
Zdroj: autor

Obrázek 75: Konfigurace WLAN klienta – ověření



Zdroj: autor

Obrázek 76: Konfigurace WLAN klienta – připojeno



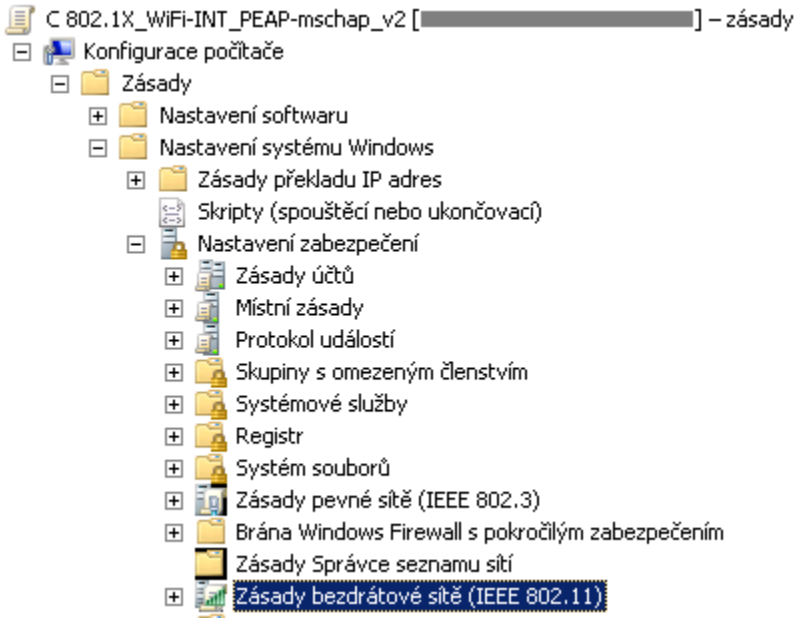
Zdroj: autor

4.9.2.2 Automatické nastavení – GPO

Z praktických důvodů byla opět použita centrální distribuce konfigurace bezdrátové sítě s využitím GPO. Podobně jako v případě připojení kabelem, bylo nezbytné vytvořit novou zásadu konfigurace počítače a aplikovat ji na organizační jednotku v Active Directory, která obsahuje všechny přenosné osobní počítače. Samotná konfigurace obnáší nastavení profilu, názvů sítě „WiFi-INT“, odškrtnutí volby „připojovat automaticky, pokud je tato síť v dosahu“, konfiguraci ověřování „WPA2-podnikové“, šifrování „AES“, metodu ověřování „protokol PEAP“ a volbu způsobu ověřování „ověřování uživatele“. Ostatní

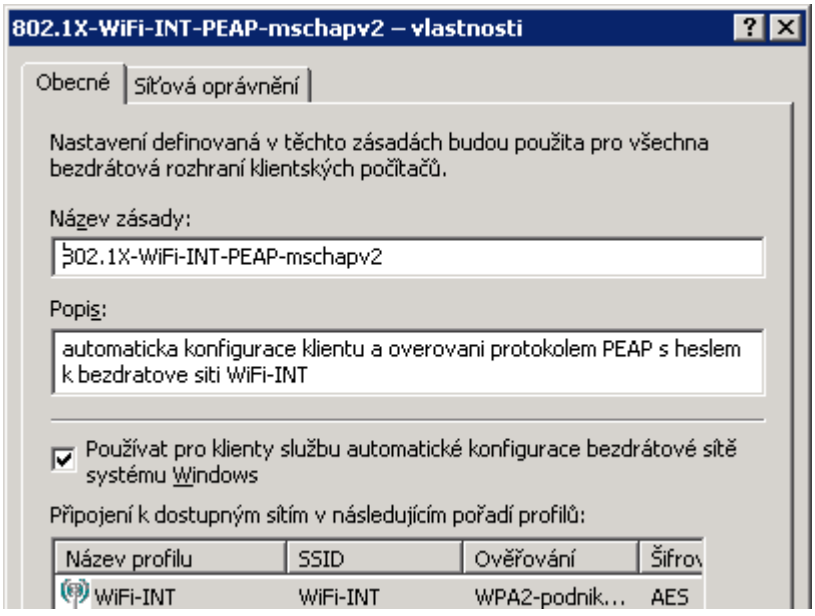
neklíčové volby mohou zůstat ve výchozím nastavení. Vše lze nalézt na Obrázcích 77, 78, 79, 80 a 81.

Obrázek 77: Konfigurace WLAN klienta – GPO



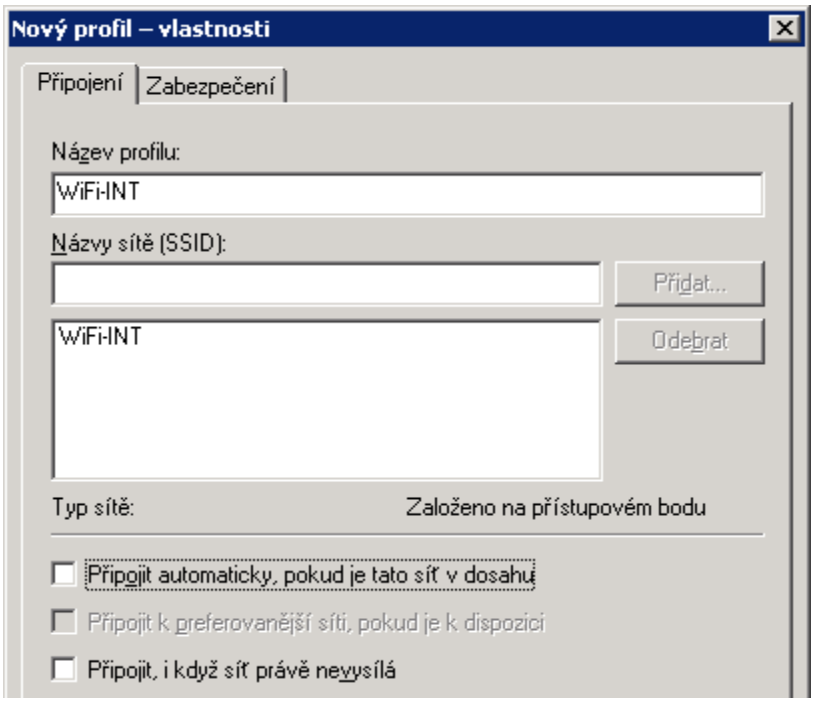
Zdroj: autor

Obrázek 78: Konfigurace WLAN klienta – GPO – obecné



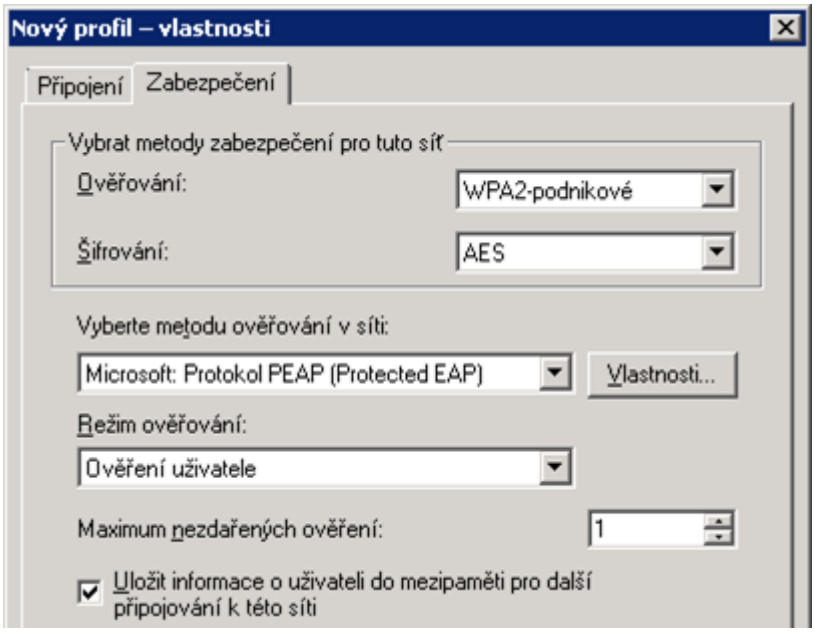
Zdroj: autor

Obrázek 79: Konfigurace WLAN klienta – GPO – SSID #1



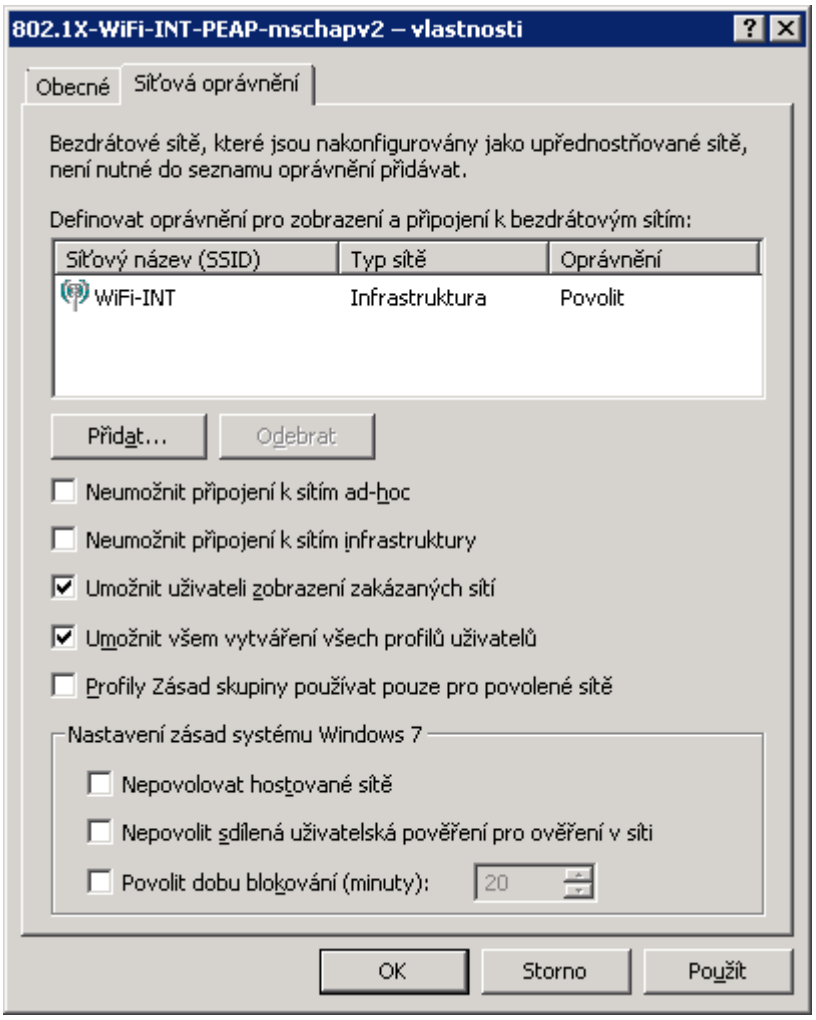
Zdroj: autor

Obrázek 80: Konfigurace WLAN klienta – GPO – SSID #2



Zdroj: autor

Obrázek 81: Konfigurace WLAN klienta – GPO – oprávnění



Zdroj: autor

4.10 MAC Authentication Bypass (MAB)

Nezbytnou součástí řešení je autentizace zařízení, které nepodporují standard 802.1X, nebo nemají obslužné uživatele. Protože ověřování MAB je ze své vlastní podstaty fungování náchylné na síťové útoky a případné riziko podvrhnutí MAC adresy je veliké, bude tato metoda autentizace používána pouze pro vybraná zařízení a ve speciálních virtuálních sítích, které nejsou kritické pro chod organizace a jsou na síťové úrovni odděleny od ostatních důležitých sítí pro klientské stanice a serverové prostředky. Ověřování pomocí MAB bylo použito pro IP telefonní přístroje, tiskárny a multifunkční zařízení, výrobní stroje a ve výjimečných případech pro další speciální zařízení.

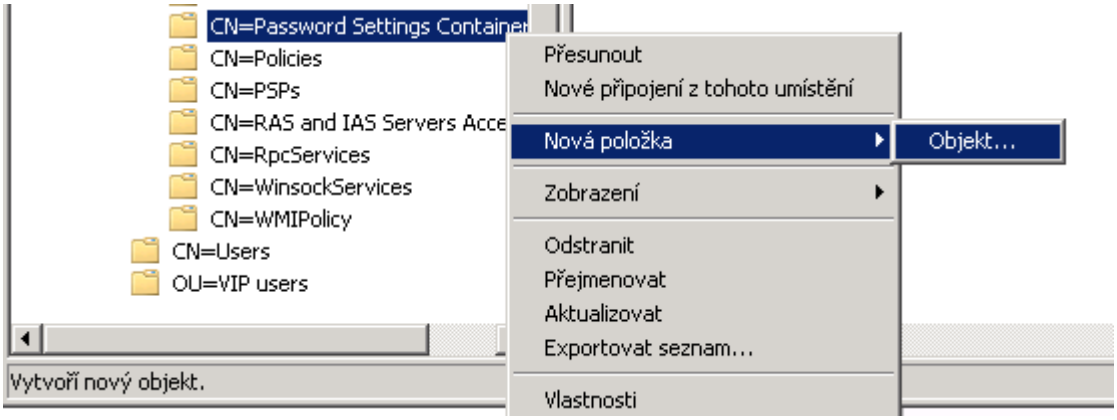
Pro údržbu MAB účtů byla z důvodu relativně malého počtu takovýchto zařízení a za účelem udržení jednoduchosti zvolena stejná „databáze“ jako pro běžné uživatelské účty, tedy Active Directory. Při samotné realizaci bylo nalezeno zásadní omezení při tvorbě těchto účtů, které vyplívá ze zavedené politiky správy a komplexnosti přístupových hesel. Tato politika za normálních okolností neumožňovala vytvářet speciální jednoúčelové uživatelské účty zařízení, kde je jméno a heslo účtu shodné.

4.10.1 Granulárně definovaná politika hesel

Pro správnou funkčnost autentizace pomocí MAC adres, které budou uloženy formou uživatelských účtů v adresáři Active Directory, je nutné povolit výjimku z GPO bezpečnostní politiky hesel. Toho se docílí pomocí tzv. „Fine-grained password policy“. Speciální a vybrané objekty v adresáři pak mohou být definovány s jinými, v tomto případě nižšími nároky na komplexitu hesel, než běžní uživatelé. Hodnota MAC zařízení adresy bude zároveň uživatelské jméno i heslo objektu v Active Directory. [15; 20]

Postup konfigurace podrobných zásad pro hesla a zamykání účtů se skládá ze čtyř kroků. V první řadě bylo nutné vytvořit nový objekt Nastavení hesel pomocí Editoru ADSI. Ten lze spustit na doménovém řadiči příkazem „adsiedit.msc“. Po připojení editorem ADSI k doménovému řadiči, bylo nutné v sekci „DC=název-domény“, „CN=System“, „CN=Password Settings Container“, vytvořit nový objekt. Objekt se tvoří pomocí třídy „msDS-PasswordSettings“. Vytváření zásady hesel znázorňuje Obrázek 82. [21]

Obrázek 82: MAB vytvoření politiky hesel



Zdroj: autor

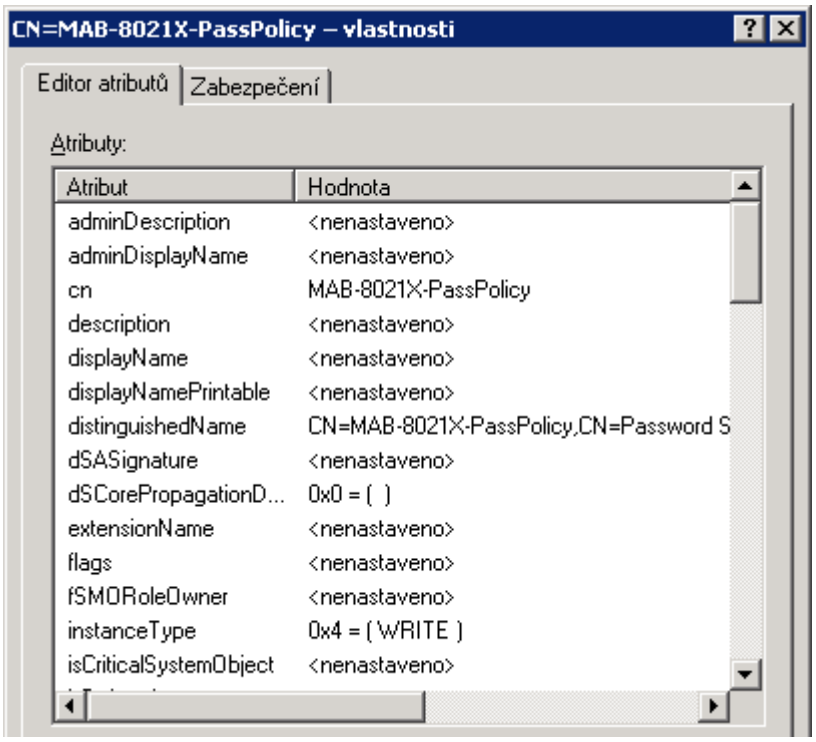
Objekt byl pojmenován „MAB-8021X-PassPolicy“. Hodnoty jednotlivých použitých parametrů jsou zřejmé z Tabulky 5 a výsledné nastavení zachycuje Obrázek 83.

Tabulka 5: MAB – atributy politiky hesel

název atributu	hodnota	popis atributu
msDS-PasswordSettingsPrecedence	20	priorita zásady 20
msDS-PasswordReversibleEncryptionEnabled	TRUE	reverzibilní šifrování hesla
msDS-PasswordHistoryLength	0	žádná délka historie hesel
msDS-PasswordComplexityEnabled	FALSE	vypnuté vynucení složitosti hesla
msDS-MinimumPasswordLength	12	min. délka hesla 12 znaků
msDS-MinimumPasswordAge	00:00:00:00	minimální stáří hesla 0 sec
msDS-MaximumPasswordAge	N/A	maximální stáří hesla vypnutá
msDS-LockoutThreshold	10	uzamčení po 10 pokusech
msDS-LockoutObservationWindow	00:00:30:00	sledování uzamčení 30 min
msDS-LockoutDuration	00:00:30:00	uzamčení účtů 30min

Zdroj: autor

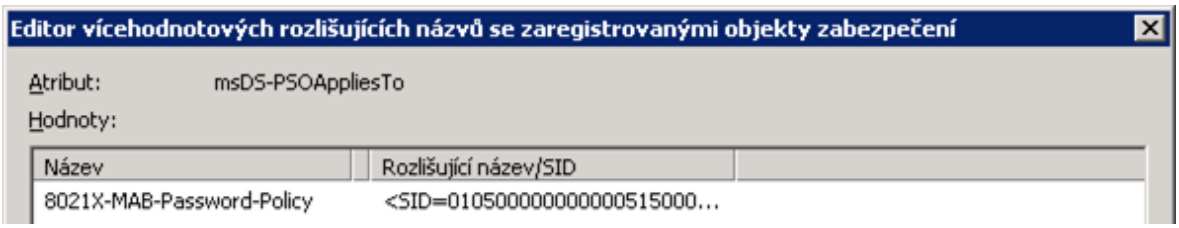
Obrázek 83: MAB – výsledné nastavení zásady hesel



Zdroj: autor

Dalším důležitým krokem bylo přidělení nové politiky hesel správné, dříve vytvořené, globální doménové skupině „8021X-MAB-Password-Policy“ atributem „msDS-PSOAppliesTo“. Toto nastavení je zřejmé z Obrázku 84. Uživatelským účtům, které se stanou členy této skupiny, je po změně členství možné nastavit heslo shodné s uživatelským jménem.

Obrázek 84: MAB – přiřazení zásady skupině



Zdroj: autor

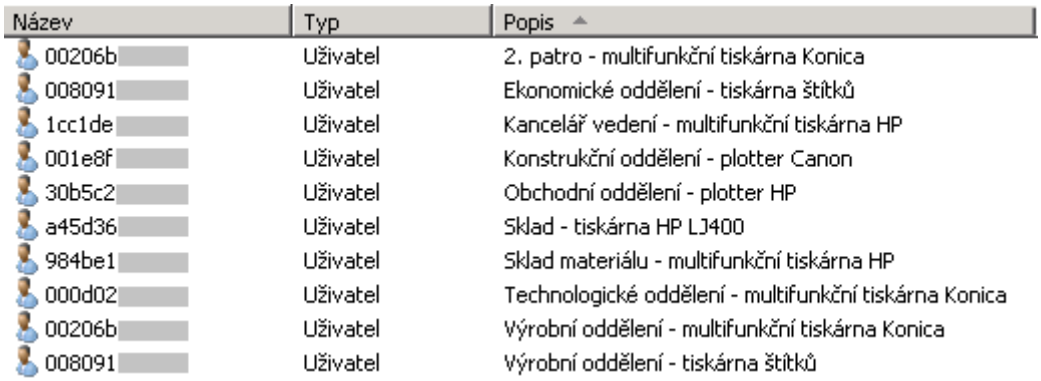
Pro zprovoznění granulárně definované politiky hesel bylo nutné zvýšení úrovně funkčnosti domény a doménové struktury služby Active Directory na verzi 2008.

4.10.2 Definování účtů pro MAB

Všem vybraným zařízením, které potřebovali přístup do počítačové sítě, byl vydefinován účet ve vyhrazené organizační jednotce AD. Uživatelské jméno a heslo bylo konfigurováno shodně, dle konkrétní MAC adresy zařízení. Každý nový uživatelský účet je konfigurován se členstvím ve skupině pro politiku hesel a konkrétní virtuální síť, například „8021X-MAB-Password-Policy“ a „8021X-vLAN-70“ pro každou tiskárnu a multifunkční zařízení.

Obrázek 85 znázorňuje výseč výsledného seznamu nastavených uživatelských účtů pro síťová zařízení bez podpory 802.1X v Active Directory.

Obrázek 85: Uživatelské účty pro MAB – výsledná konfigurace



Název	Typ	Popis
00206b	Uživatel	2. patro - multifunkční tiskárna Konica
008091	Uživatel	Ekonomické oddělení - tiskárna štítků
1cc1de	Uživatel	Kancelář vedení - multifunkční tiskárna HP
001e8f	Uživatel	Konstrukční oddělení - plotter Canon
30b5c2	Uživatel	Obchodní oddělení - plotter HP
a45d36	Uživatel	Sklad - tiskárna HP LJ400
984be1	Uživatel	Sklad materiálu - multifunkční tiskárna HP
000d02	Uživatel	Technologické oddělení - multifunkční tiskárna Konica
00206b	Uživatel	Výrobní oddělení - multifunkční tiskárna Konica
008091	Uživatel	Výrobní oddělení - tiskárna štítků

Zdroj: autor

4.11 Příprava a zkušební provoz

Příprava a ověřování funkčnosti celého systému probíhaly v neprodukčním testovacím prostředí a předcházely implementaci řešení v reálném provozu. Testovací infrastruktura byla oddělena od systémů využívaných běžnými uživateli pro provoz podniku. Samostatné prostředí bylo nezbytné pro řádné vyladění nastavení a odstranění všech chyb s minimálním dopadem na fungování společnosti.

Následná konfigurace finálního řešení do produkčních systémů probíhala v několika zaváděcích etapách.

První etapa zahrnovala provoz v monitorovacím režimu. Veškeré součásti systému byly nakonfigurovány a připraveny dle předcházejících kapitol. V této fázi byla použita mírně upravená konfigurace síťových portů, která umožňuje provádět autentizaci, autorizaci a účtování, ale bez ohledu na její objektivní výsledek připojeného uživatele či zařízení úspěšně ověří. Konfigurace režimu síťových portů používala tzv. „Open access“. Tímto způsobem bylo možné testovat a ověřit chování všech prvků a částí řešení zabezpečeného přístupu k lokální počítačové síti v reálném provozu bez negativního vlivu na běžný provoz a zaměstnance společnosti. Potvrzením korektního chování a funkčnosti bylo možné přistoupit k další fázi.

Přepnutí do reálného režimu ověřování přístupů probíhalo v etapách, kdy se postupně vypínal monitorovací mód na jednotlivých přepínačích. Pořadí bylo zvoleno od nejméně

kritických, po nejdůležitější. Každý jednotlivý switch bylo po přepnutí do produkčního stavu ověřování nutno podrobit akceptačním testům.

4.12 Akceptační testy

Hlavním cílem akceptačních testů bylo ověřit správné fungování před používáním systému v každodenním provozu. Testy měly za úkol potvrdit a zaznamenat funkčnost jednotlivých operací řešení. Zároveň odhalit slabá místa, která bylo třeba napravit. V praxi zkoušky ověřovaly především, zda je autentizace jako celek funkční, umožňuje-li přístup do sítě pouze autentizovaným a autorizovaným uživatelům, jestli funguje účtování RADIUS a další.

Testy bylo nutné provést pro drátovou i bezdrátovou část sítě. Probíhaly v návaznosti na přepínání z monitorovacího do funkčního režimu ověřování síťových přepínačů. Výjimky z testů měly síťové porty určené pro páteřní a serverovou infrastrukturu, které nebyly zahrnuty do konfigurace IEEE 802.1X. Vše probíhalo mimo hlavní pracovní dobu podniku. Podrobnou specifikaci provedených akceptačních testů obsahuje Příloha A.

Součástí akceptačních testů bylo i ověření, že k autentizaci je opravdu využíván zabezpečený protokol PEAP s využitím šifrovaného tunelu protokolem TLS. Obrázek 86 zachycuje komunikaci mezi klientem a síťovým přepínačem. Z detailní analýzy je zřejmé, že komunikace je šifrována protokolem TLS. Obrázek 87 zobrazuje detaily jednoho bloku dat protokolu RADIUS stejného procesu autentizace uživatele na směrovači mezi NPS serverem a síťovým přepínačem. Z podrobných informací je vidět, že použitý protokol je PEAP.

Obrázek 86: Analýza síťového provozu – PEAP – klient

No.	Time	Source	Destination	Protocol	Length	Info
2	0.021620	Dell_22:75:23	Nearest	EAPOL	19	Start
3	0.024126	50:06:ab:35:cb:66	Nearest	EAP	60	Request, Identity [RFC3748]
56	6.618915	Dell_22:75:23	Nearest	EAP	28	Response, Identity [RFC3748]
57	6.638970	50:06:ab:35:cb:66	Nearest	EAP	60	Request, PEAP [Palekar]
58	6.642228	Dell_22:75:23	Nearest	TLSv1	159	Client Hello
59	6.658090	50:06:ab:35:cb:66	Nearest	TLSv1	173	Server Hello, Change Cipher Spec, Encrypted Handshake Message
60	6.661414	Dell_22:75:23	Nearest	TLSv1	87	Change Cipher Spec, Encrypted Handshake Message
68	8.345352	50:06:ab:35:cb:66	Nearest	TLSv1	125	Application Data
69	8.346943	Dell_22:75:23	Nearest	TLSv1	61	Application Data
70	8.375968	50:06:ab:35:cb:66	Nearest	TLSv1	61	Application Data
71	8.376744	Dell_22:75:23	Nearest	TLSv1	61	Application Data
72	8.394803	50:06:ab:35:cb:66	Nearest	TLSv1	77	Application Data
73	8.395468	Dell_22:75:23	Nearest	TLSv1	77	Application Data
74	8.420598	50:06:ab:35:cb:66	Nearest	TLSv1	77	Application Data
75	8.421533	Dell_22:75:23	Nearest	TLSv1	61	Application Data
76	8.439513	50:06:ab:35:cb:66	Nearest	TLSv1	93	Application Data
78	8.442255	Dell_22:75:23	Nearest	TLSv1	125	Application Data
79	8.492084	50:06:ab:35:cb:66	Nearest	TLSv1	109	Application Data
80	8.493350	Dell_22:75:23	Nearest	TLSv1	61	Application Data
81	8.510849	50:06:ab:35:cb:66	Nearest	TLSv1	125	Application Data
82	8.514757	Dell_22:75:23	Nearest	TLSv1	125	Application Data
83	8.535251	50:06:ab:35:cb:66	Nearest	EAP	60	Success

Zdroj: autor

Obrázek 87: Analýza síťového provozu – PEAP – server

```
▷ User Datagram Protocol, Src Port: 1812 (1812), Dst Port: 49205 (49205)
◢ RADIUS Protocol
    Code: Access-Challenge (11)
    Packet identifier: 0x7d (125)
    Length: 90
  ▷ Authenticator: 97f22f825b545fb87cec516db592eb6f [correct]
    [This is a response to a request in frame 1]
    [Time from request: 0.015705000 seconds]
  ◢ Attribute Value Pairs
    ◢ AVP: l=6 t=Session-Timeout(27): 30
        [Length: 4]
        Session-Timeout: 30
    ◢ AVP: l=8 t=EAP-Message(79) Last Segment[1]
        [Length: 6]
        EAP fragment: 010200061920
      ◢ Extensible Authentication Protocol
          Code: Request (1)
          Id: 2
          Length: 6
          Type: Protected EAP (EAP-PEAP) (25)
        ◢ EAP-TLS Flags: 0x20
            0... .... = Length Included: False
            .0.. .... = More Fragments: False
            ..1. .... = Start: True
            .... .000 = Version: 0
```

Zdroj: autor

4.13 Produkční povoz a údržba

Po akceptačních testech následoval rutinní provoz systému. Samotné řešení nevyžaduje zvýšené nároky na administraci.

4.13.1 Provoz

Standard IEEE 802.1X přináší výhody dynamické konfigurace portů. Není potřeba konfigurovat každý síťový port samostatně, dle účelu použití. Nastavení a provoz síťových přepínačů je tedy jednodušší a statičtější. Odpadají konfigurační změny na úrovni sítě pro každé nové zařízení, uživatele, při stěhování a další. Změny nastavení jsou nutné pouze v případě změny v topologii sítě, například zapojení nového serveru, přepínače, vytvoření nové virtuální sítě a podobně. Každý nový zaměstnanec získá automaticky při vytvoření doménového účtu i přístup k počítačové síti. Konfigurace klientských stanic zaměstnanců pro IEEE 802.1X je také statická a řízena centrálně.

Každé nové zařízení, které nepodporuje standard 802.1X, musí mít vydefinován účet v Active Directory a přiřazenu správnou skupinu zabezpečení reflektující relevantní VLAN. Fluktuace těchto zařízení v běžném provozu je však minimální.

4.13.2 Údržba

Mezi nutnou údržbu systému patří pravidelná kontrola protokolu událostí RADIUS serveru, autentizačních protokolů síťových přepínačů a prvků bezdrátové sítě. Nový NPS server bylo nezbytné zařadit do plánů pravidelných kontrol, záloh a aktualizací. Na ostatních částech systému jsou tyto úkony prováděny na pravidelné bázi již dlouhodobě.

4.14 Výkonnostní dopady

Na základě zkušeností z provozu lze konstatovat, že dopad na výkon síťových přepínačů, serverovou infrastrukturu i klientských stanic jsou minimální a nebyly pozorovány žádné problémy. Doba autentizace k síti se pohybuje v řádech stovek milisekund a pro uživatele je téměř nezaznamenatelná.

4.15 Vybrané problémy realizace a způsoby řešení

Během realizace bylo nutné vyřešit celou řadu neočekávaných situací. Pro řešení a podrobnou analýzu jednotlivých problémů lze využít níže uvedené postupy a vzorové výpisy záznamů protokolů.

4.15.1 Monitoring

Pro podrobnější zaznamenávání informací o průběhu autentizace a autorizace je výhodné zprovoznit zasílání SNMP trap zpráv. Funkci lze zapnout dle Obrázku 88 nebo z příkazové řádky dle Příkladu 1.

Obrázek 88: Konfigurace zasílání SNMP trap zpráv – Cisco – web

Zdroj: autor

Příklad 17: Konfigurace zasílání SNMP trap zpráv – Cisco – CLI

```
sw12-SG300-52P#show running-config
…
dot1x traps authentication quiet
dot1x traps authentication failure 802.1x mac web
dot1x traps authentication success 802.1x mac web
logging host 10.0.200.2 severity debugging description "syslog"
…
```

Zdroj: autor

Vzorová SNMP trap zpráva o úspěšné autentizaci je zachycena v Příkladu 18.

Příklad 18: Vzorová SNMP zpráva úspěšné autentizace

```
Jan 14 23:19:11 monitor snmptrapd[1026]: 2016-01-14 23:19:11
10.0.200.242(via UDP: [10.0.200.242]:161->[10.0.200.2]:162)
TRAP, SNMP v1, community public#012#011.1.3.6.1.6.3.1.1.5 Link
Up Trap (0) Uptime: 12 days,
9:06:00.94#012#011.1.3.6.1.2.1.2.2.1.1.55 = INTEGER:
55#011.1.3.6.1.2.1.2.2.1.7.55 = INTEGER:
1#011.1.3.6.1.2.1.2.2.1.8.55 = INTEGER: 1

Jan 14 23:19:11 monitor snmptrapd[1026]: 2016-01-14 23:19:11
10.0.200.242(via UDP: [10.0.200.242]:161->[10.0.200.2]:162)
TRAP, SNMP v1, community public#012#011.1.3.6.1.4.1.9.6.1.101
Enterprise Specific Trap (151) Uptime: 12 days,
9:06:00.94#012#011.1.3.6.1.4.1.9.6.1.101.2.3.1.0 = STRING:
"%STP-W-PORTSTATUS: gi7: STP status Forwarding, aggregated
(1)#015#012"#011.1.3.6.1.4.1.9.6.1.101.2.3.2.0 = INTEGER:
1#011.1.3.6.1.4.1.9.6.1.101.57.2.8.1.0 = INTEGER:
55#011.1.3.6.1.4.1.9.6.1.101.57.2.8.2.0 = INTEGER: 0

Jan 14 23:19:11 monitor snmptrapd[1026]: 2016-01-14 23:19:11
10.0.200.242(via UDP: [10.0.200.242]:161->[10.0.200.2]:162)
TRAP, SNMP v1, community public#012#011.1.3.6.1.4.1.9.6.1.101
Enterprise Specific Trap (184) Uptime: 12 days,
9:06:00.96#012#011.1.3.6.1.4.1.9.6.1.101.2.3.1.0 = STRING:
"%SEC-I-PORTAUTHORIZED: Port gi7 is
Authorized#015#012"#011.1.3.6.1.4.1.9.6.1.101.2.3.2.0 =
INTEGER: 0

Jan 14 23:19:11 monitor snmptrapd[1026]: 2016-01-14 23:19:11
10.0.200.242(via UDP: [10.0.200.242]:161->[10.0.200.2]:162)
TRAP, SNMP v1, community public#012#011.1.3.6.1.4.1.9.6.1.101
Enterprise Specific Trap (203) Uptime: 12 days,
9:06:00.98#012#011.1.3.6.1.4.1.9.6.1.101.2.3.1.0 = STRING:
"%SEC-I-SUPPLICANTAUTHORIZED: username kocis with MAC
5c:26:0a:22:75:23 is authorized on port
gi7#015#012"#011.1.3.6.1.4.1.9.6.1.101.2.3.2.0 = INTEGER: 0
```

Zdroj: autor

4.15.2 Zaznamenávání protokolu událostí

Protokoly událostí je vhodné zasílat na centrální server, kde jsou uchovány a k disposici pro diagnostiku v reálném čase i zpětnou kontrolu. Konfiguraci této funkce lze provést podle Příkladu 19.

Příklad 19: Konfigurace zasílání protokolů událostí – Cisco – CLI

```
sw12-SG300-52P#show running-config
…
logging host 10.0.200.2 severity debugging description "syslog"
…
```

Zdroj: autor

Vzorový protokol událostí úspěšné autentizace je zachycen v Příkladu 20.

Příklad 20: Vzorový protokol událostí úspěšné autentizace

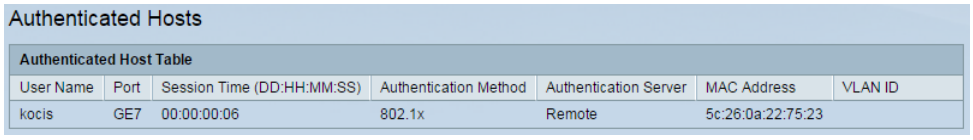
```
==> %LINK-W-Down.log <==
local7,warning,Jan 14 23:21:03 10.0.200.242  gi7, aggregated
(1)

==> %STP-W-PORTSTATUS.log <==
local7,warning,Jan 14 23:21:08 10.0.200.242 gi6: STP status
Forwarding

==> %SEC-I-PORTAUTHORIZED.log <==
local7,info,Jan 14 23:21:42 10.0.200.242 Port gi6 is Authorized

==> %SEC-I-SUPPLICANTAUTHORIZED.log <==
local7,info,Jan 14 23:21:42 10.0.200.242 username kocis with
MAC 5c:26:0a:22:75:23 is authorized on port gi6
```

Zdroj: autor

4.15.3 Autentizovaný uživatel

Korektně autentizovaný uživatel je viditelný ve webovém rozhraní administrace přepínače. Příkladem může být Obrázek 89.

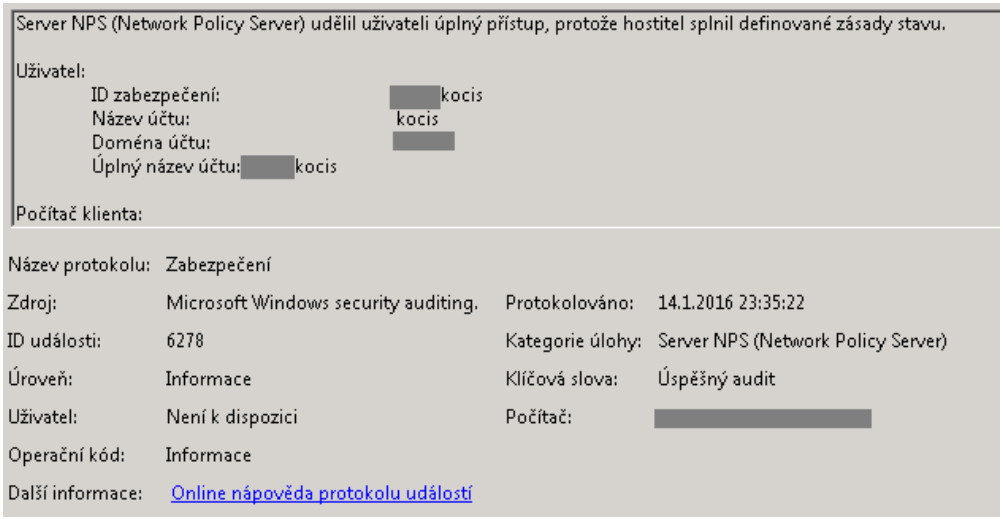
Obrázek 89: Ukázka autentizovaného uživatele na síťovém portu



Zdroj: autor

Obdobně lze ověřit úspěšnou autentizaci díky záznamu a účtování na serveru NPS, viz Obrázek 90.

Obrázek 90: Ukázka autentizovaného uživatele – NPS



Zdroj: autor

4.15.4 802.1X statistiky

Praktickou představu o aktuálním stavu konfigurace virtuálních sítí, lze získat výpisem pomocí příkazu „show VLAN“, viz Příklad 21.

Příklad 21: Seznam VLAN – Cisco – CLI

```
sw12-SG300-52P#show vlan
Created by: D-Default, S-Static, G-GVRP, R-Radius Assigned VLAN

Vlan     Name          Tagged Ports     UnTagged Ports    Created by
---- ------------- ----------------- ----------------- --------------
 1           1                                 gi1-52        V
 20     phone-vlan            gi52          gi1-6,gi8-12     SR
 30    pub-wifi-vlan        gi51-52                           S
 40    kamerova-vlan        gi51-52                           S
 50     stroje-vlan           gi52              gi28         SR
 60    spec-dev-vlan          gi52                           S
 70      tisk-vlan            gi52             gi19-24       SR
 80    int-WiFi-vlan          gi52                           S
200   management-vlan         gi52                           S
998     unauth-vlan           gi52                           S
999     guest-vlan            gi52               gi7         S
```

Zdroj: autor

Podrobnou analýzu nastavení standardu 802.1X na síťovém přepínači Cisco, lze provést díky výpisu informací příkazem „show dot1x“. Názorný výpis je k disposici v Příkladu 22.

Příklad 22: Výpis informací 802.1X – Cisco – CLI

```
sw12-SG300-52P#show dot1x

Authentication is enabled
Authenticating Servers: Radius, None
Unauthenticated VLANs: 998
Guest VLAN: VLAN 999, timeout: immediately
Authentication failure traps are enabled for 802.1x, mac, web
Authentication success traps are enabled for 802.1x, mac, web
Authentication quiet traps are enabled
…
gi6
 Host mode: single-host
 Authentication methods: 802.1x+mac
 Port Administrated Status: auto
 Guest VLAN: enabled
 VLAN Radius Attribute: enabled, static
 Open access: disabled
 Server timeout: 30 sec
 Port Operational Status: authorized
 * Port is down or not present
 Applied Authenticating Server: Radius
 Applied Authentication method: 802.1x
 Session Time (HH:MM:SS): 00:13:23
 MAC Address: 5c:26:0a:22:75:23
 Username: kocis
 Violation:
  Mode: protect
  Trap: disabled
  Trap Min Interval: 10 sec
  Violations were detected: 0
 Reauthentication is enabled
 Reauthentication period: 3600 sec
 Silence period: 0 sec
 Quiet period: 60 sec
 Interfaces 802.1X-Based Parameters
  Tx period: 30 sec
  Supplicant timeout: 30 sec
  Max req: 2
 Authentication success: 4
 Authentication fails: 1
…
```

Zdroj: autor

4.16 Ekonomické aspekty řešení

Důležitým atributem řešení zabezpečeného přístupu k lokální počítačové síti jsou ekonomické náklady spojené s realizací a provozem celého systému.

4.16.1 Náklady na implementaci

Náklady na pořízení nezbytného HW a SW byly minimální. Pro implementaci byla použita již nakoupená síťová zařízení. Vzhledem k pravidlům licencování společnosti Microsoft nebylo nutné pořizovat další licenci produktu Windows Server. Licence umožňuje při zakoupení tohoto produktu v edici Standard a jeho provozu ve virtualizovaném prostředí, nainstalovat a legálně užívat dvě instance samotného serveru.

Časová náročnost implementace navrženého řešení byla 160 hodin.

4.16.2 Náklady na provoz

Provozní náklady jsou také minimální. Celý systém je téměř bezúdržbový. Pro správce sítě a informačních systémů podniku přibyla povinnost udržovat a spravovat jeden nový Microsoft server. Tuto skutečnost může kompenzovat fakt, že konfigurace síťových přepínačů je nyní neměnná. Síťové porty se chovají dynamicky a není nutné promítat běžné změny a úpravy v topologii sítě do jejich konfigurace, jako tomu bylo dříve.

Vzhledem k faktu, že je využita stávající databáze uživatelů, konfigurace klientských stanic probíhá automaticky, nepřináší autentizace a autorizace uživatelů k počítačové síti žádnou další zátěž na lidské zdroje.

5 ZHODNOCENÍ VÝSLEDKŮ A DOPORUČENÍ

Teoretická část diplomové práce shrnuje důležitá fakta a poznatky nutné pro realizaci komplexního řešení zabezpečeného přístupu k lokální počítačové síti v praxi.

Charakterizovány jsou základní bezpečnostní požadavky, vysvětleny principy autentizace a autorizace a podrobně popsány způsoby zabezpečení. Důraz je kladen na různé autentizační metody a TLS protokol, který se využívá i v současných implementacích standardu IEEE 802.1X a protokolu EAP. Popis tohoto standardu, potřebných komponent a protokolů, stejně jako aktuální možnosti realizace, jsou zpracovány v posledních kapitolách teoretické části.

Navazující praktická část popisuje požadavky podniku na zabezpečení počítačové sítě vycházející z provedené analýzy aktuální situace před implementací. Dále zpracovává návrh řešení a detailně zachycuje potřebné změny v topologii, nutné přípravy prostředí, instalace a konfigurace jednotlivých částí celého systému. V neposlední řadě sumarizuje postup zavádění do provozu včetně akceptačních testů a některé problémy s tím spojené. Stručný přehled ekonomických aspektů je nedílnou součástí.

Řešení zabezpečeného přístupu k lokální počítačové síti je funkční a splňuje obecné, teoretické i praktické požadavky podniku na zabezpečení přístupu k síti. Přesto lze nalézt několik doporučení na další rozvoj a rozšíření.

Systém umožňuje třídění uživatelů do virtuálních sítí. Toho se již využívá, ale většina uživatelů sdílí společnou síť. Doporučením do budoucna je navrhnout a implementovat detailnější členění a segmentaci uživatelských sítí, dle jednotlivých typů uživatelů a jejich potřeb s ohledem na zásady minimálních dostupných přístupových práv. Kromě návrhu a implementace bude segmentace obnášet pořízení výkonnějšího síťového směrovače paketů, který zajistí, že data přenášená mezi jednotlivými sítěmi nebudou zatížena zpožděním a rychlost přenosu nebude omezena nedostatečným výkonem směrovače. Segmentace ostatních počítačových sítí podniku je dostatečná již nyní.

Jednou z doporučených možností vylepšení dostupnosti řešení může být pořízení a nasazení sekundárních RADIUS a Active Directory serverů, připravených tak, aby systém uživatele ověřoval i v případě výpadku nebo nedostupnosti primárních serverů.

Dalším doporučeným krokem ve vylepšení celého řešení je zavedení tzv. „zásad stavu“ pro klientské osobní počítače. Při správné implementaci této kontroly bude do sítě umožněn přístup pouze stanicím splňujícím definované požadavky na aktuálnost a stav zabezpečení klientských operačních systému Microsoft Windows. Mezi volitelné požadavky patří například stav instalace kritických bezpečnostních záplat, zapnuté automatické aktualizace, spuštěný a aktualizovaný Antivirový software a další. V případě potřeby je možné rozšířit řízení přístupu k síti i o časové podmínky. Všechny zmíněné možnosti nabízí nainstalovaný a provozovaný Network Policy Server a lze je relativně jednoduše uvést do provozu.

Vhodným krokem bude zavedení ověřování uživatelů pomocí uživatelských certifikátů. Použití certifikátů pro ověřování identity uživatelů přináší další vrstvu zabezpečení, kdy je uživatel autentizován na základě toho, že „něco má“ a „něco zná“. Nese sebou ale komplikace s procesem vydávání, obnovování a ukončování platnosti uživatelských certifikátů. Pro takové řešení bude nutné mít plán a proces pro správu kompletní infrastruktury veřejných klíčů a připraveny postupy pro případy vypršení uživatelského certifikátu a jeho obnovy bez možnosti úspěšné autentizace k počítačové síti uživatelem. Následně bude možné i firemní počítače autentizovat pro ně vydaným certifikátem a umístit je do vyhrazené virtuální sítě s přístupem k základním síťovým prostředkům, například službám doménového řadiče, CA, atp., ještě před autentizací uživatele. Nyní jsou neautorizované stanice umístěny do tzv. „Guest VLAN“ bez ohledu na jejich původ a typ.

Realizovaný systém zabezpečení přináší funkční blokování přístupu neoprávněných osob do kabelové firemní počítačové sítě. Autentizované uživatele a zařízení automaticky člení dle typu a zařazení do jednotlivých virtuálních sítí. Zároveň přináší bezpečnou formu autentizace a autorizace přístupu k bezdrátové síti, které díky tomu může být zkonfigurována tak, že zpřístupňuje interní firemní informační systémy. Neověřené uživatele a zařízení v případě bezdrátové sítě odmítne, v kabelové počítačové síti je umístí do neautorizované sítě s minimálními přístupy, tzv. „Guest VLAN“. Celkově lze říci, že úroveň zabezpečení infrastruktury a informačních technologií podniku byla zavedením tohoto systému zvýšena a doplňuje ostatní vrstvy ochrany systémů a dat společnosti.

Při řízení počítačové bezpečnosti se nesmí zapomínat na skutečnost, že velmi často bývá nejslabším článkem bezpečnostního řetězce uživatel. Protože žádný systém není stoprocentně bezpečný a vždy je maximálně tak silný, jak silný je nejslabší jeho článek, je nutné pamatovat na další bezpečnostní opatření i na vyšších vrstvách síťového modelu a opakovaná školení uživatelů. Všechny metody zabezpečení je nutné provozovat jako celek a brát v potaz fakt, že zabezpečení informačních systémů a sítí není jednorázový úkol, ale soustavná a náročná činnost.

6 ZÁVĚR

Potřeba ověřování identity uživatelů a řízení přístupu k síti a síťovým prostředků se v současné době stávají základním bezpečnostním opatřením. Přes tuto skutečnost mnoho společností soustředí pozornost na důkladnou ochranu perimetru a další ochranná opatření. Ověřování lokálních přístupů k počítačové síti pak zůstává v pozadí, přestože podpora standardu IEEE 802.1X je poměrně rozšířená.

Na základě výzkumu a analýzy informačních zdrojů diplomové práce bylo zjištěno, že obor informační bezpečnosti zabývající se problematikou řízeného přístupu k lokální počítačové síti je velice rozsáhlý. Realizace zabezpečení samotného přístupu k počítačové síti vyžaduje komplexní znalosti z mnoha odvětví informačních technologií. Při volbě vhodné kombinace produktů a dodržení doporučených postupů lze s využitím přiměřeného úsilí a prostředků dosáhnout dobře fungujícího sytému ochrany, s minimálním dopadem na běžnou práci a zvyky uživatelů.

Práce shrnuje a vysvětluje důležitá fakta a principy z oboru autentizace a autorizace přístupů k lokálním počítačovým sítím. Dále popisuje jednu konkrétní implementaci v praxi. Uceluje tak danou problematiku a může sloužit jako průvodce realizací řízeného přístupu k počítačové síti s využitím standardu IEEE 802.1X a aktuálně dostupných technologií.

Implementované řešení zabezpečeného přístupu k lokální počítačové síti je plně funkční a splňuje požadavky společnosti, ve které bylo zaváděno. Realizované řešení zvýšilo celkovou úroveň zabezpečení informačních systémů. Práce také rozebírá další doporučení a změny, které ale znamenají zásadnější úpravy a investice, proto byly ponechány jako plán pro další rozvoj podniku. Na základě výše uvedeného lze konstatovat, že diplomová práce naplnila své cíle.

7 SEZNAM POUŽITÝCH ZDROJŮ

1. **VPN-Consortium.** VPN Technologies: Definitions and Requirements. *Virtual Private Network Consortium.* [Online] 07 2008. [Citace: 06. 01 2016.] Dostupné z: http://www.vpnc.org/vpn-technologies.html.

2. **GEIER, James T.** *Implementing 802.1X security solutions for wired and wireless networks.* Hoboken, N.J. : Wiley, c2008. ISBN 0470168609.

3. **STEWART, J. Michael, Herbert J MATTORD a Andrew GREEN.** *Network security, firewalls, and VPNs: the definitive guide to firewalls, VPNs, routers, and intrusion detection systems.* 2nd ed. Burlington, Mass : Jones, 2014. str. 346. ISBN 978-1-284-03167-6.

4. **NORTCUTT, Stephen, Joel SCAMBRAY a George KURTZ.** *Inside network perimeter security: the definitive guide to firewalls, VPNs, routers, and intrusion detection systems.* 10th anniversary ed. Indianapolis : New Riders, 2003. str. 678. ISBN 07-357-1232-8.

5. **MATYÁŠ, Václav a Krhovják, Jan.** *Autentizace uživatelů a autorizace elektronických transakcí.* příručka managera. Praha : Tate International, c2007.

6. **DOUCEK, Petr.** *Řízení bezpečnosti informací, 2. rozšířené vydání o BCM.* 2., přeprac. vyd. Praha : Professional Publishing, 2011. ISBN 9788074310508.

7. **LASEK, Petr.** Využití protokolu SSL pro vytváření VPN (2). *Svět sítí.* [Online] 04. 05 2004. [Citace: 07. 01 2016.] Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Vyuziti-protokolu-SSL-pro-vytvareni-VPN-2-452004.

8. **BALLAD, Bill, Tricia BALLAD a Erin K BANKS.** *Access control, authentication, and public key infrastructure: the definitive guide to firewalls, VPNs, routers, and intrusion detection systems.* Jones. Sudbury, MA : Jones, 2011. str. 391. ISBN 978-0-7637-9128-5.

9. **APIS Ltd.** Biometrics principles. *Biometria.* [Online] 2016. [Citace: 12. 01 2016.] http://www.biometria.sk/en/principles-of-biometrics.html.

10. **DAS, Ravindra.** *Biometric technology, authentication, biocryptography, and cloud-based architecture.* Boca Raton : CRC Press/Taylor & Francis, 2015. ISBN 9781466592452.

11. **SMITH, Richard E.** *Elementary information security.* Second edition. Burlington, MA : Jones & Bartlett Learning, 2016. ISBN 1284055930.

12. **BROWN, Edwin Lyle.** *802.1X port-based authentication.* Boca Raton : Auerbach, c2007. ISBN 9781420044645.

13. **CISCO SYSTEMS, Inc.** Wired 802.1X Deployment Guide. *Cisco.* [Online] 01. 09 2011. [Citace: 05. 12 2015.] http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html.

14. **ABOBA, B., a další.** Extensible Authentication Protocol (EAP). [Online] 06 2004. [Citace: 11. 02 2016.] https://tools.ietf.org/html/rfc3748.

15. **CISCO SYSTEMS, Inc.** MAC Authentication Bypass Deployment Guide. *CISCO.* [Online] 13. 05 2011. [Citace: 24. 01 2016.] http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/config_guide_c17-663759.pdf.

16. **SANTUKA, Vivek, Banga, Premdeep a Carroll, Brandon.** *AAA identity management security.* Indianapolis, IN : Cisco Press, c2011. ISBN 9781587141447.

17. **MICROSOFT Corporation.** Policies in NPS. *Technet Microsoft.* [Online] 29. 03 2012. [Citace: 18. 12 2015.] https://technet.microsoft.com/en-us//library/cc772279.aspx.

18. **CISCO Systems, Inc.** Cisco 300 Series Managed Switches Administration. *CISCO.* [Online] 2015. [Citace: 22. 12 2015.] http://www.cisco.com/c/dam/en/us/td/docs/switches/lan/csbms/sf30x_sg30x/administration_guide/Cisco_300Sx_v1_4_AG.pdf.

19. **MICROSOFT Corporation.** Active Directory and Active Directory Domain Services Port Requirements. *Technet.* [Online] 06 2009. [Citace: 12. 01 2016.] https://technet.microsoft.com/cs-cz/library/dd772723(v=ws.10).aspx.

20. —. AD DS, Fine-Grained Password Policies. *Technet Microsoft.* [Online] 19. 10 2012. [Citace: 16. 11 2015.] https://technet.microsoft.com/en-us/library/cc770394%28v=ws.10%29.aspx.

21. **MICROSOFT Corp.** AD-DS Fine-Grained Password and Account Lockout Policy. *Technet Microsoft.* [Online] 20. 08 2012. [Citace: 16. 11 2015.] https://technet.microsoft.com/en-us/library/cc770842%28v=ws.10%29.aspx.

22. **KOČIŠ, Jan.** Zabezpečený webový přístup k privátní síti. *Bakalářská práce (Bc.).* Praha : Česká zemědělská univerzita v Praze, Provozně ekonomická fakulta, katedra informačních technologií, 2014.

8 SEZNAM ZKRATEK

AAA – Authentication, Authorization, Accounting

AD – Active Directory

AD-DS – Active Directory Domain Services

ADSI – Active Directory Service Interfaces

AES – Advanced Encryption Standard

AP – Access Point

CA – Certification Authority

CAT5e – Active Directory Domain Services

CLI – Command Line Interface

CN – Common Name

CRL – Certificate Revocation List

DC – Domain Controller

DDOS – Distributed Denial of Service

DES – Data Encryption Standard

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name Service

EAP – Extensible Authentication Protocol

EAPOL – Extensible Authentication Protocol Over LAN

ESSID – Extended Service Set Identifier

FAR – False Acceptance Rate

FRR – False Rejection Rate

GPO – Group Policy Object (Microsoft Windows)

HTTP – Hypertext Transfer Protocol

HTTPS – Hypertext Transfer Protocol Secure

HW – Hardware

CHAP – Challenge Handshake Authentication Protocol

IEEE – Institute of Electrical and Electronics Engineers

IETF – Internet Engineering Task Force

IP – Internet Protocol

IS – Information System

LAN – Local Area Network

LDAP – Lightweight Directory Access Protocol

LDAP(s) – Lightweight Directory Access Protocol Secure

LTS – Long Term Support

MAB – MAC Authentication Bypass

MAC – Media Access Control

MD5 – Message Digest 5

MS – Microsoft

MS-CHAP – Microsoft Challenge Handshake Authentication Protocol

NAS – Network Access Server

NPS – Network Policy Server

NT – New Technology (Windows NT)

OS – Operating System

OSI – Open System Interconnection

OTP – One Time Password

PBX – Private Branch Exchange

PC – Personal Computer

PEAP – Protected Extensible Authentication Protocol

PGP – Pretty Good Privacy

PIN – Personal Identification Number

PKI – Public Key Infrastructure

RADIUS – Remote Authentication Dial in User Service

RFC – Request for Comments

RFID – Radio Frequency Identification

RPC – Remote Procedure Call

RSA – public-key cryptosystems (Ron **R**ivest, Adi **S**hamir, Leonard **A**dleman)

SHA – Secure Hash Algorithm

SMB – Server Message Block

SMS – Short Message Service

SMTP – Simple Mail Transfer Protocol

SNMP – Simple Network Management Protocol

SOAP – Simple Object Access Protocol

SSH – Secure Shell

SSID – Service Set Identifier

SSL – Secure Sockets Layer

SW – Software

SYSLOG – System Log

TCP – Transmission Control Protocol

TLS – Transport Layer Security

TTLS – Tunnelled Transport Layer Security

UDP – User Datagram Protocol

VLAN – Virtual Local Area Network

VNC – Virtual Network Computing

VoIP – Voice Over Internet Protocol

VPN – Virtual Private Network

Wi-Fi – Wireless Fidelity

WLAN – Wireless LAN

WPA – Wi-Fi Protected Access

9 PŘÍLOHY

9.1 Příloha A

9.1.1 Akceptační testy LAN

Tabulka 6: Akceptační test #1

Číslo testu	**1**
Název testu	**Guest VLAN**
Popis testu	Připojení zařízení bez podpory standardu IEEE 802.1X, které není v seznamu MAB, ke každému síťovému portu přepínače.
Úspěšný výsledek testu	1. Síťový port se aktivuje,
	2. po neúspěšné autentizaci se port přepne do VLAN 999,
	3. zařízení získá síťovou IP adresu ze serveru DHCP,
	4. zařízení je dostupné na síti,
	5. zařízení **nemá** přístup k interním síťovým zdrojům,
	6. zařízení **nemá** přístup do internetu,
	7. zařízení **je dostupné** pro správu administrátorem.

Zdroj: autor

Tabulka 7: Akceptační test #2

Číslo testu	**2**
Název testu	**Úspěšná autentizace**
Popis testu	Připojení zařízení s podporou standardu IEEE 802.1X, které není v seznamu MAB, ke každému síťovému portu přepínače.
Úspěšný výsledek testu	1. Síťový port se aktivuje,
	2. přepne se do správné VLAN,
	3. zařízení získá síťovou IP adresu ze serveru DHCP,
	4. zařízení je dostupné na síti,
	5. zařízení **má** přístup k interním síťovým zdrojům,
	6. zařízení **má** přístup do internetu.

Zdroj: autor

Tabulka 8: Akceptační test #3

Číslo testu	**3**
Název testu	**Neúspěšná autentizace**
Popis testu	Připojení zařízení s podporou standardu IEEE 802.1X, které není v seznamu MAB a nemá nakonfigurované 802.1X ověřování, ke každému síťovému portu přepínače.
Úspěšný výsledek testu	1. Síťový port se aktivuje,
	2. uživatel je vyzván k autentizaci k síti (vloží špatné údaje),
	3. port přepne se do VLAN 999,
	4. zařízení získá síťovou IP adresu ze serveru DHCP,
	5. zařízení je dostupné na síti,
	6. zařízení **nemá** přístup k interním síťovým zdrojům,
	7. zařízení **nemá** přístup do internetu.

Zdroj: autor

Tabulka 9: Akceptační test #4

Číslo testu	**4**
Název testu	**Úspěšná autentizace MAB – VLAN 20,50,60,70,80**
Popis testu	Připojení zařízení bez podpory standardu IEEE 802.1X, které **je** v seznamu MAB, ke každému síťovému portu přepínače.
Úspěšný výsledek testu	1. Síťový port se aktivuje,
	2. po pár sekundách se přepínač pokusí ověřit zařízení pomocí MAC adresy,
	3. port se přepne do správné VLAN,
	4. zařízení získá síťovou IP adresu ze serveru DHCP,
	5. zařízení je dostupné na síti,
	6. zařízení **má** přístup k interním síťovým zdrojům.

Zdroj: autor

Tabulka 10: Akceptační test #5

Číslo testu	**5**
Název testu	**Úspěšná opakovaná autentizace v pravidelných intervalech – LAN**
Popis testu	Zařízení s podporou standardu IEEE 802.1X, je připojeno síťovému portu přepínače a je autentizované. Vyčká se 60-65 min a ověří funkčnost. Test je dostatečné provést jedenkrát pro každý přepínač.
Úspěšný výsledek testu	1. Síťový port je stále v autorizovaném stavu,
	2. v protokolu událostí je vidět aktuální úspěšný pokus o autentizaci,
	3. zařízení **má** přístup k interním síťovým zdrojům.

Zdroj: autor

Tabulka 11: Akceptační test #6

Číslo testu	**6**
Název testu	**Zaznamenávání operací síťového přepínače ve vzdáleném protokolu**
Popis testu	Vizuální kontrolou protokolu událostí na centrálním serveru se ověří, zda přepínač zasílá informace o událostech na vzdálený server protokolem SYSLOG.
Úspěšný výsledek testu	1. Pro přepínač vznikl na serveru nový soubor s protokolem,
	2. obsah souboru se v reálném čase aktualizuje a doplňuje.

Zdroj: autor

9.1.2 Akceptační testy WLAN

Tabulka 12: Akceptační test #7

Číslo testu	**7**
Název testu	**Úspěšná autentizace WiFi-INT – manuálně**
Popis testu	Připojení **ne**firemního přenosného osobního počítače nebo mobilního zařízení k bezdrátové síti WiFi-INT. Zadání uživatelského jména a hesla.
Úspěšný výsledek testu	1. Připojení k bezdrátové síti se aktivuje,
	2. zařízení získá síťovou IP adresu ze serveru DHCP,
	3. zařízení je dostupné na síti,
	4. zařízení **má** přístup k interním síťovým zdrojům.

Zdroj: autor

Tabulka 13: Akceptační test #8

Číslo testu	**8**
Název testu	**Neúspěšná autentizace – WiFi-INT**
Popis testu	Pokus o připojení přenosného osobního počítače, bez nakonfigurovaného ověřování k bezdrátové síti WiFi-INT a úmyslné zadání nesprávné kombinace jména a hesla.
Úspěšný výsledek testu	1. Pokus o připojení k bezdrátové síti je neúspěšný,
	2. zařízení **nezíská** síťovou IP adresu ze serveru DHCP,
	3. zařízení **není** dostupné na síti,
	4. zařízení **nemá** přístup k interním síťovým zdrojům,
	5. zařízení **nemá** přístup do internetu.

Zdroj: autor

Tabulka 14: Akceptační test #9

Číslo testu	**9**
Název testu	**Úspěšná autentizace WiFi-INT – GPO**
Popis testu	Připojení firemního přenosného osobního počítače k bezdrátové síti WiFi-INT.
Úspěšný výsledek testu	1. Připojení k bezdrátové síti se aktivuje,
	2. zařízení získá síťovou IP adresu ze serveru DHCP,
	3. zařízení je dostupné na síti,
	4. zařízení **má** přístup k interním síťovým zdrojům.

Zdroj: autor

Tabulka 15: Akceptační test #10

Číslo testu	**10**
Název testu	**Funkční přístupy k interním zdrojům – WiFi-INT**
Popis testu	Připojení firemního přenosného osobního počítače k bezdrátové síti WiFi-INT. Testování dostupnosti a funkčnosti Terminal serveru, Informačního systému, tiskáren.
Úspěšný výsledek testu	1. Připojení na vzdálenou plochu terminálového serveru je funkční,
	2. aplikace informačního systému lze spustit a funguje běžným způsobem,
	3. na síťové tiskárně je funkční tisk.

Zdroj: autor

9.1.3 Akceptační testy obecné

Tabulka 16: Akceptační test #11

Číslo testu	**11**
Název testu	**Účtování RADIUS serveru**
Popis testu	Na autentizačním serveru NPS se sleduje protokol událostí Služby Síťové zásady a přístup.
Úspěšný výsledek testu	1. Protokol událostí NPS serveru se aktualizuje, 2. v reálném čase přibývají informace o autentizaci a připojení uživatelů.

Zdroj: autor