



Kupní smlouva

uzavřená dle ustanovení § 2085 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen občanský zákoník)

Číslo smlouvy: _____

Smluvní strany:

Kupující:

zastoupený ve věcech smluvních:
sídlo:
IČ:
DIČ:
bankovní spojení:
dále jen „**kupující**“

Město Šternberk

Ing. Stanislav Orság, starosta
Horní náměstí 78/16, 785 01 Šternberk
00299529
CZ 00299529
19-1801688399/0800

a

Prodávající:

zastoupený ve věcech smluvních:
sídlo:
IČ (IČO):
DIČ:
bankovní spojení:
dále jen „**prodávající**“

MERIT GROUP a.s.

Petr Weigel, statutární ředitel
Březinova 136/7, 779 00 Olomouc
64609995
CZ699000785
377897583/0300

I.

Předmět smlouvy

- Kupující vyhlásil výběrové řízení s názvem **Zvýšení kvality a dostupnosti infrastruktury pro vzdělávání v ZŠ Šternberk**, kterým poptával dodávku pro část 2 předmětného výběrového řízení:
Dodávka ICT včetně zajištění konektivity, jak jsou blíže specifikovány v přílohách č. 1 až 4, které tvoří nedílnou součást této smlouvy
(dále jen „**movité věci**“ nebo „**předmět prodeje**“).
- Prodávající prohlašuje, že je **majitelem movitých věcí** specifikovaných blíže v příloze č. 1.
- Prodávající prodává** kupujícímu předmět prodeje a kupující jej **kupuje** a **zavazuje se zaplatit** za něj kupní cenu sjednanou v čl. II. této smlouvy.
- Prodávající prodává kupujícímu předmět prodeje včetně všech jeho součástí a příslušenství, jakož i včetně práv a povinností s ním spojených, a to ve stavu, v jakém se nachází ke dni podpisu této smlouvy, což kupující bere podpisem této smlouvy výslovně na vědomí.

II.

Kupní cena

- Smluvní strany sjednaly cenu za předmět prodeje včetně ve výši 7.619.242 Kč bez DPH, DPH 21 %: 1.600.041 Kč, **celková cena včetně DPH 9.219.283 Kč** (devětmilionůdvěstědevatenáct tisícdvěstěosmdesáttří korun českých včetně DPH). Cena je konečná včetně všech poplatků a daní.
- Dohodnutou kupní cenu **zaplatí kupující** prodávajícímu nejpozději do 30 dnů od předání sestaveného předmětu prodeje v řádném stavu, a to bezhotovostně na účet prodávajícího uvedený v záhlaví této smlouvy.

3. Prodávající bere na vědomí, že kupní cena příp. její část bude **hrazena z finančních prostředků získaných formou dotace** z programu Integrovaného regionálního operačního programu Zvýšení kvality a dostupnosti infrastruktury pro vzdělávání v ZŠ Šternberk, registrační číslo projektu CZ.06.2.67/0.0/0.0/16_063/0003826.

Prodávající se zavazuje při plnění této smlouvy dodržet podmínky poskytovatele dotace, které jsou zveřejněny na <http://www.irop.mmr.cz>.

4. Sjednaná kupní cena zahrnuje zejména:
- a) dodávku a sestavení předmětu prodeje v místě plnění včetně jeho kompletace se stávajícím zařízením kupujícího – zajistit kompatibilitu s technologickými zařízeními kupujícími, instalaci, zprovoznění (dále také „sestavení předmětu prodeje“),
 - b) manipulaci s předmětem prodeje včetně vynášky do místa plnění,
 - c) dopravu předmětu prodeje na místo určení, včetně cestovních výloh osob zajišťujících přepravu a sestavení předmětu prodeje,
 - d) dodání dokumentace k předmětu prodeje v českém jazyce, jako je zejména:
 - záruční list,
 - prohlášení o shodě výrobku,
 - technická specifikace,
 - návod k obsluze.
5. Kupujícímu vznikne nárok na úhradu kupní ceny, tzn. i na vystavení daňového dokladu na kupní cenu nejdříve dodáním předmětu prodeje v řádném stavu a splněním všech činností sjednaných v odst. 3. tohoto článku.
6. Kupní cena se považuje za uhrazenou jejím odepsáním z účtu kupujícího.

III.

Způsob, místo a doba splnění

1. Prodávající splní řádně a včas svůj závazek uvedený v čl. I. této smlouvy předáním v řádném stavu předmětu prodeje spolu s veškerým příslušenstvím kupujícímu, včetně sestavení předmětu prodeje, v místě plnění oproti zápisu o předání a převzetí předmětu prodeje. Dle dohody smluvních stran se prodávající zavazuje předat předmět prodeje kupujícímu, včetně provedení činností sjednaných v čl. II. bodu 4. této smlouvy, **nejpozději do 31.08.2019**. Zahájení plnění bude bezodkladně po podpisu této smlouvy.
2. Smluvní strany se dohodly, že **místem plnění** a převzetí předmětu prodeje je:
- **Základní škola Dr. Hrubého 2**, Šternberk, příspěvková organizace, Dr. Hrubého 319/2, 78501 Šternberk
 - **Základní škola náměstí Svobody 3**, Šternberk, příspěvková organizace, nám. Svobody 1264/3, 78501 Šternberk
 - **Základní škola Svatoplukova 7**, Šternberk, příspěvková organizace, Svatoplukova 1419/7, 78501 Šternberk
- (v textu smlouvy jako „místo plnění“).
3. Prodávající oznámí kupujícímu možnost zahájení se sestavováním předmětu prodeje v místě plnění písemně prostřednictvím pošty nebo e-mailu, příp. telefonicky. Smluvní strany se zavazují nejpozději do tří dnů ode dne tohoto oznámení dohodnout (e-mailem, příp. telefonicky) přesný termín sestavení předmětu prodeje, příp. zahájení s jeho sestavováním tak, aby bylo možno uskutečnit dodání a převzetí předmětu prodeje v čase plnění dle bodu 1. tohoto článku smlouvy. V případě, že se smluvní strany do tří dnů ode dne oznámení nedohodnou, platí, že termín sestavení předmětu prodeje, příp. zahájení s jeho sestavováním je pátý pracovní den ode dne oznámení kupujícímu dle tohoto bodu smlouvy o možnosti zahájení sestavování předmětu prodeje.
4. Kupující se zavazuje poskytnout prodávajícímu součinnost nutnou ke splnění jeho závazků vyplývajících z této smlouvy, zejména umožnit mu přístup do místa plnění a sestavení předmětu prodeje na místě plnění v termínu stanoveném touto smlouvou.
5. Kupující se dále zavazuje před termínem zahájení sestavování zboží připravit staveniště a nutná média tak, aby bylo možné řádně provést sestavení předmětu prodeje a jeho odborného zapojení, jakož i zajistí v případě potřeby svého IT pracovníka.

6. Kupující je povinen předmět prodeje v dohodnuté době řádně převzít a potvrdit zápis o převzetí. V případě, že tak bezdůvodně neučiní nebo předmět prodeje odmítne převzít, má prodávající právo plnit náhradním uskladněním. Odesláním výzvy k převzetí předmětu prodeje prodávající uvědomí kupujícího nejpozději do 15 dnů od marného uplynutí lhůty k převzetí předmětu prodeje o náhradním uskladnění a o zamýšleném prodeji tohoto předmětu prodeje.
7. Nebezpečí škody na předmětu prodeje a vlastnické právo k předmětu prodeje přechází z prodávajícího na kupujícího okamžikem fyzického předání a převzetí předmětu prodeje.
8. Pro případ prodlení s úhradou kupní ceny nebo její části dle této smlouvy sjednávají smluvní strany smluvní pokutu ve výši 0,05 % z dlužné částky za každý i započatý den prodlení.
9. Pro případ prodlení prodávajícího se splněním této smlouvy, tzn. dodávkou předmětu prodeje v řádném stavu a splněním povinností sjednaných v této smlouvě, vznikne kupujícímu nárok na smluvní pokutu ve výši 0,05 % z kupní ceny vč. DPH za každý i započatý den prodlení.
10. Bude-li prodávající v prodlení s plněním této smlouvy po dobu delší než 30 dnů, je kupující oprávněn odstoupit od této smlouvy.

IV.

Záruka a reklamace

1. Prodávající odpovídá kupujícímu za to, že předmět prodeje nemá při převzetí vady. Zejména prodávající odpovídá kupujícímu za to, že předmět prodeje v době, kdy je kupující převzal, odpovídá požadované jakosti a provedení.
2. Předmět prodeje bude dodán nový, v nejvyšší možné kvalitě odpovídající příslušným právním předpisům a technickým normám, způsobilý k použití k účelu, k němuž je určen. Záruční doba na předmět prodeje je 24 měsíců ode dne jeho převzetí v řádném stavu kupujícím.
3. Kupující je povinen provést při převzetí jeho řádnou kontrolu.
- 3.1. **Zjevné vady**, spočívající zejména ve vadách vzhledu předmětu prodeje, je povinen ihned reklamovat zápisem do předávacího protokolu.
- 3.2. **Skryté vady**, nezjistitelné běžnou prohlídkou nebo vady, které se projeví či vzniknou později, je oprávněn kupující reklamovat do 30 dnů od jejich zjištění nebo od okamžiku, kdy mohly být při náležité odborné péči zjištěny, nejpozději však do konce záruční doby. Reklamace může být učiněna telefonickým oznámením nebo e-mailem. O učiněné reklamaci smluvní strany sepsí reklamační protokol, ve kterém prodávající uvede, zda reklamaci uznává, případně důvody pro které ji neuznává. Prodávající se zavazuje reklamaci odstranit do 30 dnů od jejího přijetí. Smluvní strany se výslovně dohodly na vyloučení ustanovení § 1921 odst. 3 a § 2112 občanského zákoníku.
4. Prodávající prohlašuje, že:
 - 4.1. na předmětu prodeje nevážnou ke dni uzavření této smlouvy žádné právní závady, zejména žádné závazky, zástavní práva, budoucí zástavní práva, podzástavní práva, předkupní práva, zákaz zcizení nebo zatížení, nájemní práva nebo jiná omezení ve prospěch třetích osob.
 - 4.2. neprobíhá žádné soudní, rozhodčí ani jiné řízení vztahující se k předmětu prodeje, zejména žádné řízení o určení vlastnického práva nebo exekuční řízení, a mezi prodávajícím a žádnou třetí osobou neexistují nevyřízené žaloby, spory, nároky nebo požadavky týkající se předmětu prodeje.
 - 4.3. předmět prodeje není v okamžiku uzavření této smlouvy předmětem konkurzního, insolvenčního, vyrovnávacího, exekučního nebo podobného řízení a že předmět prodeje nebyl vložen jako nepeněžitý vklad do základního kapitálu prodávajícího,
 - 4.4. prodávající není v úpadku ani v hrozícím úpadku.
5. Prokáže-li se některé z prohlášení prodávajícího uvedené v čl. I. odst. 2 a čl. IV. odst. 4. této smlouvy jako nepřesné, nepravdivé, případně neúplné, je prodávající oprávněn odstoupit od této smlouvy a/nebo požadovat náhradu škody mu tím způsobenou.

V.

Závěrečná ujednání

1. Pokud nebylo v této smlouvě výslovně ujednáno jinak, platí v ostatním příslušná ustanovení občanského zákoníku a předpisů souvisejících, vše v platném znění.

2. Veškeré změny této smlouvy mohou být provedeny po dohodě smluvních stran písemnými vzestupně očíslovanými dodatky. Smluvní strany se dohodly, že nabídka na změnu či doplnění smlouvy nemůže být přijata s dodatky, výhradami, omezeními či jinými změnami, a to i v případě, že tyto odchylky mění obsah nabídky pouze nepodstatně (ustanovení § 1740 odst. 3 občanského zákoníku se proto nepoužije).
3. Smluvní strany se dohodly, že veškeré písemnosti související s touto smlouvou jim budou doručovány na adresu uvedenou v záhlaví této smlouvy, nesdělí-li jedna smluvní strana druhé smluvní straně písemně jinou adresu pro doručování písemností, nebo do datové schránky, má-li ji smluvní strana zřízenou. Smluvní strany se dále dohodly pro případ, že některá ze smluvních stran zmaří doručení písemnosti zaslané prostřednictvím držitele poštovní licence tím, že neoznámí druhé smluvní straně změnu adresy pro doručování písemností nebo odmítne převzít zásilku, tato se bude považovat za doručenou třetím pracovním dnem po odeslání.
4. Tato smlouva je vyhotovena ve 2 exemplářích, každé s platností originálu, z nichž po jednom obdrží každý účastník této smlouvy.
5. Účastníci této smlouvy výslovně prohlašují, že:
 - a) si tuto smlouvu před jejím podpisem řádně přečetli, porozuměli jejímu obsahu, a že tato smlouva byla sepsána dle jejich svobodné, vážné a shodné vůle, nikoli v tísní,
 - b) při uzavírání smlouvy jednali s běžnou péčí a opatrností, poctivě a ctíc zákonná ustanovení a
 - c) jsou si vědomi vzájemných práv a povinností a okolností jejich smluvního vztahu, svá postavení považují za vzájemně rovná a vzájemná plnění za vyvážená na důkaz čehož připojují na závěr své podpisy.
6. Smluvní strany souhlasí s tím, že obsah smlouvy není obchodním tajemstvím a smluvní strany mohou smlouvu zveřejnit v rozsahu a za podmínek, jež vyplývají z obecně závazných právních předpisů.
7. Smluvní strany souhlasí s tím, že smlouva bude zveřejněna v registru smluv dle příslušných ustanovení zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Smluvní strany se dohodly, že zákonnou povinnost dle § 5 odst. 2 zákona o registru smluv splní Město Šternberk. Současně berou smluvní strany na vědomí, že v případě nesplnění zákonné povinnosti je smlouva do 3 (tří) měsíců od jejího podpisu bez dalšího zrušena od samého počátku.
8. Tato smlouva nabývá platnosti dnem podpisu a účinnosti dnem zveřejnění v registru smluv dle příslušných ustanovení zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

Příloha č. 1: Technická specifikace nabízeného řešení ZŠ Dr. Hrubého

Příloha č. 2: Technická specifikace nabízeného řešení ZŠ nám. Svobody

Příloha č. 3: Technická specifikace nabízeného řešení ZŠ Svatoplukova7

Příloha č. 4: Položkový rozpočet

Doložka platnosti právního jednání dle ustanovení § 41 zákona č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů:

Na straně kupujícího rozhodla o uzavření této smlouvy Rada města Šternberka dne 04.02.2019 usnesením č. 211/7

Ve Šternberku dne

V Olomouci dne

.....
Ing. Stanislav Orság
starosta

.....
Petr Weigel, statutární ředitel
MERIT GROUP a.s.

Technická specifikace

Centrální systém řízení a monitorování sítě

Vyžadován je centrální systém řízení a monitorování všech níže poptávaných komponent a to prostřednictvím jednotného webového rozhraní.

Centrální systém řízení a monitorování sítě (povinné parametry)	
<i>Bod</i>	<i>Popis</i>
1.	Centrální systém řízení a monitorování sítě musí umožnit zabezpečenou vzdálenou správu, plnou konfiguraci a monitorování současně pro všechny poptávané komponenty sítě (bezpečnostní brány, přepínače, bezdrátové přístupové body a systém správy mobilních zařízení) a to prostřednictvím jednotného integrovaného webového rozhraní.
2.	Systém musí zajistit automatickou aktualizaci softwaru a instalaci bezpečnostních záplat do všech zařízení v systému a to v uživatelsky definovaném čase.
3.	Systém musí umožnit změny konfigurace více zařízení stejného typu současně a konfigurace nových zařízení pomocí šablon.
4.	Centrální systém řízení a monitorování sítě musí podporovat následující metody autentizace klientů LAN a WLAN infrastruktury: - 802.1X ověření na základě údajů interní databáze systému - 802.1X ověření prostřednictvím RADIUS serveru - Webová autentizace na základě údajů interní databáze systému - Webová autentizace prostřednictvím RADIUS nebo LDAP serveru - Webová autentizace prostřednictvím Facebook účtu - Možnost vytvoření vlastního webového portálu
5.	Centrální systém řízení a monitorování sítě musí být schopen zobrazit všechny klientská zařízení připojená k síti školy během minimálně posledních 10 dnů. Výpis by měl obsahovat minimálně následující informace: - Uživatelské jméno - IP a MAC adresa zařízení - Objem uživatelem / zařízením přenesených dat za dané období s rozpadem na jednotlivé rozpoznávané aplikace
6.	Systém musí být schopen zobrazit seznam top žáků / studentů, kteří za dané období ve školní síti přenesli nejvíce dat.
7.	Systém musí být schopen zobrazit polohu a stav všech zařízení v systému v geografické mapě a také graficky zobrazit reálnou fyzickou topologii sítě školy.
8.	Systém musí být schopen zobrazit polohu všech klientských zařízení v závislosti na způsobu jejich připojení a to buď přímo v plánech jednotlivých podlaží, v geografické mapě nebo v kontextu portu příslušného LAN přepínače.
9.	Systém musí být provozován v režimu vysoké dostupnosti.
10.	Základní konektivita a přístup do Internetu musí být pro klienty zachován i v případě, že je Centrální systém řízení a monitorování sítě dočasně nedostupný.
11.	I v případě nedostupnosti Centrálního systému řízení a monitorování sítě musí být zajištěna možnost autentizace a autorizace nových klientů LAN i WLAN infrastruktury prostřednictvím 802.1x protokolu pomocí RADIUS.
12.	Systém musí umožnit rozdělení administrátorů do skupin s různými právy přístupu.
13.	Pro autentizaci administrátora přistupujícího přes webové rozhraní musí systém podporovat minimálně RADIUS protokol, SAML a dvoufaktorovou autentizaci.
14.	Systém musí být schopen odesílat správcům emailové zprávy o důležitých systémových událostech.
15.	Systém musí být schopen odesílat zprávy na vzdálený SYSLOG server.
16.	Systém musí podporovat SNMP protokol pro vzdálenou správu a monitorování.
17.	Systém musí podporovat XML API pro integraci s navazujícími systémy školy poskytující informace o připojených komponentách sítě a také klientských zařízeních.

18.	Systém musí sledovat změny konfigurace systému a zahrnutých síťových komponent – Informace musí minimálně obsahovat: - položku konfigurace - uživatelské jméno administrátora, který změnu provedl - novou hodnotu proměnné, v které ke změně došlo
19.	Systém musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
20.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně všech aktualizací softwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Systém musí být v době prodeje výrobcem plně podporován a na žádnou jeho část nesmí být vyhlášeno ukončení prodeje.

Next-Gen Firewall, IPS a anti-malware

Zařízení určené k ochraně síťového prostředí před hrozbami na bázi pokročilých útoků. Kromě funkcí tzv. Nex.Gen FW (typicky chápáné jako aplikační a identity-based FW) je schopno provádět inspekci provozu s detekcí a ochranou před útoky na úrovni síťového provozu. V oblasti ochrany proti malware je možno aktivovat analýzu souborů včetně dynamické analýzy (tzv. sandboxing) i ukládání nebezpečných souborů do karantény. Zařízení lze použít i pro URL filtraci na úrovni kategorií, konkrétních URL či podle reputace serverů v Internetu.

Požadovaná funkcionality/vlastnost	Způsob splnění požadované funkcionality/vlastnosti
Výkon a funkcionality firewallu	
Formát zařízení	Appliance, 1RU
Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených	1
Minimální počet 1Gb 10/100/1000 BaseT Ethernet	8
Podporovaný počet současně otevřených spojení stavový FW/aplikační FW	Min.100000M/100000
Rychlost vytváření nových spojení přes stavový FW	Min. 10K/s
Propustnost stavového firewallu (multiprotokolový režim)	Min. 500 Mbps
Propustnost aplikačního FW (next-gen FW) – (top parametry)	Min. 450 Mbps
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (top parametry)	Min. 250 Mbps
Propustnost aplikačního FW (next-gen FW) – (transakční profil, 450B průměrná velikost paketu)	Min. 180 Mbps
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (transakční profil, 450B průměrná velikost paketu)	Min. 115 Mbps
VPN propustnost	Min. 175 Mbps
Současný počet VPN spojení (IPSec/SSL)	Min. 100
Podpora L2 (transparentního) módu s podporou NAT a PAT	Ano
Podpora L3 (routovaného) módu s podporou NAT a PAT	Ano
Podporovaný počet VLAN	Min. 50
Podpora stateful failover	active/standby
Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru	Ano
Cluster firewallů se musí vzhledem k další infrastruktuře tvářit jako jeden prvek s podporou LACP	Ano
Cluster podporuje stavovou inspekci nesymetrického provozu vstupující do různých firewallů clusteru	Ano
Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podporou LACP	Ano
Podpora virtuálních bezpečnostních kontextů (virtuálních firewallů) s možností rozšíření až na 250 kontextů	Ano
Dynamické směrování - podpora alespoň RIP, OSPF, BGP	Ano
Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	Ano

Podpora Policy based Routing	Ano
Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	Ano
Podpora filtrace IPv4, IPv6	Ano
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	Ano
Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích	Ano
Podpora inspekce IPv6 provozu	Ano
Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	Ano
Podpora NAT64 a DNS64	Ano
Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód případně pro řízení přístupu podle uživatelské identity, typu aplikace, apod.	Ano
Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	Ano
Možnost rozšíření o funkce NextGen FW	Ano
Možnost rozšíření o funkce NextGen IPS	Ano
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	Ano
Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech	Ano
API rozhraní pro sdílení kontextových informací s dalšími systémy	Ano
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	Ano
Funkce IPS a anti-malware	
Možnost definovat typ provozu předávaný k inspekci do IPS	Ano
Podpora také IDS režimu – pasivního monitorování (TAP režim)	Ano
Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)	Ano
Možnost obejít IPS funkcí při zahlcení nebo nedostupnosti	Ano
Podpora 802.1Q tagovaných rámců	Ano
Podpora různých IPS politik pro různé typy provozu	Ano
Inspekce pro IPv4 i IPv6	Ano
Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému	Ano
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií	Ano
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	Ano
Podpora aplikace pro psaní zákaznických filtrů	Ano
Podpora importu komunitních filtrů/signatur Snort	Ano
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	Ano
IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	Ano
IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C	Ano
IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii	Ano
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	Ano

Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku	Ano
Funkce pro kontrolu DLP (např. pomocí Snort preprocesorů)	Ano
Podpora vrstev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	Ano
Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	Ano
Možnost definice uživatelské vrstvy politik	Ano
Předdefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik	Ano
Různé politiky lze sdílet a aplikovat na různé senzory	Ano
Podpora aktivní inline ochrany před malware s detekcí známých nebo podezřelých malware nezávislé na aktuálních databázích AV dodavatelů	Ano
Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry	Ano
Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat	Ano
Zobrazení trajektorie malware – pohyb, mutace, přenosy v síti mezi stanicemi přímo v GUI centralizované konzole	Ano
Možnost ochrany před malware až do úrovně koncových stanic s centralizovanou správou bezpečnostních politik, blacklistů pro aplikace, řízení spouštění aplikací, přesun malware do karantény, blacklistů pro síťovou komunikaci, apod.	Ano
Retrospektivní ochrana koncových stanic (chytré telefony), stanice s Windows, Mac OS – pokud je později SW kód rozpoznán v operačním centru dodavatele jako malware je na koncových stanicích okamžitě přesunut do karantény	Ano
Informace o trajektorii malware mezi stanicemi, karanténě, síťových komunikacích získávané a centralizované pro jednotlivé koncové stanice	Ano
IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	Ano
Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“	Ano
Možnost automatické i manuální klasifikace stanice jako „kritické“ se zohledněním v pravidlech, reportech apod.	Ano
Podpora „remediation“ modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	Ano
Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly	Ano
Podpora databází reputací adres v Internetu (Security Intelligence)	Ano
Funkce Next-Gen FW	
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	Ano
Podpora pasivního monitorování (TAP režim)	Ano
Podpora 802.1Q tagovaných rámců	Ano
Podporovaných aplikací	Min. 3000
Kategorie aplikací (nebezpečné, důležité, apod.)	Ano
URL kategorií	Min. 80
Kategorizovaných světových URL	Min. 280 milionů
Řízení přístupu k WWW - Web Usage Control (WCU)	Ano
Filtrace podle typů aplikací webových i ne-webových	Ano
Filtrace podle reputace serverů	Ano
SSL inspekce (dekrypce/enkrypce)	Ano
Security Intelligence database – známé uzly botnet sítí C&C	Ano
Security Intelligence database – známé adresy anonymních proxy, otevřených mail relay, apod.	Ano

Security Intelligence database – známé nebezpečné URL adresy a jmenné domény	Ano
Možnost integrovat vlastní reputační databáze	Ano
Podpora komunitních, otevřených standardů popisu apliací (OpenAppID)	Ano
Filtry mohou zohlednit roli a identitu uživatele	Ano
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	Ano
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	Ano
Řešení musí být schopné pasivního sběru informací o síťových zařízeních a zobrazení:	Typ zařízení Operační systém Dodavatel OS Použité síť. protokoly Použité síť. služby Otevřené porty síť. služeb Potenciální zranitelnosti
Přehled o síťových spojení má poskytovat minimálně tyto informace:	Čas startu a konce flow Akce (allow, deny,...) Důvod případného blokování Zdroj. a cíl. adresa Vstupní a výstupní zóna Vstupní a výstupní rozhraní Zdroj. a cíl. port Aplikační protokol IPS událost, pokud vznikne Riziková úroveň IPS události Použitá síťová aplikace Rizikovost aplikace „Business impact“ aplikace Množství přenesených dat
Správa	
Vzdálené správa přes grafické rozhraní bez nutnosti instalace zvláštního SW	Ano
Přístup ke GUI http/https protokolem	Ano
Možnost vzdáleného přístupu protokolem ssh přímo do FW	Ano
Možnost přístupu k textovým logům (syslog) přímo ve FW	Ano
Možnost lokální správy v případě nasazení jednoho FW (omezené možnosti nastavení)	Ano
Možnost centrální správy při nasazení více firewallů	Ano
Při centrální správě: možnost sdílených bezpečnostních politik	Ano
Při použití clusteru se spravuje pouze jeden logický prvek	Ano
Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu	Ano
Zobrazení logů a událostí v grafickém rozhraní správy	Ano
Možnost zaslání informace o TCP nebo UDP toku procházejícím firewallem (start a konec spojení, identifikovaný uživatel, přenesený objem dat, typ služby, délka trvání spojení) na TACACS nebo RADIUS server.	Ano
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	Ano
Funkce IPS a Next-Gen FW vyžadující dlouhodobější ukládání dat, korelace, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního systému (centrální dohledové konzole)	Ano
Centrální dohledová konzole musí být schopna dohledovat a spravovat	Ano

více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod.	
Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	Ano
Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole	Ano
Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	Ano
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu	Ano
Pro reporty lze definovat template definující formát a obsah reportu	Ano
Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu	Ano
V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N	Ano
Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů	Ano
Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.	Ano
Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	Ano
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.	Ano
Podpora posílání událostí formou syslog, email, SNMP na externí platformy	Ano
Podpora Event Streamer API (eStreamer) pro sdílení informací se externími systémy. Minimálně pro tyto SIEM:	ArcSight BMC Remedy Trustwave NetForensics Novell Sentinel Hawk Network Defense Q1Labs-QRadar Log Rhythm SIEM 2.0 LogLogic Splunk
Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay	Ano
Podpora JDBC API pro přístup z externích systémů k databázím centralizovaného managementu	Ano
Podpora řízeného přístupu podle rolí administrátorů	Ano
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	Ano
Možnost založit pro daný incident „ticket“ přímo v prostředí GUI managementu	Ano
Workflow pro předávání „ticketů“ mezi administrátory	Ano
Konkrétní bezpečnostní incident až na úrovni paketu lze přiložit k danému „tiketu“ pro další analýzu	Ano
Možnost definice politik pro sledování odpovídajících parametrů „zdraví“ na senzorech a centralizované konzoli (zařízení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)	Ano
Zákaznický definovatelný limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví“	Ano
Různé politiky pro sledování „zdraví“ lze aplikovat na různé senzory nebo centralizovanou konzoli	Ano

LAN L2 přepínač 24 portů PoE+

Síťový přepínač je zařízení, které umožňuje připojit koncové LAN klienty, bezdrátové přístupové body a ostatní zařízení v systému. Volitelná optická rozhraní slouží k agregaci dalších přepínačů školy.

LAN přepínač 24 portů PoE+ je inteligentní přepínač s 24x 10/100/1000Base-T porty s podporou PoE/PoE+ a 4x 1/10GE SPF porty.

LAN L2 přepínač 24 portů PoE+ (povinné parametry)	
<i>Bod</i>	<i>Popis</i>
1.	Zařízení musí být možné nainstalovat stojanu 19 ".
2.	Zařízení musí mít minimálně 24x RJ-45 10/100/1000Base-T rozhraní.
3.	Zařízení musí mít minimálně 4x 1/10 GE SFP/SFP+ rozhraní pro uplink/downlink.
4.	Zařízení musí podporovat stohování více zařízení stejného typu pomocí dedikovaných fyzických portů s propustností minimálně 80 Gb/s.
5.	RJ-45 rozhraní na zařízení musí podporovat funkci auto-MDIX.
6.	Zařízení musí podporovat PoE (IEEE 802.3af-2003) na všech RJ45 rozhraní.
7.	Zařízení musí podporovat PoE+ (IEEE 802.3at-2009) na alespoň polovině RJ45 rozhraní.
8.	Zařízení musí podporovat jumbo frame 9600 bajtů.
9.	Zařízení musí podporovat L2 protokoly: 802.1D, 802.1w, 802.1Q, 802.3ad.
10.	Zařízení musí podporovat minimálně 16000 MAC adres.
11.	Zařízení musí podporovat minimálně 4095 virtuálních sítí LAN (802.1Q).
12.	Zařízení musí podporovat L3 funkce: statické směrování, DHCP relay.
13.	Zařízení musí podporovat 802.1x na všech rozhraních.
14.	Zařízení musí podporovat autentizaci pomocí MAC adres prostřednictvím protokolu RADIUS.
15.	Propustnost zařízení musí být nejméně 128 Gb/s.
16.	Zařízení musí podporovat principy QoS dle 802.1p a DSCP a umožnit klasifikaci paketů dle zdrojových a cílových TCP/UDP portů (dle 4. vrstvy ISO/OSI).
17.	Zařízení musí podporovat zachytávání klientského provozu per port s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
18.	Zařízení musí podporovat funkci testování připojených UTP/STP kabelů – zjištění stavu jednotlivých párů a celkové délky kabelu.
19.	Zařízení musí podporovat funkci rozpoznávání klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
20.	Zařízení musí podporovat filtrování procházejících uživatelských dat dle zdrojových a cílových IP adres a UDP/TCP portů.
21.	Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
22.	Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
23.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje.
24.	Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

LAN L3 přepínač 24 portů

LAN L3 přepínač 24 portů je inteligentní přepínač s 24x 10/100/1000Base-T porty a 4x 10G SPF+ porty.

LAN přepínač (povinné parametry)	
<i>Bod</i>	<i>Popis</i>
1.	Zařízení musí být možné nainstalovat stojanu 19 ".
2.	Zařízení musí podporovat možnost fyzického stohování s propustností minimálně 80 Gb/s.
3.	Zařízení musí mít minimálně 24x RJ-45 10/100/1000Base-T rozhraní.
4.	Zařízení musí mít minimálně 4x 10G SFP+ rozhraní pro uplink/downlink.

5.	RJ-45 rozhraní na zařízení musí podporovat funkci auto-MDIX.
6.	Zařízení musí podporovat jumbo frame 9600 bajtů.
7.	Zařízení musí podporovat L2 protokoly: 802.1D, 802.1w, 802.1Q, 802.3ad.
8.	Zařízení musí podporovat L3 funkce a protokoly: statické směrování, dynamické směrování pomocí OSPFv2, DHCP relay/server a VRRP.
9.	Zařízení musí podporovat minimálně 16000 MAC adres.
10.	Zařízení musí podporovat minimálně 4095 virtuálních sítí LAN (802.1Q).
11.	Zařízení musí podporovat 802.1x na všech rozhraních.
12.	Zařízení musí podporovat autentizaci pomocí MAC adres prostřednictvím protokolu RADIUS.
13.	Propustnost zařízení musí být nejméně 128 Gb/s.
14.	Zařízení musí podporovat principy QoS dle 802.1p a DSCP a umožnit klasifikaci paketů dle zdrojových a cílových TCP/UDP portů (dle 4. vrstvy ISO/OSI).
15.	Zařízení musí podporovat zachytávání klientského provozu per port s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
16.	Zařízení musí podporovat funkci testování připojených UTP/STP kabelů – zjištění stavu jednotlivých párů a celkové délky kabelu.
17.	Zařízení musí podporovat funkci rozpoznávání klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
18.	Zařízení musí podporovat filtrování procházejících uživatelských dat dle zdrojových a cílových IP adres a UDP/TCP portů.
19.	Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
20.	Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
21.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje.
22.	Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

Bezdrátový přístupový bod

Bezdrátový přístupový bod je zařízení, které umožňuje klientům připojení do bezdrátové sítě.

Bezdrátový přístupový bod (povinné parametry)	
Bod	Popis
1.	Zařízení musí podporovat následující Wi-Fi standardy: 802.11b, 802.11g, 802.11a, 802.11n, 802.11ac Wave2.
2.	Zařízení musí být schopno pracovat současně v pásmu 2,4 GHz a 5 GHz.
3.	Zařízení musí v případě standardu 802.11ac podporovat šířku kanálu až 80MHz.
4.	Zařízení musí podporovat centrálně řízené automatické nastavení výběru kanálu a vysílacích výkonů a to včetně dynamické reakce na změnu prostředí.
5.	Zařízení musí podporovat 2x2:2 MU-MIMO a beamforming.
6.	Zařízení musí podporovat PoE napájení dle standardu 802.3af.
7.	Zařízení musí být dodáno s úchytem na stěnu a/nebo strop.
8.	Zařízení musí být uzamykatelné proti krádeži.
9.	Zařízení musí mít alespoň jedno 100/1000Base-T rozhraní.
10.	Zařízení musí umožnit konfiguraci minimálně 8 SSID na každém z 802.11 rádii.
11.	Zařízení musí podporovat následující bezpečnostní standardy: WEP, WPA2-PSK, WPA2-Enterprise s 802.1X autentizací.
12.	Zařízení musí podporovat šifrování AES.
13.	Zařízení musí podporovat ověřování PEAP (MSCHAPv2)
14.	Zařízení musí podporovat standardy 802.11r, 802.11k a 802.11v pro rychlý roaming klientů a rozložení zátěže mezi jednotlivými AP infrastruktury.
15.	Zařízení musí podporovat VLAN tagging (802.1Q) na jeho ethernetovém rozhraní.
16.	Zařízení podporuje principy QoS dle WMM, 802.1p a DSCP.
17.	Zařízení musí podporovat funkci rozpoznávání tříd klientských aplikací (dle 7. vrstvy

	ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
18.	Zařízení musí být schopné omezit šířku pásma pro každé jednotlivé SSID, pro každého z klientů a také dle rozpoznávaných tříd aplikací (dle 7. vrstvy ISO/OSI).
19.	Zařízení musí umožnit QoS klasifikaci paketů dle rozpoznávaných tříd aplikací (dle 7. vrstvy ISO/OSI) pomocí DSCP a 802.1p tagu.
20.	Zařízení musí podporovat BLE (Bluetooth Low Energy) dle specifikace Bluetooth 4.0.
21.	Zařízení musí umožňovat spektrální analýzu pro detekci zdrojů rušení (non-WiFi interference) v pásmu 2,4 a 5GHz s možností zobrazení diagramů v reálném čase. Funkce spektrální analýzy nesmí omezit základní funkci AP – poskytování datové konektivity klientským zařízením.
22.	Zařízení musí umožnit filtrování procházejících uživatelských dat dle cílových IP adres a/nebo UDP/TCP portů.
23.	Zařízení musí umožnit zakázat komunikaci vybraných klientů a to až dle rozpoznávaných tříd aplikací (dle 7. vrstvy ISO/OSI) a v případě http i dle DNS jména cílového serveru.
24.	Zařízení musí mít integrovanou funkci detekce a zastavení útoku na bezdrátovou infrastrukturu (wIDS/wIPS). Tato funkce musí být dostupná v reálném čase na všech kanálech (i neobsluhovaných) a nesmí omezit základní funkci AP – poskytování datové konektivity klientským zařízením.
25.	Zařízení musí podporovat zachytávání klientského provozu s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
26.	Zařízení musí podporovat L3 roaming klientských zařízení mezi různými subnety školy.
27.	Zařízení musí umožnit tunelovat SSID pro návštěvy přímo na bezpečnostní bránu v DMZ školy.
28.	Zařízení musí umožnit izolaci jednotlivých uživatelských zařízení tak, aby tato zařízení nemohla komunikovat mezi sebou (v rámci celého SSID školy).
29.	Zařízení musí být v případě nedostupnosti drátové ethernet konektivity schopné jako uplink dynamicky využít jedno ze svých rádii – mesh link přes některé z okolních AP.
30.	Zařízení musí umožnit spolu s Centrálním systémem řízení a monitorování sítě lokalizaci klientských zařízení v mapě jednotlivých podlaží na základě triangulace dle síly signálu.
31.	Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
32.	Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
33.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje.
34.	Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

Netflow analyzer

Monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent – systém pro monitorování a sběr provozně-lokačních údajů na úrovni rozhraní WAN i LAN a to bez negativních vlivů na zátěž a propustnost zařízení s kapacitou pro uchování dat po dobu minimálně 2 měsíců

Vlastnosti zařízení	
Rack-mount zařízení	maximální velikost 1 RU
Počet monitorovacích portů	min. 4 x 10/100/1000 Mbps (metalika - RJ45)
Management port	1x 10/100/1000 Mbps metalický
Minimální výkon na každém monitorovacím portu	1 480 000 paketů za sekundu
Možnost nastavení rychlosti monitorované linky 10/100/1000Mb/s	na metalických rozhraních
Jednoduchá instalace a nastavení	Ano

zařízení prostřednictvím příkazové řádky	
Pasivní zapojení bez vlivu na monitorovanou síť	zapojení pomocí TAPů
Nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích, nesmí docházet k ovlivňování chování sítě	Ano
Přesný nezávislý autonomní zdroj NetFlow statistik	podpora IPv4, IPv6, VLAN, MPLS, GRE
Podpora monitorování MAC adres	
Podpora standardizovaných protokolů pro výměnu dat o IP tocích	NetFlow v5, v9 - RFC3954, IPFIX
Detekce aplikací dle standardu NBAR2, monitorování a analýza HTTP provozu a VoIP statistik	Ano
Zabezpečená vzdálená správa, dohled a konfigurace	HTTPS (GUI), SSH
Vestavěný kolektor pro dočasné ukládání NetFlow statistik (zajištění redundance)	obsahuje uživatelsky definovaný dashboard, automatickou tvorbu reportů, detekci aktivních zařízení a detailní analytické možnosti
Úložná kapacita vestavěného kolektoru	min. 500 GB
Možnost doplnit o další moduly	např. behaviorální analýza, monitoring výkonu webových aplikací
Časová synchronizace zařízení proti centrálnímu zdroji času na síti	Ano
Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména	Ano
Správa uživatelů a přístupových práv na zařízení	Ano
Podpora vzdálené autentizace uživatelů	LDAP (Active Directory)
Plná zákaznická podpora v českém jazyce	Ano

Server do racku pro DNSSEC a RADIUS

Pro zajištění služeb DNSSEC A RADIUS serveru bude instalován HW server, na kterém bude spuštěn OS plně kompatibilní s Microsoft Windows Server a bude začleněn do stávající serverové infrastruktury jako člen domény. Server musí splňovat následující kritéria:

- Jednosocketový server o velikosti 1U včetně ramena pro vedení kabelů umožňujícího vysunutí zapnutého serveru z racku pro servisní účely
- 1 procesor (min 4 jádra, 8 vláken), min. 8MB cache dle passmark min. 9900 bodů
- Podpora paměti DDR-4 o frekvenci 2400MHz
- Možnost maximálního rozšíření na minimálně 64GB
- min. 32GB DDR-4
- Integrovaný RAID SAS řadič s podporou RAID 0/1/5/6/10 včetně 2GB flash paměti nebo baterií zálohovanou RAM paměti
- Min. 4 pozice pro 3.5" hot-swap SAS/SATA/SSD disky
- Min. 2x 600GB 10000 otáček hotplug disky
- Min. 4 porty USB 3.0
- Možnost rozšíření až 3-mi PCI-e kartami, z toho alespoň 2x PCIe Gen3 s x8 bus
- 2x 1Gbit LAN porty
- 1x Dedikovaný management port RJ-45
- Větráčky v serveru musí být redundantní

- 2x Napájecí zdroje s redundancí napájení 1+1, min. požadovaný výkon jednoho zdroje je 450W
- Zdroje musí splňovat požadavky na certifikaci energetické účinnosti, např. ECOS Consulting 80 Plus (min. PLATINIUM), popř. je nutno doložit, že mají při napětí 230V účinnost min. 94%
- Certifikace a podpora výrobce pro OS MS Windows Server 2012 R2 a výše
- Požadovaná 5 letá servisní podpora s opravou v místě instalace serveru a s garantovanou opravou následující pracovní den od nahlášení případné závady

Software pro Server

Požadavky na operační systém pro servery:

- Licence pro serverový operační systém pro provoz 1 operačního systému na 1 fyzickém serveru, který je součástí nabídky
- Možnost downgrade verze operačního systému
- Nevázanost licence na dodaném hardware
- Operační systém musí být plně kompatibilní s provozovanými aplikacemi a současnou serverovou infrastrukturou a Active Directory
- Součástí dodávky požadujeme také 40ks licencí pro přístup uživatelů k doméně (Active Directory) kompatibilní se stávající platformou školy

Ostatní služby infrastruktury a platformy

DNSSEC resolver – zřízení DNSSEC resolveru v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

AD, LDAP - využití stávající AD s databází uživatelů a skupin uživatelů v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

SSO - předpokládáme instalaci SSO (Single Sign On) utility jako součást bezpečnostní brány do standardního serverového operačního systému.

RADIUS - předpokládáme instalaci RADIUS serveru v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

Strukturovaná kabeláž pro wifi

Pro zajištění komunikace a současně napájení wifi sítě bude dobudována strukturovaná kabeláž ke všem 42 ks wifi access pointů. Kabeláž bude uložena v existujících lištách nebo budou instalovány nové lišty dle potřeby. Strukturovaná kabeláž bude zakončena ve stávajícím centrálním datovém rozvaděči na patch panelu. Požadovaná kabeláž je min. UTP Cat 5e. Součástí dodávky bude potřebný počet patchcordu do datového rozvaděče a další vybavení rozvaděče.

Učebna IVT velká

Pro zajištění potřebného technického zázemí v učebně IVT, bude osazeno 16 PC s příslušenstvím a provedena rekonstrukce datových a napájecích rozvodů k počítačům.

Celkem bude k dispozici 20 přípojných míst strukturované sítě a 20 zásuvek s 230V přivedených do jednotlivých lavic, kam budou instalovány PC s příslušenstvím.

PC s příslušenstvím

- Case minitower se zdrojem splňujícím ENERGY STAR® certified; EPEAT® Gold

- Procesor splňující výkon min. 12000 bodů passmark
- minimálně RAM 8GB DDR4
- minimálně HDD 256GB SSD
- Mechanika DVDRW
- Klávesnice, myš
- Výstup na monitor DP nebo HDMI
- Operační systém plně kompatibilní se současným systémem školy (aktuálně Windows)
- Monitor s úhlopříčkou min. 21,5 - 22" s rozlišením min. 1920 x 1080, IPS, odezvou 5ms, 250cd, rozhraním min. 1x HDMI
- Záruka 36 měsíců onsite NBD
- PC i monitor od stejného výrobce
- Kabel na propojení PC a LCD HDMI nebo DP
- balík kancelářských aplikací plně kompatibilní s OS a systémem školy (aktuálně MS Office)

Software pro správu třídy

Pro řízení jakékoliv výuky využívající PC bude implementován systém, který umožní sledovat, ovládat a řídit všechny počítače z učitelského pracoviště.

Správa Třídy

- Zapínání a vypínání všech počítačů ve třídě z počítače učitele.
- Dálkové "Odhlášení" všech počítačů.
- Zaslání dálkového "Přihlášení" na začátku vyučovací hodiny na všechny počítače studentů.
- Ponechání obrazovek studentů prázdných k získání pozornosti.
- Zablokování myši a klávesnic studentů při podávání pokynů.
- Rozmístění tak, aby počítač učitele představoval rozmístění fyzické třídy.
- Použití profilů jednotlivých učitelů k předložení prvků, které každý z učitelů potřebuje.
- Vizuelní odměňování jednotlivých studentů k povzbuzení snahy nebo chování.

Správa Tiskárny

- Brání studentům v tisku ve třídě.
- Omezení použití tiskárny počtem stránek.
- Před tiskem se požaduje schválení učitele.

Správa Zařízení

- Brání kopírování dat na nebo z USB úložiště a CDR / DVD zařízení.
- Brání tvorbě nových síťových připojení.

Registrace Studentů

- Požadavek na standardní a uživatelské informace od každého studenta na začátku vyučovací hodiny.
- Distribuce souborů na více počítačů jedním úkonem.
- Náhled na shrnutí pro studenta „njetím myši“ na ikonu studenta.
- Použití přizpůsobených úkonů pro jednotlivé studenty nebo skupiny studentů.

Rozdávání a Sbírání Souborů

- Transfer souborů na a ze zvoleného počítače jedním úkonem.
- Distribuce souborů na více počítačů jedním úkonem.
- Rozdávání a automatický sběr souborů s připojenými údaji každého studenta.

Pokyny v Reálném Čase (Režim Ukázky)

- Ukázání obrazovky učitele zvoleným studentům.
- Ukázání specifického počítače zvoleným studentům.
- Ukázání jen zvolené aplikace zvoleným studentům.
- Ukažte soubor Replay (předchozí nahrávka obrazovky) vybraným studentům, a výstup jak video soubor.
- Přehrání video souboru zvoleným studentům.

- Předložení prezentací optimalizovaných pro bezdrátové sítě.
- Zanechání záznamu Ukázky na počítači studenta k pozdějšímu prohlédnutí.
- Zvuková interakce se studenty během demonstrace tématu.
- Ukažte obrazovku studenta (Mód prohlížení)

Společné Prohlížení Internetu

Umožňuje učiteli otevírat zvolené webové stránky a synchronizovat je s prohlížečem na počítačích všech studentů. Když učitel naviguje webovými stránkami, počítače studentů ho následují.

Náhled na Obrazovky Studentů v Reálném Čase (Režim Monitorování)

- Monitorování celé třídy jedním pohledem.
- náhled přes studentské počítače v předem definovaných skupinách.
- Pokrytí dalšími informacemi včetně aktivní aplikace nebo aktivní webové stránky.
- Zoom pro optimalizované miniatury studentů s vysokým rozlišením.

Monitorování Instant Messengerů Sledování Klávesnic v Reálném Čase Měření a Kontrola Internetu

- Monitorování veškerého využití Internetu studenty.
- Náhled na všechny webové stránky otevřené v pozadí na všech počítačích.
- Otevírání a zavírání webových stránek na všech zvolených počítačích jedním úkonem.
- Záznam úplné historie využití Internetu pro třídu.
- Předchází přístupu na všechny nebo na omezené webové stránky.
- Povoluje pouze přístup na schválené webové stránky.

Monitorování Audia v Reálném Čase a Jazykové Nástroje Průzkumy Studentů

- Tvorba průzkumu s využitím předem dodaných nebo uživatelských odpovědí.
- Okamžité prohlédnutí všech odpovědí a shrnutí pro třídu.
- Dynamická tvorba skupin založená na odpovědích studentů.
- Publikace výsledků průzkumu všem studentům.

Zkoušení a kvízy Studentů

- Tvorba knihovny zdrojů a otázek, které lze sdílet.
- Tvorba libovolného počtu testů s využitím otázek z vaší knihovny.
- Nyní využívá 8 různých stylů otázek.
- Tvorba otázek se 2 až 4 možnými odpověďmi.
- Nastavení úrovně hodnocení zkoušek (např. přes 75% = hodnocení A).
- Sledování pokroku studentů a sledování správných nebo nesprávných odpovědí na otázky v reálném čase.
- Automatické známkování testů, aby byly výsledky dostupné okamžitě po jejich dokončení.
- Zobrazení výsledků jednotlivým studentům.
- Předložení výsledků (včetně zdůraznění správných odpovědí) třídě.
- Instalace návrháře testů na samostatném systému.

Technická konzole pro správce umožní:

- Monitorovat všechny počítače ve školní síti v jednom pohledu.
- Monitorovat využití aplikací a Internetu na počítači každého studenta.
- Přenášet soubory a složky do zvolených nebo všech počítačů.
- Seskupovat všechny počítače podle třídy / fyzického místa.
- Generovat úplné hardwarové systémové informace pro zvolené počítače.
- Generovat úplné informace o softwaru pro každý počítač včetně Hotfixů.
- Prohlížet a kontrolovat služby, procesy a aplikace běžící na každém PC.
- Poskytovat přímou technickou pomoc učitelům v libovolné třídě.
- Zapínat, vypínat, restartovat nebo se přihlásit na počítače ve třídě dálkově.
- Provádět výkonnou 1:1 dálkovou kontrolu PC na libovolně zvoleném počítači.

Zabezpečení

- Jedinečný "zabezpečovací klíč", aby byla vaše kopie nekompatibilní s ostatními kopiemi.
- Omezení konektivity pouze na systémy s odpovídající softwarovou licenci.
- Profily učitelů, z nichž každý umožňuje uživatelské úrovně funkčnosti dle požadavku.
- Použití AD profilů k omezení toho, kteří uživatelé smějí používat software učitele nebo technika.
- Použití AD profilů k vynucení konfigurací pro učitele a klienta.
- Kontrola přístupu a použití přenosných mediálních zařízení ve třídě.
- Automatická opakovaná aplikace omezení po restartování počítače studenta.

Deník Studenta

- Podrobné údaje o vyučovací hodině a cíle.
- Poznámky učitele.
- Poznámky jednotlivých studentů.
- Snímky obrazovky z prezentace (a vysvětlení).
- Virtuální obrazovky bílé tabule.
- Výsledky zkoušek jednotlivých studentů.
- URL webových stránek používaných během vyučovací hodiny.
- Kopie přepisů libovolných chatů třídy.

Učebna IVT malá

Software pro správu třídy – viz. učebna velká - identické

Montážní a implementační práce - pro splnění standardu konektivity škol

Hardware

- Doprava na místo
- Fyzická montáž do datového rozvaděče
 - Prostor připraví zákazník
 - Popis jednotlivých dodaných prvků – popisky, štítky
 - Fotodokumentace
- Zapojení, oživení do sítě zákazníka
 - Konfigurace MGMT IP adres
 - Aktualizace dle doporučení výrobce na poslední verze FW, BIOS
 - Doložení dle výrobce o aktuálnosti
- Vyvázání kabeláže
 - Popis kabelů
 - Dokumentace + fotodokumentace k zapojení
- Dodavatel zajistí všechny potřebné kabely vč. PDU
 - LAN
 - Opt.
 - Power
 - Jiné
- Instalace žákovských PC a implementace do stávající infrastruktury
- Implementace systému řízení výuky v učebnách
- Fyzická likvidace odpadu, odvoz

Software

- Virtualizační platforma
- Instalace operačních systémů
- Konfigurace všech potřebných rolí dle standardu konektivity do škol včetně RADIUS serveru
- Konfigurace operačních systémů, rolí dle doporučení výrobce
- Konfigurace MGMT reportů
 - Reportování stavů HW
 - RAID, FAN, PSU, CPU, RAM, HDD
 - Poštovní server dodá zákazník

- Instalace jednotlivých serverů / zařízení dle standartu konektivity do škol

Na WAN připojení k internetu:

- plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)
- validující DNSSEC resolver na straně školy
- podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)
- síťové zařízení podporující rate limiting, antispoofting, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality
- zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirovou kontrolou stahovaného obsahu
- možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků
- podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online
- u software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu.

Povinné minimální bezpečnostní parametry projektu (bez ohledu typ síťového připojení):

- Monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent (např. NetFlow) – systém pro monitorování a sběr provozně-lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízení s kapacitou pro uchování dat po dobu minimálně 2 měsíců
- Povinné řešení systému správy uživatelů (Identity Management), tj. centrální databáze identit (LDAP, AD, apod.) a její využití pro autentizaci uživatelů (žáci i učitelé) za účelem bezpečného a auditovatelného přístupu k síti, resp. síťovým službám.
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel

V oblasti pevné LAN musí projekt splňovat následující minimální parametry:

- Minimální konektivita stanic a dalších koncových zařízení zařízení 100Mbit/s full duplex
- Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,...)
- Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s full duplex
- Páteřní rozvody mezi budovami v areálu realizovány prostřednictvím optických, metalických vláken popř. bezdrátovými spoji v licencovaném pásmu (povolení ČTÚ)
- Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3)¹ s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,...

V případě řešení bezdrátových sítí (wifi) pak musí projekt naplňovat následující minimální parametry:

- Podpora mechanismu izolace klientů

¹ Požadavek se týká prvků, přes které je veden veškerý provoz, resp. jde o centrální prvky. Podružné přepínače (chodbové, ořezbové) musí splňovat pouze požadavek na neblokující architekturu přepínacího subsystému

- Návrh topologie wifi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou ve v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů
- Centralizovaná architektura správy wifi sítě (centrální řadič, centrální management, tzv. thin access pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení)
- Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD ...)
- Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz
- Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu

Všechny body výše vychází z daného standartu, který je nutno dodržet.

- Plná integrace nového řešení do stávající infrastruktury ICT školy

Dokumentace

- Kompletní dokumentace vč. Fotodokumentace HW zapojení
 - Zálohy konfigurací na přiloženém CD
 - Obálka vč. Uživatelských jmen a hesel
 - Seznam vytvořených uživatelů vč. Vzdálených přístupů
 - Kompletní dokumentace nastavení jednotlivých rolí dle standartu
- Výstupní protokol, který prověří fungování daného standartu
- Provedení site survey wifi pokrytí – zakres do dodaných půdorysů
- Veškeré licence v tištěné i elektronické formě na přiloženém CD
- Předávací protokol o předání dokumentací

Předání

1. Zaškolení obsluhy, předání informací o celém řešení
2. Testovací provoz, který ověří funkčnost (cca 1 měsíc)

Technická specifikace

Centrální systém řízení a monitorování sítě

Vyžadován je centrální systém řízení a monitorování všech níže poptávaných komponent a to prostřednictvím jednotného webového rozhraní.

Centrální systém řízení a monitorování sítě (povinné parametry)	
<i>Bod</i>	<i>Popis</i>
1.	Centrální systém řízení a monitorování sítě musí umožnit zabezpečenou vzdálenou správu, plnou konfiguraci a monitorování současně pro všechny poptávané komponenty sítě (bezpečnostní brány, přepínače, bezdrátové přístupové body a systém správy mobilních zařízení) a to prostřednictvím jednotného integrovaného webového rozhraní.
2.	Systém musí zajistit automatickou aktualizaci softwaru a instalaci bezpečnostních záplat do všech zařízení v systému a to v uživatelsky definovaném čase.
3.	Systém musí umožnit změny konfigurace více zařízení stejného typu současně a konfigurace nových zařízení pomocí šablon.
4.	Centrální systém řízení a monitorování sítě musí podporovat následující metody autentizace klientů LAN a WLAN infrastruktury: - 802.1X ověření na základě údajů interní databáze systému - 802.1X ověření prostřednictvím RADIUS serveru - Webová autentizace na základě údajů interní databáze systému - Webová autentizace prostřednictvím RADIUS nebo LDAP serveru - Webová autentizace prostřednictvím Facebook účtu - Možnost vytvoření vlastního webového portálu
5.	Centrální systém řízení a monitorování sítě musí být schopen zobrazit všechny klientská zařízení připojená k síti školy během minimálně posledních 10 dnů. Výpis by měl obsahovat minimálně následující informace: - Uživatelské jméno - IP a MAC adresa zařízení - Objem uživatelem / zařízením přenesených dat za dané období s rozpadem na jednotlivé rozpoznané aplikace
6.	Systém musí být schopen zobrazit seznam top žáků / studentů, kteří za dané období ve školní síti přenesli nejvíce dat.
7.	Systém musí být schopen zobrazit polohu a stav všech zařízení v systému v geografické mapě a také graficky zobrazit reálnou fyzickou topologii sítě školy.
8.	Systém musí být schopen zobrazit polohu všech klientských zařízení v závislosti na způsobu jejich připojení a to buď přímo v plánech jednotlivých podlaží, v geografické mapě nebo v kontextu portu příslušného LAN přepínače.
9.	Systém musí být provozován v režimu vysoké dostupnosti.
10.	Základní konektivita a přístup do Internetu musí být pro klienty zachován i v případě, že je Centrální systém řízení a monitorování sítě dočasně nedostupný.
11.	I v případě nedostupnosti Centrálního systému řízení a monitorování sítě musí být zajištěna možnost autentizace a autorizace nových klientů LAN i WLAN infrastruktury prostřednictvím 802.1x protokolu pomocí RADIUS.
12.	Systém musí umožnit rozdělení administrátorů do skupin s různými právy přístupu.
13.	Pro autentizaci administrátora přistupujícího přes webové rozhraní musí systém podporovat minimálně RADIUS protokol, SAML a dvoufaktorovou autentizaci.
14.	Systém musí být schopen odesílat správcům emailové zprávy o důležitých systémových událostech.
15.	Systém musí být schopen odesílat zprávy na vzdálený SYSLOG server.
16.	Systém musí podporovat SNMP protokol pro vzdálenou správu a monitorování.
17.	Systém musí podporovat XML API pro integraci s navazujícími systémy školy poskytující informace o připojených komponentách sítě a také klientských zařízeních.
18.	Systém musí sledovat změny konfigurace systému a zahrnutých síťových komponent – Informace musí minimálně obsahovat:

	- položku konfigurace - uživatelské jméno administrátora, který změnu provedl - novou hodnotu proměnné, v které ke změně došlo
19	Systém musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
20	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně všech aktualizací softwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Systém musí být v době prodeje výrobcem plně podporován a na žádnou jeho část nesmí být vyhlášeno ukončení prodeje.

Next-Gen Firewall, IPS a anti-malware

Zařízení určené k ochraně síťového prostředí před hrozbami na bázi pokročilých útoků. Kromě funkcí tzv. Nex.Gen FW (typicky chápáné jako aplikační a identity-based FW) je schopno provádět inspekci provozu s detekcí a ochranou před útoky na úrovni síťového provozu. V oblasti ochrany proti malware je možno aktivovat analýzu souborů včetně dynamické analýzy (tzv. sandboxing) i ukládání nebezpečných souborů do karantény. Zařízení lze použít i pro URL filtraci na úrovni kategorií, konkrétních URL či podle reputace serverů v Internetu.

Požadovaná funkcionality/vlastnost	Způsob splnění požadované funkcionality/vlastnosti
Výkon a funkcionality firewallu	
Formát zařízení	Appliance, 1RU
Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management, standardně osazených	1
Minimální počet 1Gb 10/100/1000 BaseT Ethernet	8
Podporovaný počet současně otevřených spojení stavový FW/aplikační FW	Min.100000M/100000
Rychlost vytváření nových spojení přes stavový FW	Min. 10K/s
Propustnost stavového firewallu (multiprotokolový režim)	Min. 500 Mbps
Propustnost aplikačního FW (next-gen FW) – (top parametry)	Min. 450 Mbps
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (top parametry)	Min. 250 Mbps
Propustnost aplikačního FW (next-gen FW) – (transakční profil, 450B průměrná velikost paketu)	Min. 180 Mbps
Propustnost aplikačního FW + IPS (next-gen FW, IPS) - (transakční profil, 450B průměrná velikost paketu)	Min. 115 Mbps
VPN propustnost	Min. 175 Mbps
Současný počet VPN spojení (IPSec/SSL)	Min. 100
Podpora L2 (transparentního) módu s podporou NAT a PAT	Ano
Podpora L3 (routovaného) módu s podporou NAT a PAT	Ano
Podporovaný počet VLAN	Min. 50
Podpora stateful failover	active/standby
Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru	Ano
Cluster firewallů se musí vzhledem k další infrastruktuře tvářet jako jeden prvek s podporou LACP	Ano
Cluster podporuje stavovou inspekci nesymetrického provozu vstupující do různých firewallů clusteru	Ano
Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podporou LACP	Ano
Podpora virtuálních bezpečnostních kontextů (virtuálních firewallů) s možností rozšíření až na 250 kontextů	Ano
Dynamické směrování - podpora alespoň RIP, OSPF, BGP	Ano
Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	Ano
Podpora Policy based Routing	Ano
Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do	Ano

paketů, fragmentací, apod.	
Podpora filtrace IPv4, IPv6	Ano
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	Ano
Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích	Ano
Podpora inspekce IPv6 provozu	Ano
Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	Ano
Podpora NAT64 a DNS64	Ano
Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód případně pro řízení přístupu podle uživatelské identity, typu aplikace, apod.	Ano
Funkce QoS až na úrovni jednotlivých toků (flow) s podporou LLQ	Ano
Možnost rozšíření o funkce NextGen FW	Ano
Možnost rozšíření o funkce NextGen IPS	Ano
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	Ano
Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech	Ano
API rozhraní pro sdílení kontextových informací s dalšími systémy	Ano
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	Ano
Funkce IPS a anti-malware	
Možnost definovat typ provozu předávaný k inspekci do IPS	Ano
Podpora také IDS režimu – pasivního monitorování (TAP režim)	Ano
Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)	Ano
Možnost obejít IPS funkce při zahlcení nebo nedostupnosti	Ano
Podpora 802.1Q tagovaných rámců	Ano
Podpora různých IPS politik pro různé typy provozu	Ano
Inspekce pro IPv4 i IPv6	Ano
Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému	Ano
IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií	Ano
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	Ano
Podpora aplikace pro psaní zákaznických filtrů	Ano
Podpora importu komunitních filtrů/signatur Snort	Ano
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	Ano
IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	Ano
IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C	Ano
IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii	Ano
Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	Ano
Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku	Ano
Funkce pro kontrolu DLP (např. pomocí Snort preprocesorů)	Ano

Podpora vrstev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	Ano
Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	Ano
Možnost definice uživatelské vrstvy politik	Ano
Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik	Ano
Různé politiky lze sdílet a aplikovat na různé senzory	Ano
Podpora aktivní inline ochrany před malware s detekcí známých nebo podezřelých malware nezávislé na aktuálních databázích AV dodavatelů	Ano
Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry	Ano
Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat	Ano
Zobrazení trajektorie malware – pohyb, mutace, přenosy v síti mezi stanicemi přímo v GUI centralizované konzole	Ano
Možnost ochrany před malware až do úrovně koncových stanic s centralizovanou správou bezpečnostních politik, blacklistů pro aplikace, řízení spouštění aplikací, přesun malware do karantény, blacklistů pro síťovou komunikaci, apod.	Ano
Retrospektivní ochrana koncových stanic (chytře telefony), stanice s Windows, Mac OS – pokud je později SW kód rozpoznán v operačním centru dodavatele jako malware je na koncových stanicích okamžitě přesunut do karantény	Ano
Informace o trajektorii malware mezi stanicemi, karanténě, síťových komunikacích získávané a centralizované pro jednotlivé koncové stanice	Ano
IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	Ano
Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“	Ano
Možnost automatické i manuální klasifikace stanice jako „kritické“ se zohledněním v pravidlech, reportech apod.	Ano
Podpora „remediation“ modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	Ano
Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly	Ano
Podpora databází reputací adres v Internetu (Security Intelligence)	Ano
Funkce Next-Gen FW	
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	Ano
Podpora pasivního monitorování (TAP režim)	Ano
Podpora 802.1Q tagovaných rámců	Ano
Podporovaných aplikací	Min. 3000
Kategorie aplikací (nebezpečné, důležité, apod.)	Ano
URL kategorií	Min. 80
Kategorizovaných světových URL	Min. 280 milionů
Řízení přístupu k WWW - Web Usage Control (WCU)	Ano
Filtrace podle typů aplikací webových i ne-webových	Ano
Filtrace podle reputace serverů	Ano
SSL inspekce (dekrypce/enkrypce)	Ano
Security Intelligence database – známé uzly botnet sítí C&C	Ano
Security Intelligence database – známé adresy anonymních proxy, otevřených mail relay, apod.	Ano
Security Intelligence database – známé nebezpečné URL adresy a jmenné domény	Ano
Možnost integrovat vlastní reputační databáze	Ano

Podpora komunitních, otevřených standardů popisu apliací (OpenAppID)	Ano
Filtry mohou zohlednit roli a identitu uživatele	Ano
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	Ano
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	Ano
Řešení musí být schopné pasivního sběru informací o síťových zařízeních a zobrazení:	Typ zařízení Operační systém Dodavatel OS Použité síť. protokoly Použité síť. služby Otevřené porty síť. služeb Potenciální zranitelnosti
Přehled o síťových spojení má poskytovat minimálně tyto informace:	Čas startu a konce flow Akce (allow, deny,...) Důvod případného blokování Zdroj. a cíl. adresa Vstupní a výstupní zóna Vstupní a výstupní rozhraní Zdroj. a cíl. port Aplikační protokol IPS událost, pokud vznikne Riziková úroveň IPS události Použitá síťová aplikace Rizikovost aplikace „Business impact“ aplikace Množství přenesených dat
Správa	
Vzdálené správa přes grafické rozhraní bez nutnosti instalace zvláštního SW	Ano
Přístup ke GUI http/https protokolem	Ano
Možnost vzdáleného přístupu protokolem ssh přímo do FW	Ano
Možnost přístupu k textovým logům (syslog) přímo ve FW	Ano
Možnost lokální správy v případě nasazení jednoho FW (omezené možnosti nastavení)	Ano
Možnost centrální správy při nasazení více firewallů	Ano
Při centrální správě: možnost sdílených bezpečnostních politik	Ano
Při použití clusteru se spravuje pouze jeden logický prvek	Ano
Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu	Ano
Zobrazení logů a událostí v grafickém rozhraní správy	Ano
Možnost zaslání informace o TCP nebo UDP toku procházejícím firewallem (start a konec spojení, identifikovaný uživatel, přenesený objem dat, typ služby, délka trvání spojení) na TACACS nebo RADIUS server.	Ano
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	Ano
Funkce IPS a Next-Gen FW vyžadující dlouhodobější ukládání dat, korelace, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního systému (centrální dohledové konzole)	Ano
Centrální dohledová konzole musí být schopna dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod.	Ano
Centrální dohledová konzole musí být schopna poskytovat aktualizaci a	Ano

distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	
Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole	Ano
Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	Ano
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu	Ano
Pro reporty lze definovat template definující formát a obsah reportu	Ano
Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu	Ano
V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N	Ano
Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů	Ano
Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.	Ano
Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	Ano
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.	Ano
Podpora posílání událostí formou syslog, email, SNMP na externí platformy	Ano
Podpora Event Streamer API (eStreamer) pro sdílení informací se externími systémy. Minimálně pro tyto SIEM:	ArcSight BMC Remedy Trustwave NetForensics Novell Sentinel Hawk Network Defense Q1Labs-QRadar Log Rhythm SIEM 2.0 LogLogic Splunk
Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay	Ano
Podpora JDBC API pro přístup z externích systémů k databázím centralizovaného managementu	Ano
Podpora řízeného přístupu podle rolí administrátorů	Ano
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	Ano
Možnost založit pro daný incident „ticket“ přímo v prostředí GUI managementu	Ano
Workflow pro předávání „ticketů“ mezi administrátory	Ano
Konkrétní bezpečnostní incident až na úrovni paketu lze přiložit k danému „tiketu“ pro další analýzu	Ano
Možnost definice politik pro sledování odpovídajících parametrů „zdraví“ na senzorech a centralizované konzoli (zařízení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)	Ano
Zákaznický definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví“	Ano
Různé politiky pro sledování „zdraví“ lze aplikovat na různé senzory nebo centralizovanou konzoli	Ano

LAN L2 přepínač 48 portů

Síťový přepínač je zařízení, které umožňuje připojit koncové LAN klienty, bezdrátové přístupové body a ostatní zařízení v systému. Volitelná optická rozhraní slouží k agregaci dalších přepínačů školy.

LAN přepínač 48 portů je inteligentní přepínač s 48x 10/100/1000Base-T porty a 4x 1/10GE SPF porty.

LAN L2 přepínač 48 portů (povinné parametry)	
Bod	Popis
1.	Zařízení musí být možné nainstalovat stojanu 19 ".
2.	Zařízení musí mít minimálně 48x RJ-45 10/100/1000Base-T rozhraní.
3.	Zařízení musí mít minimálně 4x 1/10 GE SFP/SFP+ rozhraní pro uplink/downlink.
4.	Zařízení musí podporovat stohování více zařízení stejného typu pomocí dedikovaných fyzických portů s propustností minimálně 80 Gb/s.
5.	RJ-45 rozhraní na zařízení musí podporovat funkci auto-MDIX.
6.	Zařízení musí podporovat jumbo frame 9600 bajtů.
7.	Zařízení musí podporovat L2 protokoly: 802.1D, 802.1w, 802.1Q, 802.3ad.
8.	Zařízení musí podporovat minimálně 16000 MAC adres.
9.	Zařízení musí podporovat minimálně 4095 virtuálních sítí LAN (802.1Q).
10.	Zařízení musí podporovat L3 funkce: statické směrování, DHCP relay.
11.	Zařízení musí podporovat 802.1x na všech rozhraních.
12.	Zařízení musí podporovat autentizaci pomocí MAC adres prostřednictvím protokolu RADIUS.
13.	Propustnost zařízení musí být nejméně 128 Gb/s.
14.	Zařízení musí podporovat principy QoS dle 802.1p a DSCP a umožnit klasifikaci paketů dle zdrojových a cílových TCP/UDP portů (dle 4. vrstvy ISO/OSI).
15.	Zařízení musí podporovat zachytávání klientského provozu per port s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
16.	Zařízení musí podporovat funkci testování připojených UTP/STP kabelů – zjištění stavu jednotlivých párů a celkové délky kabelu.
17.	Zařízení musí podporovat funkci rozpoznávání klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
18.	Zařízení musí podporovat filtrování procházejících uživatelských dat dle zdrojových a cílových IP adres a UDP/TCP portů.
19.	Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
20.	Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
21.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje.
22.	Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

LAN L2 přepínač 24 portů

Síťový přepínač je zařízení, které umožňuje připojit koncové LAN klienty, bezdrátové přístupové body a ostatní zařízení v systému. Volitelná optická rozhraní slouží k agregaci dalších přepínačů školy.

LAN přepínač 24 portů je inteligentní přepínač s 24x 10/100/1000Base-T porty a 4x 1/10GE SPF porty.

LAN L2 přepínač 24 portů (povinné parametry)	
Bod	Popis
1.	Zařízení musí být možné nainstalovat stojanu 19 ".

2.	Zařízení musí mít minimálně 24x RJ-45 10/100/1000Base-T rozhraní.
3.	Zařízení musí mít minimálně 4x 1/10 GE SFP/SFP+ rozhraní pro uplink/downlink.
4.	Zařízení musí podporovat stohování více zařízení stejného typu pomocí dedikovaných fyzických portů s propustností minimálně 80 Gb/s.
5.	RJ-45 rozhraní na zařízení musí podporovat funkci auto-MDIX.
6.	Zařízení musí podporovat jumbo frame 9600 bajtů.
7.	Zařízení musí podporovat L2 protokoly: 802.1D, 802.1w, 802.1Q, 802.3ad.
8.	Zařízení musí podporovat minimálně 16000 MAC adres.
9.	Zařízení musí podporovat minimálně 4095 virtuálních sítí LAN (802.1Q).
10.	Zařízení musí podporovat L3 funkce: statické směrování, DHCP relay.
11.	Zařízení musí podporovat 802.1x na všech rozhraních.
12.	Zařízení musí podporovat autentizaci pomocí MAC adres prostřednictvím protokolu RADIUS.
13.	Propustnost zařízení musí být nejméně 128 Gb/s.
14.	Zařízení musí podporovat principy QoS dle 802.1p a DSCP a umožnit klasifikaci paketů dle zdrojových a cílových TCP/UDP portů (dle 4. vrstvy ISO/OSI).
15.	Zařízení musí podporovat zachytávání klientského provozu per port s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
16.	Zařízení musí podporovat funkci testování připojených UTP/STP kabelů – zjištění stavu jednotlivých párů a celkové délky kabelu.
17.	Zařízení musí podporovat funkci rozpoznávání klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
18.	Zařízení musí podporovat filtrování procházejících uživatelských dat dle zdrojových a cílových IP adres a UDP/TCP portů.
19.	Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
20.	Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
21.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje.
22.	Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

LAN L2 přepínač 24 portů PoE+

Síťový přepínač je zařízení, které umožňuje připojit koncové LAN klienty, bezdrátové přístupové body a ostatní zařízení v systému. Volitelná optická rozhraní slouží k agregaci dalších přepínačů školy.

LAN přepínač 24 portů PoE+ je inteligentní přepínač s 24x 10/100/1000Base-T porty s podporou PoE/PoE+ a 4x 1/10GE SPF porty.

LAN L2 přepínač 24 portů PoE+ (povinné parametry)	
Bod	Popis
1.	Zařízení musí být možné nainstalovat stojanu 19 ".
2.	Zařízení musí mít minimálně 24x RJ-45 10/100/1000Base-T rozhraní.
3.	Zařízení musí mít minimálně 4x 1/10 GE SFP/SFP+ rozhraní pro uplink/downlink.
4.	Zařízení musí podporovat stohování více zařízení stejného typu pomocí dedikovaných fyzických portů s propustností minimálně 80 Gb/s.
5.	RJ-45 rozhraní na zařízení musí podporovat funkci auto-MDIX.
6.	Zařízení musí podporovat PoE (IEEE 802.3af-2003) na všech RJ45 rozhraních.
7.	Zařízení musí podporovat PoE+ (IEEE 802.3at-2009) na alespoň polovině RJ45 rozhraní.
8.	Zařízení musí podporovat jumbo frame 9600 bajtů.
9.	Zařízení musí podporovat L2 protokoly: 802.1D, 802.1w, 802.1Q, 802.3ad.
10.	Zařízení musí podporovat minimálně 16000 MAC adres.

11.	Zařízení musí podporovat minimálně 4095 virtuálních sítí LAN (802.1Q).
12.	Zařízení musí podporovat L3 funkce: statické směrování, DHCP relay.
13.	Zařízení musí podporovat 802.1x na všech rozhraních.
14.	Zařízení musí podporovat autentizaci pomocí MAC adres prostřednictvím protokolu RADIUS.
15.	Propustnost zařízení musí být nejméně 128 Gb/s.
16.	Zařízení musí podporovat principy QoS dle 802.1p a DSCP a umožnit klasifikaci paketů dle zdrojových a cílových TCP/UDP portů (dle 4. vrstvy ISO/OSI).
17.	Zařízení musí podporovat zachytávání klientského provozu per port s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
18.	Zařízení musí podporovat funkci testování připojených UTP/STP kabelů – zjištění stavu jednotlivých párů a celkové délky kabelu.
19.	Zařízení musí podporovat funkci rozpoznávání klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
20.	Zařízení musí podporovat filtrování procházejících uživatelských dat dle zdrojových a cílových IP adres a UDP/TCP portů.
21.	Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
22.	Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
23.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje.
24.	Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

LAN L3 přepínač 24 portů

LAN L3 přepínač 24 portů je inteligentní přepínač s 24x 10/100/1000Base-T porty a 4x 10G SFP+ porty.

LAN přepínač (povinné parametry)	
Bod	Popis
1.	Zařízení musí být možné nainstalovat stojanu 19".
2.	Zařízení musí podporovat možnost fyzického stohování s propustností minimálně 80 Gb/s.
3.	Zařízení musí mít minimálně 24x RJ-45 10/100/1000Base-T rozhraní.
4.	Zařízení musí mít minimálně 4x 10G SFP+ rozhraní pro uplink/downlink.
5.	RJ-45 rozhraní na zařízení musí podporovat funkci auto-MDIX.
6.	Zařízení musí podporovat jumbo frame 9600 bajtů.
7.	Zařízení musí podporovat L2 protokoly: 802.1D, 802.1w, 802.1Q, 802.3ad.
8.	Zařízení musí podporovat L3 funkce a protokoly: statické směrování, dynamické směrování pomocí OSPFv2, DHCP relay/server a VRRP.
9.	Zařízení musí podporovat minimálně 16000 MAC adres.
10.	Zařízení musí podporovat minimálně 4095 virtuálních sítí LAN (802.1Q).
11.	Zařízení musí podporovat 802.1x na všech rozhraních.
12.	Zařízení musí podporovat autentizaci pomocí MAC adres prostřednictvím protokolu RADIUS.
13.	Propustnost zařízení musí být nejméně 128 Gb/s.
14.	Zařízení musí podporovat principy QoS dle 802.1p a DSCP a umožnit klasifikaci paketů dle zdrojových a cílových TCP/UDP portů (dle 4. vrstvy ISO/OSI).
15.	Zařízení musí podporovat zachytávání klientského provozu per port s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
16.	Zařízení musí podporovat funkci testování připojených UTP/STP kabelů – zjištění stavu jednotlivých párů a celkové délky kabelu.
17.	Zařízení musí podporovat funkci rozpoznávání klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
18.	Zařízení musí podporovat filtrování procházejících uživatelských dat dle zdrojových a

	cílových IP adres a UDP/TCP portů.
19.	Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
20.	Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
21.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje.
22.	Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

Bezdrátový přístupový bod

Bezdrátový přístupový bod je zařízení, které umožňuje klientům připojení do bezdrátové sítě.

Bezdrátový přístupový bod (povinné parametry)	
Bod	Popis
1.	Zařízení musí podporovat následující Wi-Fi standardy: 802.11b, 802.11g, 802.11a, 802.11n, 802.11ac Wave2.
2.	Zařízení musí být schopno pracovat současně v pásmu 2,4 GHz a 5 GHz.
3.	Zařízení musí v případě standardu 802.11ac podporovat šířku kanálu až 80MHz.
4.	Zařízení musí podporovat centrálně řízené automatické nastavení výběru kanálu a vysílacích výkonů a to včetně dynamické reakce na změnu prostředí.
5.	Zařízení musí podporovat 2x2:2 MU-MIMO a beamforming.
6.	Zařízení musí podporovat PoE napájení dle standardu 802.3af.
7.	Zařízení musí být dodáno s úchytem na stěnu a/nebo strop.
8.	Zařízení musí být uzamykatelné proti krádeži.
9.	Zařízení musí mít alespoň jedno 100/1000Base-T rozhraní.
10.	Zařízení musí umožnit konfiguraci minimálně 8 SSID na každém z 802.11 rádii.
11.	Zařízení musí podporovat následující bezpečnostní standardy: WEP, WPA2-PSK, WPA2-Enterprise s 802.1X autentizací.
12.	Zařízení musí podporovat šifrování AES.
13.	Zařízení musí podporovat ověřování PEAP (MSCHAPv2)
14.	Zařízení musí podporovat standardy 802.11r, 802.11k a 802.11v pro rychlý roaming klientů a rozložení zátěže mezi jednotlivými AP infrastruktury.
15.	Zařízení musí podporovat VLAN tagging (802.1Q) na jeho ethernetovém rozhraní.
16.	Zařízení podporuje principy QoS dle WMM, 802.1p a DSCP.
17.	Zařízení musí podporovat funkci rozpoznávání tříd klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
18.	Zařízení musí být schopné omezit šířku pásma pro každé jednotlivé SSID, pro každého z klientů a také dle rozpoznávaných tříd aplikací (dle 7. vrstvy ISO/OSI).
19.	Zařízení musí umožnit QoS klasifikaci paketů dle rozpoznávaných tříd aplikací (dle 7. vrstvy ISO/OSI) pomocí DSCP a 802.1p tagu.
20.	Zařízení musí podporovat BLE (Bluetooth Low Energy) dle specifikace Bluetooth 4.0.
21.	Zařízení musí umožňovat spektrální analýzu pro detekci zdrojů rušení (non-WiFi interference) v pásmu 2,4 a 5GHz s možností zobrazení diagramů v reálném čase. Funkce spektrální analýzy nesmí omezit základní funkci AP – poskytování datové konektivity klientským zařízením.
22.	Zařízení musí umožnit filtrování procházejících uživatelských dat dle cílových IP adres a/nebo UDP/TCP portů.
23.	Zařízení musí umožnit zakázat komunikaci vybraných klientů a to až dle rozpoznávaných tříd aplikací (dle 7. vrstvy ISO/OSI) a v případě http i dle DNS jména cílového serveru.
24.	Zařízení musí mít integrovanou funkci detekce a zastavení útoku na bezdrátovou infrastrukturu (wIDS/wIPS). Tato funkce musí být dostupná v reálném čase na všech kanálech (i neobsluhovaných) a nesmí omezit základní funkci AP – poskytování datové konektivity klientským zařízením.
25.	Zařízení musí podporovat zachytávání klientského provozu s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených

	klientů.
26.	Zařízení musí podporovat L3 roaming klientských zařízení mezi různými subnety školy.
27.	Zařízení musí umožnit tunelovat SSID pro návštěvy přímo na bezpečnostní bránu v DMZ školy.
28.	Zařízení musí umožnit izolaci jednotlivých uživatelských zařízení tak, aby tato zařízení nemohla komunikovat mezi sebou (v rámci celého SSID školy).
29.	Zařízení musí být v případě nedostupnosti drátové ethernet konektivity schopné jako uplink dynamicky využít jedno ze svých rádii – mesh link přes některé z okolních AP.
30.	Zařízení musí umožnit spolu s Centrálním systémem řízení a monitorování sítě lokalizaci klientských zařízení v mapě jednotlivých podlaží na základě triangulace dle síly signálu.
31.	Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
32.	Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
33.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje.
34.	Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

Netflow analyzer

Monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent – systém pro monitorování a sběr provozně-lokačních údajů na úrovni rozhraní WAN i LAN a to bez negativních vlivů na zátěž a propustnost zařízení s kapacitou pro uchování dat po dobu minimálně 2 měsíců

Vlastnosti zařízení	
Rack-mount zařízení	maximální velikost 1 RU
Počet monitorovacích portů	min. 4 x 10/100/1000 Mbps (metalika - RJ45)
Management port	1x 10/100/1000 Mbps metalický
Minimální výkon na každém monitorovacím portu	1 480 000 paketů za sekundu
Možnost nastavení rychlosti monitorované linky 10/100/1000Mb/s	na metalických rozhraních
Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky	Ano
Pasivní zapojení bez vlivu na monitorovanou síť	zapojení pomocí TAPů
Nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích, nesmí docházet k ovlivňování chování sítě	Ano
Přesný nezávislý autonomní zdroj NetFlow statistik	podpora IPv4, IPv6, VLAN, MPLS, GRE
Podpora monitorování MAC adres	
Podpora standardizovaných protokolů pro výměnu dat o IP tocích	NetFlow v5, v9 - RFC3954, IPFIX
Detekce aplikací dle standardu NBAR2, monitorování a analýza HTTP provozu a VoIP statistik	Ano
Zabezpečená vzdálená správa, dohled a konfigurace	HTTPS (GUI), SSH
Vestavěný kolektor pro dočasné ukládání NetFlow statistik (zajištění redundance)	obsahuje uživatelsky definovaný dashboard, automatickou tvorbu reportů, detekci aktivních zařízení a

	detailní analytické možnosti
Úložná kapacita vestavěného kolektoru	min. 500 GB
Možnost doplnit o další moduly	např. behaviorální analýza, monitoring výkonu webových aplikací
Časová synchronizace zařízení proti centrálnímu zdroji času na síti	Ano
Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména	Ano
Správa uživatelů a přístupových práv na zařízení	Ano
Podpora vzdálené autentizace uživatelů	LDAP (Active Directory)
Plná zákaznická podpora v českém jazyce	Ano

Server do racku pro DNSSEC a RADIUS

Pro zajištění služeb DNSSEC A RADIUS serveru bude instalován HW server, na kterém bude spuštěn OS plně kompatibilní s Microsoft Windows Server a bude začleněn do stávající serverové infrastruktury jako člen domény. Server musí splňovat následující kritéria:

- Jednosocketový server o velikosti 1U včetně ramena pro vedení kabelů umožňujícího vysunutí zapnutého serveru z racku pro servisní účely
- 1 procesor (min 4 jádra, 8 vláken), min. 8MB cache dle passmark min. 9900 bodů
- Podpora paměti DDR-4 o frekvenci 2400MHz
- Možnost maximálního rozšíření na minimálně 64GB
- min. 32GB DDR-4
- Integrovaný RAID SAS řadič s podporou RAID 0/1/5/6/10 včetně 2GB flash paměti nebo baterií zálohovanou RAM paměti
- Min. 4 pozice pro 3.5" hot-swap SAS/SATA/SSD disky
- Min. 2x 600GB 10000 otáček hotplug disky
- Min. 4 porty USB 3.0
- Možnost rozšíření až 3-mi PCI-e kartami, z toho alespoň 2x PCIe Gen3 s x8 bus
- 2x 1Gbit LAN porty
- 1x Dedikovaný management port RJ-45
- Větráčky v serveru musí být redundantní
- 2x Napájecí zdroje s redundancí napájení 1+1, min. požadovaný výkon jednoho zdroje je 450W
- Zdroje musí splňovat požadavky na certifikaci energetické účinnosti, např. ECOS Consulting 80 Plus (min. PLATINIUM), popř. je nutno doložit, že mají při napětí 230V účinnost min. 94%
- Certifikace a podpora výrobce pro OS MS Windows Server 2012 R2 a výše
- Požadovaná 5 letá servisní podpora s opravou v místě instalace serveru a s garantovanou opravou následující pracovní den od nahlášení případné závady

Software pro Server

Požadavky na operační systém pro servery:

- Licence pro serverový operační systém pro provoz 1 operačního systému na 1 fyzickém serveru, který je součástí nabídky
- Možnost downgrade verze operačního systému
- Nevázanost licence na dodaném hardware

- Operační systém musí být plně kompatibilní s provozovanými aplikacemi a současnou serverovou infrastrukturou a Active Directory

Server do racku pro hypervizor a Active Directory

Pro zajištění provozu všech aplikací bude instalován HW server, na kterém bude spuštěn hypervizor umožňující provoz jednotlivých virtuálních serverů. Server musí splňovat následující kritéria:

- Dvousocketový server o velikosti 2U včetně ramena pro vedení kabelů umožňujícího vysunutí zapnutého serveru z racku pro servisní účely
- 2 procesory (min 8 jader každý), podpora HT, každý minimálně o výkonu 11600 bodů dle passmark
- Podpora pamětí DDR-4 o frekvenci 2666MHz
- Možnost maximálního rozšíření na minimálně 24x DIMM
- Min. 64GB DDR-4 2666MHz
- Server musí umožňovat odstavení vadného ranku paměti za chodu a alokování na jiný bank anebo požadujeme dvojnásobný počet DIMM modulů o stejné kapacitě a využití memory mirroring
- Integrovaný SAS RAID řadič s podporou RAID 0/1/5/10 včetně min. 2GB flash paměti nebo baterií zálohovanou RAM paměti
- Min. 8 pozic pro 2,5" hot-swap SAS/SATA/SSD disky, možnost rozšířit na 28 pozic
- Min. 2x 1,2TB 12G SAS, 2,5", 10krpm disky
- Min. 2x 2TB 12G SAS 7,2krpm 2,5", Business Critical disky
- Disky musí mít rámečky vybaveny indikátorem proti vytažení disku, na kterém se provádí datové operace nebo musí být takový disk proti případnému vytažení blokován
- Slot pro interní flash kartu (SD, microSD) pro boot hypervizoru
- Min. 4 porty USB 3.0, z toho minimálně 1x interní
- Možnost rozšíření až šesti PCI-e kartami, z toho alespoň 3x PCIe Gen3 s x16 bus
- 6x 1Gbit LAN porty nezabírající rozšiřující PCIe sloty
- 1x vyhrazený port LAN pro správu (10/100/1000 Mb/s),
- Integrovaný řadič vzdálené správy kompatibilní s IPMI 2.0, přesměrování KVM po LAN, časově neomezená licence
- Větráčky v serveru musí být vyměnitelné za provozu a redundantní
- 2x Napájecí zdroje s redundancí napájení 1+1, max. výkon jednoho zdroje je 450W
- Zdroje musí podporovat řízení spotřeby CPU instalovaných v poptávaných serverech
- Zdroje musí splňovat požadavky na certifikaci energetické účinnosti, např. ECOS Consulting 80 Plus (min. PLATINIUM), popř. je nutno doložit, že mají při napětí 230V účinnost min. 94%
- Požadovaná 5 letá servisní podpora s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady

Software pro Server pro hypervizor a Active Directory

Požadavky na operační systém pro virtualizované servery:

- Licence pro serverový operační systém pro provoz 4 virtuálních serverů na 1 fyzickém serveru, který je součástí nabídky
- Operační systém musí být plně kompatibilní s provozovanými aplikacemi a Active Directory
- Součástí dodávky požadujeme 90 licencí pro klientská zařízení (počítače, notebooky, tablety) a 40 licencí pro uživatele pro přístup k Active Directory serveru
- Součástí dodávky požadujeme 40 licencí pro uživatele pro vzdálený přístup (RDS) k serveru plně kompatibilního s operačním systémem

- Součástí dodávky požadujeme licence pro 40 uživatelů poštovního serveru plně kompatibilního s operačním systémem a MS Exchange

Hypervizor

Požadavky na použitý hypervisor:

- Hypervizor musí podporovat provoz virtuálních serverů s OS Windows Server 2008 až 2016, RedHat Enterprise Linux (RHEL), Debian GNU/Linux a FreeBSD.

Záložní zdroj UPS pro server

Jako záložní zdroj napětí, pro případ výpadku elektrické energie, požadujeme UPS s následujícími vlastnostmi:

- Záložní zdroj do racku, výška max. 2U
- Smart Line interactive
- Vstupní napětí 230V, konektor IEC-320 C14
- Výstupní výkon min. 1000W, min. 4x IEC 320 C13
- Včetně komunikační karty a managementu SNMP

Záložní zdroj UPS pro aktivní prvky

Jako záložní zdroj napětí, pro případ výpadku elektrické energie, požadujeme UPS s následujícími vlastnostmi:

- Záložní zdroj do racku, výška max. 2U
- Smart Line interactive
- Vstupní napětí 230V, konektor IEC-320 C14
- Výstupní výkon min. 500W, min. 4x IEC 320 C13

NAS uložení pro zálohování

Požadavky na NAS uložení pro zálohování:

- Min. 4 diskové uložení
- Podpora 3,5" SATA disků
- Osazení min. 2x4TB disky, SATA 7200rpm, 64MB určené pro NAS
- Podpora RAID 0,1,5,6
- Min. 2x 1Gbps LAN port
- Min. 4GB RAM
- Podpora iSCSI
- Dálkové ovládání

Zálohovací SW

Požadavky na software pro zálohování serveru:

- Licence na zálohovací SW, která umožní zálohování virtuálních serverů
- Zálohování pro 4 virtuální servery nebo licence na 2x CPU - ve variantě zálohování i pro poštovní server kompatibilní s MS Exchange
- Zálohování a obnova virtuálních serverů, jednotlivých souborů
- Zálohování a obnova objektů Active Directory

- Integrovaná deduplikace komprese a šifrování dat
- Podpora zálohování na externí diskové uložení NAS
- Rychlá obnova pomocí bootovacího CD ISO
- Včetně základní podpory a ochrany upgrade min. 1 rok

Bezpečnostní software pro stanice a server

Licence na 3 roky pro 3x server a 100x pracovní stanice / mobilní zařízení

Produkt

- Podpora operačních systémů MS:
 - Windows XP a vyšší,
 - Windows server 2003 a vyšší.
- Antivirový klient pro systémy:
 - Windows, Linux, macOS, Android.
- Real-Time ochrana před všemi typy PUA a malwaru:
 - viry, červy, trojskými koňmi (backdoor, adware, spyware, rootkit, bootkit, ransomware...).
- Správa zařízení pro Windows, macOS a Linux umožňující blokaci externích zařízení a médií s podporou whitelistování dle:
 - výrobce, modelu nebo sériového čísla,
 - uživatelů nebo skupin (např. administrátorů) v AD,
 - lokálního času.
- Možnost blokace přístupu na definované weby nebo skupiny webů dle kategorií s možností whitelistování dle přihlášeného uživatele / skupiny v AD nebo času.
- Lokální anti-spam s úspěšností detekce 99 % a vyšší.
- Lokální anti-spam s možností definování důvěryhodných a spamových adres.
- Nativní 64-bitové jádro.
- Ochrana komunikace e-mailovými protokoly:
 - POP3, POP3S, IMAP, IMAPS, HTTP, MAPI.

Technologie

- Antivirus, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb.
- Personální firewall pro zabránění neautorizovanému přístupu k zařízení se schopností automatického přebírání pravidel z brány Windows Firewall.
- HIPS pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení.
- Aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb.
- Systém pro blokaci exploitů využívajících zero-day zranitelností, jenž pokrývá nejpoužívanější vektory útoku:
 - síťové protokoly, Flash Player, Javu, Microsoft Office, webové prohlížeče, e-mailové klienty, PDF čtečky...
- Systém pro detekci malwaru již na síťové úrovni poskytující ochranu i před zneužitím zranitelností na síťové vrstvě.
- Pokročilá kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování.
- Možnost zapnutí detekce potenciálně nechtěných, zneužitelných a podezřelých aplikací.
- Cloud kontrola souborů pro urychlení skenování pracujících na základě reputace souborů.
- Kontrola souborů v průběhu stahování pro snížení celkového času kontroly.
- Funkce pro ochranu před skriptovými útoky využívajícími:
 - JavaScript,
 - Windows PowerShell,
 - Windows Script Host.
- Funkce ochrany proti zapojení do botnetu pracujících s detekcí síťových signatur.
- Ochrana před síťovými útoky skenující síťovou komunikaci a blokující pokusy o zneužití zranitelností na síťové úrovni.
- Kontrola s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací.
- Lokální i cloudový sandbox.
- Speciální modul behaviorální analýzy pro detekce nových typů ransomwaru.
- Systém reputace a cache pro získání informací o závadnosti stahovaných souborů a URL adres.
- Cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur.
- Technologie pro detekci rootkitů obvykle se maskujících za součásti operačního systému.

- Skenr firmwaru BIOSu a UEFI.
- Skenování souborů v cloudu (OneDrive & Office 365).

Ostatní

- Podpora Microsoft NAP.
- Možnost odložení aktualizací a běžných klientských úloh pro lepší využití systémových prostředků.
- Provádění kontrol při nečinnosti zařízení:
 - vypnuté obrazovce, aktivním spojiči obrazovky, uzamčení počítače, odhlášení uživatele.
- Ovládání bezpečnostního programu pomocí Příkazového řádku.
- Podpora ochrany na IPv6.
- Možnost řízení šířky pásma pro stahování aktualizací.
- HIPS s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory.
- Možnost vrácení i odložení aktualizací modulů.
- Možnost instalovat plnohodnotné antivirové řešení na virtuální stanici/server.
- Modulární instalace.
- Automatická synchronizace bezpečnostních produktů v clusteru.
- Zabezpečení pro VMware vShield a NSX.
- Možnost importu/exportu nastavení.
- Prezentační režim umožňující potlačení méně důležitých upozornění při práci v celoobrazovkovém režimu aplikace.
- Možnost tvorby výjimek na procesy.
- Ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému.
- Možnost vzdáleného definování akce při připojení výměnných médií (kontrolovat, nekontrolovat, nechat na uživateli).
- Možnost využití sdílené reputační cache v rámci lokální sítě (umožňuje přeskočení skenování stejných souborů, které již byly zkontrolovány na jiném zařízení a tím výrazně zrychlit kontrolu celé sítě).
- Duální aktualizací profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (vhodné pro cestující uživatele s notebooky).
- Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS...).
- Možnost odesílání e-mailových upozornění a událostí přímo z klienta.
- Integrovaný komplexní diagnostický nástroj umožňující řešit problémy s infiltrací, jakožto i jiné softwarové a hardwarové nekorektní chování (obsahuje informace procesech, službách, síťových připojeních, ovladačích, problémových položkách v registrech...).
- Upozornění při připojení k nezabezpečené bezdrátové síti nebo síti se slabým zabezpečením, jejíž šifrování lze snadno prolomit.
- Využití Microsoft Antimalware Scan Interface (AMSI) pro kontrolu skriptů (PowerShell, wscript.exe a cscript.exe).
- Podpora Protected Services – službu produktu je možné chránit proti nechtěné modifikaci standardní součástí operačního systému.
- Podpora odebíratele obrazovky pro zrakově postižené.

Vzdálená správa

- Webová konzole.
- Možnost instalace na Windows i Linux.
- Předpřipravená virtual appliance pro virtuální prostředí VMware, Microsoft Hyper-V a Microsoft Azure, Oracle Virtual Box.
- Možnost konfigurace linuxové virtual appliance přes uživatelsky přívětivé webové rozhraní Webmin.
- Nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta a bezpečnostního programu.
- Offline uplatňování politik a spouštění úloh při výskytu definované události (například: odpojení od sítě při nalezení škodlivého kódu).
- Vzdálená správa v cloudu výrobce bezpečnostního produktu (správa bez vlastního serveru).
- Server/proxy architektura pro síťovou pružnost – snížení zátěže při stahování aktualizací detekčních modulů výrobce.
- Administrace v nejpoužívanějších jazycích (s možností dynamického přepínání) včetně češtiny.
- Vzdálená instalace a aktualizace bezpečnostního programu.
- Široké možnosti konfigurace oprávnění administrátorů (například možnost správy pouze části infrastruktury, které konkrétnímu administrátorovi podléhá).
- Podpora mirroru.
- Zabezpečení přístupu administrátorů do vzdálené správy pomocí 2FA.

- Možnost přihlašování administrátorů pomocí doménových účtů.
- Instalace a odinstalace aplikací 3. stran.
- Vyčítání informací o verzích softwaru 3. stran.
- Vzdálená aktivace bezpečnostního programu.
- Jedna konzole vzdálené správy pro konfiguraci bezpečnostních produktů na mobilní zařízení (MDM), desktopové systémy, souborové servery, mail servery i ochranu gateway.
- Export/import konfigurace bezpečnostního programu z klienta.
- Jednorázové testování virtuálních stanic i bez nainstalovaného bezpečnostního programu.
- Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce.
- Vzdálené získání zachyceného škodlivého souboru z klienta.
- Jednoduchá aktualizace serveru pro vzdálenou správu pomocí webového rozhraní správcovské konzole.
- Detekce nespravovaných (rizikových) počítačů komunikujících na síti.
- Vzdálené odebrání licence klientovi.
- Odeslání zprávy na jakékoli zařízení (počítač, mobilní zařízení...), které se následně zobrazí uživateli na obrazovce.
- Vzdálená odinstalace antivirového řešení 3. strany.
- Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku.
- Vzdálený restart/vypnutí cílového klienta.
- U mobilních zařízení dostupné vzdálené:
 - nalezení, uzamknutí, odemknutí, siréna, vymazání obsahu, rozšířený reset do továrního nastavení.
- Možnost navazování úloh pro zautomatizování činností bez zásahu administrátora. Například: Automatická detekce antiviru 3. strany > automatická odinstalace > automatický zpožděný restart pro možnost uložení rozdělané práce klienta > automatická instalace nového bezpečnostního programu > automatická aktivace nového bezpečnostního programu.
- Koncovému klientovi může administrátor vzdáleně ukončit proces, zablokovat síťového spojení, odstranit klíče z registru, odstranit DNS záznam, odstranit soubor, odstranit naplánovanou úlohu, zastavit a odinstalovat službu...
- Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny.
- Dynamicky se měnící Dashboard s interaktivními přehledy pro okamžité zjištění stavu spravované sítě.
- Responzivní design webové konzole vzdálené správy umožňující management klientů pomocí mobilních zařízení (telefonu/tabletu).
- Automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů (například: 5 % všech počítačů / 50 klientů hlásí problémy).
- Podpora SNMP Trap, Syslogu a qRadar SIEM.
- Podpora instalace skriptem - *.bat, *.sh, *.ini (GPO, SSCM...).
- Rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu.
- Reportování stavu antiviru 3. strany, včetně vzdálené správy (instalace/odinstalace aplikací, vynucování aktualizací OS...) klientů chráněných jinými bezpečnostními programy.
- Schopnost zaslat reporty a upozornění na e-mail.
- Přidání zařízení do vzdálené správy pomocí:
 - synchronizace s Active Directory,
 - ruční přidání pomocí dle IP adresy nebo názvu zařízení,
 - proprietární technologie pro vyhledání nechráněných zařízení v síti.
- Několikaminutové automatické zablokování (IP adresy) přístupu do konzole vzdálené správy po několika neúspěšných pokusech o přihlášení.
- Možnost vyčítat informace o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty...).
- Schopnost zaslat reporty a upozornění na e-mail.
- Přehled o všech souborech z celé sítě, které byly odeslány na servery vendora pro hloubkovou analýzu z důvodu možného výskytu škodlivého kódu.
- Vzdálené ovládání endpointů prostřednictvím RMM (Remote Monitoring and Management) nástrojů:
 - Connectwise Automate,
 - Autotask AEM,
 - SolarWinds N-Central,
 - Kaseya,
 - ConnectWise Manage,

- ConnctetWise Automate (LabTech),
- Autotask,
- Tigerpaw,
- Salesforce.
- MDM vzdálené správy podporuje operační systémy:
– Android, iOS.

Provozní

- Dodavatel musí mít pro případy rozšíření zabezpečení také řešení pro:
– MDM, DLP, 2FA, šifrování, EDR.
- Technická podpora v češtině.
- Cena za prodloužení licence nižší než cena nové licence.

Ostatní služby infrastruktury a platformy

DNSSEC resolver – zřízení DNSSEC resolveru v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

AD, LDAP - využití stávající AD s databází uživatelů a skupin uživatelů v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

SSO - předpokládáme instalaci SSO (Single Sign On) utility jako součást bezpečnostní brány do standardního serverového operačního systému.

RADIUS - předpokládáme instalaci RADIUS serveru v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

Strukturovaná kabeláž

Pro zajištění vnitřní konektivity ve všech prostorách školy budou vybudovány nové rozvody strukturované kabeláže. Do každé třídy budou přivedeny 2 segmenty strukturované kabeláže, do každého kabinetu a sborovny bude přivedeno 6 segmentů strukturované kabeláže UTP min. Cat 5e. Celkem bude instalováno 130 segmentů plus propojení rozvaděčů mezi sebou vždy min. dvěma kabely.

Pro zajištění komunikace a současně napájení wifi sítě bude dobudována strukturovaná kabeláž ke všem 40 ks wifi access pointů. Požadovaná kabeláž je min. UTP Cat 5e.

Veškeré uvedené rozvody budou instalovány v plastových lištách a zakončeny vždy dvojzásuvkou RJ-45 v popsanych místnostech. Součástí budou i potřebné rozvaděčové skříně včetně potřebného vybavení (patchpanely, vyvazovací panely, propojovací kabely UTP) v odpovídajícím množství. Součástí bude i projektová dokumentace skutečného provedení.

Učebna ICT 1

Pro zajištění potřebného technického zázemí v učebně ICT, bude osazeno 30 PC s příslušenstvím a provedena rekonstrukce datových a napájecích rozvodů k počítačům.

Celkem bude k dispozici 30 přípojných míst strukturované sítě a 30 zásuvek s 230V přivedených do jednotlivých lavic, kam budou instalovány PC s příslušenstvím.

PC s příslušenstvím

- Case minitower se zdrojem splňujícím ENERGY STAR® certified; EPEAT® Gold
- Procesor splňující výkon min. 12000 bodů passmark

- minimálně RAM 8GB DDR4
- minimálně HDD 256GB SSD
- Mechanika DVDRW
- Klávesnice, myš
- Výstup na monitor DP nebo HDMI
- Operační systém plně kompatibilní se současným systémem školy (aktuálně Windows)
- Monitor s úhlopříčkou minimálně 21,5 - 22" s rozlišením minimálně 1920 x 1080, IPS, odezvou 5ms, 250cd, rozhraním min. 1x HDMI
- Záruka 36 měsíců onsite NBD
- PC i monitor od stejného výrobce
- Kabel na propojení PC a LCD HDMI nebo DP
- balík kancelářských aplikací plně kompatibilní s OS a systémem školy (aktuálně MS Office)

Učebna ICT 2

Pro zajištění potřebného technického zázemí v učebně ICT, bude osazeno 30 PC s příslušenstvím a provedena rekonstrukce datových a napájecích rozvodů k počítačům.

Celkem bude k dispozici 30 přípojných míst strukturované sítě a 30 zásuvek s 230V přivedených do jednotlivých lavic, kam budou instalovány PC s příslušenstvím.

PC s příslušenstvím

- Case minitower se zdrojem splňujícím ENERGY STAR® certified; EPEAT® Gold
- Procesor splňující výkon min. 12000 bodů passmark
- minimálně RAM 8GB DDR4
- minimálně HDD 256GB SSD
- Mechanika DVDRW
- Klávesnice, myš
- Výstup na monitor DP nebo HDMI
- Operační systém plně kompatibilní se současným systémem školy (aktuálně Windows)
- Monitor s úhlopříčkou min. 21,5 - 22" s rozlišením min. 1920 x 1080, IPS, odezvou 5ms, 250cd, rozhraním min. 1x HDMI
- Záruka 36 měsíců onsite NBD
- PC i monitor od stejného výrobce
- Kabel na propojení PC a LCD HDMI nebo DP
- balík kancelářských aplikací plně kompatibilní s OS a systémem školy (aktuálně MS Office)

Montážní a implementační práce - pro splnění standardu konektivity škol

Hardware

- Doprava na místo
- Fyzická montáž do datového rozvaděče
 - Prostor připraví zákazník
 - Popis jednotlivých dodaných prvků – popisky, štítky
 - Fotodokumentace
- Zapojení, oživení do sítě zákazníka
 - Konfigurace MGMT IP adres
 - Aktualizace dle doporučení výrobce na poslední verze FW, BIOS
 - Doložení dle výrobce o aktuálnosti

- Vyvázání kabeláže
 - Popis kabelů
 - Dokumentace + fotodokumentace k zapojení
- Dodavatel zajistí všechny potřebné kabely vč. PDU
 - LAN
 - Opt.
 - Power
 - Jiné
- Instalace žákovských PC a implementace do stávající infrastruktury nebo k novému serveru Active directory
- Fyzická likvidace odpadu, odvoz

Software

- Virtualizační platforma
- Instalace operačních systémů
- Konfigurace všech potřebných rolí dle standartu konektivity do škol včetně RADIUS serveru
- Konfigurace operačních systémů, rolí dle doporučení výrobce
- Konfigurace MGMT reportů
 - Reportování stavů HW
 - RAID, FAN, PSU, CPU, RAM, HDD
 - Poštovní server dodá zákazník
- Instalace jednotlivých serverů / zařízení dle standartu konektivity do škol

Na WAN připojení k internetu:

- plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)
- validující DNSSEC resolver na straně školy
- podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)
- síťové zařízení podporující rate limiting, antispoofting, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality
- zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirovou kontrolou stahovaného obsahu
- možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků
- podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online
- u software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu.

Povinné minimální bezpečnostní parametry projektu (bez ohledu typ síťového připojení):

- Monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent (např. NetFlow) – systém pro monitorování a sběr provozně-lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízení s kapacitou pro uchování dat po dobu minimálně 2 měsíců
- Povinné řešení systému správy uživatelů (Identity Management), tj. centrální databáze identit (LDAP, AD, apod.) a její využití pro autentizaci uživatelů (žáci i učitelé) za účelem bezpečného a auditovatelného přístupu k síti, resp. síťovým službám.
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel

V oblasti pevné LAN musí projekt splňovat následující minimální parametry:

- Minimální konektivita stanic a dalších koncových zařízení 100Mbit/s full duplex
- Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,...)
- Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s full duplex
- Páteřní rozvody mezi budovami v areálu realizovány prostřednictvím optických, metalických vláken popř. bezdrátovými spoji v licencovaném pásmu (povolení ČTÚ)
- Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3)¹ s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,...

V případě řešení bezdrátových sítí (wifi) pak musí projekt naplňovat následující minimální parametry:

- Podpora mechanismu izolace klientů
- Návrh topologie wifi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou ve v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů
- Centralizovaná architektura správy wifi sítě (centrální řadič, centrální management, tzv. thin access pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravovanými access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení)
- Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD ...)
- Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz
- Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu

Všechny body výše vychází z daného standardu, který je nutno dodržet.

- Plná integrace nového řešení do stávající infrastruktury ICT školy
- Implementace bezpečnostního softwaru

Dokumentace

- Kompletní dokumentace vč. Fotodokumentace HW zapojení
 - Zálohy konfigurací na přiloženém CD
 - Obálka vč. Uživatelských jmen a hesel
 - Seznam vytvořených uživatelů vč. Vzdálených přístupů
 - Kompletní dokumentace nastavení jednotlivých rolí dle standardu
- Výstupní protokol, který prověří fungování daného standardu
- Provedení site survey wifi pokrytí – zakres do dodaných půdorysů
- Veškeré licence v tištěné i elektronické formě na přiloženém CD
- Předávací protokol o předání dokumentací

Předání

1. Zaškolení obsluhy, předání informací o celém řešení
2. Testovací provoz, který ověří funkčnost (cca 1 měsíc)

¹ Požadavek se týká prvků, přes které je veden veškerý provoz, resp. jde o centrální prvky. Podružné přepínače (chodbové, očebnové) musí splňovat pouze požadavek na neblokující architekturu přepínacího subsystému

Technická specifikace

Centrální systém řízení a monitorování sítě

Vyžadován je centrální systém řízení a monitorování všech níže poptávaných komponent a to prostřednictvím jednotného webového rozhraní.

Centrální systém řízení a monitorování sítě (povinné parametry)	
<i>Bod</i>	<i>Popis</i>
1.	Centrální systém řízení a monitorování sítě musí umožnit zabezpečenou vzdálenou správu, plnou konfiguraci a monitorování současně pro všechny poptávané komponenty sítě (bezpečnostní brány, prepínače, bezdrátové přístupové body a systém správy mobilních zařízení) a to prostřednictvím jednotného integrovaného webového rozhraní.
2.	Systém musí zajistit automatickou aktualizaci softwaru a instalaci bezpečnostních záplat do všech zařízení v systému a to v uživatelsky definovaném čase.
3.	Systém musí umožnit změny konfigurace více zařízení stejného typu současně a konfigurace nových zařízení pomocí šablon.
4.	Centrální systém řízení a monitorování sítě musí podporovat následující metody autentizace klientů LAN a WLAN infrastruktury: - 802.1X ověření na základě údajů interní databáze systému - 802.1X ověření prostřednictvím RADIUS serveru - Webová autentizace na základě údajů interní databáze systému - Webová autentizace prostřednictvím RADIUS nebo LDAP serveru - Webová autentizace prostřednictvím Facebook účtu - Možnost vytvoření vlastního webového portálu
5.	Centrální systém řízení a monitorování sítě musí být schopen zobrazit všechny klientská zařízení připojená k síti školy během minimálně posledních 10 dnů. Výpis by měl obsahovat minimálně následující informace: - Uživatelské jméno - IP a MAC adresa zařízení - Objem uživatelem / zařízením přenesených dat za dané období s rozpadem na jednotlivé rozpoznané aplikace
6.	Systém musí být schopen zobrazit seznam top žáků / studentů, kteří za dané období ve školní síti přenesli nejvíce dat.
7.	Systém musí být schopen zobrazit polohu a stav všech zařízení v systému v geografické mapě a také graficky zobrazit reálnou fyzickou topologii sítě školy.
8.	Systém musí být schopen zobrazit polohu všech klientských zařízení v závislosti na způsobu jejich připojení a to buď přímo v plánech jednotlivých podlaží, v geografické mapě nebo v kontextu portu příslušného LAN prepínače.
9.	Systém musí být provozován v režimu vysoké dostupnosti.
10.	Základní konektivita a přístup do Internetu musí být pro klienty zachován i v případě, že je Centrální systém řízení a monitorování sítě dočasně nedostupný.
11.	I v případě nedostupnosti Centrálního systému řízení a monitorování sítě musí být zajištěna možnost autentizace a autorizace nových klientů LAN i WLAN infrastruktury prostřednictvím 802.1x protokolu pomocí RADIUS.
12.	Systém musí umožnit rozdělení administrátorů do skupin s různými právy přístupu.
13.	Pro autentizaci administrátora přistupujícího přes webové rozhraní musí systém podporovat minimálně RADIUS protokol, SAML a dvoufaktorovou autentizaci.
14.	Systém musí být schopen odesílat správcům emailové zprávy o důležitých systémových událostech.
15.	Systém musí být schopen odesílat zprávy na vzdálený SYSLOG server.
16.	Systém musí podporovat SNMP protokol pro vzdálenou správu a monitorování.
17.	Systém musí podporovat XML API pro integraci s navazujícími systémy školy poskytující informace o připojených komponentách sítě a také klientských zařízeních.

18.	Systém musí sledovat změny konfigurace systému a zahrnutých síťových komponent – Informace musí minimálně obsahovat: - položku konfigurace - uživatelské jméno administrátora, který změnu provedl - novou hodnotu proměnné, v které ke změně došlo
19.	Systém musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
20.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně všech aktualizací softwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Systém musí být v době prodeje výrobcem plně podporován a na žádnou jeho část nesmí být vyhlášeno ukončení prodeje.

LAN L2 přepínač 24 portů PoE+

Síťový přepínač je zařízení, které umožňuje připojit koncové LAN klienty, bezdrátové přístupové body a ostatní zařízení v systému. Volitelná optická rozhraní slouží k agregaci dalších přepínačů školy.

LAN přepínač 24 portů PoE+ je inteligentní přepínač s 24x 10/100/1000Base-T porty s podporou PoE/PoE+ a 4x 1/10GE SPF porty.

LAN L2 přepínač 24 portů PoE+ (povinné parametry)	
Bod	Popis
1.	Zařízení musí být možné nainstalovat stojanu 19 ".
2.	Zařízení musí mít minimálně 24x RJ-45 10/100/1000Base-T rozhraní.
3.	Zařízení musí mít minimálně 4x 1/10 GE SFP/SFP+ rozhraní pro uplink/downlink.
4.	Zařízení musí podporovat stohování více zařízení stejného typu pomocí dedikovaných fyzických portů s propustností minimálně 80 Gb/s.
5.	RJ-45 rozhraní na zařízení musí podporovat funkci auto-MDIX.
6.	Zařízení musí podporovat PoE (IEEE 802.3af-2003) na všech RJ45 rozhraní.
7.	Zařízení musí podporovat PoE+ (IEEE 802.3at-2009) na alespoň polovině RJ45 rozhraní.
8.	Zařízení musí podporovat jumbo frame 9600 bajtů.
9.	Zařízení musí podporovat L2 protokoly: 802.1D, 802.1w, 802.1Q, 802.3ad.
10.	Zařízení musí podporovat minimálně 16000 MAC adres.
11.	Zařízení musí podporovat minimálně 4095 virtuálních sítí LAN (802.1Q).
12.	Zařízení musí podporovat L3 funkce: statické směrování, DHCP relay.
13.	Zařízení musí podporovat 802.1x na všech rozhraních.
14.	Zařízení musí podporovat autentizaci pomocí MAC adres prostřednictvím protokolu RADIUS.
15.	Propustnost zařízení musí být nejméně 128 Gb/s.
16.	Zařízení musí podporovat principy QoS dle 802.1p a DSCP a umožnit klasifikaci paketů dle zdrojových a cílových TCP/UDP portů (dle 4. vrstvy ISO/OSI).
17.	Zařízení musí podporovat zachytávání klientského provozu per port s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
18.	Zařízení musí podporovat funkci testování připojených UTP/STP kabelů – zjištění stavu jednotlivých párů a celkové délky kabelu.
19.	Zařízení musí podporovat funkci rozpoznávání klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
20.	Zařízení musí podporovat filtrování procházejících uživatelských dat dle zdrojových a cílových IP adres a UDP/TCP portů.
21.	Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
22.	Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
23.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje.

24.	Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.
-----	--

LAN L3 přepínač 24 portů

LAN L3 přepínač 24 portů je inteligentní přepínač s 24x 10/100/1000Base-T porty a 4x 10G SFP+ porty.

LAN přepínač (povinné parametry)	
Bod	Popis
1.	Zařízení musí být možné nainstalovat stojanu 19".
2.	Zařízení musí podporovat možnost fyzického stohování s propustností minimálně 80 Gb/s.
3.	Zařízení musí mít minimálně 24x RJ-45 10/100/1000Base-T rozhraní.
4.	Zařízení musí mít minimálně 4x 10G SFP+ rozhraní pro uplink/downlink.
5.	RJ-45 rozhraní na zařízení musí podporovat funkci auto-MDIX.
6.	Zařízení musí podporovat jumbo frame 9600 bajtů.
7.	Zařízení musí podporovat L2 protokoly: 802.1D, 802.1w, 802.1Q, 802.3ad.
8.	Zařízení musí podporovat L3 funkce a protokoly: statické směrování, dynamické směrování pomocí OSPFv2, DHCP relay/server a VRRP.
9.	Zařízení musí podporovat minimálně 16000 MAC adres.
10.	Zařízení musí podporovat minimálně 4095 virtuálních sítí LAN (802.1Q).
11.	Zařízení musí podporovat 802.1x na všech rozhraních.
12.	Zařízení musí podporovat autentizaci pomocí MAC adres prostřednictvím protokolu RADIUS.
13.	Propustnost zařízení musí být nejméně 128 Gb/s.
14.	Zařízení musí podporovat principy QoS dle 802.1p a DSCP a umožnit klasifikaci paketů dle zdrojových a cílových TCP/UDP portů (dle 4. vrstvy ISO/OSI).
15.	Zařízení musí podporovat zachytávání klientského provozu per port s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
16.	Zařízení musí podporovat funkci testování připojených UTP/STP kabelů – zjištění stavu jednotlivých párů a celkové délky kabelu.
17.	Zařízení musí podporovat funkci rozpoznávání klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
18.	Zařízení musí podporovat filtrování procházejících uživatelských dat dle zdrojových a cílových IP adres a UDP/TCP portů.
19.	Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
20.	Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
21.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje.
22.	Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

Bezdrátový přístupový bod

Bezdrátový přístupový bod je zařízení, které umožňuje klientům připojení do bezdrátové sítě.

Bezdrátový přístupový bod (povinné parametry)	
Bod	Popis
1.	Zařízení musí podporovat následující Wi-Fi standardy: 802.11b, 802.11g, 802.11a, 802.11n, 802.11ac Wave2.
2.	Zařízení musí být schopno pracovat současně v pásmu 2,4 GHz a 5 GHz.

3.	Zařízení musí v případě standardu 802.11ac podporovat šířku kanálu až 80MHz.
4.	Zařízení musí podporovat centrálně řízené automatické nastavení výběru kanálu a vysílacích výkonů a to včetně dynamické reakce na změnu prostředí.
5.	Zařízení musí podporovat 2x2:2 MU-MIMO a beamforming.
6.	Zařízení musí podporovat PoE napájení dle standardu 802.3af.
7.	Zařízení musí být dodáno s úchytem na stěnu a/nebo strop.
8.	Zařízení musí být uzamykatelné proti krádeži.
9.	Zařízení musí mít alespoň jedno 100/1000Base-T rozhraní.
10.	Zařízení musí umožnit konfiguraci minimálně 8 SSID na každém z 802.11 rádií.
11.	Zařízení musí podporovat následující bezpečnostní standardy: WEP, WPA2-PSK, WPA2-Enterprise s 802.1X autentizací.
12.	Zařízení musí podporovat šifrování AES.
13.	Zařízení musí podporovat ověřování PEAP (MSCHAPv2)
14.	Zařízení musí podporovat standardy 802.11r, 802.11k a 802.11v pro rychlý roaming klientů a rozložení zátěže mezi jednotlivými AP infrastruktury.
15.	Zařízení musí podporovat VLAN tagging (802.1Q) na jeho ethernetovém rozhraní.
16.	Zařízení podporuje principy QoS dle WMM, 802.1p a DSCP.
17.	Zařízení musí podporovat funkci rozpoznávání tříd klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
18.	Zařízení musí být schopné omezit šířku pásma pro každé jednotlivé SSID, pro každého z klientů a také dle rozpoznávaných tříd aplikací (dle 7. vrstvy ISO/OSI).
19.	Zařízení musí umožnit QoS klasifikaci paketů dle rozpoznávaných tříd aplikací (dle 7. vrstvy ISO/OSI) pomocí DSCP a 802.1p tagu.
20.	Zařízení musí podporovat BLE (Bluetooth Low Energy) dle specifikace Bluetooth 4.0.
21.	Zařízení musí umožňovat spektrální analýzu pro detekci zdrojů rušení (non-WiFi interference) v pásmu 2,4 a 5GHz s možností zobrazení diagramů v reálném čase. Funkce spektrální analýzy nesmí omezit základní funkci AP – poskytování datové konektivity klientským zařízením.
22.	Zařízení musí umožnit filtrování procházejících uživatelských dat dle cílových IP adres a/nebo UDP/TCP portů.
23.	Zařízení musí umožnit zakázat komunikaci vybraných klientů a to až dle rozpoznávaných tříd aplikací (dle 7. vrstvy ISO/OSI) a v případě http i dle DNS jména cílového serveru.
24.	Zařízení musí mít integrovanou funkci detekce a zastavení útoku na bezdrátovou infrastrukturu (wIDS/wIPS). Tato funkce musí být dostupná v reálném čase na všech kanálech (i neobsluhovaných) a nesmí omezit základní funkci AP – poskytování datové konektivity klientským zařízením.
25.	Zařízení musí podporovat zachytávání klientského provozu s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
26.	Zařízení musí podporovat L3 roaming klientských zařízení mezi různými subnety školy.
27.	Zařízení musí umožnit tunelovat SSID pro návštěvy přímo na bezpečnostní bránu v DMZ školy.
28.	Zařízení musí umožnit izolaci jednotlivých uživatelských zařízení tak, aby tato zařízení nemohla komunikovat mezi sebou (v rámci celého SSID školy).
29.	Zařízení musí být v případě nedostupnosti drátové ethernet konektivity schopné jako uplink dynamicky využít jedno ze svých rádií – mesh link přes některé z okolních AP.
30.	Zařízení musí umožnit spolu s Centrálním systémem řízení a monitorování sítě lokalizaci klientských zařízení v mapě jednotlivých podlaží na základě triangulace dle síly signálu.
31.	Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
32.	Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
33.	Součástí dodávky musí být platná podpora od výrobce po dobu minimálně 60 měsíců a to včetně výměny vadného hardware, všech aktualizací softwaru a firmwaru, bezpečnostních aktualizací a přístupu k technické podpoře výrobce. Zařízení musí být v době prodeje výrobcem plně podporováno a nesmí být pro něj vyhlášeno ukončení prodeje.

34.	Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.
-----	--

Netflow analyzer

Monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent – systém pro monitorování a sběr provozně-lokačních údajů na úrovni rozhraní WAN i LAN a to bez negativních vlivů na zátěž a propustnost zařízení s kapacitou pro uchování dat po dobu minimálně 2 měsíců

Vlastnosti zařízení	
Rack-mount zařízení	maximální velikost 1 RU
Počet monitorovacích portů	min. 4 x 10/100/1000 Mbps (metalika - RJ45)
Management port	1x 10/100/1000 Mbps metalický
Minimální výkon na každém monitorovacím portu	1 480 000 paketů za sekundu
Možnost nastavení rychlosti monitorované linky 10/100/1000Mb/s	na metalických rozhraních
Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky	Ano
Pasivní zapojení bez vlivu na monitorovanou síť	zapojení pomocí TAPů
Nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích, nesmí docházet k ovlivňování chování sítě	Ano
Přesný nezávislý autonomní zdroj NetFlow statistik	podpora IPv4, IPv6, VLAN, MPLS, GRE
Podpora monitorování MAC adres	
Podpora standardizovaných protokolů pro výměnu dat o IP tocích	NetFlow v5, v9 - RFC3954, IPFIX
Detekce aplikací dle standardu NBAR2, monitorování a analýza HTTP provozu a VoIP statistik	Ano
Zabezpečená vzdálená správa, dohled a konfigurace	HTTPS (GUI), SSH
Vestavěný kolektor pro dočasné ukládání NetFlow statistik (zajištění redundance)	obsahuje uživatelsky definovaný dashboard, automatickou tvorbu reportů, detekci aktivních zařízení a detailní analytické možnosti
Úložná kapacita vestavěného kolektoru	min. 500 GB
Možnost doplnit o další moduly	např. behaviorální analýza, monitoring výkonu webových aplikací
Časová synchronizace zařízení proti centrálnímu zdroji času na síti	Ano
Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména	Ano
Správa uživatelů a přístupových práv na zařízení	Ano
Podpora vzdálené autentizace uživatelů	LDAP (Active Directory)
Plná zákaznická podpora v českém jazyce	Ano

Server do racku pro DNSSEC a RADIUS

Pro zajištění služeb DNSSEC A RADIUS serveru bude instalován HW server, na kterém bude spuštěn OS plně kompatibilní s Microsoft Windows Server a bude začleněn do stávající serverové infrastruktury jako člen domény. Server musí splňovat následující kritéria:

- Jednosocketový server o velikosti 1U včetně ramena pro vedení kabelů umožňujícího vysunutí zapnutého serveru z racku pro servisní účely
- 1 procesor (min 4 jádra, 8 vláken), min. 8MB cache dle passmark min. 9900 bodů
- Podpora paměti DDR-4 o frekvenci 2400MHz
- Možnost maximálního rozšíření na minimálně 64GB
- min. 32GB DDR-4
- Integrovaný RAID SAS řadič s podporou RAID 0/1/5/6/10 včetně 2GB flash paměti nebo baterií zálohovanou RAM paměti
- Min. 4 pozice pro 3.5" hot-swap SAS/SATA/SSD disky
- Min. 2x 600GB 10000 otáček hotplug disky
- Min. 4 porty USB 3.0
- Možnost rozšíření až 3-mi PCI-e kartami, z toho alespoň 2x PCIe Gen3 s x8 bus
- 2x 1Gbit LAN porty
- 1x Dedikovaný management port RJ-45
- Větráčky v serveru musí být redundantní
- 2x Napájecí zdroje s redundancí napájení 1+1, min. požadovaný výkon jednoho zdroje je 450W
- Zdroje musí splňovat požadavky na certifikaci energetické účinnosti, např. ECOS Consulting 80 Plus (min. PLATINIUM), popř. je nutno doložit, že mají při napětí 230V účinnost min. 94%
- Certifikace a podpora výrobce pro OS MS Windows Server 2012 R2 a výše
- Požadovaná 5 letá servisní podpora s opravou v místě instalace serveru a s garantovanou opravou následující pracovní den od nahlášení případné závady

Software pro Server

Požadavky na operační systém pro servery:

- Licence pro serverový operační systém pro provoz 1 operačního systému na 1 fyzickém serveru, který je součástí nabídky
- Možnost downgrade verze operačního systému
- Nevázanost licence na dodaném hardware
- Operační systém musí být plně kompatibilní s provozovanými aplikacemi a současnou serverovou infrastrukturou a Active Directory
- Součástí dodávky požadujeme také 40ks licencí pro přístup uživatelů k doméně (Active Directory) kompatibilní se stávající platformou školy

Ostatní služby infrastruktury a platformy

DNSSEC resolver – zřízení DNSSEC resolveru v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

AD, LDAP - využití stávající AD s databází uživatelů a skupin uživatelů v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

SSO - předpokládáme instalaci SSO (Single Sign On) utility jako součást bezpečnostní brány do standardního serverového operačního systému.

RADIUS - předpokládáme instalaci RADIUS serveru v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

Strukturovaná kabeláž pro wifi

Pro zajištění komunikace a současně napájení wifi sítě bude dobudována strukturovaná kabeláž ke všem 25 ks wifi access pointů.

Dále bude vybudováno 8 ks nových segmentů sítě do učebny číslo 2 a provedena úprava nevyhovující strukturované kabeláže v kanceláři zástupce ředitele.

Kabeláž bude uložena v existujících lištách nebo budou instalovány nové lišty dle potřeby.

Strukturovaná kabeláž bude zakončena ve stávajícím centrálním datovém rozvaděči na patch panelu.

Požadovaná kabeláž je min. UTP Cat 5e. Součástí dodávky bude potřebný počet patchcordu do datového rozvaděče a další vybavení rozvaděče.

Učebna IVT č.7

Pro zajištění potřebného technického zázemí v učebně IVT, bude osazeno 19 PC s příslušenstvím.

PC s příslušenstvím

- Case minitower se zdrojem splňujícím ENERGY STAR® certified; EPEAT® Gold
- Procesor splňující výkon min. 12000 bodů passmark
- minimálně RAM 8GB DDR4
- minimálně HDD 256GB SSD
- Mechanika DVDRW
- Klávesnice, myš
- Výstup na monitor DP nebo HDMI
- Operační systém plně kompatibilní se současným systémem školy (aktuálně Windows)
- Monitor 21,5 - 22" s rozlišením 1920 x 1080, IPS, odezvou 5ms, 250cd, rozhraním min. 1x HDMI
- Záruka 36 měsíců onsite NBD
- PC i monitor od stejného výrobce
- Kabel na propojení PC a LCD HDMI nebo DP
- balík kancelářských aplikací plně kompatibilní s OS a systémem školy (aktuálně MS Office)

Software pro správu třídy

Pro řízení jakékoliv výuky využívající PC bude implementován systém, který umožní sledovat, ovládat a řídit všechny počítače z učitelského pracoviště.

Správa Třídy

- Zapínání a vypínání všech počítačů ve třídě z počítače učitele.
- Dálkové "Odhlášení" všech počítačů.
- Zaslání dálkového "Přihlášení" na začátku vyučovací hodiny na všechny počítače studentů.

- Ponechání obrazovek studentů prázdných k získání pozornosti.
- Zablokování myši a klávesnic studentů při podávání pokynů.
- Rozmístění tak, aby počítač učitele představoval rozmístění fyzické třídy.
- Použití profilů jednotlivých učitelů k předložení prvků, které každý z učitelů potřebuje.
- Vizuální odměňování jednotlivých studentů k povzbuzení snahy nebo chování.

Správa Tiskárny

- Brání studentům v tisku ve třídě.
- Omezení použití tiskárny počtem stránek.
- Před tiskem se požaduje schválení učitele.

Správa Zařízení

- Brání kopírování dat na nebo z USB úložiště a CDR / DVD zařízení.
- Brání tvorbě nových síťových připojení.

Registrace Studentů

- Požadavek na standardní a uživatelské informace od každého studenta na začátku vyučovací hodiny.
- Distribuce souborů na více počítačů jedním úkonem.
- Náhled na shrnutí pro studenta „najatím myši“ na ikonu studenta.
- Použití přizpůsobených úkonů pro jednotlivé studenty nebo skupiny studentů.

Rozdávání a Sbírání Souborů

- Transfer souborů na a ze zvoleného počítače jedním úkonem.
- Distribuce souborů na více počítačů jedním úkonem.
- Rozdávání a automatický sběr souborů s připojenými údaji každého studenta.

Pokyny v Reálném Čase (Režim Ukázky)

- Ukázání obrazovky učitele zvoleným studentům.
- Ukázání specifického počítače zvoleným studentům.
- Ukázání jen zvolené aplikace zvoleným studentům.
- Ukažte soubor Replay (předchozí nahrávka obrazovky) vybraným studentům, a výstup jak video soubor.
- Přehrání video souboru zvoleným studentům.
- Předložení prezentací optimalizovaných pro bezdrátové sítě.
- Zanechání záznamu Ukázky na počítači studenta k pozdějšímu prohlédnutí.
- Zvuková interakce se studenty během demonstrace tématu.
- Ukažte obrazovku studenta (Mód prohlížení)

Společné Prohlížení Internetu

Umožňuje učiteli otevírat zvolené webové stránky a synchronizovat je s prohlížečem na počítačích všech studentů. Když učitel naviguje webovými stránkami, počítače studentů ho následují.

Náhled na Obrazovky Studentů v Reálném Čase (Režim Monitorování)

- Monitorování celé třídy jedním pohledem.
- náhled přes studentské počítače v předem definovaných skupinách.
- Pokrytí dalšími informacemi včetně aktivní aplikace nebo aktivní webové stránky.
- Zoom pro optimalizované miniatury studentů s vysokým rozlišením.

Monitorování Instant Messengerů

Sledování Klávesnic v Reálném Čase

Měření a Kontrola Internetu

- Monitorování veškerého využití Internetu studenty.
- Náhled na všechny webové stránky otevřené v pozadí na všech počítačích.
- Otevírání a zavírání webových stránek na všech zvolených počítačích jedním úkonem.
- Záznam úplné historie využití Internetu pro třídu.
- Předchází přístupu na všechny nebo na omezené webové stránky.
- Povoluje pouze přístup na schválené webové stránky.

Monitorování Audia v Reálném Čase a Jazykové Nástroje Průzkumy Studentů

- Tvorba průzkumu s využitím předem dodaných nebo uživatelských odpovědí.
- Okamžité prohlédnutí všech odpovědí a shrnutí pro třídu.
- Dynamická tvorba skupin založená na odpovědích studentů.
- Publikace výsledků průzkumu všem studentům.

Zkoušení a kvízy Studentů

- Tvorba knihovny zdrojů a otázek, které lze sdílet.
- Tvorba libovolného počtu testů s využitím otázek z vaší knihovny.
- Nyní využívá 8 různých stylů otázek.
- Tvorba otázek se 2 až 4 možnými odpověďmi.
- Nastavení úrovně hodnocení zkoušek (např. přes 75% = hodnocení A).
- Sledování pokroku studentů a sledování správných nebo nesprávných odpovědí na otázky v reálném čase.
- Automatické známkování testů, aby byly výsledky dostupné okamžitě po jejich dokončení.
- Zobrazení výsledků jednotlivým studentům.
- Předložení výsledků (včetně zdůraznění správných odpovědí) třídě.
- Instalace návrháře testů na samostatném systému.

Technická konzole pro správce umožní:

- Monitorovat všechny počítače ve školní síti v jednom pohledu.
- Monitorovat využití aplikací a Internetu na počítači každého studenta.
- Přenášet soubory a složky do zvolených nebo všech počítačů.
- Seskupovat všechny počítače podle třídy / fyzického místa.
- Generovat úplné hardwarové systémové informace pro zvolené počítače.
- Generovat úplné informace o softwaru pro každý počítač včetně Hotfixů.
- Prohlížet a kontrolovat služby, procesy a aplikace běžící na každém PC.
- Poskytovat přímou technickou pomoc učitelům v libovolné třídě.
- Zapínat, vypínat, restartovat nebo se přihlásit na počítače ve třídě dálkově.
- Provádět výkonnou 1:1 dálkovou kontrolu PC na libovolně zvoleném počítači.

Zabezpečení

- Jedinečný "zabezpečovací klíč", aby byla vaše kopie nekompatibilní s ostatními kopiemi.
- Omezení konektivity pouze na systémy s odpovídající softwarovou licencí.
- Profily učitelů, z nichž každý umožňuje uživatelské úrovně funkčnosti dle požadavku.
- Použití AD profilů k omezení toho, kteří uživatelé smějí používat software učitele nebo technika.
- Použití AD profilů k vynucení konfigurací pro učitele a klienta.
- Kontrola přístupu a použití přenosných mediálních zařízení ve třídě.
- Automatická opakovaná aplikace omezení po restartování počítače studenta.

Deník Studenta

- Podrobné údaje o vyučovací hodině a cíle.
- Poznámky učitele.
- Poznámky jednotlivých studentů.
- Snímky obrazovky z prezentace (a vysvětlení).
- Virtuální obrazovky bílé tabule.
- Výsledky zkoušek jednotlivých studentů.
- URL webových stránek používaných během vyučovací hodiny.
- Kopie přepisů libovolných chatů třídy.

Montážní a implementační práce - pro splnění standardu konektivity škol

Hardware

- Doprava na místo
- Fyzická montáž do datového rozvaděče
 - Prostor připraví zákazník
 - Popis jednotlivých dodaných prvků – popisky, štítky
 - Fotodokumentace
- Zapojení, oživení do sítě zákazníka
 - Konfigurace MGMT IP adres
 - Aktualizace dle doporučení výrobce na poslední verze FW, BIOS
 - Doložení dle výrobce o aktuálnosti
- Vyvázání kabeláže
 - Popis kabelů
 - Dokumentace + fotodokumentace k zapojení
- Dodavatel zajistí všechny potřebné kabely vč. PDU
 - LAN
 - Opt.
 - Power
 - Jiné
- Instalace žákovských PC a implementace do stávající infrastruktury
- Implementace systému řízení výuky v učebnách
- Fyzická likvidace odpadu, odvoz

Software

- Virtualizační platforma
- Instalace operačních systémů
- Konfigurace všech potřebných rolí dle standartu konektivity do škol včetně RADIUS serveru
- Konfigurace operačních systémů, rolí dle doporučení výrobce
- Konfigurace MGMT reportů
 - Reportování stavů HW
 - RAID, FAN, PSU, CPU, RAM, HDD
 - Poštovní server dodá zákazník
- Instalace jednotlivých serverů / zařízení dle standartu konektivity do škol

Na WAN připojení k internetu:

- plná podpora připojení do veřejného internetu přes protokol IPv4 i IPv6 (dual-stack)
- validující DNSSEC resolver na straně školy
- podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)
- síťové zařízení podporující rate limiting, antispoofing, ACL/xACL, rozhraní musí obsahovat všechny potřebné komponenty a licence pro zajištění řádné funkcionality
- zařízení umožňující kontrolu http a https provozu, kategorizaci a selekci obsahu dostupného pro vybrané skupiny uživatel (učitel, žák), blokování nežádoucích kategorií obsahu, antivirovou kontrolou stahovaného obsahu
- možnost snadné/automatické rekonfigurace ACL/FW na základě identifikovaných útoků
- podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online
- u software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu.

Povinné minimální bezpečnostní parametry projektu (bez ohledu typ síťového připojení):

- Monitorování IP (IPv4 a IPv6) datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) - RFC3954 nebo ekvivalent (např. NetFlow) – systém pro monitorování a

sběr provozně-lokačních údajů minimálně na úrovni rozhraní WAN, ideálně i LAN) a to bez negativních vlivů na zátěž a propustnost zařízení s kapacitou pro uchování dat po dobu minimálně 2 měsíců

- Povinné řešení systému správy uživatelů (Identity Management), tj. centrální databáze identit (LDAP, AD, apod.) a její využití pro autentizaci uživatelů (žáci i učitelé) za účelem bezpečného a auditovatelného přístupu k síti, resp. síťovým službám.
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel

V oblasti pevné LAN musí projekt splňovat následující minimální parametry:

- Minimální konektivita stanic a dalších koncových zařízení zařízení 100Mbit/s full duplex
- Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,...)
- Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s full duplex
- Páteří rozvody mezi budovami v areálu realizovány prostřednictvím optických, metalických vláken popř. bezdrátovými spoji v licencovaném pásmu (povolení ČTÚ)
- Aktivní prvky (centrální směrovače a centrální přepínače; L2 i L3)¹ s neblokující architekturou přepínacího subsystému (wire speed), podpora 802.1Q VLAN, podpora 802.1X, radius based MAC autentizace,...

V případě řešení bezdrátových sítí (wifi) pak musí projekt naplňovat následující minimální parametry:

- Podpora mechanismu izolace klientů
- Návrh topologie wifi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou ve v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů
- Centralizovaná architektura správy wifi sítě (centrální řadič, centrální management, tzv. thin access pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení)
- Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD ...)
- Podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz
- Podpora WPA2, PoE, multi SSID, ACL pro filtrování provozu

Všechny body výše vychází z daného standartu, který je nutno dodržet.

- Plná integrace nového řešení do stávající infrastruktury ICT školy

Dokumentace

- Kompletní dokumentace vč. Fotodokumentace HW zapojení
 - Zálohy konfigurací na přiloženém CD
 - Obálka vč. Uživatelských jmen a hesel
 - Seznam vytvořených uživatelů vč. Vzdálených přístupů
 - Kompletní dokumentace nastavení jednotlivých rolí dle standartu
- Výstupní protokol, který prověří fungování daného standartu
- Provedení site survey wifi pokrytí – zakres do dodaných půdorysů
- Veškeré licence v tištěné i elektronické formě na přiloženém CD
- Předávací protokol o předání dokumentací

¹ Požadavek se týká prvků, přes které je veden veškerý provoz, resp. jde o centrální prvky. Podružné přepínače (chodbové, očebnové) musí splňovat pouze požadavek na neblokující architekturou přepínacího subsystému

Předání

1. Zaškolení obsluhy, předání informací o celém řešení
2. Testovací provoz, který ověří funkčnost (cca 1 měsíc)

VZ "Dodávka ICT včetně zajištění konektivity"

Dodavatel:	
Název:	MERIT GROUP a.s.
Sídlo:	Březinova 7, Olomouc 779 00
Osoba oprávněná:	Petr Weigel - statutární ředitel
IČ:	64609995
DIČ:	CZ699000785
Kontaktní e-mail:	milan.medvedik@merit.cz
Tel:	605720587

	Cena v Kč bez DPH	DPH 21%	Cena v Kč s DPH
Rozpočet ZŠ Dr. Hrubého 2, Šternberk, příspěvková organizace - konektivita	1 979 941 Kč	415 788 Kč	2 395 729 Kč
Rozpočet ZŠ náměstí Svobody 3, Šternberk, příspěvková organizace - konektivita	3 974 549 Kč	834 655 Kč	4 809 204 Kč
Rozpočet ZŠ Svatoplukova 7, Šternberk, příspěvková organizace - konektivita	1 664 752 Kč	349 598 Kč	2 014 350 Kč
Součet	7 619 242 Kč	1 600 041 Kč	9 219 283 Kč

Petr Weigel, statutární ředitel

ZŠ Dr. Hrubého 2, Šternberk, příspěvková organizace
Položkový rozpočet
KONEKTIVITA

Název	Popis	Počet	MJ	Cena za ks bez DPH	Cena za ks vč. DPH	Cena celkem bez DPH	Cena celkem vč. DPH
Montáž	Montáž - Next-Gen Firewall, IPS a anti-malware včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	1 000 Kč	1 210 Kč	1 000 Kč	1 210 Kč
Dodávka	Dodávka - Next-Gen Firewall, IPS a anti-malware včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	152 852 Kč	184 951 Kč	152 852 Kč	184 951 Kč
Montáž	Montáž - LAN přepínač - L3 - 24 včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	1	ks	500 Kč	605 Kč	500 Kč	605 Kč
Dodávka	Dodávka - LAN přepínač - L3 - 24 včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	1	ks	62 842 Kč	76 039 Kč	62 842 Kč	76 039 Kč
Montáž	Montáž - LAN přepínač - L2 - 24P včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	2	ks	500 Kč	605 Kč	1 000 Kč	1 210 Kč
Dodávka	Dodávka - LAN přepínač - L2 - 24P včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	2	ks	51 146 Kč	61 887 Kč	102 292 Kč	123 773 Kč
Montáž	Montáž - Bezdrátový přístupový bod - včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	42	ks	350 Kč	424 Kč	14 700 Kč	17 787 Kč
Dodávka	Dodávka - Bezdrátový přístupový bod - včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	42	ks	10 789 Kč	13 055 Kč	453 138 Kč	548 297 Kč
Montáž	Montáž - Monitorování sítě - Netflow sonda včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	500 Kč	605 Kč	500 Kč	605 Kč

Dodávka	Dodávka - Monitorování sítě - Netflow sonda včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	280 781 Kč	339 745 Kč	280 781 Kč	339 745 Kč
Montáž	Montáž - Monitorování sítě - síťový hardware pro připojení Netflow sondy včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	500 Kč	605 Kč	500 Kč	605 Kč
Dodávka	Dodávka - Monitorování sítě - síťový hardware pro připojení Netflow sondy včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	71 380 Kč	86 370 Kč	71 380 Kč	86 370 Kč
Montáž	Montáž - Server do racku pro DNSSEC a RADIUS včetně záruky 5 let	1	ks	1 000 Kč	1 210 Kč	1 000 Kč	1 210 Kč
Dodávka	Dodávka - Server do racku pro DNSSEC a RADIUS včetně záruky 5 let	1	ks	73 934 Kč	89 460 Kč	73 934 Kč	89 460 Kč
Montáž	Montáž - Software pro server - operační systém	1	ks	5 000 Kč	6 050 Kč	5 000 Kč	6 050 Kč
Dodávka	Dodávka - Software pro server - operační systém	1	ks	6 942 Kč	8 400 Kč	6 942 Kč	8 400 Kč
Montáž	Montáž - Software pro server - přístupové uživatelské licence	40	ks	100 Kč	121 Kč	4 000 Kč	4 840 Kč
Dodávka	Dodávka - Software pro server - přístupové uživatelské licence	40	ks	234 Kč	283 Kč	9 360 Kč	11 326 Kč
Montáž	Montáž - Žákovský PC - ICT učebna velká - specifikace v příloze Technické požadavky	16	ks	500 Kč	605 Kč	8 000 Kč	9 680 Kč
Dodávka	Dodávka - Žákovský PC - ICT učebna velká - specifikace v příloze Technické požadavky	16	ks	19 188 Kč	23 217 Kč	307 008 Kč	371 480 Kč
Montáž	Montáž - software pro správu třídy včetně podpory 5 let - ICT učebna velká - specifikace v příloze Technické požadavky	16	ks	250 Kč	303 Kč	4 000 Kč	4 840 Kč
Dodávka	Dodávka - software pro správu třídy včetně podpory 5 let - ICT učebna velká - specifikace v příloze Technické požadavky	16	ks	3 128 Kč	3 785 Kč	50 048 Kč	60 558 Kč
Montáž	Montáž - software pro správu třídy včetně podpory 5 let - ICT učebna malá - specifikace v příloze Technické požadavky	16	ks	250 Kč	303 Kč	4 000 Kč	4 840 Kč
Dodávka	Dodávka - software pro správu třídy včetně podpory 5 let - ICT učebna malá - specifikace v příloze Technické požadavky	16	ks	3 128 Kč	3 785 Kč	50 048 Kč	60 558 Kč

Montáž	Montáž - implementační práce - pro splnění standardu konektivity škol a podle specifikace v příloze Technické požadavky	1	kpl	125 000 Kč	151 250 Kč	125 000 Kč	151 250 Kč
Dodávka + montáž	Dodávka + Montáž - strukturovaná kabeláž pro 42 ks wifi AP - specifikace v příloze Technické požadavky	1	ks	93 249 Kč	112 831 Kč	93 249 Kč	112 831 Kč
Dodávka + montáž	Dodávka + Montáž - rekonstrukce rozvodů strukturované kabeláže ICT učebna velká - specifikace v příloze Technické požadavky	1	kpl	49 895 Kč	60 373 Kč	49 895 Kč	60 373 Kč
Dodávka + montáž	Dodávka + Montáž - rekonstrukce rozvodů 230V ICT učebna velká - specifikace v příloze Technické požadavky	1	kpl	19 972 Kč	24 166 Kč	19 972 Kč	24 166 Kč
Montáž	Montáž - Zaškolení obsluhy	1	kpl	8 000 Kč	9 680 Kč	8 000 Kč	9 680 Kč
Montáž	Montáž - Dokumentace skutečného provedení	1	kpl	19 000 Kč	22 990 Kč	19 000 Kč	22 990 Kč

Cena celkem bez DPH:	1 979 941 Kč
DPH:	415 788 Kč
Cena celkem s DPH:	2 395 729 Kč

ZŠ náměstí Svobody 3, Šternberk
Položkový rozpočet
KONEKTIVITA

Název	Popis	Počet	MJ	Cena za ks bez DPH	Cena za ks vč. DPH	Cena celkem bez DPH	Cena celkem vč. DPH
Montáž	Montáž - Next-Gen Firewall, IPS a anti-malware včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	1 000 Kč	1 210 Kč	1 000 Kč	1 210 Kč
Dodávka	Dodávka - Next-Gen Firewall, IPS a anti-malware včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	142 308 Kč	172 193 Kč	142 308 Kč	172 193 Kč
Montáž	Montáž - LAN přepínač - L3 - 24 včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	1	ks	500 Kč	605 Kč	500 Kč	605 Kč
Dodávka	Dodávka - LAN přepínač - L3 - 24 včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	1	ks	62 842 Kč	76 039 Kč	62 842 Kč	76 039 Kč
Montáž	Montáž - LAN přepínač - L2 - 24 včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	3	ks	500 Kč	605 Kč	1 500 Kč	1 815 Kč
Dodávka	Dodávka - LAN přepínač - L2 - 24 včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	3	ks	39 338 Kč	47 599 Kč	118 014 Kč	142 797 Kč
Montáž	Montáž - LAN přepínač - L2 - 48 včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	4	ks	500 Kč	605 Kč	2 000 Kč	2 420 Kč
Dodávka	Dodávka - LAN přepínač - L2 - 48 včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	4	ks	53 826 Kč	65 129 Kč	215 304 Kč	260 518 Kč
Montáž	Montáž - LAN přepínač - L2 - 24P včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	3	ks	500 Kč	605 Kč	1 500 Kč	1 815 Kč

Dodávka	Dodávka - LAN přepínač - L2 - 24P včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	3	ks	51 146 Kč	61 887 Kč	153 438 Kč	185 660 Kč
Montáž	Montáž - Bezdrátový přístupový bod - včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	40	ks	350 Kč	424 Kč	14 000 Kč	16 940 Kč
Dodávka	Dodávka - Bezdrátový přístupový bod - včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	40	ks	10 789 Kč	13 055 Kč	431 560 Kč	522 188 Kč
Montáž	Montáž - Monitorování sítě - Netflow sonda včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	500 Kč	605 Kč	500 Kč	605 Kč
Dodávka	Dodávka - Monitorování sítě - Netflow sonda včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	280 781 Kč	339 745 Kč	280 781 Kč	339 745 Kč
Montáž	Montáž - Monitorování sítě - síťový hardware pro připojení Netflow sondy včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	500 Kč	605 Kč	500 Kč	605 Kč
Dodávka	Dodávka - Monitorování sítě - síťový hardware pro připojení Netflow sondy včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	71 380 Kč	86 370 Kč	71 380 Kč	86 370 Kč
Montáž	Montáž - Server do racku pro DNSSEC a RADIUS včetně záruky 5 let	1	ks	1 000 Kč	1 210 Kč	1 000 Kč	1 210 Kč
Dodávka	Dodávka - Server do racku pro DNSSEC a RADIUS včetně záruky 5 let	1	ks	73 934 Kč	89 460 Kč	73 934 Kč	89 460 Kč
Montáž	Montáž - Software pro server pro DNSSEC a RADIUS - operační systém	1	ks	5 000 Kč	6 050 Kč	5 000 Kč	6 050 Kč
Dodávka	Dodávka - Software pro server pro DNSSEC a RADIUS - operační systém	1	ks	6 942 Kč	8 400 Kč	6 942 Kč	8 400 Kč
Montáž	Montáž - Server do racku pro hypervizor a Active Directory včetně záruky 5 let	1	ks	1 000 Kč	1 210 Kč	1 000 Kč	1 210 Kč
Dodávka	Dodávka - Server do racku pro hypervizor a Active Directory včetně záruky 5 let	1	ks	142 877 Kč	172 881 Kč	142 877 Kč	172 881 Kč
Montáž	Montáž - Software pro server pro hypervizor a Active Directory	1	ks	60 000 Kč	72 600 Kč	60 000 Kč	72 600 Kč

Dodávka	Dodávka - Software pro server pro hypervizor a Active Directory	1	ks	92 678 Kč	112 140 Kč	92 678 Kč	112 140 Kč
Montáž	Montáž - Žákovský PC - ICT učebna 1 - specifikace v příloze Technické požadavky	30	ks	500 Kč	605 Kč	15 000 Kč	18 150 Kč
Dodávka	Dodávka - Žákovský PC - ICT učebna 1 - specifikace v příloze Technické požadavky	30	ks	19 188 Kč	23 217 Kč	575 640 Kč	696 524 Kč
Montáž	Montáž - Žákovský PC - ICT učebna 2 - specifikace v příloze Technické požadavky	30	ks	500 Kč	605 Kč	15 000 Kč	18 150 Kč
Dodávka	Dodávka - Žákovský PC - ICT učebna 2 - specifikace v příloze Technické požadavky	30	ks	19 188 Kč	23 217 Kč	575 640 Kč	696 524 Kč
Montáž	Montáž - záložní zdroj UPS pro server - specifikace v příloze Technické požadavky	1	ks	500 Kč	605 Kč	500 Kč	605 Kč
Dodávka	Dodávka - záložní zdroj UPS pro server - specifikace v příloze Technické požadavky	1	ks	28 800 Kč	34 848 Kč	28 800 Kč	34 848 Kč
Montáž	Montáž - záložní zdroj UPS pro aktivní prvky - specifikace v příloze Technické požadavky	3	ks	500 Kč	605 Kč	1 500 Kč	1 815 Kč
Dodávka	Dodávka - záložní zdroj UPS pro aktivní prvky - specifikace v příloze Technické požadavky	3	ks	12 197 Kč	14 758 Kč	36 591 Kč	44 275 Kč
Montáž	Montáž - NAS úložiště pro zálohování - specifikace v příloze Technické požadavky	1	ks	500 Kč	605 Kč	500 Kč	605 Kč
Dodávka	Dodávka - NAS úložiště pro zálohování - specifikace v příloze Technické požadavky	1	ks	16 405 Kč	19 850 Kč	16 405 Kč	19 850 Kč
Montáž	Montáž - Software pro zálohování - specifikace v příloze Technické požadavky	1	ks	4 000 Kč	4 840 Kč	4 000 Kč	4 840 Kč
Dodávka	Dodávka - Software pro zálohování - specifikace v příloze Technické požadavky	1	ks	16 798 Kč	20 326 Kč	16 798 Kč	20 326 Kč
Montáž	Montáž - bezpečnostní software pro pracovní stanice a server - specifikace v příloze Technické požadavky	1	ks	12 000 Kč	14 520 Kč	12 000 Kč	14 520 Kč
Dodávka	Dodávka - bezpečnostní software pro pracovní stanice a server - specifikace v příloze Technické požadavky	1	ks	50 400 Kč	60 984 Kč	50 400 Kč	60 984 Kč
Montáž	Montáž - implementační práce - pro splnění standardu konektivity škol a podle specifikace v příloze Technické požadavky	1	kpl	125 000 Kč	151 250 Kč	125 000 Kč	151 250 Kč
Dodávka + montáž	Dodávka + Montáž - strukturovaná kabeláž pro 40 ks wifi AP - specifikace v příloze Technické požadavky	1	ks	56 195 Kč	67 996 Kč	56 195 Kč	67 996 Kč
Dodávka + montáž	Dodávka + Montáž - strukturovaná kabeláž pro PC - specifikace v příloze Technické požadavky	1	ks	394 055 Kč	476 807 Kč	394 055 Kč	476 807 Kč

Dodávka + montáž	Dodávka + Montáž - rekonstrukce rozvodů strukturované kabeláže ICT učebna 1 - specifikace v příloze Technické požadavky	1	kpl	33 596 Kč	40 651 Kč	33 596 Kč	40 651 Kč
Dodávka + montáž	Dodávka + Montáž - rekonstrukce rozvodů 230V ICT učebna 1 - specifikace v příloze Technické požadavky	1	kpl	31 286 Kč	37 856 Kč	31 286 Kč	37 856 Kč
Dodávka + montáž	Dodávka + Montáž - rekonstrukce rozvodů strukturované kabeláže ICT učebna 2 - specifikace v příloze Technické požadavky	1	kpl	33 799 Kč	40 897 Kč	33 799 Kč	40 897 Kč
Dodávka + montáž	Dodávka + Montáž - rekonstrukce rozvodů 230V ICT učebna 2 - specifikace v příloze Technické požadavky	1	kpl	31 286 Kč	37 856 Kč	31 286 Kč	37 856 Kč
Montáž	Montáž - Zaškolení obsluhy	1	kpl	15 000,00	18 150 Kč	15 000 Kč	18 150 Kč
Montáž	Montáž - Dokumentace skutečného provedení	1	kpl	25 000,00	30 250 Kč	25 000 Kč	30 250 Kč

Cena celkem bez DPH:	3 974 549 Kč
DPH:	834 655 Kč
Cena celkem s DPH:	4 809 204 Kč

ZŠ Svatoplukova 7, Šternberk, příspěvková organizace
Položkový rozpočet
KONEKTIVITA

Název	Popis	Počet	MJ	Cena za ks bez DPH	Cena za ks vč. DPH	Cena celkem bez DPH	Cena celkem vč. DPH
Montáž	Montáž - prodloužení supportu a platnosti všech licencí o 5 let pro Zyxel USG210 - Content Filtering/Anti-Spam/Anti-Virus /IDP	1	ks	1 000 Kč	1 210 Kč	1 000 Kč	1 210 Kč
Dodávka	Dodávka - prodloužení supportu a platnosti všech licencí o 5 let pro Zyxel USG210 - Content Filtering/Anti-Spam/Anti-Virus /IDP	1	ks	67 920 Kč	82 183 Kč	67 920 Kč	82 183 Kč
Montáž	Montáž - LAN přepínač - L3 - 24 včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	1	ks	500 Kč	605 Kč	500 Kč	605 Kč
Dodávka	Dodávka - LAN přepínač - L3 - 24 včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	1	ks	62 842 Kč	76 039 Kč	62 842 Kč	76 039 Kč
Montáž	Montáž - LAN přepínač - L2 - 24P včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	3	ks	500 Kč	605 Kč	1 500 Kč	1 815 Kč
Dodávka	Dodávka - LAN přepínač - L2 - 24P včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	3	ks	51 146 Kč	61 887 Kč	153 438 Kč	185 660 Kč
Montáž	Montáž - Bezdrátový přístupový bod - včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	25	ks	350 Kč	424 Kč	8 750 Kč	10 588 Kč
Dodávka	Dodávka - Bezdrátový přístupový bod - včetně supportu a platnosti všech licencí 10 let - specifikace v příloze Technické požadavky	25	ks	10 789 Kč	13 055 Kč	269 725 Kč	326 367 Kč
Montáž	Montáž - Monitorování sítě - Netflow sonda včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	500 Kč	605 Kč	500 Kč	605 Kč

Dodávka	Dodávka - Monitorování sítě - Netflow sonda včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	280 781 Kč	339 745 Kč	280 781 Kč	339 745 Kč
Montáž	Montáž - Monitorování sítě - síťový hardware pro připojení Netflow sondy včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	500 Kč	605 Kč	500 Kč	605 Kč
Dodávka	Dodávka - Monitorování sítě - síťový hardware pro připojení Netflow sondy včetně supportu a platnosti všech licencí 5 let - specifikace v příloze Technické požadavky	1	ks	71 380 Kč	86 370 Kč	71 380 Kč	86 370 Kč
Montáž	Montáž - Server do racku pro DNSSEC a RADIUS včetně záruky 5 let	1	ks	500 Kč	605 Kč	500 Kč	605 Kč
Dodávka	Dodávka - Server do racku pro DNSSEC a RADIUS včetně záruky 5 let	1	ks	73 934 Kč	89 460 Kč	73 934 Kč	89 460 Kč
Montáž	Montáž - Software pro server - operační systém	1	ks	5 000 Kč	6 050 Kč	5 000 Kč	6 050 Kč
Dodávka	Dodávka - Software pro server - operační systém	1	ks	6 942 Kč	8 400 Kč	6 942 Kč	8 400 Kč
Montáž	Montáž - Software pro server - přístupové uživatelské licence	40	ks	100 Kč	121 Kč	4 000 Kč	4 840 Kč
Dodávka	Dodávka - Software pro server - přístupové uživatelské licence	40	ks	234 Kč	283 Kč	9 360 Kč	11 326 Kč
Montáž	Montáž - Žákovský PC - ICT učebna velká - specifikace v příloze Technické požadavky	19	ks	500 Kč	605 Kč	9 500 Kč	11 495 Kč
Dodávka	Dodávka - Žákovský PC - ICT učebna velká - specifikace v příloze Technické požadavky	19	ks	19 188 Kč	23 217 Kč	364 572 Kč	441 132 Kč
Montáž	Montáž - software pro správu třídy včetně podpory 5 let - ICT učebna - specifikace v příloze Technické požadavky	19	ks	200 Kč	242 Kč	3 800 Kč	4 598 Kč
Dodávka	Dodávka - software pro správu třídy včetně podpory 5 let - ICT učebna - specifikace v příloze Technické požadavky	19	ks	3 128 Kč	3 785 Kč	59 432 Kč	71 913 Kč
Montáž	Montáž - implementační práce - pro splnění standardu konektivity škol a podle specifikace v příloze Technické požadavky	1	kpl	125 000 Kč	151 250 Kč	125 000 Kč	151 250 Kč
Dodávka + montáž	Dodávka + Montáž - strukturovaná kabeláž pro 25 ks wifi AP - specifikace v příloze Technické požadavky	1	ks	45 217 Kč	54 713 Kč	45 217 Kč	54 713 Kč

Dodávka + montáž	Dodávka + Montáž - úprava rozvodů strukturované kabeláže kancelář zástupce ředitele - specifikace v příloze Technické požadavky	1	kpl	6 438 Kč	7 790 Kč	6 438 Kč	7 790 Kč
Dodávka + montáž	Dodávka + Montáž - strukturovaná kabeláž učebna č.2 - specifikace v příloze Technické požadavky	1	kpl	5 221 Kč	6 317 Kč	5 221 Kč	6 317 Kč
Montáž	Montáž - Zaškolení obsluhy	1	kpl	8 000 Kč	9 680 Kč	8 000 Kč	9 680 Kč
Montáž	Montáž - Dokumentace skutečného provedení	1	kpl	19 000 Kč	22 990 Kč	19 000 Kč	22 990 Kč

Cena celkem bez DPH:	1 664 752 Kč
DPH:	349 598 Kč
Cena celkem s DPH:	2 014 350 Kč