Zabezpečení podnikové sítě pomocí autentizace uživatelů

Tomáš Kallus

Bakalářská práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Tomáš Kallus**
Osobní číslo:	**A17167**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Zabezpečení podnikové sítě pomocí autentizace uživatelů**
Téma práce anglicky:	**User Authentication for Corporate Network Security**

Zásady pro vypracování

1. Popište aktuální stav počítačové sítě.
2. Uveďte hlavní nedostatky v zabezpečení sítě.
3. Analyzujte možnosti zvýšení bezpečnosti sítě.
4. Zrealizujte zabezpečení pomocí autentizace uživatelů.
5. Popište nasazení na koncových zařízeních.

Rozsah bakalářské práce:
Rozsah příloh:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. KUROSE, James F. a Keith W. ROSS. Počítačové sítě. Brno: Computer Press, 2014, 622 s. ISBN 9788025138250.
2. HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 5., aktualiz. vyd. Brno: Computer Press, 2011, 303 s. ISBN 9788025131763.
3. STALLINGS, William a Lawrie BROWN. Computer security: principles and practice. Third edition. Boston: Pearson, [2015], 840 s. Always learning. ISBN 9781292066172.
4. HPE OfficeConnect 1920S 8G/24G/48G Switch Series Management and Configuration Guide [online]. listopad 2018, , 226 [cit. 2019-11-08]. Dostupné z: https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-a00003478en_us
5. STANEK, William R. Microsoft Windows Server 2012: kapesní rádce administrátora. Brno: Computer Press, 2015, 736 s. ISBN 9788025138175.

Vedoucí bakalářské práce: **Ing. Jiří Korbel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **7. prosince 2019**
Termín odevzdání bakalářské práce: **25. května 2020**

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Ve Zlíně dne 7. prosince 2019

Jméno, příjmení: Tomáš Kallus

Název bakalářské práce: Zabezpečení podnikové sítě pomocí autentizace uživatelů

Prohlašuji, že

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

Prohlašuji,

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

Tomáš Kallus v. r.

Ve Zlíně, dne

.....
podpis diplomanta

ABSTRAKT

Bakalářská práce se zabývá zabezpečením počítačové sítě ve fiktivní společnosti WAXEN s.r.o. formou ověřování uživatelů. Ověřování uživatelů bude realizováno prostřednictvím protokolu IEEE 802.1X. V první, teoretické části, bude obecně popsána síť a její součásti, analýza hrozeb a současný způsob zabezpečení. V praktické části bude charakterizována aktuální infrastruktura sítě společnosti, dále pak vytvoření testovacího prostředí, spuštění a nastavení síťových prvků, serveru pro ověření a nastavení jednotlivých koncových stanic. V závěru bude krátce popsán plán nasazení a kalkulace. Cílem práce je nastínění problematiky bezpečnosti a ukázka postupu, který lze využít pro aplikování zabezpečení sítě v reálném provozu.

Klíčová slova: počítačová síť, RADIUS, Windows Server 2019, switch, zabezpečení sítě, IEEE 802.1X

ABSTRACT

The bachelor's thesis deals with the security of a computer network in a fictitious company WAXEN s.r.o. in the form of user authentication. User authentication will be implemented via the IEEE 802.1X protocol. In the first theoretical part the network and its components, threat analysis and the current method of security will be described in general. The practical part will characterize the current infrastructure of the company's network, then the creation of a test environment, start-up and setup of network elements, a server for authentication and setup of individual workstations. In the end will be briefly described the deployment plan and calculation. The aim of the work is to outline the issue of security and demonstrate the procedure that can be used to apply network security in real operation.

Keywords: Network, RADIUS, Windows Server 2019, switch, Network security, IEEE 802.1X

Chci poděkovat vedoucímu bakalářské práce Ing. Jiřímu Korbelovi, PhD. za vedení.

Dále bych rád poděkoval mým blízkým za jejich morální podporu při studiu.

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

OBSAH

ÚVOD

Záměrem společnosti je zabezpečení počítačové sítě proti neoprávněnému připojení neschválených zařízení k síti. Společnost popisovaná v bakalářské práci bude nazývána WAXEN s.r.o., jež je společností nefigurující v aktuálním reálném obchodním rejstříku. Prostory, ve kterých společnost sídlí, obsahují dva propojené rozlehlé areály. V prvním areálu se nachází kancelářská budova a několik budov výroby, v druhém areálu se nachází dvě budovy výroby a jedna kancelář. Společnost zaměstnává 150 zaměstnanců a vlastní 80 pracovních stanic připojených k datové síti. Datové rozvody jsou rovnoměrně rozmístěny ve všech budovách s velkým počtem přípojných míst. Programátoři společnosti pracují s laptopy v různých prostorách a vyžadují připojení k síti v každé budově. Současně je nutné zajistit přístup k síti pro externí pracovníky. V současné síti je těžké zajistit bezpečnost před připojením nežádoucího zařízení do sítě. Původně bylo realizováno vypínání jednotlivých datových zásuvek na úrovni síťového switche. Programátor, vyžadující připojení, kontaktoval pracovníka IT (Information Technology) s žádostí o povolení konkrétní datové zásuvky. IT administrátor následně datovou zásuvku povolil. Povolení zásuvky IT administrátorem má dvě základní nevýhody. Programátor musí počkat, než administrátor zásuvku povolí a druhá nevýhoda spočívá v absenci oznámení programátora, že již zásuvku nepotřebuje. Nastává situace, kdy programátor opustí pracovní místo, a datová zásuvka zůstává povolená. Řešení formou povolení datových zásuvek se tedy neosvědčilo a všechny zásuvky zůstávají povolené.

Je velice časově náročné, aby pracovník IT kontroloval každodenně všechny datové zásuvky, zda v nich není připojené cizí zařízení. Jedná se zhruba o 200 zásuvek v obou areálech společnosti. Cizím zařízením jsou zde myšleny zejména soukromé notebooky zaměstnanců, nebo soukromé wifi routery, ke kterým si následně zaměstnanci připojují soukromé telefony. V dnešní době plné kryptovacích virů je připojení nezabezpečeného notebooku či telefonu velké riziko pro celou společnost.

Bakalářská práce popisuje bezpečnostní analýzu IT infrastruktury, nedostatky a možnosti zvýšení bezpečnosti sítě. Bude popsán způsob zabezpečení s využitím ověřování uživatelů. Protokol IEEE 802.1X nabízí způsob ověření uživatele při připojení zařízení k síti. Uživatel bude po připojení vyzván k zadání uživatelského jména a hesla. Protokol IEEE 802.1X umožní identifikovat uživatele a po autentifikaci ho připojit do správné sítě. V případě neznalosti uživatelských přístupů je port automaticky zakázán. V závěru práce bude uvedena

kalkulace nákladů pro společnost WAXEN s.r.o. a krátce budou popsány jednotlivé kroky nasazení.

Cílem práce je vytvoření postupu, jakým způsobem realizovat zabezpečení sítě využitím ověření uživatelů prostřednictvím protokolu 802.1X. K realizaci jsou nezbytné alespoň základní znalosti z oblasti Microsoft Windows Serverů a počítačových sítí.

I. TEORETICKÁ ČÁST

1 POČÍTAČOVÁ SÍŤ

Nástup využití počítačů byl bezesporu velký milník ve způsobu zpracování a získávání informací. První počítače byly velké stroje postavené jen za určitým úkolem a pracující podle pevně daného programu, uloženého na děrném štítku. S rozvíjejícím se světem výpočetní techniky byla nutná výměna informací mezi počítači. Po prvních pokusech s propojením počítačů se nakonec nejvíce rozšířilo propojení pomocí sítě [1][2].

V počátcích zavedení sítí nebylo úplně nezbytné řešit jejich bezpečnost, a to z důvodu nedostatku znalostí uživatelů. Sítě mohli obsluhovat jen odborníci, kteří měli dostatečnou znalost problematiky sítí. Rozvoj výpočetní techniky však pokročil a dnes dokáže připojit počítač k síti téměř každý. S tím přichází i zvýšené bezpečnostní riziko zneužití a poškození sítě samotné, nebo jednotlivých serverů, dat či síťových zařízení.

Počítačová síť je soustava dvou a více vzájemně propojených zařízení. Jejím účelem je zajištění komunikace, sdílení a výměna informací. Samotná fyzická realizace sítě může být provedena několika prostředky. Mezi dnes nejběžnější patří použití metalického nebo optického kabelu a bezdrátového přenosu. Aby mohl samotný počítač komunikovat přes propojené datové kabely, nebo bezdrátově, musí použít protokol, který převádí data na signály přenášené po datovém médiu a zpět. I oblast protokolů prošla vývojem, na jejímž konci zůstal jeden z nejpoužívanějších protokolů, TCP/IP. V dnešní době má počítač nebo mobilní telefon bez připojení k síti velice omezené možnosti [3][4].

Ze nejrozšířenější síť lze považovat Internet. Internet je celosvětová síť, která se skládá z miliónů menších vzájemně propojených podsítí. Připojení počítače nebo mobilního telefonu k této síti je dnes zcela běžné. S rozvojem elektroniky je možné k Internetu připojit i jiná zařízení, jako například televize, ledničky, pračky, ovládání ústředního topení, bezpečnostních systémů, požárních systémů nebo třeba kamer [3].

Pro účel realizace zabezpečení je popisovaná vnitřní síť společnosti WAXEN s.r.o. Vnitřní síť využívá celá řada důležitých systémů, jako je například informační a výrobní systém, docházkový systém, kamerový, bezpečnostní a požární systém a další. Síť je složena jak z kabelových rozvodů, za použití optických i metalických kabelů, tak i z bezdrátových zařízení. Bezdrátová část sítě pokrývá jen vybrané části areálů. Vnitřní síť je prostřednictvím routeru připojena do vnější sítě Internet. Připojení k Internetu umožňuje společnosti komunikovat se zákazníky, partnery, dodavateli. Zaměstnancům poskytuje Internet přístup

k datům společnosti z vnější sítě, například z domova. Vnitřní síť je chráněna výkonným Firewallem.

1.1 Terminologie

Před samotným popisem problematiky je nutné charakterizovat jednotlivé použité technologie, nezbytné pro realizaci samotného zabezpečení.

1.1.1 IT Infrastruktura

IT infrastrukturou jsou myšleny datové rozvody vnitřní sítě, síťové zařízení jako jsou switche, tiskárny, servery, výrobní terminály, docházkový systém. Současně i veškerá data jako uložené na serverech společnosti jako jsou dokumenty nebo data informačních a výrobních systémů.

1.1.2 Protokol TCP/IP

V dnešní době nejpoužívanější síťový model. Jedná se o soubor protokolů pro komunikaci v počítačové síti. TCP/IP je rozdělen do 4 vrstev a každá z těchto vrstev má svou úlohu při komunikaci [3].

Tabulka 1 Popis vrstev síťového modelu TCP/IP [3].

Aplikační	Aplikační protokoly, RADIUS, http a další
Transportní	TCP – spojovaná, potvrzovaná služba, UDP – nespojovaná nepotvrzovaná služba
Síťová (Internetová)	Zajišťuje adresaci, předávání a směrování.
Vrstva síťového rozhraní	Nejnižší vrstva s přístupem k přenosovému médiu.

1.1.3 Firewall

Jedná se o zařízení, určené pro bezpečné oddělení vnitřní sítě od vnější sítě Internet. Uživatelé vnitřní sítě společnosti tak mohou přistupovat informacím dostupným na Internetu [3].

1.1.4 Router

Router, někdy nazýván směrovač. Zařízení, které odděluje k němu připojené sítě a směruje mezi nimi síťový provoz. Například mezi vnitřní sítí společnosti a Internetem.

1.1.5 Active Directory Domain Services

Active Directory Domain Services (Dále jen ADDS) je adresářová služba, která sdružuje informace ve formě objektů hlavně o připojených počítačích, serverech, účtech uživatelů a počítačů a bezpečnostních skupinách. Pro lepší komunikaci se službou ADDS v síti, má služba své jméno tzv. doménu. Součástí informací o uživatelích jsou informace o bezpečnostních skupinách, do kterých patří, a jejich přístupové údaje. Každý účet, použitý pro přihlášení k vnitřní síti, je ověřen na serveru se službou ADDS. Následně služba rozhodne, zda se uživatel může přihlásit, nebo přihlášení zamítne. Pro realizaci zabezpečení protokolem IEEE 802.1X budou využity informace o uživatelích k jejich ověření pro připojení k vnitřní síti [5].

1.1.6 DNS server

DNS, Domain Name System (Dále jen DNS) je služba plnící funkci překladu jména serveru na IP adresu. Při přístupu k jakémukoliv serveru, ať už internímu nebo veřejné www stránce, je službou DNS přeložen název cílového serveru na jeho IP adresu. Po překladu již pokračuje komunikace pomocí IP adresy. Překlad probíhá na pozadí a samotný uživatel nepozná, že k němu došlo. Služba DNS je nezbytnou součástí služby ADDS [5].

1.1.7 Group Policy

Jedná se o systémovou politiku. Group Policy je databáze klíčů a hodnot uložená ve stromové struktuře. Používá se pro nastavení počítače, serverů, nebo aplikací. Každý počítač a server se systémem Microsoft Windows, má svou vlastní systémovou politiku. Součástí serveru se službou Active Directory je konzole Group policy management s politikou na úrovni domény. Pomocí této konzole ji lze měnit a upravovat dle požadavků administrátora. Počítač nebo server, připojený k doméně, při startu načítá doménovou politiku, která má přednost před systémovou politikou počítače. Pomocí ADDS a Group Policy je možné měnit toto nastavení a tím dosáhnout požadovaného chování. Administrátor tak může provést změny na jednom místě. Doménovou politiku si načtou všechny nebo jen vybrané počítače a při spouštění systému aplikují požadované změny. Pomocí Group Policy lze upravit

chování systému nebo například hromadně instalovat aplikace na vybraných počítačích. Administrátor tedy nemusí obcházet všechny počítače jeden po druhém, aby je nastavil [6].

1.1.8 RADIUS

RADIUS, Remote Authentication Dial In User Service, je služba pro vzdálené ověření. Vystupuje jako server zprostředkující ověření mezi klientem a serverem. Jako klient zde vystupuje zařízení „síťový switch“. Jako server pak Windows server se službou ADDS [7].

1.1.9 DHCP server

Dynamic Host Configuration Protocol, jedná se o protokol, pomocí kterého probíhá síťové nastavení klienta po připojení k síti. DHCP server odpovídá žádostem klientů o přidělení IP adresy, kterou přiděluje z definovaného rozsahu. Spolu s IP adresou klient obdrží i masku podsítě, IP adresu výchozí brány a IP adresu DNS serveru [5].

1.1.10 Certifikační Autorita

Certifikační autorita plní funkci vydavatele certifikátů. U vydaných certifikátů ověřuje jejich platnost a informace uvedené v samotném certifikátu. Vydáním certifikátu certifikační autoritou a přidělení konkrétnímu serveru lze ověřit jeho pravost. Na serverech Microsoft plní službu certifikační autority role serveru s názvem Active Directory Certificate Services (Dále jen ADCS) [8].

1.1.11 Wildcard certifikát

Jedná se o typ certifikátu někdy označovaný jako hvězdičkový. Wildcard certifikátem je možné ověřit všechny subdomény. V případě domény WAXEN.cz bude například ověřena i subdoména WAXEN-radius.WAXEN.cz, což je název serveru. Je tak možné jedním univerzálním typem certifikátu ověřit pravost všech serverů a počítačů připojených v doméně ADDS [9].

1.1.12 Ověřování pomocí protokolu IEEE 802.1X

IEEE 802.1X je protokol určený pro autentizaci. Definuje způsob ověření klienta v síti. Aby bylo možné tento způsob zabezpečení realizovat, je nutná podpora tohoto protokolu v samotném síťovém prvku, prostřednictvím kterého se uživatel připojuje k síti [10].

1.1.13 Protokol EAP

Extensible Authentication Protocol (Dále jen EAP) je autentizační framework, pomocí kterého se navazuje spojení mezi klientem a serverem. Při navázání spojení dochází k vyjednání autentizační metody. Switch v prvotní komunikaci s klientem povoluje jen protokol EAP. Pomocí EAP se navazuje bezpečné spojení pro odeslání uživatelského jména a hesla [11][12].

1.1.14 PEAP

Protected EAP (Dále jen PEAP), je novější verze protokolu EAP. Hlavní nedostatek u protokolu EAP je počáteční výměna zpráv, která je odesílána v prostém textu. PEAP využívá EAP-TLS, kdy je v prvním kroku vytvořen zabezpečený tunel a až tímto tunelem dochází k první komunikaci EAP [13].

1.1.15 Protokol CHAP

Challenge Handshake Authentication Protocol, protokol sloužící k autentizaci uživatele. Specifikace je popsána v RFC-1994. Společnost Microsoft později tento protokol vylepšila na verzi 2. Součástí vylepšené verze 2 je podpora protokolu PEAP [14][15][16].

1.1.16 VLAN

Virtuální síť, jedná se o síť v síti. Jeden fyzický kabelový spoj nebo port na switchi může přenášet jednu klasickou síť a několik virtuálních sítí. Virtuální sítě jsou od sebe odděleny a jsou na sobě nezávislé. Virtuální sítě jsou označeny identifikátorem ID a jsou takzvaně tagované a netagované. Tagovaná VLAN síť označuje každý rámec identifikátorem VLAN sítě. Jedná se o číslo v rozmezí 1 až 4096. U netagovaných VLAN sítí nejsou rámce označené a samotné oddělení od ostatních sítí probíhá na úrovni switche. Každý port může být členem jen jedné netagované VLAN sítě, ale může patřit do více tagovaných sítí současně. Sítě se dělí o přenosové médium. Rychlost média se tak dělí počtem virtuálních sítí [3], [17].

1.1.17 Switch

Switch je hardwarový aktivní prvek, ke kterému se připojují další switche nebo koncové zařízení jako jsou počítače servery tiskárny a další. Je to klíčový prvek tvořící samotnou síť.

1.1.18 Data

Pojmem data jsou zde myšleny veškeré elektronické dokumenty, poštovní zprávy, soubory používaných programů, nastavení serverů včetně databáze uživatelů v ADDS, jakož i databáze, které jsou využívány výrobním, docházkovým, informačním a mzdovým systémem.

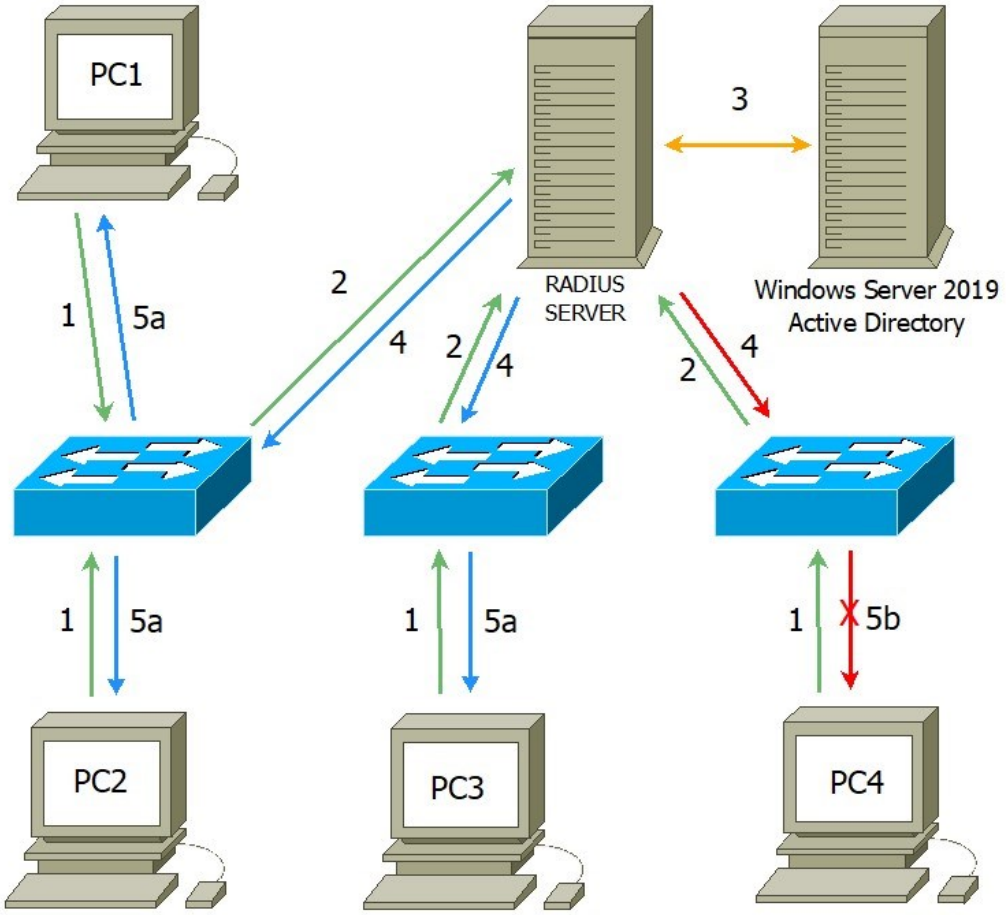
1.1.19 HYPER-V

Virtualizační prostředí z produkce Microsoftu. Umožňuje provoz virtuálních serverů. Na jednom fyzickém serveru tedy může být spuštěno více virtuálních serverů.

1.2 Princip ověření

Ve výchozím nastavení je síťové zařízení nastaveno bez ověření. Akceptuje každé koncové zařízení, které se připojí. Po zapnutí a konfiguraci ověřování je na každém portu povolen jen protokol EAP pro ověření klienta, ostatní komunikace je zakázána. Připojení uživatele k síti:

1. po připojení klienta si vyžádá protokol IEEE 802.1X autentizační údaje předávané prostřednictvím protokolu PEAP. Uživatel zadává uživatelské jméno a heslo a údaje odesílá na síťový prvek. V tomto případě síťový switch,
2. pomocí protokolu PEAP předává switch autentifikační údaje na RADIUS server,
3. RADIUS server předává autentifikační údaje službě ADDS. Server ADDS vyhodnotí obdržené údaje a výsledek ověření vrací zpět RADIUS serveru,
4. RADIUS server vrací výsledek ověření zpět k zařízení, které žádost odeslalo. Součástí výsledku ověření je informace o přidělené síti VLAN, do které má být zařízení připojeno,
5. switch přijímá výsledek z RADIUS:
   (a) **kladné ověření** – switch přidá port do správné VLAN sítě, kterou obdržel spolu s výsledkem ověření z RADIUS serveru, a povoluje plný provoz datové zásuvky,
   (b) **záporné ověření** – switch zakáže datovou zásuvku pro veškerou komunikaci. Pro opětovné vyvolání autentizace, je nutné odpojit zařízení od sítě a opětovně je připojit.



Obrázek 1 Ilustrace ověření s označením jednotlivých kroků [Vlastní zdroj].

Obrázek (Obr. 1.) ilustruje jednotlivé kroky ověření uživatele popsané v předchozí části. V případě PC1 až PC3 proběhlo ověření úspěšně. Uživatel na PC4 nebyl ověřen a port byl zakázán. V případě opakování ověření uživatele na PC4 je nutné, aby se uživatel odpojil od sítě a znovu připojil. Po opětovném připojení dojde k novému ověření.

1.3 Závěr

Uvedená terminologie obsahuje technologie a protokoly potřebné k realizaci popisovaného zabezpečení. Použité technologie a protokoly se stále vyvíjí a rozšiřují. Je pravděpodobné, že je v budoucnu nahradí modernější a vyspělejší verze.

2 ANALÝZA HLAVNÍCH NEDOSTATKŮ SÍTĚ

S růstem společnosti rostou i hrozby vyplývající z používání dat. Firma musí na jedné straně data chránit, ale na straně druhé je přístup k datům pro zaměstnance, případně pro zákazníky, klíčový. Společnost WAXEN s.r.o. se rozhodla sestavit auditorský tým z interních zaměstnanců s využitím odborníků externího dodavatele auditorských služeb. Rozsah auditu je zaměřen na IT infrastrukturu společnosti s cílem zvýšení její bezpečnosti [18][19].

2.1 Aktiva IT infrastruktury

Stanovení aktiv, která je nutné chránit v rámci IT infrastruktury společnosti:

- data – představuje dokumenty, smlouvy, data informačního systému, interní databáze, poštovní zprávy, software pro řízení výroby, ostatní software,
- hardware a síťové prvky – představuje interní servery, kde jsou data uložena, síťové switche, přístupové body bezdrátové sítě, terminály, počítače, tiskárny,
- konektivita – samotné propojení síťových prvků, datové rozvody, připojení k internetu.

2.2 Rozlehlost sítě

S růstem společnosti přímo úměrně roste i její rozloha. Nově vybudované nebo pronajaté prostory, areály i jednotlivé budovy je nutné připojit ke stávající síti. V celém areálu se nachází velké množství volně přístupných zásuvek pro připojení k síti, které zaměstnanci potřebují ke své práci. Kontrola používání sítě napříč areálem je velice složitá a v současném stavu těžko realizovatelná.

2.3 Cizí zařízení připojená v síti

Cizím zařízením je myšleno soukromé zařízení zaměstnance např. notebook nebo telefon. Připojení chytrého telefonu nebo přenosného počítače k podnikové síti, skrývá velké nebezpečí v podobě nezabezpečeného zařízení v síti. Vědomě nebo nevědomě může útočník nebo uživatel způsobit bezpečnostní incident a poškodit aktivum společnosti.

2.4 Způsob připojení k síti

Kdokoliv ze zaměstnanců nebo návštěvníků, může využít nezabezpečené datové zásuvky pro připojit k síti. Připojení je bez jakékoliv ochrany. Ochrana je řešena až na úrovni přístupu

k serveru. Neoprávněná osoba tedy bez hesla přístup k datům nemá. V tomto případě hrozí zneužití na úrovni sítě samotné. Například připojení zařízení z důvodu přístupu k internetu snižuje prostředky pro ostatní uživatele. Konektivita do internetu má omezenou rychlost. Neoprávněným přístupem dochází ke snížení rychlosti, kterou potřebují zaměstnanci k práci.

2.5 Shledané hrozby

Auditorský tým, jenž prováděl bezpečnostní audit IT infrastruktury, shledal několik hrozeb snižující bezpečnost sítě:

- nechráněné připojení k síti – jedná se o nechráněné volně dostupné datové zásuvky v obou areálech, které lze využít pro připojení do interní sítě společnosti
- zneužití připojení k internetu – příkladem může být připojený přenosný počítač zaměstnance, jenž využívá připojení k internetu pro soukromé účely
- možnost provádění útoků na vnitřní infrastrukturu, vnímané jako snaha získat data společnosti (Útoky můžou být vědomé, vedené samotným zaměstnancem, či nevědomé, prováděné například virem.)

2.6 Závěr

Závěrem kapitoly o analýze hlavních nedostatků sítě je stanovení hrozeb snižujících bezpečnost IT infrastruktury. Jako největší forma hrozby jsou vnímány volně dostupné datové zásuvky v celé firmě. Útočník může po připojení provádět různé formy útoků na vše, co je k síti připojené, nebo síť zcela zablokovat. Výsledkem tohoto auditu je stanovení bezpečnostních hrozeb pro oblast IT infrastruktury [18][19].

3 ANALÝZA MOŽNOSTI ZVÝŠENÍ BEZPEČNOSTI SÍTĚ

Bezpečností sítě rozumíme ochranu před neoprávněným přístupem. Ochrana před útoky na servery s cílem vyřadit je z provozu nebo krádež firemních dat. Uvedené hrozby můžou ochromit fungování společnosti. V následující části auditorským tým shrnuje a doporučuje způsoby vedoucí k vyšší bezpečnosti IT infrastruktury a sítě samotné.

3.1 Zvýšení počtu pracovníků IT

Síťové switche používané ve společnosti, mají jistou formu ovládání a monitorování. Existují možnosti, jak kontrolovat každé zařízení. Aktuální seznam schválených zařízení lze porovnávat s počtem připojených zařízení. Lze také využít program zaměřený na monitorování sítě. Pro zvýšení bezpečnosti sítě je vhodné zvýšit počet pracovníků IT. Stanovit povinnosti a odpovědnost nového pracovníka IT se zaměřením pro monitorování sítě a vyhodnocování neoprávněného zařízení v síti. Nevýhodou monitorování sítě je jednak ekonomická náročnost a pak detekce zařízení až po připojení k síti. Nelze předcházet neoprávněnému připojení, jen ho odhalit.

3.2 Deaktivace datových zásuvek

Jednou z možností je deaktivovat, zakázat, všechny nepoužívané datové zásuvky. V případě nutnosti lze zásuvku kdykoliv aktivovat. Jedná se o bezpečné a levné řešení, ale má svá omezení. V případě nutnosti musí uživatel kontaktovat pracovníka IT a vyžádat si povolení datové zásuvky. Útočník ale může odpojit jiné zařízení, například tiskárnu, a datovou zásuvku použít ve svůj prospěch. Řešení pomocí deaktivace zásuvek již společnost využívala a shledala ho jako nepraktické a nepoužitelné.

3.3 Dohled pracovníků nižšího managementu

Dohledem pracovníků nižšího managementu se rozumí kontrola datových zásuvek, zda v nich není připojené cizí zařízení. Mistři a vedoucí výrobních úseků jsou přítomni v prostorách po celou pracovní dobu. Lze je využít pro namátkovou vizuální kontrolu připojených zařízení.

3.4 Ochrana pomocí MAC adres

Jedná se o ochranu pomocí MAC adresy připojeného zařízení. MAC adresa slouží pro identifikaci zařízení v síti. Byla přidělena výrobcem zařízení při výrobě a je jedinečná. Na

úrovni switche lze povolit přístup k síti jen pro známé počítače, servery, tiskárny a další síťové zařízení využitím jejich MAC adres. Pro aplikaci zmíněné ochrany je nutné vést databázi MAC adres povolených zařízení. Řešení je využito pro bezdrátové sítě.

3.5 Ověřování po připojení k síti pomocí uživatelského jména a hesla

Využití protokolu IEEE 802.1X pro ověření uživatele. Pro připojení počítače nebo jakéhokoliv jiného síťového zařízení je vyžadováno zadání uživatelského jména a hesla. Po ověření přihlašovacích údajů bude přístup k síti povolen. K síti se tedy připojí pouze skupina vybraných uživatelů. Ověřování uživatelů po připojení k síti je efektivní, plně automatickou ochranou sítě. Tuto ochranu lze aplikovat s minimální investicí a provoz je ekonomicky nenáročný. Pro připojení k síti musí připojované zařízení podporovat protokol 802.1X

3.6 Zvýšení složitosti hesla

Zvýšením složitosti hesla snížíme riziko jeho prolomení. K prolomení může dojít formou sledování uživatele při přihlašování. Současně existují programy a viry, které využívají slovník hesel a ve velké rychlosti zkoušejí zadávat jednotlivá hesla. Politika hesel je stanovena na minimální délku hesla, délku životnosti hesla a kombinaci velkých a malých písmen, číslic a speciálního znaku. Doporučení je zvýšení délky hesla na 12 znaků, nutnost zadat kombinaci velkých, malých a speciálních znaků. Současně doporučuje auditorský tým snížení životnosti hesla na čtyři měsíce. Přes náročnost hesla je nutné heslo chránit před zcizením nebo vyzrazením.

3.7 Kombinace více možností zabezpečení

Kombinací více uvedených možností se bezpečnost zvyšuje. Příkladem je kombinace ověření uživatele, monitoring sítě a dohled vedoucích pracovníků jednotlivých výrobních úseků.

3.8 Závěr

Auditorský tým provádějící bezpečnostní audit IT infrastruktury shrnul a popsal možnosti zvýšení bezpečnosti sítě. Společnost WAXEN s.r.o. zvážila všechny možnosti a na základě výsledku auditu se rozhodla zavést některá z doporučovaných možností zabezpečení. Jako první opatření zvolila zvýšení složitosti hesla a zkrácení jeho životnosti. Dále se rozhodla zadat poptávku na dodávku profesionálního monitorovacího systému. Poslední zvolené

opatření je nasazení zabezpečení pomocí ověření uživatelů pro přístup k síti. Zabezpečení bude v prvním kroku realizováno formou testovacího prostředí.

II. PRAKTICKÁ ČÁST

4 INFRASTRUKTURA SPOLEČNOSTI

Společnost WAXEN s.r.o. působí ve strojírenském průmyslu a zabývá se výrobou strojů pro logistiku. Pro svůj provoz potřebuje odpovídající prostor. V jednom z areálů je realizovaná hrubá výroba jednotlivých komponentů produktů, v druhém se provádí samotná kompletace finálních výrobků. V rámci celé organizace je nasazený výrobní program, který je prostřednictvím terminálů dostupný ve všech částech společnosti. Areály jsou propojeny optickým spojem o rychlosti 1 Gbps. Zmíněný spoj zajišťuje přístup k výrobnímu SW, sdíleným datům a Internetu v obou areálech.

4.1 Areál 1

Areál 1 je hlavní část společnosti. V tomto areálu je kompletační výrobní budova, sklady, expedice, řízení výroby, kancelářská budova a hlavní serverovna.

4.1.1 Serverovna

Jedná se o malou místnost s hlavní částí infrastruktury společnosti, která se nachází v budově výroby. V rozvaděči je centrální switch, firewall, brána do Internetu a servery s instalovanými Windows servery. Servery jsou celkem čtyři, ale pro potřebu zabezpečení budou nutné jen dva. Hlavní server s instalovanou službou Active Directory, který bude sloužit jako databáze uživatelů, a RADIUS server v roli sprostředkovatele ověření. Zbylé dva servery plní v síti jinou úlohu a pro realizaci popisovaného zabezpečení nejsou důležité.

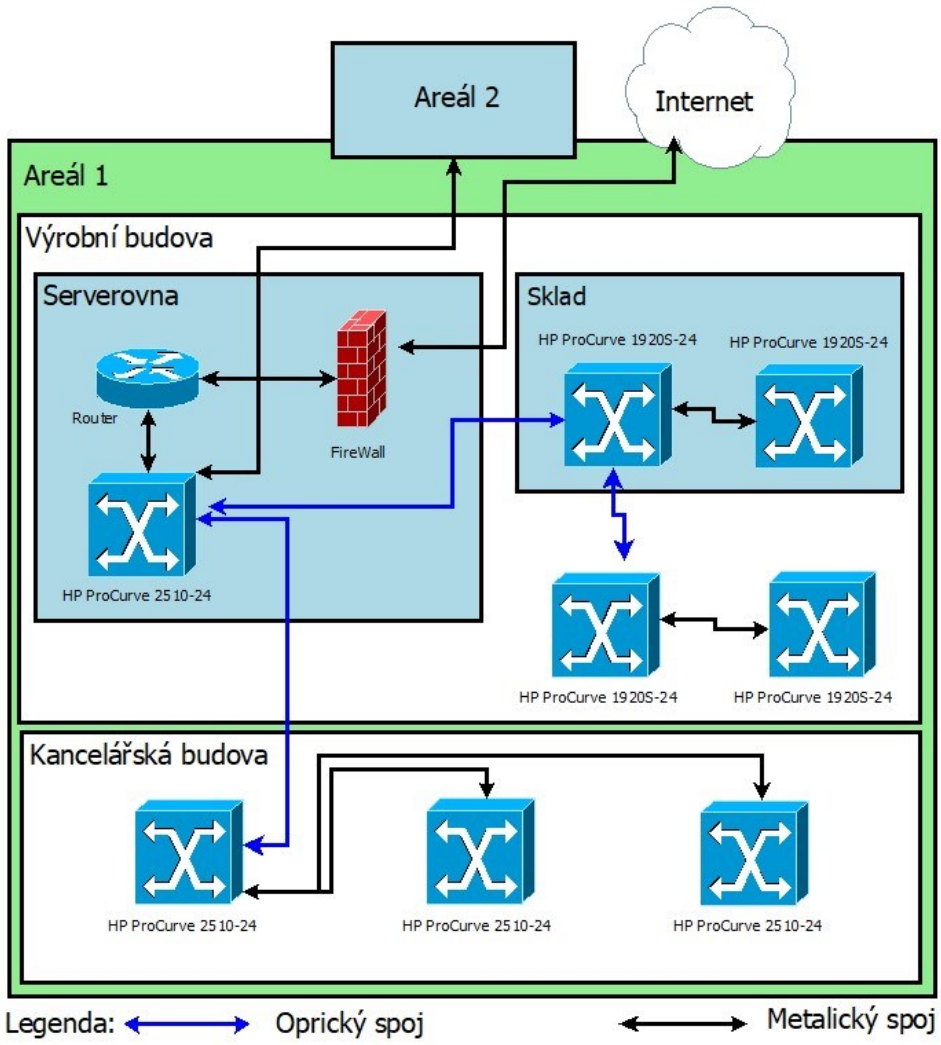
4.1.2 Výroba, sklady

Výroba je nejrozlehlejší z budov společnosti. Pro pokrytí všech míst výroby jsou potřebné dva propojené rozvaděče. Oba obsahují dva 24 portové switche HPE ProCurve 1920s. Vzájemný spoj mezi rozvaděči je realizován optickým spojem.

4.1.3 Kancelářská budova

Kancelářská budova je dvoupodlažní budovou s jednou rozvodnou se třemi switchi HP ProCurve 2510. Celkem je v hlavní budově 15 kanceláří, z toho jsou dvě větší kanceláře s deseti pracovními místy.

4.1.4 Infrastruktura areálu 1



Obrázek 2 IT infrastruktura areálu 1 [Vlastní zdroj].

4.2 Areál 2

Nachází se dva kilometry od hlavního areálu 1. Spojení mezi Areálem 1 a Areálem 2 je provedeno opět optickým spojem. Areál 2 má tři budovy a pouze tři switche. Jeden switch HP ProCurve 2510 a dva HP ProCurve 1920s. Hlavní switch je zde HP ProCurve 2510.

4.2.1 Budova A

Jedná se o hlavní budovu, která je propojena s Areálem 1. Spoj s budovou B a C je realizován prostřednictvím metalického spoje. V budově je instalován laser pro pálení plechů, ohraňovací stroj, stolní vrtačky a nachází se zde i sklad materiálu pro laser. Obsluha laseru má k dispozici malou kancelář pro čtyři pracovníky. Každý stroj má dostupný výrobní terminál, celkem čtyři. Pomocí terminálu zaznamenává obsluha do výrobního systému informace o provedených činnostech.

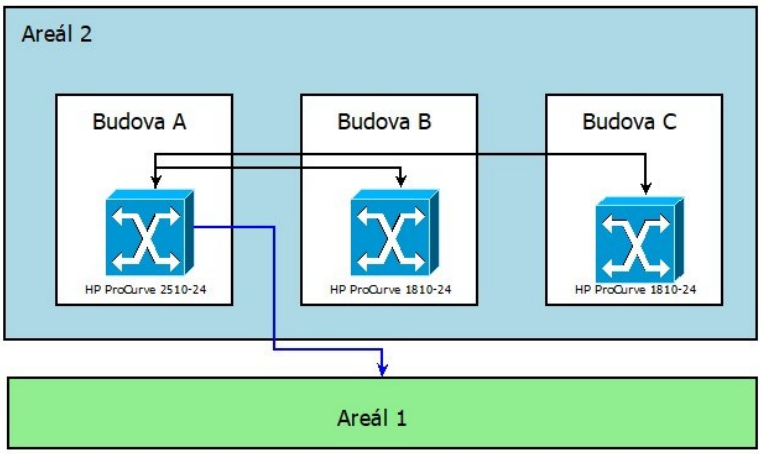
4.2.2 Budova B

Svařovna. Zde se svařují velké konstrukce z připraveného materiálu. Pracovníci mají čtyři terminály, které jsou nutné pro záznam výkonu jejich práce. V budově jsou další přípojná místa jako rezerva pro budoucí použití.

4.2.3 Budova C

Zde se nachází tři pilky, sklad hutního materiálu a kancelář pro mistra a technologii. Pro obsluhu pilek jsou instalovány dva terminály.

4.2.4 Infrastruktura Areálu 2



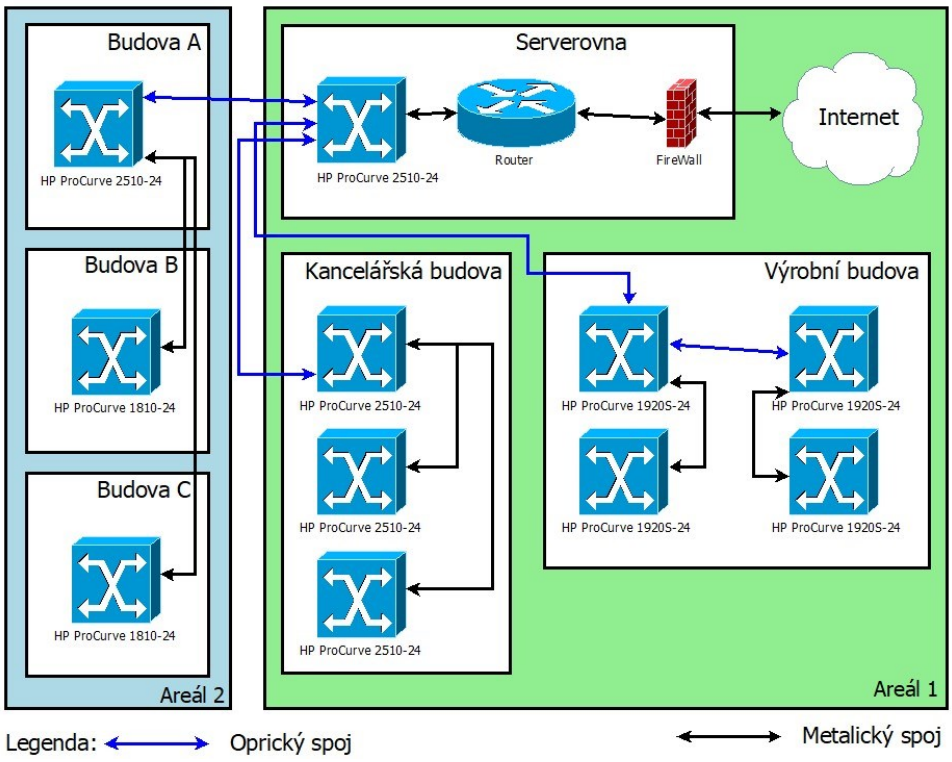
Obrázek 3 IT infrastruktura areálu 2 [Vlastní zdroj].

4.3 IT infrastruktura společnosti

V síti jsou tři druhy síťových switchů. Jedná se o HP ProCurve 2510 , HP ProCurve 1810 a HPE ProCurve 1920s. První dva jmenované jsou nevhodné pro aplikaci zabezpečení, nepodporují protokol IEEE 802.1X. Tyto switche je nutné před samotnou realizací nahradit novějším modelem HPE 1920s.

Tabulka 2 Inventář aktuálních síťových switchů [Vlastní zdroj].

Areál 1	Počet portů	Budova
HP ProCurve 2510	24	Serverovna
HP ProCurve 2510	24	Kancelářská budova
HP ProCurve 2510	24	Kancelářská budova
HP ProCurve 2510	24	Kancelářská budova
HPE ProCurve 1920s	24	Budova Výroby
HPE ProCurve 1920s	24	Budova Výroby
HPE ProCurve 1920s	24	Budova Výroby
HPE ProCurve 1920s	24	Budova Výroby
Areál 2		
HP ProCurver 2510	24	Budova A
HP ProCurve 1810	24	Budova B
HP ProCurve 1810	24	Budova C



Obrázek 4 Rozložení jednotlivých síťových prvků ve společnosti [Vlastní zdroj].

4.4 Závěr

Uvedená infrastruktura společnosti popisuje dva areály a jejich účel, rozložení jednotlivých částí sítě, popis a propojení jednotlivých switchů. Popis nevychází z reálného prostředí a byl vytvořen jen pro účel této práce.

5 REALIZACE TESTOVACÍHO PROSTŘEDÍ

Před samotnou realizací je vhodné postavit testovací prostředí a vše před nasazením otestovat. V rámci přípravy je vyčleněn jeden fyzický server s instalovaným virtualizačním systémem HYPER-V. V něm jsou instalovány a spuštěny dva virtuální servery. Jeden se službou Active Directory, DHCP a DNS, druhý s instalovanou rolí Certifikační autority a Network Policy and Access Server (Dále jen NPAS), která obsahuje server RADIUS.

Tabulka 3 Popis použitých serverů pro testovací prostředí [Vlastní zdroj].

Název Serveru	**Systém/IP adresa**	**Spuštěné služby**
Hyper-V	Windows server 2019 IP adresa 192.168.200.100	Virtualizační systém Hyper-V
WAXEN-PDC	Windows server 2019 IP adresa 192.168.200.181	AD DS, DHCP server, DNS server
WAXEN-RADIUS	Windows server 2019 IP adresa 192.168.200.182	AD CS, NPAS

5.1 Konfigurace serveru WAXEN-PDC

Po instalaci základního systému musí být provedena prvotní konfigurace. Jako první krok je změna názvu serveru na WAXEN-PDC. Po změně bude nutné server restartovat. Druhým krokem je změna IP adresy serveru na 192.168.200.181. Nyní můžou být instalovány jednotlivé role serveru.

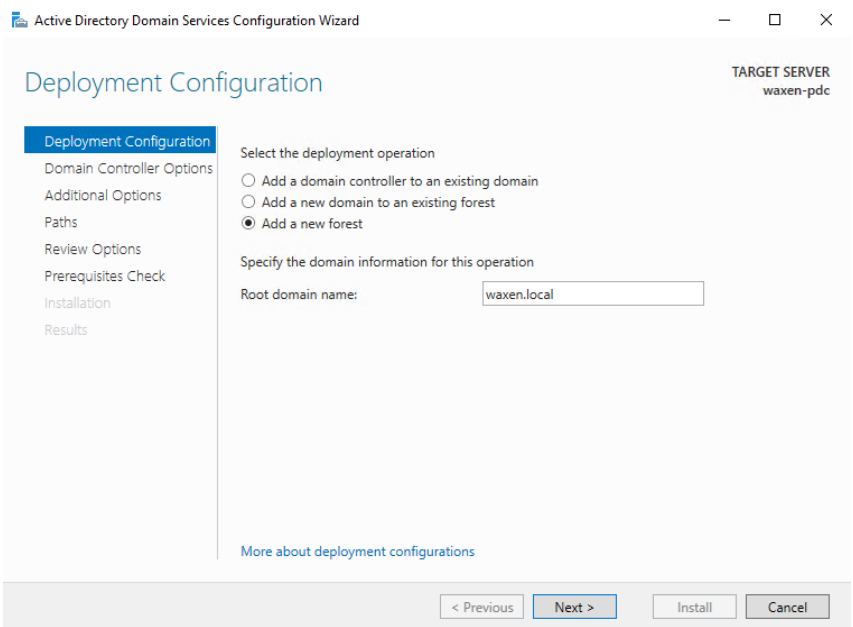
5.1.1 Instalace Active Directory

Součástí systému je program „Server Manager“, který je automaticky spuštěn po přihlášení k serveru. Na úvodní obrazovce jsou základní konfigurační možnosti a zobrazení stavu jednotlivých rolí a serverů. Tlačítko „Add roles and Features” spouští průvodce přidáním nových rolí serveru. Průvodce obsahuje několik kroků.

1. Zobrazení základní informace o průvodci
2. Typ instalace – „Role-based or feature-based installation”. Instalace rolí nebo funkcí serveru.

3. Výběr cílového serveru, na kterém bude instalace provedena. V tomto případě bude dostupný pouze jeden server WAXEN-PDC.
4. Výběr instalovaných rolí – pří výběru níže uvedených rolí bude zobrazen dialog s funkcemi, které jednotlivé role vyžadují:
    a. Active Directory Domain Services
    b. DNS Server
    c. DHCP Server
5. V dalších krocích není nutné nic měnit, tlačítkem „Install" na konci průvodce bude spuštěna instalace vybraných rolí.

Po spuštění může být průvodce ukončený, instalace bude probíhat na pozadí. O dokončené základní instalaci informuje žlutý vykřičník u notifikační ikonky praporku v aplikaci „Server Management". Po rozkliknutí notifikací a kliknutí na odkaz „Promote this server to a domain controller" bude spuštěna konfigurace Active Directory. Současně bude dokončena konfigurace DNS.



Obrázek 5 Úvodní konfigurace Active Directory [Vlastní zdroj].

Konfigurace je složena z postupných kroků. Uvedené hodnoty níže jsou individuální, v ostatních krocích zůstávají výchozí hodnoty nastavení.

1. Deployment Configuration:
    a. Výběr „Add" a „new forest".

b. Root domain name: waxen.local.

2. Domain Controller Options:

a. Heslo pro obnovu služby v případě její havárie.

Tlačítkem „Install“ bude spuštěn proces dokončení instalace, na jejímž konci bude server restartován.

Po dokončení instalace Active Directory a restartu serveru následuje vytvoření uživatele. Pro administraci uživatelských účtů slouží konzole „Active Directory Users and Computers“, která je dostupná v „Server manager“ v menu „Tools“. Pomocí konzole je třeba vytvořit bezpečnostní skupinu názvem „gInternalEmployees“ a uživatele Test. Uživatel Test bude členem této skupiny.

5.1.2 DHCP

Pro vyvolání dodatečné konfigurace DHCP serveru slouží odkaz „Complete DHCP configuration” v notifikační liště aplikace „Server Manager“. Konfigurace jen autorizuje DHCP server ve službě Active Directory, po dokončení je server připravený. Aby plnil svou funkci musí být vytvořen rozsah přidělovaných IP adres. Pro jeho administraci je k dispozici konzole DHCP dostupná z menu „Tools“. Konzole obsahuje dvě části. V levé části je stromová struktura serveru a v pravé části jsou doplňující informace. Průvodce přidáním nového rozsahu „New Scope“ je dostupný pravým tlačítkem myši nad položkou „IPv4“. Tabulka (Tab. 4) obsahuje hodnoty zadané v průvodci.

Tabulka 4 Nastavení rozsahu DHCP serveru [Vlastní zdroj].

Popis	**Hodnota**
Name	VLAN 10
Rozsah IP adres	192.168.200.10 – 192.168.200.160
Maska sítě	255.255.255.0
Výchozí brána	192.168.200.181
Životnost zapůjčení IP adresy	8 dní
Server DNS	192.168.200.181
Název domény	waxen.local

5.2 Konfigurace serveru WAXEN-RADIUS

Konfigurace serveru RADIUS je již pro účel zabezpečení klíčová a specifická. Po instalaci serveru je nutné změnit nastavení sítě. IP adresa je pro tento server 192.168.200.182. Následně je server nutné připojit do domény waxen.local. Pro připojení serveru k doméně slouží průvodce dostupný pod odkazem „workgroup" v aplikaci Server Manager a podnabídce Local Server.

Prvním krokem v konfiguraci je specifikovat síťové switche, které budou přistupovat k RADIUS serveru a tím budou mít povoleno žádat o autentifikaci připojených zařízení. V případě, že bude žádat o autentizaci switch, který nebude na serveru uvedený jako klient, bude žádost ze strany serveru RADIUS odmítnuta. Pro testovací účel bude dostačující přidání pouze jednoho switche, nazvaného SW Production. V druhém kroku bude popsáno nastavení síťových zásad Network Policies. Nastavení Network Policies je složitější a bude doplněno obrázky s nastavením. Ke konfiguraci RADIUS serveru slouží konzole Network Policy Server, která je dostupná v aplikaci pro správu serveru Server Manager.

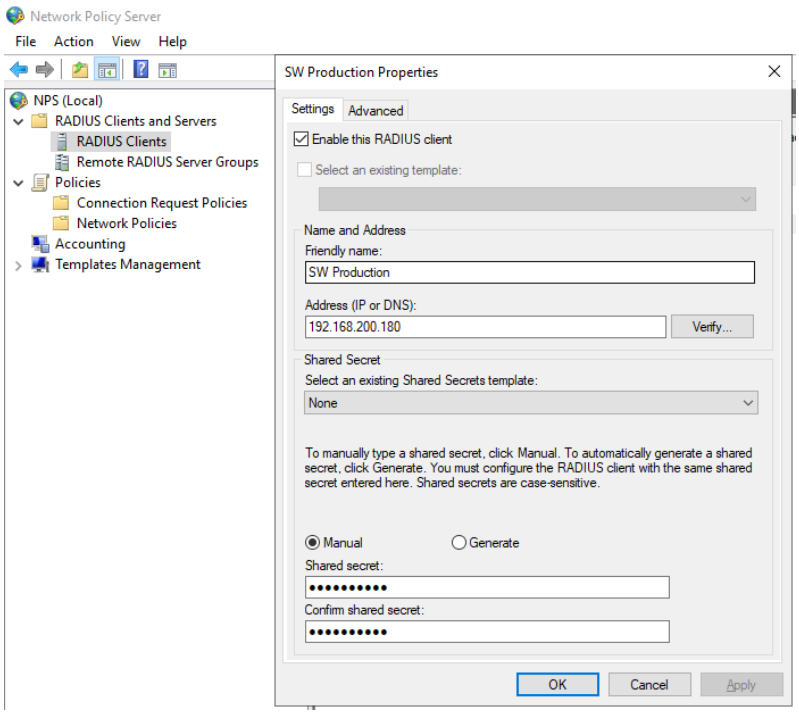
5.2.1 Přidání klienta, switche

Před samotnou konfigurací je nezbytné instalovat roli „Network Policy and Access Server". Postup přidání role je obdobný jako při přidání rolí v předchozí kapitole. Po instalaci role bude v menu Tools v Server Manageru dostupná konzole pro konfiguraci s názvem „Network Policy Server". Základní okno konzole je rozdělené na dvě části. V levé části jsou stromově rozdělené jednotlivé části konfigurace a monitoringu, v pravé části jsou náhledy

jednotlivých částí. Výchozí obrazovkou je „Getting Started" s možností spuštění průvodce konfigurace.

Pro přidání nového switche jako klienta slouží položka „RADIUS Clients" v levé části. Po kliknutí na tuto položku je dostupná možnost „New" v nabídce „Action" v horní části okna. Současně je možnost přidání nového switche pomocí kontextové nabídky vyvolané kliknutím pravého tlačítka myši nad položkou „RADIUS Clients". Po kliknutí na volbu „New" dojde k vyvolání dialogového okna pro přidání klienta. Pro přidání switche jsou důležité položky označené jako Friendly name, Address (IP or DNS) a Shared secret.

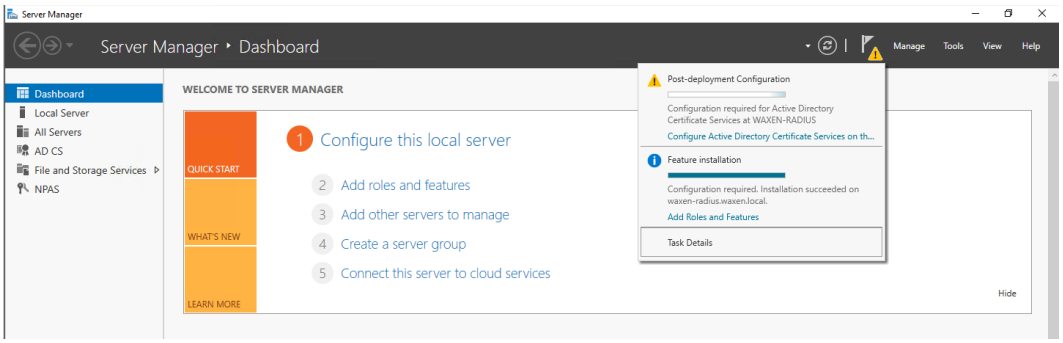
- Friendly name – Obsahuje jméno switche. Pro testovací prostředí byl zvolen název switche SW Production. Volba jména je čistě na administrátorovi, který konfiguruje RADIUS. Název by měl mít vypovídající hodnotu, aby bylo z jeho názvu zřejmé, o jaký switch jde. V případě společnosti WAXEN s.r.o. jde celkem o jedenáct switchů, které je dobré rozlišit.
- Address (IP or DNS) – IP adresa switche. Pokud je vložen DNS záznam pro přidávaný switch, je možné použít jeho jméno. Tlačítko „Verify" slouží k ověření DNS jména.
- Shared secret – Sdílený klíč je textový řetězec pro šifrování přenosu. Stejný klíč bude nastaven i na straně switche.



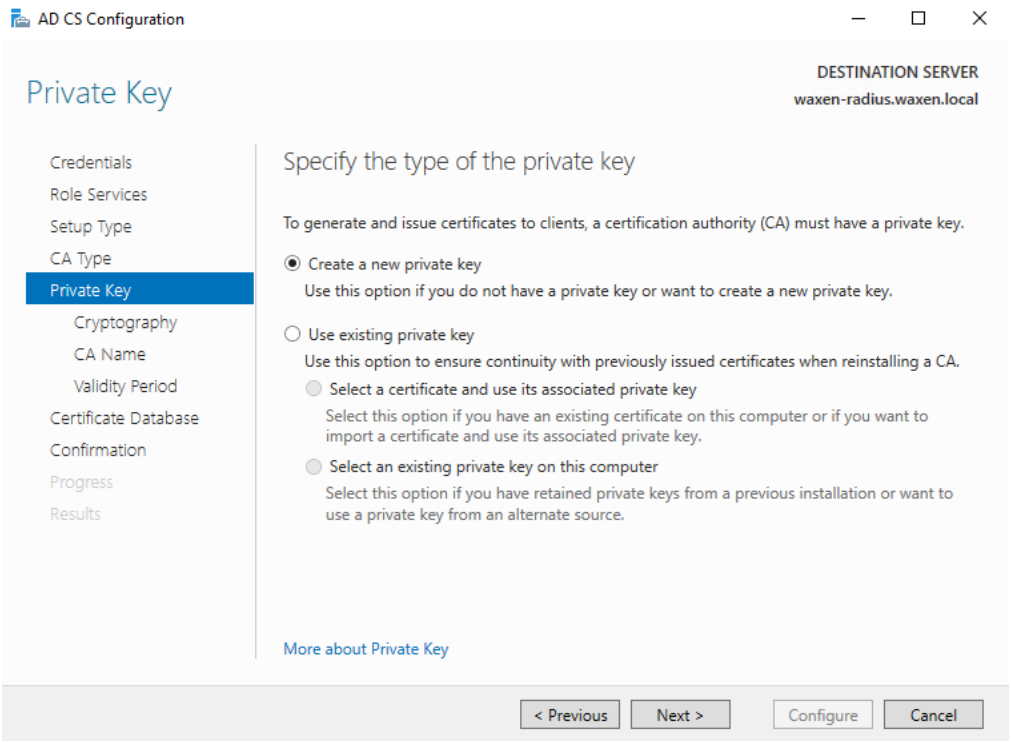
Obrázek 6 Nastavení klienta pro ověřování [Vlastní zdroj].

5.2.2 Certifikační autorita

Pro správnou funkci ověření musí mít server platný certifikát. V testovacím prostředí pro náš účel poslouží nekomerční certifikát vydaný a podepsaný instalovanou certifikační autoritou, označovaný jako self-signed certificate. K vytvoření tohoto certifikátu je nutné nainstalovat a spustit roli serveru AC CS. Aby mohla certifikační autorita vydávat certifikáty klientům, potřebuje privátní klíč. Klíč bude vygenerován v průběhu post-instalační konfiguraci služby. Konfigurace služby bude spuštěna po kliknutí na odkaz „Configure Active Directory Certificate Services on the destination server“ v notifikační liště. Obrázek (Obr. 7) zobrazuje odkaz pro post-instalační konfiguraci služby AC CS v notifikační části aplikace Server Manager.



Obrázek 7 Notifikace aplikace Server Manager [Vlastní zdroj].



Obrázek 8 Konfigurace certifikační autority, privátního klíče [Vlastní zdroj].

V dalším kroku generování primárního klíče je možnost specifikovat algoritmus, délku klíče a délku jeho platnosti. Všechny nabízené hodnoty lze ponechat ve výchozím stavu. Certifikační autorita ověřuje platnost certifikátů a všech informací v nich uvedených. V produkčním nasazení je doporučeno využití některé z komerčních společností, které vydávají ověřené certifikáty, a použít hvězdičkový Wildcard certifikát.

5.2.3 Nastavení Network Policies

Na základní obrazovce konzole Network Policy Server je zobrazeno rozbalovací menu s výběrem možnosti konfigurace. Při výběru volby „RADIUS server for 802.1X Wireless or Wired Connection" z rozbalovacího menu se změní tlačítko pro konfiguraci na „Configure 802.1X". Kliknutím na toto tlačítko bude spuštěn průvodce konfigurace o několika krocích. První okno konfigurace slouží pro výběr typu připojení a zvolení názvu tohoto nastavení. Pro popisovaný způsob zabezpečení je to volba „Secure Wired (Ethernet) Connections" a jako název síťové politiky byl zvolen VLAN10 – Internal.

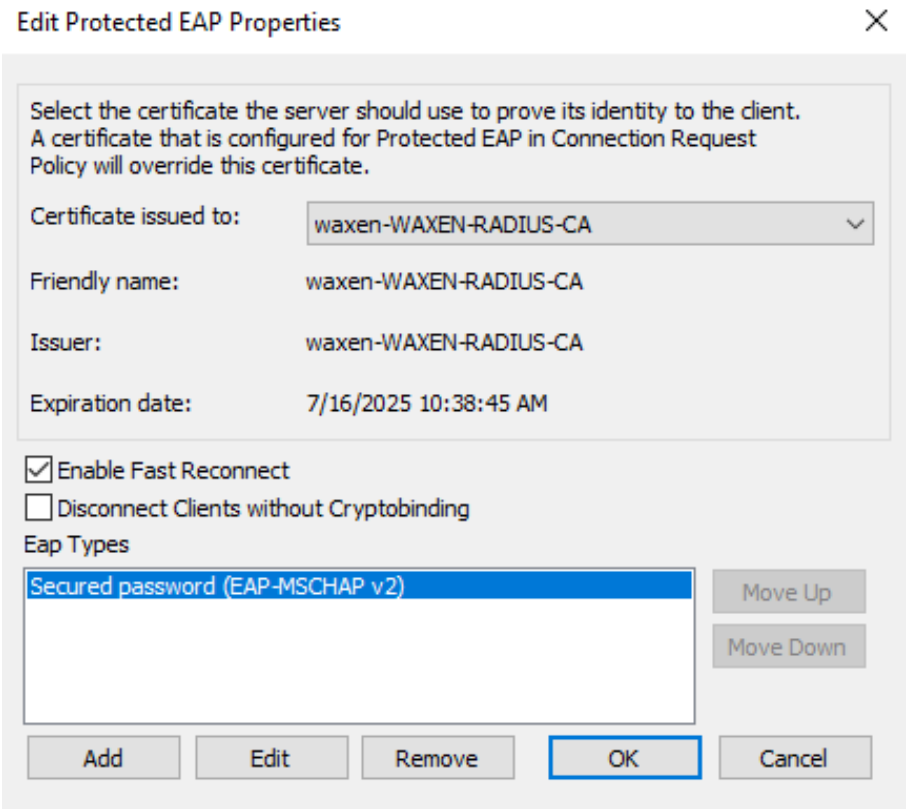
Další krok definuje seznam klientů, switchů, které můžou žádat o autentifikaci pro vytvářenou síťovou politiku. Tlačítko „Add" slouží pro přidání switche do seznamu klientů, vybrán je jediný switch, který byl v předchozím kroku přidán do seznamu RADIUS klientů. V testovacím prostředí je pouze jeden, ale v produkčním prostředí jich bude více a budou

přidány všechny, u kterých budeme vyžadovat ověření. Po kliknutí na tlačítko „Next" pokračuje průvodce dalším krokem, výběrem autentifikační metody.

Autentifikační metody ověření jsou tři:

1. Ověření pomocí Microsoft Smart karty nebo jiného certifikátu.
2. Microsoft Protected EAP (PEAP).
3. Microsoft Secure password (EAP-MSCHAP v2).

Vzhledem k možnosti ověřování pomocí jména a hesla by mohla svádět k výběru volba třetí, ale není to správně. Pro popisované zabezpečení je správná druhá volba, a sice „Microsoft Protected EAP (PEAP)". V následné konfiguraci této metody tlačítkem „Configure", je jako výchozí hodnota EAP typu zvolena možnost „Secured password (EAP-MSCHAP v2)". Právě tento EAP typ zajistí ověření jménem a heslem uživatele. V horní části konfigurace je výběr certifikátu, který bude použit k prokázání identity serveru. V testovacím prostředí je pouze jeden a je nastaven jako výchozí. Ve spodní části okna je pod tlačítkem „edit" možnost nastavit počet pokusů o autentifikaci.



Obrázek 9 Konfigurace Microsoft Protected EAP(PEAP) [Vlastní zdroj].

Následující krok konfigurace slouží k nastavení bezpečnostní skupiny. Účet uživatele může být zařazen do více bezpečnostních skupin. Tlačítkem „Add" může být přidána bezpečnostní skupina, která bude akceptována pro ověření. Pro testovací prostředí je vložena skupina gInternalEmployees, která byla vytvořena při konfiguraci služby Active Directory. Výběrem skupiny gInternalEmployees je zajištěno připojení a ověření pouze uživatelů z uvedené skupiny. Je to způsob, jak jednoduchým způsobem určovat, který uživatel se může připojit k síti. Například uživatelé využívající výrobní terminály mají také účty v Active Directory, ale připojení k síti nepotřebují. Uživatelé bez členství ve skupině gInternalEmployees se tedy k síti se nepřipojí.

V dalším kroku se nachází „Traffic control configuration", jedná se o konfiguraci RADIUS atributů. Atributy jsou po ověření předány klientovi ověření, v tomto případě obdrží informace switch, který o ověření požádal RADIUS server. Níže jsou uvedeny tři atributy, které jsou důležité pro správnou funkčnost ověření. Výběrem názvu atributu a kliknutím na tlačítko „edit" je umožněno nastavení hodnoty atributu. Tlačítko „Add", v nově zobrazeném dialogu konfigurace vybraného atributu, pak umožňuje výběr správné hodnoty.

Nastavení správných hodnot atributů:

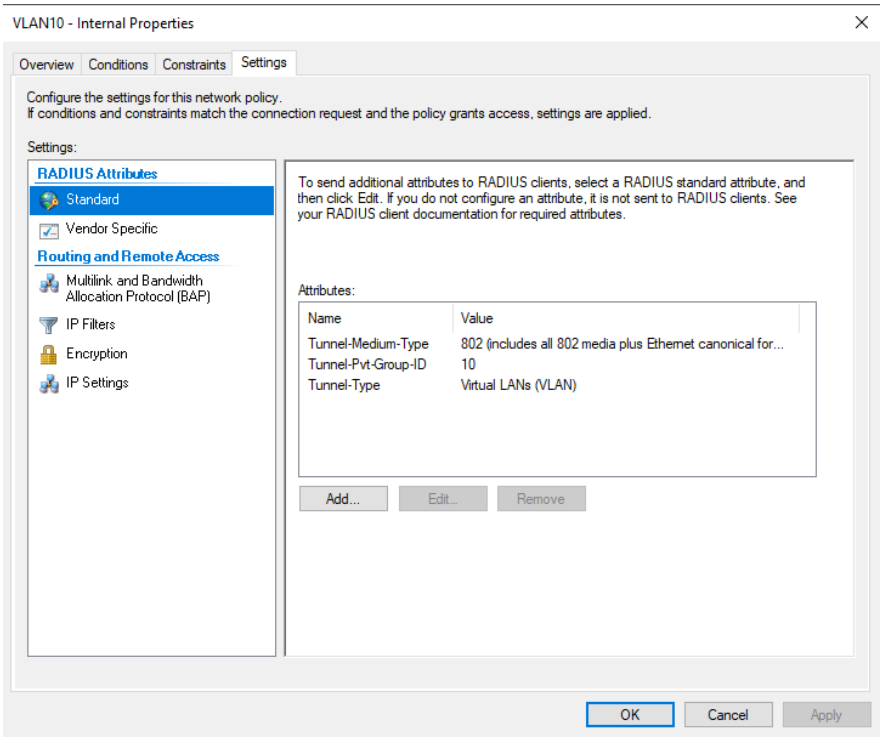
- tunel-Type: Virtual LANs (VLAN),
- tunel-Medium-Type: 802 (Includes all 802 media plus Ethernet canonical format),
- tunel-Pvt-Group-ID: 10.

Za zmínku stojí hodnota atributu Tunel-Pvt-Group-ID. Jedná se o číslo VLAN sítě, do které bude uživatel přidán po úspěšném ověření. Tímto krokem je nastavení síťových zásad u konce. V následujícím okně průvodce je ještě možné zobrazit detailní konfiguraci. Tlačítko „finish" ukončí průvodce a uloží nastavení.

Informace zadané v průběhu konfigurace nejsou jediné, které jsou ve výsledném nastavení. Do výsledného nastavení jsou doplněny některé výchozí hodnoty automaticky. Konkrétně v nastavení RADIUS atributů přibyly dva atributy, Framed-Protokol a Service-Type. Tyto dva atributy je potřeba odstranit, protože switch HP 1920s je nepodporuje. V případě, že hodnoty nebudou odstraněny, dojde sice k úspěšnému ověření, ale port bude i tak zakázán. V logu switche pak bude informace o nepodporovaném atributu. V levé části Network policy serveru jsou pod položkou „Network Policies" zobrazené všechny profily. Právě vytvořený profil VLAN10 – Internal by měl být na prvním místě s hodnotou 1 ve sloupci Processing

Order. Kliknutím na profil bude otevřen dialog s konfigurací. Na záložce Settings je nastavení RADIUS atributů s možností odstranit nepodporované atributy.

Nyní je konfigurace RADIUS serveru kompletní.



Obrázek 10 Nastavení Network Policy a RADIUS atributů [Vlastní zdroj].

5.3 Nastavení switche

Následující kapitola popisuje nastavení switche. Co vše je nezbytné nastavit a popis jednotlivých kroků. Ve výchozím stavu zná switch jen jednu výchozí VLAN síť označenou číslem ID 1, takzvaně tagem. Všechny porty switche jsou zařazeny do této VLAN sítě. Jedná se o netagovanou VLAN, tedy jednotlivé rámce neobsahují VLAN ID. V prvním kroku je nutné přidat novou VLAN s ID 10. Do této VLAN přiřadit porty pro připojení serverů a také zvolit tuto VLAN jako administrační. Tím bude zajištěno, že k administraci switche se dostane jen ověřený uživatel a současně bude pro switch dostupný RADIUS server pro ověření. Následně bude popsána konfigurace jednotlivých portů. Každý port může plnit funkci ověření, nebo být již ověřen. V síti existují zařízení, které protokol IEEE 802.1X nepodporují. Například starší tiskárny nebo Laser pro řezání ocelových plechů ve výrobní hale. Pro tento případ lze port přepnout do režimu „Force Authorized", tedy trvale autorizován a nebude vyžadováno zadání jména a hesla.

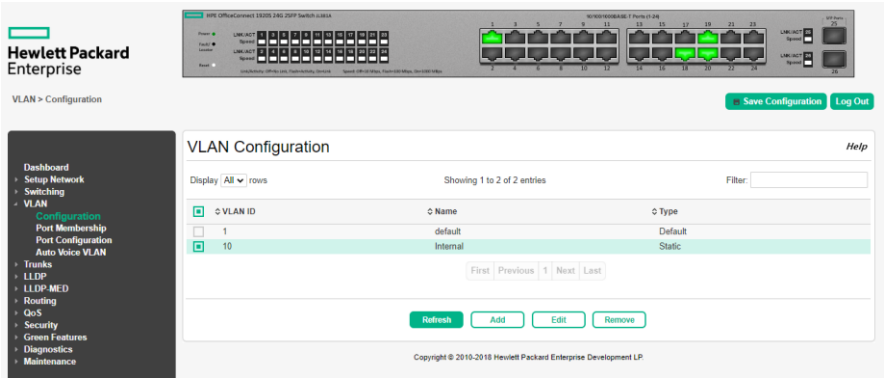
5.3.1 Nastavení IP adresy switche

Ve výchozím nastavení má switch HP 1920s IP adresu 192.168.1.1. Ta musí být změněna na 192.168.200.180. Po prvním přihlášení do Administrace switche přes webové rozhraní je zobrazena úvodní stránka s úvodními informacemi. Jako první lze nastavit název switche a jeho umístnění. V levé části je menu s nastavením. Po kliknutí na položku „Setup Networking“ se zobrazí další podnabídky a současně v pravé části nastavení IP adresy. Ve spodní části je pak možnost vybrat administrační síť VLAN v poli označeném jako Management VLAN ID. Po nastavení nové IP adresy je nutné konfiguraci potvrdit tlačítkem „Apply” ve spodní části stránky. Zde je třeba upozornit na uložení konfigurace. Tlačítkem „Apply” potvrdíme nastavení, ale současně je nutné konfiguraci uložit tlačítkem „Save Configuration” v pravé horní části. V případě, že není konfigurace uložena a dojde k restartu switche, bude obnovena poslední uložená konfigurace. Tohoto chování lze využít při samotné konfiguraci. Při špatném nastavení administrační VLAN sítě dojde ke ztrátě komunikace a nemožnosti nastavení opravit, restartem switche se tak lze vrátit zpět do poslední uložené konfigurace. Po správném nastavení se konfigurace uloží a pokračuje se dalším nastavením [20].

5.3.2 Nastavení VLAN

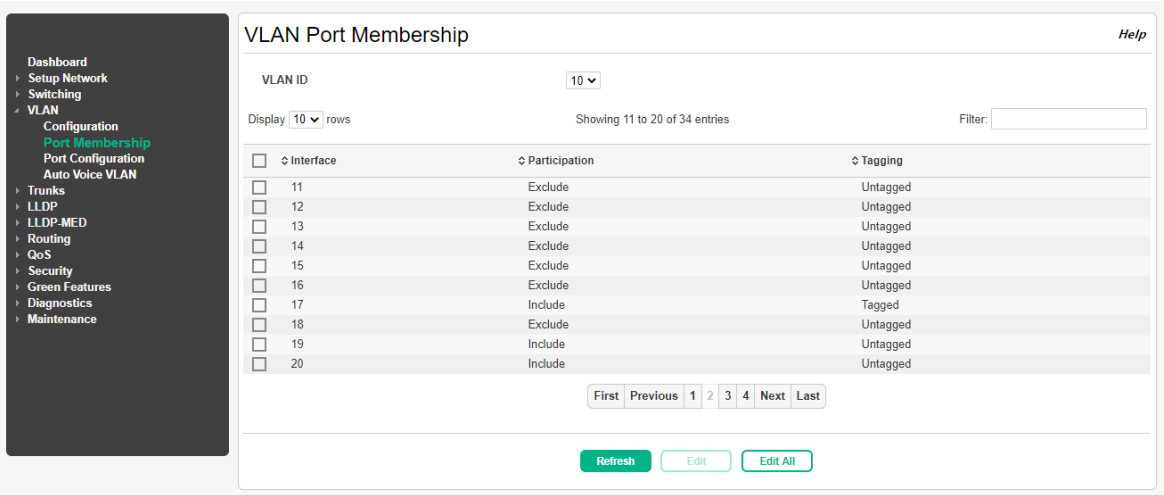
Nastavení a přidělení portů do správné VLAN se provádí v menu VLAN. Menu obsahuje několik podnabídek [20].

Nabídka Configuration slouží pro přidání a nastavení samotných VLAN sítí. Tlačítko „Add” slouží k přidání požadované sítě. Po kliknutí na „Add” se zobrazí dialogové okno pro zadání ID sítě. Následně lze u přidané sítě změnit její název tlačítkem „Edit“ [20].



Obrázek 11 ukázka nastavení VLAN sítě [Vlastní zdroj].

Nabídka „Port Membership" na obrázku (Obr. 12) obsahuje tabulku všech portů switche. V horní části nad tabulkou se nachází rozbalovací menu s výběrem VLAN sítě. Ve třech sloupcích je postupně zobraceno číslo portu, vztah k vybrané síti a v posledním sloupci je stav tagu. Sloupec „Participation" může nabývat dvou hodnot, „Include" nebo „Exclude". „Include" znamená, že je port členem vybrané VLAN sítě, „Exclude" naopak říká, že do této sítě nepatří. V posledním sloupci „Tagging" je pak informace, zda je port tagovaný nebo není. Na obrázku číslo 10 je zobrazeno nastavení sítě VLAN s Id 10. Z nastavení na obrázku (Obr. 12) lze vyčíst, že port číslo 17 je členem této sítě a je tagovaný. Porty 19 a 20 jsou také členy této sítě, ale jsou netagované. Ostatní porty členy nejsou [20].



Obrázek 12 Ukázka nastavení VLAN ID 10 [Vlastní zdroj].

Pro účel testování je port číslo 20 určen pro připojení fyzického serveru s instalovanými virtuálními servery waxen-pdc.waxen.local a waxen-radius.waxen.local. Jelikož jsou servery virtuální, sdílejí jeden fyzický port. VLAN síť s ID 10 je interní síť určená pro ověřené uživatele. Servery jsou tedy připojeny do této sítě přímo, bez ověření. Port číslo 19 je pro účel testování přidělený také do této interní sítě.

V nabídce „Port Configuration" lze zobrazit aktuální náhled nastavení jednotlivých portů. Lze tak získat rychlý náhled do jakých sítí jednotlivé porty patří. Součástí je možnost dalšího nastavení, které ale není pro účel této práce důležité. Lze ho ponechat ve výchozím stavu.

Po správném nastavení VLAN a přidělení portů 19 a 20 se lze vrátit zpět do nastavení sítě v menu „Setup Network", podnabídky „Get Connected" a přepnout v části Management VLAN, v položce Management VLAN ID, na nově vytvořenou síť s ID 10. Po přepnutí bude administrační prostředí switche dostupné jen z portů 19 a 20. Po dokončení konfigurace pak bude po ověření dostupná administrace switche i z ostatních portů [20].

5.3.3 Nastavení RADIUS serveru

Ještě před samotnou konfigurací zabezpečení portů, je nutné přidat RADIUS server. Pro konfiguraci zabezpečení portů a nastavení RADIUS serveru slouží nabídka „Security". K nastavení serveru RADIUS slouží stejně pojmenovaná podnabídka. Ve spodní části stránky je tlačítko „Add" pro přidání nového RADIUS serveru. V zobrazovaném dialogovém okně je nutné vyplnit následující údaje [20]:

- sever name – název serveru se rolí RADIUS, v testovacím prostředí se jedná o název WAXEN-RADIUS-Server,
- IP Address – 192.168.200.182 – IP adresa RADIUS serveru,
- secret – Jedná se o „Shared secret", tedy sdílený klíč zadaný při konfiguraci RADIUS klienta v kapitole 5.2.1.

Ostatní hodnoty zůstávají výchozí. Po přidání RADIUS serveru je dále nutné zapnout ověřovací mód „802.1X Authentication mode" přepnutím na „Enable" a přidat „NAS-IP Address" jako IP adresu RADIUS serveru [20].

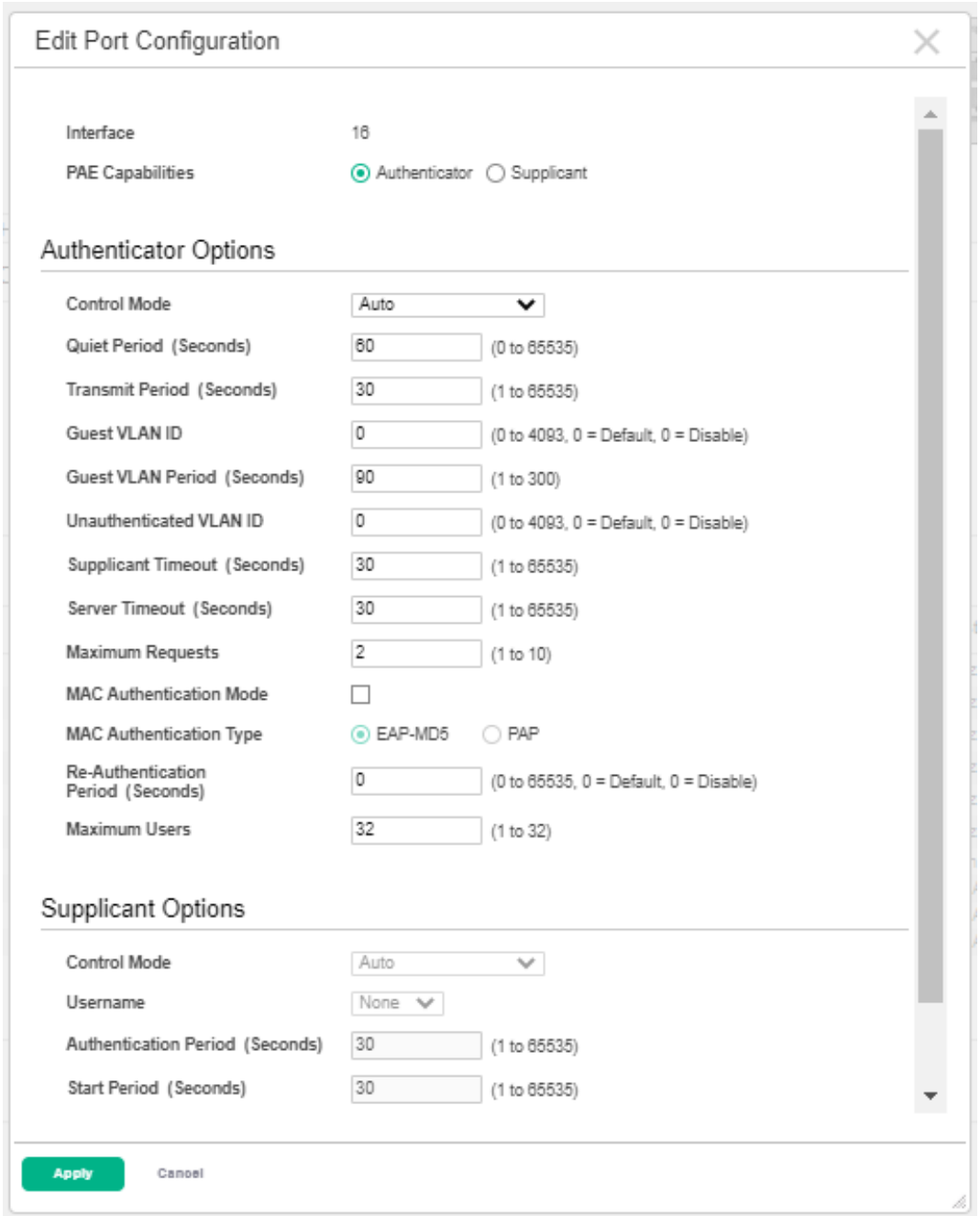
5.3.4 Nastavení zabezpečení portů

Podnabídka „Port Access Control" obsahuje konfiguraci samotných portů. V prvním kroku je třeba popsat důležité nastavení potřebné pro popisované zabezpečení [20].

- Admin Mode – volba zapíná a vypíná 802.1X mód switche.
- VLAN Assignment mode – pokud je volba povolena, přiřadí ověřené zařízení do VLAN sítě obdržené ze serveru RADIUS.
- Dynamic VLAN Creation Mode – zapíná možnost automatického vytváření VLAN. V případě testovacího switche byla vytvořena VLAN s ID 10 ručně. Pokud je volba povolená a switch obdrží po autentifikaci uživatele ID sítě, která neexistuje, switch tuto síť automaticky vytvoří. V případě realizace popisovaného zabezpečení nebude zmíněná funkce využita [20].

Pod tímto základním nastavením je tabulka pro nastavení jednotlivých portů. Pro administraci je nutné konfigurovat každý port zvlášť. Výhodou je výchozí nastavení, které s tímto typem zabezpečení počítá, není tedy třeba nic měnit. Po označení portu a kliknutím na tlačítko edit se zobrazí dialogové okno s konfigurací. Každý port má dva režimy [20].

- Authenticator – Port vynucuje ověření a zaslané informace předává RADIUS serveru. V případě kladného ověření je port povolen, v případě neověření ze strany serveru je port zakázán.
- Supplicant – Port musí být před povolením ověřen serverem.



Obrázek 13 Ukázka nastavení zabezpečení portu 16 [Vlastní zdroj].

Pro správnou funkci ověření portu zůstanou výchozí hodnoty. Změna je ale nezbytná pro porty, ve kterých jsou připojené servery a zařízení, které protokol 802.1X nepodporují. Pro tento účel je port v režimu „Supplicant" a v sekci „Supplicant Options" je volba" Control

Mode“ nastavena na „Force Authorized”. Tímto nastavením se stává port trvale ověřený a připojený do interní sítě. Na obrázku (Obr. 14) je zobrazeno nastavení portů číslo 11 až 20. Z tabulky lze vyčíst, že porty 17 až 20 jsou trvale ověřeny. Současně jsou tyto porty zařazeny do VLAN sítě 10, tedy interní sítě [20].

Interface	PAE Capabilities	Control Mode	Operating Control Mode	PAE State	Backend State
11	Authenticator	Auto	N/A	Initialize	Idle
12	Authenticator	Auto	N/A	Initialize	Idle
13	Authenticator	Auto	N/A	Initialize	Idle
14	Authenticator	Auto	N/A	Initialize	Idle
15	Authenticator	Auto	N/A	Initialize	Idle
16	Authenticator	Auto	N/A	Initialize	Idle
17	Supplicant	Force Authorized	Force Authorized	Disconnected	Idle
18	Supplicant	Force Authorized	Force Authorized	Force Authorized	Idle
19	Supplicant	Force Authorized	Force Authorized	Force Authorized	Idle
20	Supplicant	Force Authorized	Force Authorized	Force Authorized	Idle

First Previous 1 2 3 Next Last

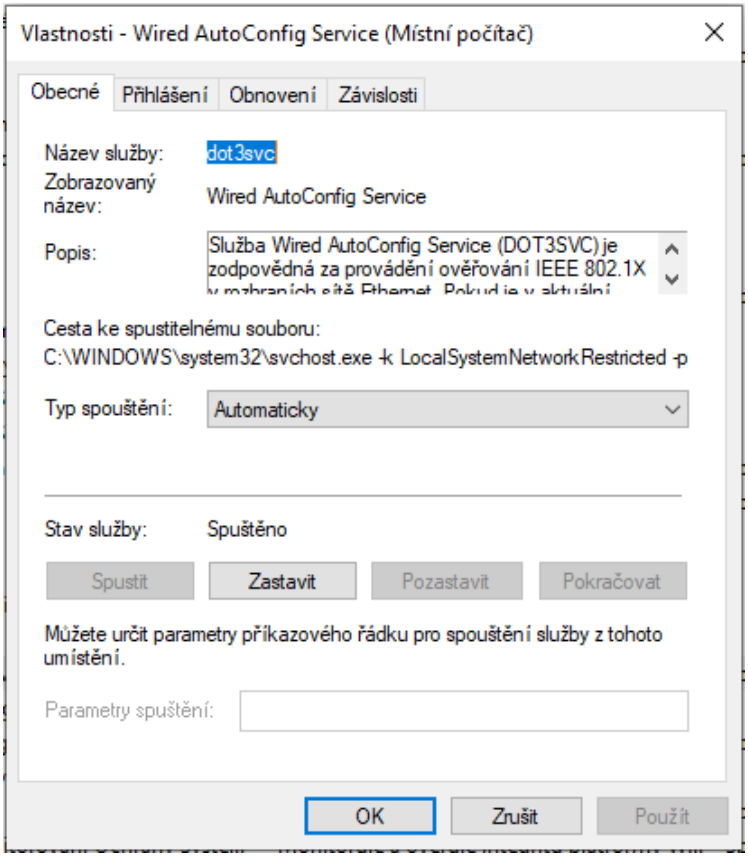
Obrázek 14 Tabulka nastavení zabezpečení portů [Vlastní zdroj].

5.4 Příprava a konfigurace počítače

Nastavení počítače bude popsáno na systému Microsoft Windows 10 verze 1909. Zmíněný systém není nakonfigurován pro použití ověřování na úrovni sítě. Po instalaci čistého systému chybí v nastavení síťového adaptéru důležitá záložka s názvem Ověřování. Důvodem pro chybějící nastavení je systémová služba „Wired AutoConfig Service”, která je výchozím stavu vypnutá. Prvním krokem je tedy povolení této služby.

5.4.1 Spuštění služby Wired AutoConfig Service

Pro spuštění konzole pro administraci služeb slouží aplikace Services. V české verzi operačního systému se tato aplikace jmenuje Služby. Název aplikace stačí napsat do vyhledávacího políčka Windows a po zobrazení aplikace v seznamu vyhledaných položek stisknout klávesu enter. Po spuštění konzole se zobrazí okno se všemi službami systému Windows. Vyhledáním a kliknutím na službu „Wired AutoConfig Service” se zobrazí dialogové okno s nastavením. Změnou hodnoty v rozbalovací nabídce „Typ spuštění“ na „Automaticky“ je zajištěno její spuštění při startu počítače. Změnou této hodnoty se ale služba nespustí. Ke spuštění dojde až po restartu počítače. Pro spuštění služby bez restartu lze kliknout na tlačítko „Spustit“.



Obrázek 15 Služba Wired AutoConfig Service [Vlastní zdroj].

5.4.2 Nastavení síťového adaptéru

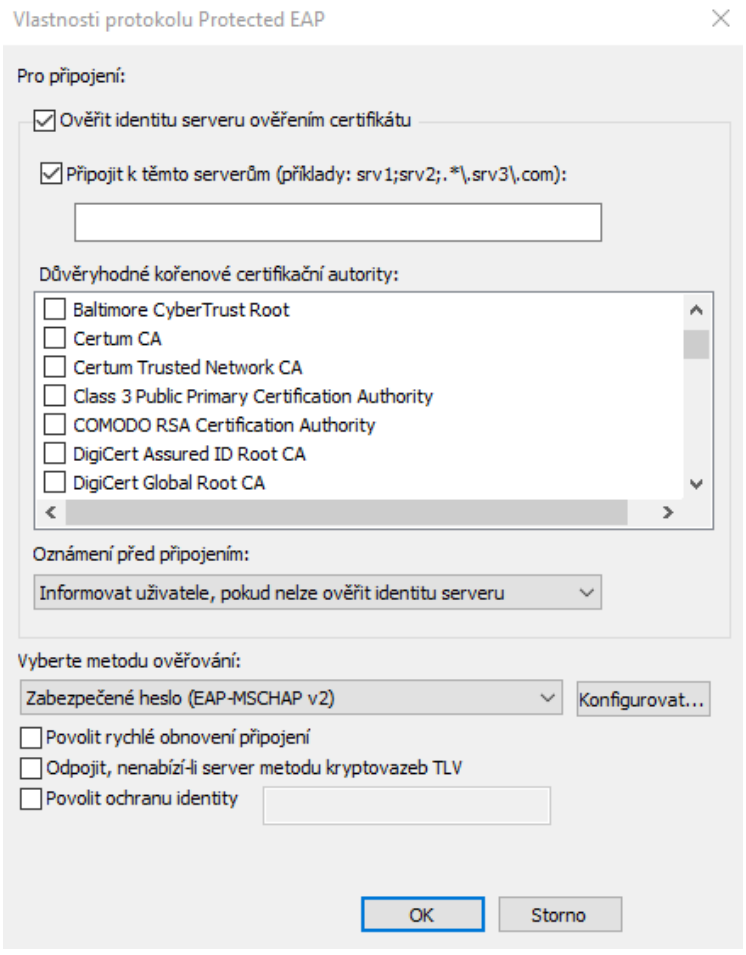
Nastavení adaptéru je dostupné z kontextové nabídky po kliknutí pravým tlačítkem na ikonu síťového připojení. Okno se síťovými adaptéry je dostupné po zadání příkazu ncsp.cpl ve vyhledávacím poli a potvrzením spuštění klávesou enter. Záložka Ověřování je již dostupná a hned na její základní straně je nutné zaškrtnout políčko vedle volby „Povolení ověřování podle standardu IEEE 802.1X“. V rozbalovacím menu pro metodu ověřování v síti pak musí být vybrána volba „Microsoft: Protocol PEAP (Protected EAP)“. Dle uvážení je možné zaškrtnout volbu „Zapamatovat přihlašovací údaje pro toto připojení pro každé přihlášení“.

Další důležitou součástí je nastavení protokolu PEAP, které je dostupné pod tlačítkem nastavení. Potřebné hodnoty nastavené v tomto dialogu jsou uvedené a popsané v následujícím seznamu:

- povolení volby „Ověřit identitu serveru ověřením certifikátu“ a současně i druhou volbu „Připojit k těmto serverům“. V případě použití certifikátu vydaného vlastní certifikační autoritou je vhodné do systému počítače nainstalovat certifikát

Certifikační autority a ten v seznamu vybrat. Jinak se bude zobrazovat okno s informací o neověřeném certifikátu serveru,

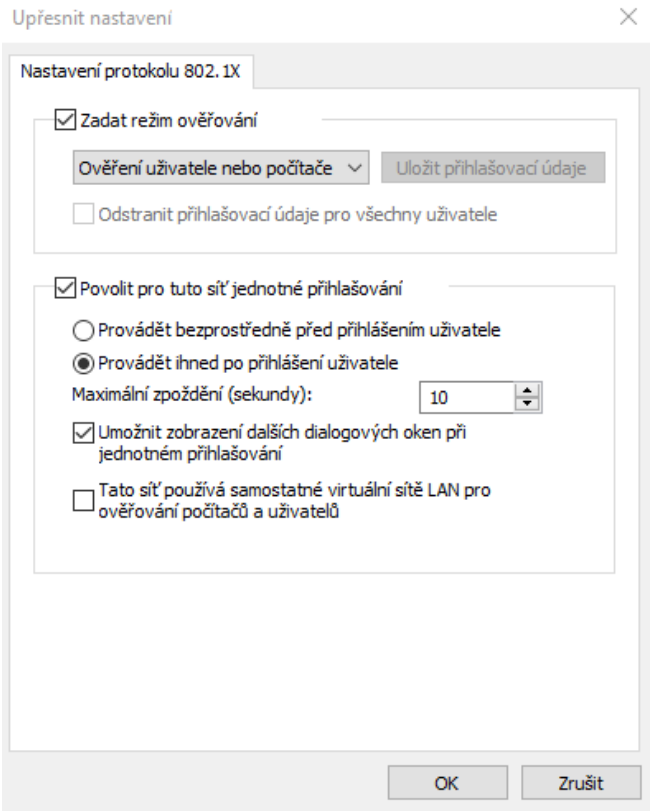
- oznámení před připojením – „Informovat uživatele, pokud nelze ověřit identitu serveru“,
- vyberte možnost ověřování – „Zabezpečené heslo (EAP-MSCHAP v2)“. V konfiguraci této volby je jen jedna možnost a sice „Automaticky použít mé uživatelské jméno a heslo“. Pokud je tato volba povolena, po připojení se automaticky použije jméno a heslo zadané uživatelem při přihlášení do systému Windows. Pro počítače připojené v doméně waxen.local je dobré tuto volbu zapnout. V případě, že bude připojovaný počítač v jiné doméně, nebo bude používat lokální účet počítače, je nutné tuto volbu vypnout. Po připojení do sítě pak bude vyvoláno dialogové okno pro zadání uživatelského jména a hesla,
- ostatní tři volby zůstanou vypnuté.



Obrázek 16 Nastavení protokolu PEAP [Vlastní zdroj].

Pod tlačítkem „Další nastavení“ na záložce Ověřování se skrývají další možnosti nastavení popsané níže.

- Povolená položka „Režim ověřování“. V této části lze zvolit ověření počítače, uživatele, nebo obou současně. Může zde zůstat výchozí hodnota, tedy „Ověření uživatele nebo počítače“.
- Povolení volby „Povolit pro tuto síť jednotné přihlášení“ – Zde povolit „Provádět ihned po přihlášení Uživatele“. První volba „Provádět ještě před přihlášením“ má smysl v případě, že je nutné přistupovat k síti ještě před přihlášením.
- Povolit položku „Umožnit zobrazení dalších dialogových oken při jednotném přihlašování“.
- Poslední volba „Tato síť používá samostatné virtuální sítě LAN pro ověřování počítačů a uživatelů“ zůstane nepovolená. Speciální VLAN síť pro ověřování není použita.

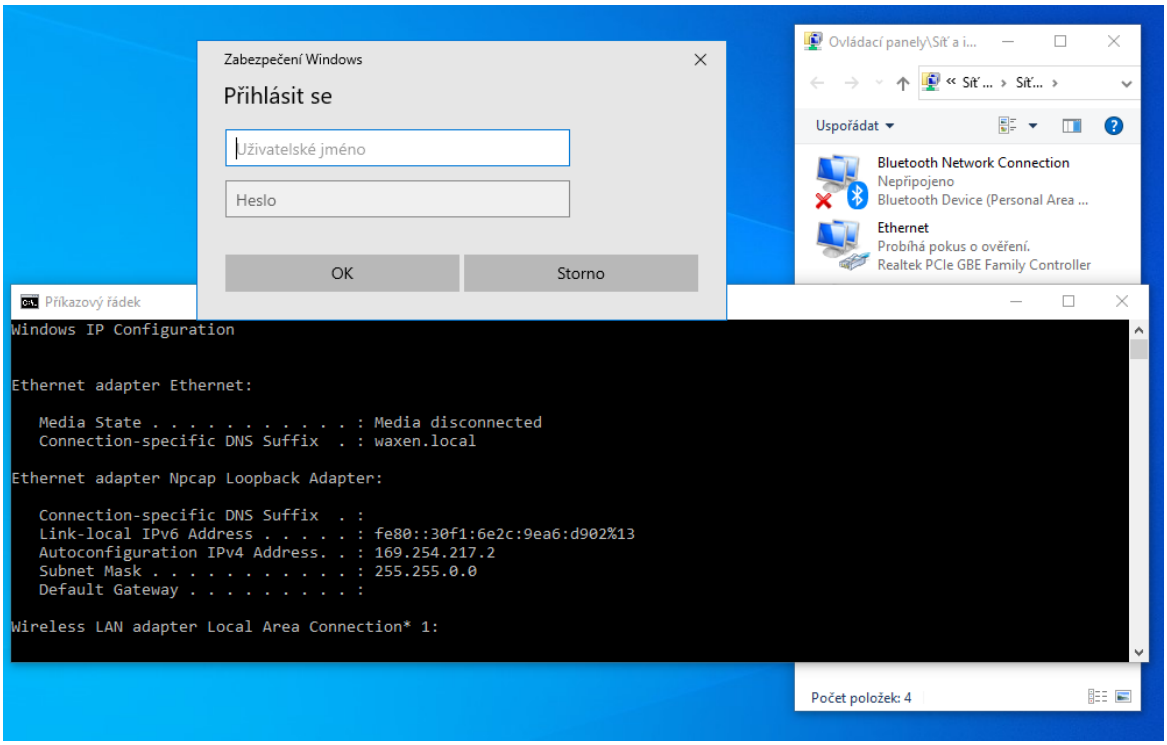


Obrázek 17 Nastavení ověřování [Vlastní zdroj].

Konfigurace testovacího prostředí je dokončena. Poslední částí je otestování funkčnosti zabezpečení.

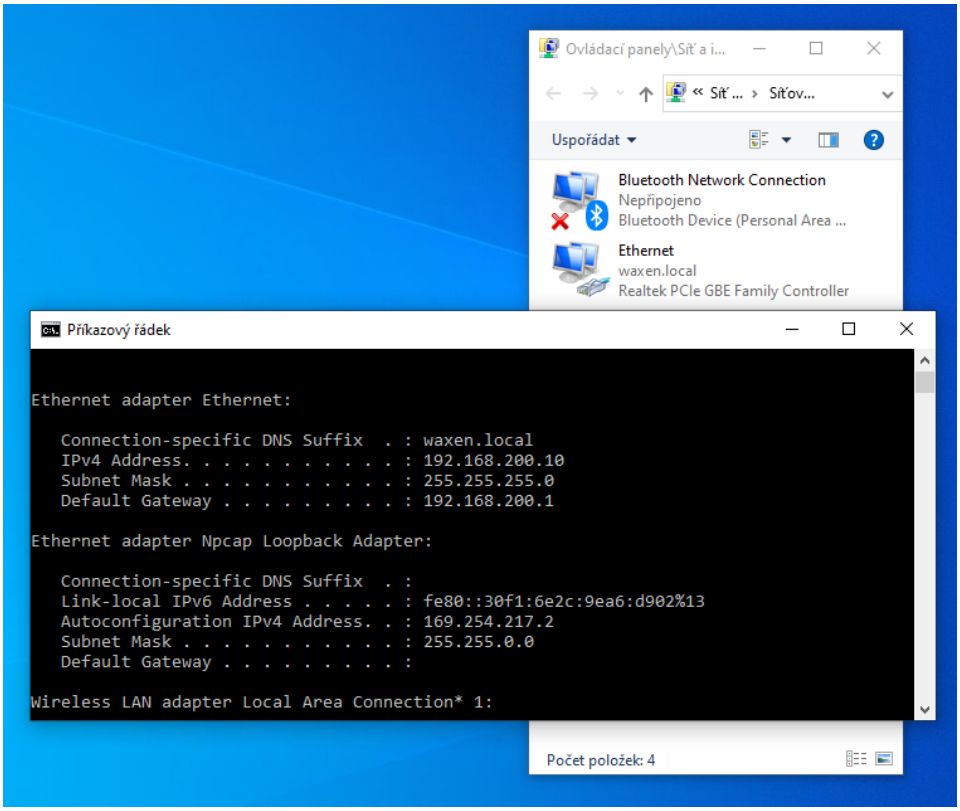
5.5 Test a ověření funkčnosti

Obrázek (Obr. 18) ukazuje stav po připojení síťového kabelu. Jsou zde zobrazena tři okna. V okně příkazového řádku můžeme vidět stav adaptéru, je označen „Ethernet adapter Ethernet“. V tomto případě je stav „disconnected”, odpojeno. Dále je zde zobrazeno okno „Zabezpečení Windows“ pro zadání jména a hesla. V posledním okně, označeném názvem „Ovládací panely“, je u adaptéru Ethernet zobrazen stav „Probíhá pokus o ověření“.



Obrázek 18 Ukázka prvního kroku po připojení k síti [Vlastní zdroj].

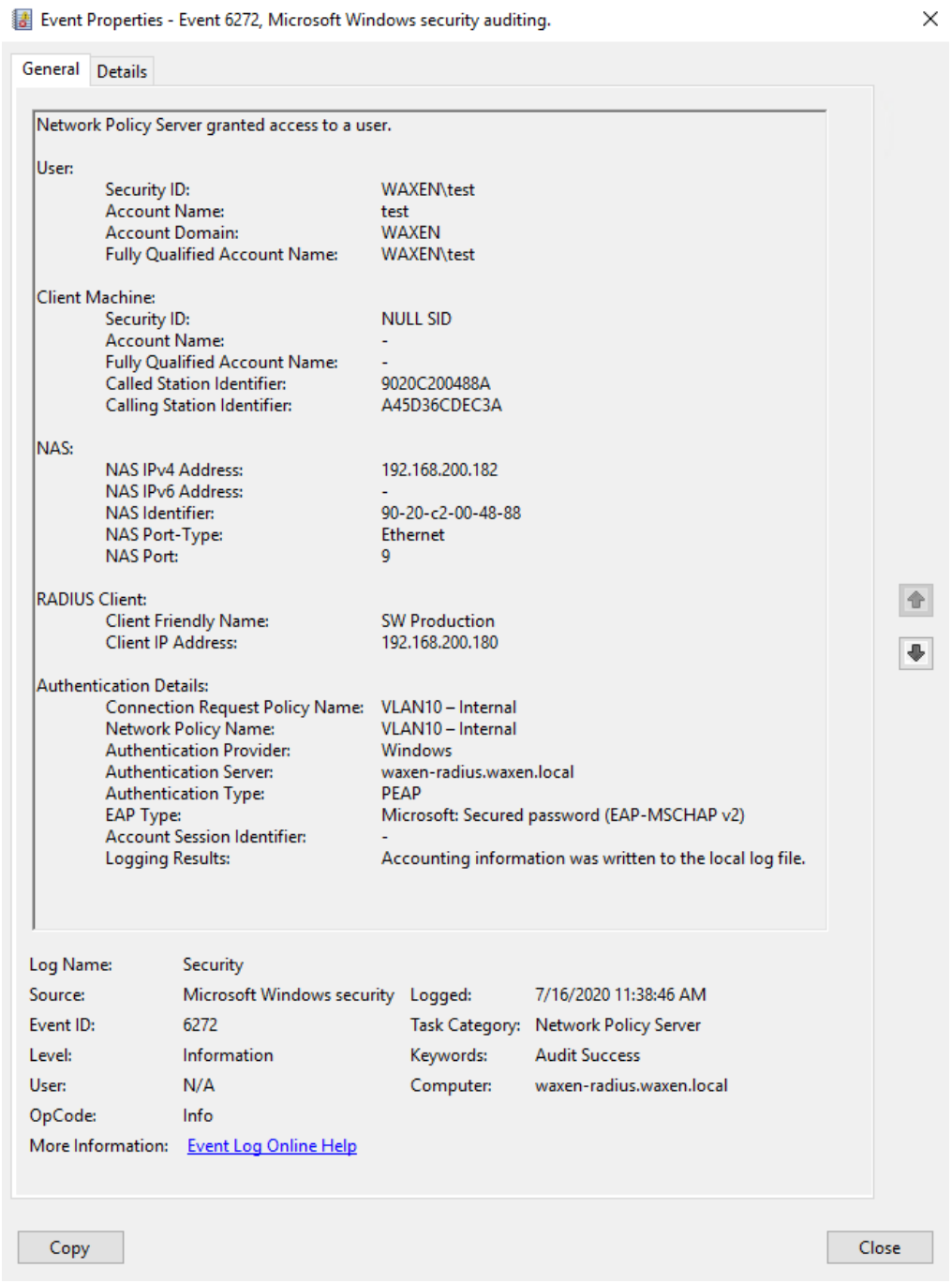
Obrázek (Obr. 19) již ukazuje stav po ověření. V okně ovládacích panelů je u připojení Ethernet zobrazen stav „waxen.local“, což indikuje úspěšné připojení k síti. V okně příkazového řádku je zobrazena přidělená IP adresa. Zařízení, v tomto případě notebook, získal z DHCP serveru adresu 192.168.200.10.



Obrázek 19 Stav připojení po autentifikaci [Vlastní zdroj].

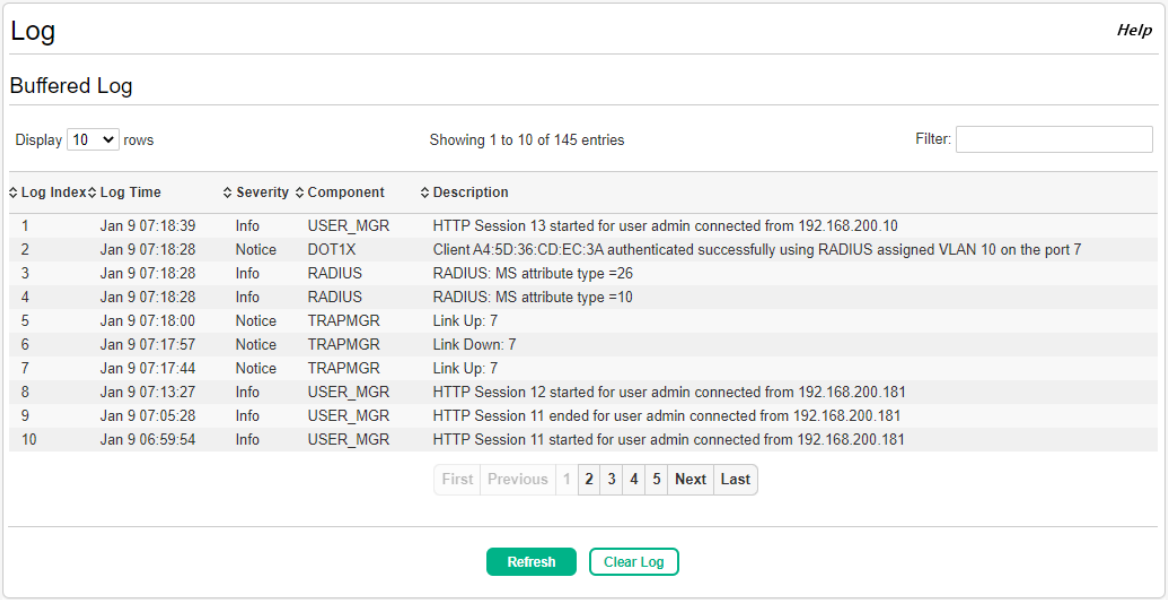
5.6 Logování událostí

Při hledání chyb a problémů lze využít logování událostí. Jednou z možností je Windows Event Viewer a druhou možností je log v administračním rozhraní switche. RADIUS server zaznamenává pokus o autentifikaci v systémové logovací službě Windows. Pro zobrazení záznamů slouží program Event Viewer. Každý záznam v Event Viewer má své ID události, v případě autentifikace RADIUS serverem se jedná o ID událost 6272 a najdeme ji v aplikaci v části Security.



Obrázek 20 Event Viewer, záznam o úspěšné autentifikaci [Vlastní zdroj].

Pro nahlédnutí do logu switche slouží stránka v administraci v menu „Diagnostics" a podmenu „Log". Log switche obsahuje podrobné informace nejen o ověřování uživatelů. Lze zde najít úspěšné i neúspěšné autentifikace.



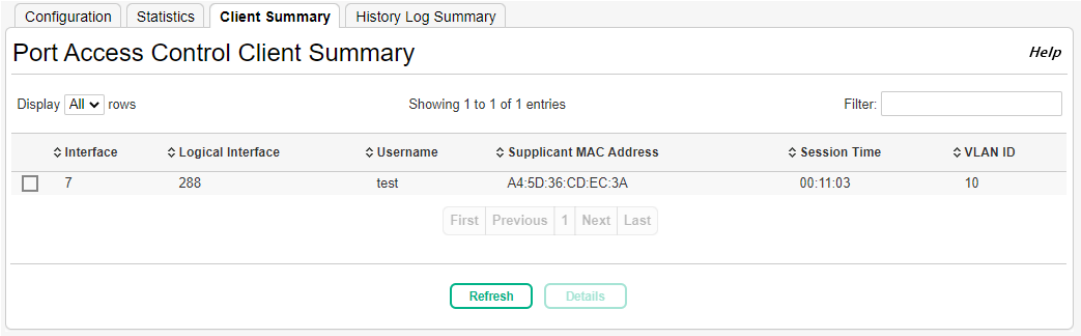
Obrázek 21 Ukázka úspěšné autentifikace na 2. řádku v logu switche HP [Vlastní zdroj].

5.7 Monitoring

Switch HP 1920s má možnost událostí monitorovat. Po přihlášení k administraci switche se nachází v menu „Security". V podmenu „RADIUS" na záložce „RADIUS Statistics", je zobrazen počet úspěšných a neúspěšných přístupů. Další informace administrátor získá v podnabídce „Port Access Control". Statistiky odeslaných žádostí zobrazuje záložka „Statistics". Zajímavější je záložka „Client Summary", kde je přehledná tabulka ověřených zařízení. Tabulka obsahuje:

- číslo portu, ke kterému je zařízení připojeno,
- uživatelské jméno,
- fyzická adresa zařízení,
- jak dlouho je zařízení připojené,
- v jaké je VLAN síti.

Na záložce „History Log Summary" je zobrazena historie jednotlivých portů. Jsou zde uvedeny informace obsahující port switche, datum, MAC adresu připojeného zařízení, jaká byla přidělena VLAN síť a informace o úspěšné nebo neúspěšné autentifikaci.



Obrázek 22 Ukázka aktuálně ověřených uživatelů [Vlastní zdroj].

5.8 Kalkulace a náklady na realizaci

Zmíněný popis zabezpečení je postavený na produktech HP, konkrétně se jedná o switch HP 1920s. Switch byl vybrán z důvodu podpory protokolu IEEE 802.1X. Další faktor, který hrál roli v rozhodování, byla skutečnost, že společnost WAXEN s.r.o. již čtyři uvedené switche vlastní. Snižují se tak náklady na investici do nových switchů. Aktuální cena uvedeného switche je 3.533,- Kč [21].

Tabulka 5 Kalkulace nákladů na výměnu switchů [Vlastní zdroj].

Areál 1	Nutná výměna	Cena v Kč bez DPH	Umístnění
HP ProCurve 2510	Ano	3.533,-	Serverovna
HP ProCurve 2510	Ano	3.533,-	Kancelářská budova
HP ProCurve 2510	Ano	3.533,-	Kancelářská budova
HP ProCurve 2510	Ano	3.533,-	Kancelářská budova
HPE ProCurve 1920s	Ne		Budova Výroby
HPE ProCurve 1920s	Ne		Budova Výroby
HPE ProCurve 1920s	Ne		Budova Výroby
HPE ProCurve 1920s	Ne		Budova Výroby
Areál 2			
HP ProCurver 2510	Ano	3.533,-	Budova A
HPE ProCurve 1810	Ano	3.533,-	Budova B
HPE ProCurve 1810	Ano	3.533,-	Budova C
Součet		24.731,-	

Z tabulky vychází náklady na nové switche ve výši 24.731,- Kč bez DPH. Další licence pro Windows servery nejsou nutné, společnost vlastní dostatečné množství licencí. Po dohodě s IT oddělením se společnost rozhodla realizovat zabezpečení vlastními lidskými zdroji. Odhad práce pro nasazení vč. testovacího prostředí je 24 hodin.

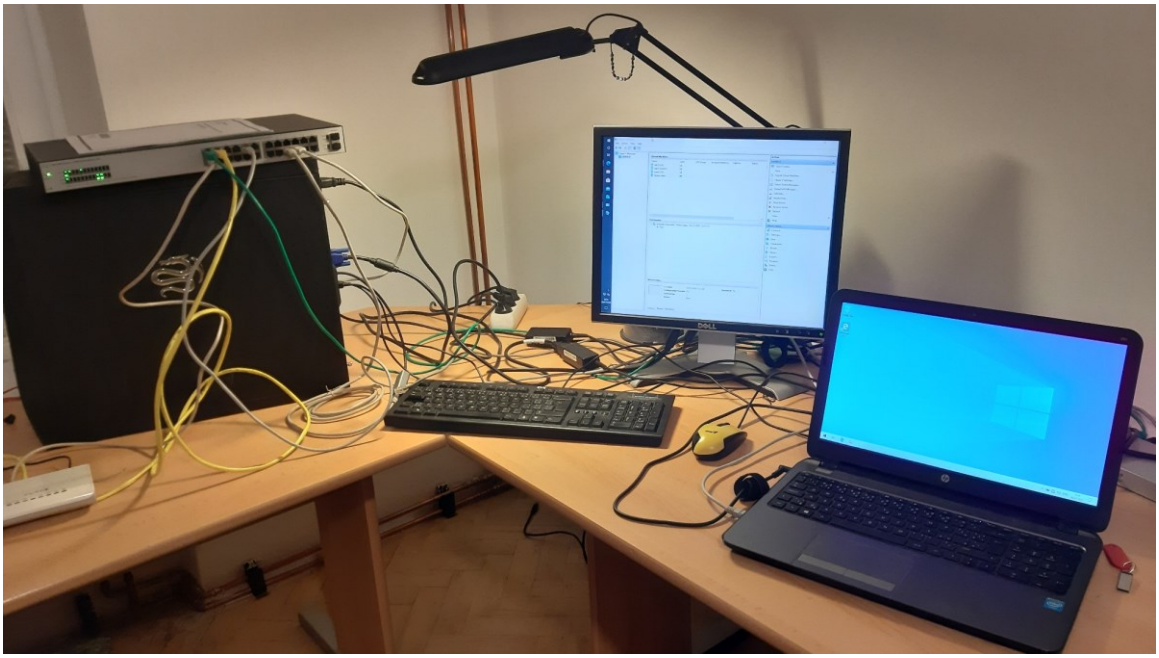
Tabulka 6 Ilustrace nákladů na realizaci vlastním pracovníkem IT [22].

Hrubá mzda pracovníka IT	50.000,- Kč
Náklady zaměstnavatele, superhrubá mzda	66.900,- Kč
Počet pracovních dnů v měsíci srpnu 2020	21 dnů
Hodinové náklady na pracovníka IT	364,- Kč
Náklady na realizaci (24 hodin x 364,- Kč)	8.736,- Kč

Platy zaměstnanců nejsou veřejně známé, cena nákladů na realizaci vlastním zaměstnancem je tedy odhadována a může se lišit. Celková cena nákladů na realizaci je součtem nákladů na pořízení nových switchů uvedených v tabulce (Tab. 5) a nákladů na realizaci vlastním zaměstnancem uvedené v tabulce (Tab. 6). Celková cena realizace je tedy 33.467,- Kč. Pro Společnost WAXEN s.r.o. je výše investice akceptovatelná.

5.9 Závěr

Pro popisované testovací prostředí bylo použito jen minimum prostředků. Jeden fyzický server, jeden switch HP1920s, notebook a volně dostupná testovací verze Windows serveru 2019. Prostředí tak lze levně postavit kdekoliv a otestovat zabezpečení dle specifik jakékoliv jiné sítě. Zabezpečení pomocí protokolu 802.1X bylo realizováno v testovacím prostředí za použití aktuálních verzí systému Windows server, Windows 10 a switche HP 1920s. Vývojem systémů z rodiny Windows, síťových zařízení a samotných protokolů lze předpokládat, že bude realizace v budoucnosti mírně, nebo i zcela odlišná.



Obrázek 23 Testovací prostředí realizované v rámci praktické části [Vlastní zdroj].

6 STRUČNÝ PLÁN NASAZENÍ ZABEZPEČENÍ SÍTĚ

Pro realizaci zabezpečení pomocí protokolu 802.1X ve společnosti WAXEN s.r.o. je nezbytné pořídit sedm nových switchů HP 1920s, vytvořit bezpečnostní skupinu gInternalEmployees v ADDS a přidat vybrané uživatele s povolením připojení k síti do dané skupiny. Jelikož již společnost WAXEN s.r.o. službu využívá, není nutné ji nově instalovat. Bezpečnostní skupina gInternalEmployees tedy bude vytvořena v aktuální používané službě ADDS. Dalším krokem je instalace čistého serveru určeného pro instalaci rolí NPAS s RADIUS serverem a službu ADCS. Následuje nastavení jednotlivých switchů a jejich registrace jako klient na RADIUS serveru. Před spuštěním zabezpečení je nutné nastavit jednotlivé počítače. Pro tento úkol je možné využít funkcí skupinové politiky a nastavení provést na serveru se službou ADDS. Při spuštění počítače připojeného v doméně, dojde k jeho automatické konfiguraci zabezpečení s použitím protokolu IEEE 802.1X. Posledním krokem je aktivace samotného zabezpečení a nastavení portů, které mají být bez ověřování. Porty bez ověření slouží pro připojení zařízení nepodporujících protokol IEEE 802.1X a pro vzájemné propojení switchů. Aktivace může být postupná včetně průběžného monitoring stavu a funkčnosti.

6.1 Závěr

Uvedený postup vychází z IT infrastruktury společnosti WAXEN s.r.o., pro kterou je určen. Nasazení v jiné firmě s jinou IT infrastrukturou může mít postup odlišný. Vždy záleží na konkrétní situaci a IT infrastruktuře.

ZÁVĚR

Bakalářská práce pojednává o potřebě společnosti zvýšit bezpečnost dat. Byl popsán způsob zabezpečení pomocí protokolu IEEE 802.1X a testovací prostředí před samotným nasazením. V teoretické části se práce zabývala základním popisem počítačové sítě a jednotlivých technologií potřebných pro realizaci. Následně popisovala analýzu nedostatků sítě společnosti WAXEN s.r.o. a možnosti zvýšení jejího zabezpečení. V praktické části popisovala současnou Firemní infrastrukturu, rozložení budov a umístnění síťových prvků společně se servery společnosti. Bylo vytvořeno testovací prostředí s popisem jednotlivých kroků při jeho realizaci a vysvětleny možnosti monitorování přihlášených uživatelů včetně jejich zařízení. V závěru byla uvedena kalkulace nákladů na realizaci a navržen stručný postup nasazení ve společnosti WAXEN s.r.o..

Zabezpečení dat společností je v dnešní době klíčové. Popisovaný typ zabezpečení není jediný možný způsob. Firma WAXEN s.r.o. se rozhodla pro tento způsob na základě doporučení auditorského týmu z provedeného bezpečnostního auditu. Dalším faktorem v rozhodování a výběru popsaného řešení byla i finanční stránka. Síťové prvky společnosti HP jsou cenově přijatelné a celková investice je pro společnost akceptovatelná. Zvolený způsob zabezpečení umožňuje automatický přístup firemních počítačů i přístup počítačů externích pracovníků. Současně je zajištěna podpora starších síťových zařízení nepodporující protokol IEEE 802.1X. Při realizaci byla ověřena funkčnost zabezpečení včetně úspěšného testu. Systém zabezpečení lze rozšířit přidáním dalších VLAN sítí a bezpečnostních skupin s přístupem ke konkrétní VLAN síti. Zvolení konkrétní sítě, do které má uživatel přístup, je možné určit dle přístupových údajů uživatele. Lze tak dosáhnout různých přístupů pro různé skupiny uživatelů. Jelikož společnost WAXEN s.r.o. využívá ve svých areálech i bezdrátové připojení k síti, může být využito stejného způsobu ověření i pro připojení k bezdrátové síti.

Úroveň bezpečnosti připojení k síti, kterou nabízí protokol IEEE 802.1X, je pro společnost dostatečná a v kombinaci s dalšími způsoby zabezpečení zvyšuje úroveň bezpečnosti dat a IT infrastruktury.

Přínos této práce je v jejím využití i mimo společnost WAXEN s.r.o.. Popisovaný způsob zabezpečení může využít jakákoliv jiná firma a podrobný popis konfigurace může komukoliv usnadnit jeho aplikaci, případně získat orientaci v použití protokolu 802.1X.

SEZNAM POUŽITÉ LITERATURY

[1] *HISTORIE POČÍTAČŮ: Počátky počítačů* [online]. [cit. 2020-06-27]. Dostupné z: http://www.historie.sokolici.eu/pocatky.html

[2] *Informatika v kostce: Historie počítačů* [online]. , 1 [cit. 2020-06-27]. Dostupné z: http://www.ict.mazuch.net/subdom/ict/12-historie-pocitacu/

[3] KUROSE, James F. a Keith W. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 9788025138250.

[4] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 9788025131763.

[5] STANEK, William R. *Microsoft Windows Server 2012: kapesní rádce administrátora*. Brno: Computer Press, 2015, 736 s. ISBN 9788025138175.

[6] BOUŠKA, Petr. Group Policy - řízení aplikace politik. *Samuraj.cz* [online]. , 1 [cit. 2020-06-27]. Dostupné z: https://www.samuraj-cz.com/clanek/group-policy-rizeni-aplikace-politik/

[7] *Remote Authentication Dial In User Service (RADIUS*). IETF [online]. 2000 [cit. 2020-03-07]. Dostupné z: https://tools.ietf.org/html/rfc2865

[8] Certifikační autorita. *Ústav výpočetní techniky, Univerzita Karlova* [online]. 2014 [cit. 2020-06-30]. Dostupné z: https://uvt.cuni.cz/UVT-252.html

[9] *SSL Market: Wildcard certifikáty* [online]. 2005 [cit. 2020-06-30]. Dostupné z: https://www.sslmarket.cz/ssl/wildcard-certifikaty/

[10] BOUŠKA, Petr. Cisco IOS 11 - IEEE 802.1x, autentizace k portu, MS IAS. *Www.samuraj.cz* [online]. , 1 [cit. 2020-06-27]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-11-ieee-802-1x-autentizace-k-portu-ms-ias/

[11] *Extensible Authentication Protocol (EAP)*. IETF [online]. 2004 [cit. 2020-03-07]. Dostupné z: https://tools.ietf.org/html/rfc3748

[12] STALLINGS, William a Lawrie BROWN. *Computer security: principles and practice*. Third edition. Boston: Pearson, [2015], 840 s. Always learning. ISBN 9781292066172.

[13] Knowledge Base. *PEAP - Protected EAP Protocol* [online]. [cit. 2020-07-07]. Dostupné z: https://sites.google.com/site/amitsciscozone/home/switching/peap---protected-eap-protocol

[14] ZUB, Ondřej. *Autentizační protokoly používané v PPP* [online]. 2005, , 38 [cit. 2020-06-27]. Dostupné z: http://ozub81.sweb.cz/protokoly/sem/semestralka.pdf

[15] KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

[16] *IETF: Internet Standards* [online]. [cit. 2020-06-27]. Dostupné z: https://www.ietf.org/

[17] BOUŠKA, Petr. VLAN - Virtual Local Area Network. *SAMURAJ-cz* [online]. c2005–2020 [cit. 2020-07-26]. Dostupné z: https://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

[18] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.

[19] SVATÁ, Vlasta. *Audit informačního systému*. V Praze: Oeconomica, nakladatelství VŠE, 2016. ISBN 978-80-245-2168-8.

[20] *HPE OfficeConnect 1920S 8G/24G/48G Switch Series Management and Configuration Guide* [online]. 2018. [cit. 2020-06-27]. Dostupné z: https://support.hpe.com/hpsc/doc/public/display?doclocate=en_US&docId=emr_na-a00003478en_us

[21] *TSBOHEMIA.CZ: HP 1920S 24G 2SFP Switch* [online]. [cit. 2020-07-06]. Dostupné z: https://www.tsbohemia.cz/hp-1920s-24g-2sfp-switch-jl381a-_d291429.html?gclid=Cj0KCQjwl4v4BRDaARIsAFjATPmPERccQFnAgSyc2BVMgAVa5b92SZggMLgfSc9wTSVjVYbi4bt9jlwaAkhYEALw_wcB

[22] *Měšec.cz* [online]. Internet Info, c1998-2020 [cit. 2020-07-15]. Dostupné z: https://www.mesec.cz/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ADDS	Active Directory Domain Services
ADCS	Active Directory Certificate Services
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
HP	Hewlett Packard
HPE	Hewlett Packard Enterprise
HTTP	HyperText Transfer Protocol
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IT	information technology
MAC	Media Access Control
MS-CHEAP	Microsoft Challenge Handshake Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
PDC	Primary Domain Controller
RFC	Request For Comments
RADIUS	Remote Authentication Dial In User Service
TCP/IP	Transmission Control Protocol / Internet Protocol
VLAN	Virtual Local Area Network
www	World Wide Web

SEZNAM OBRÁZKŮ

SEZNAM TABULEK