DIMENSE v.o.s., Hrnčířská 15, 602 00 Brno, Česká republika,
Tel: 543 217 360, E-mail: info@dimense.cz, www.dimense.cz

Zak.č.: 5217/ZŠVED/DSP

REKONSTRUKCE PODMÍNEK PRO VYUČOVÁNÍ PŘÍRODOVĚDNÝCH PŘEDMĚTŮ NA ZŠ VEDLEJŠÍ

Brno-Bohunice, ul. Vedlejší 10
k.ú. Bohunice, p.č. 2569, 2553/2

SO 03B – ŘEŠENÍ LAN/WAN KONEKTIVITY

TECHNICKÁ ZPRÁVA

DOKUMENTACE PRO REALIZACI STAVBY

Investor:
Statutární město Brno – MČ Brno-Bohunice
Dlouhá 3, 625 00 Brno

Zodpovědný projektant:
David Střelec

Datum:
únor 2018

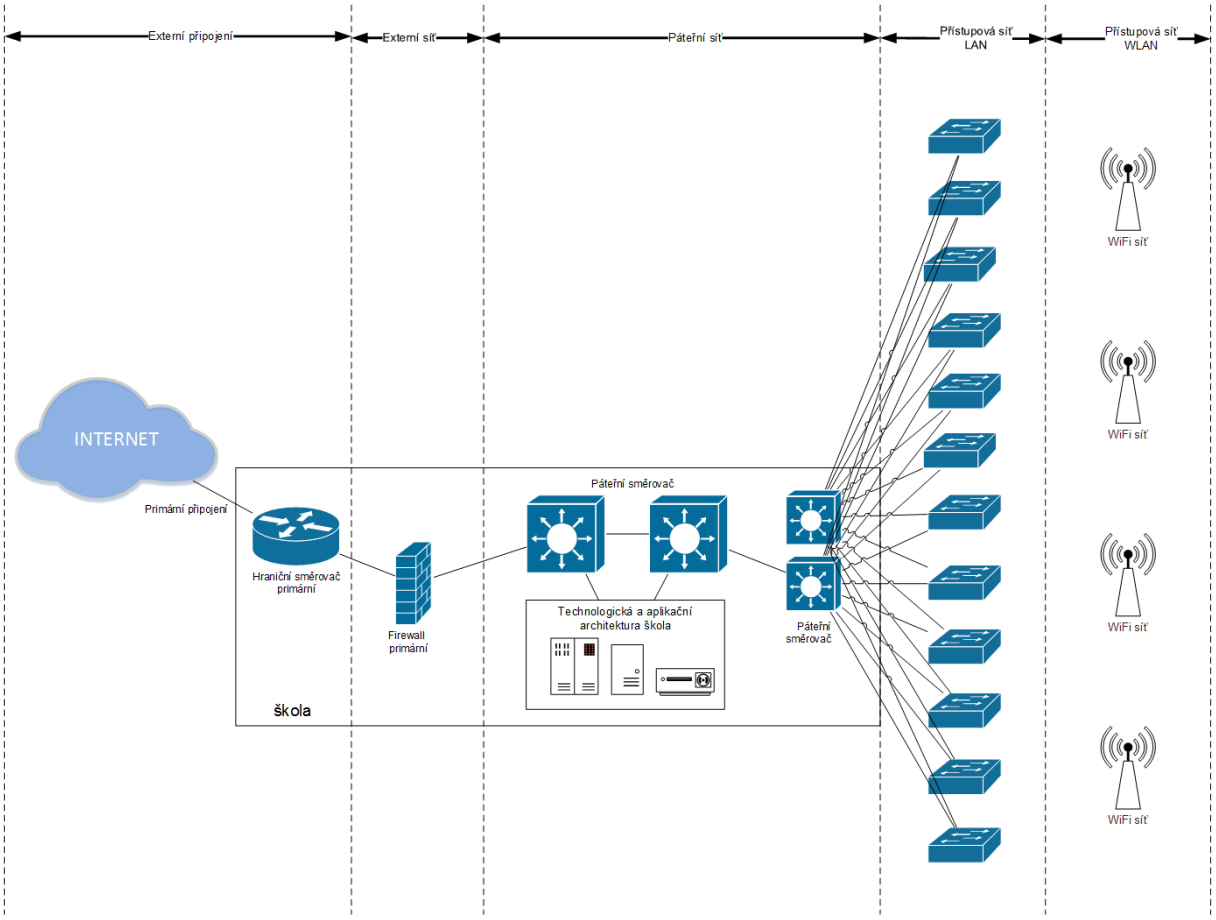
Vypracoval:
Michal Klein

Razítko:

Paré:

Aktivní prvky a jejcich paramerty

Přehledové schéma infrastrukturní architektury (přístupová, páteřní, externí vrstva sítě, externí připojení)



Základní technická kritéria školní síťové infrastruktury

Zadavatelem je vyžadováno splnění následujících základních technických kritérií a to jak v části projektu týkající se připojení školy ke službám veřejného Internetu, tak v části o vnitřní konektivitě školy.

Základní technická kritéria (povinné minimální parametry)

Popis
WAN: Šíře pásma (bandwidth) odpovídající 128kbps/student nebo 512kbps/počítač nebo taková šířka pásma, která neomezuje provoz zařízení a uživatelů.
(P9 - DOPORUČENÝ parametr) WAN: Symetrické připojení bez agregace a omezení (FUP)
WAN: Vlastní nebo poskytovatelem přidělené veřejné IPv4 i IPv6 adresy

WAN: Plná podpora připojení do veřejného internetu přes protokol IPv4 i ###IPv6### (dual-stack)
WAN: Validující DNSSEC resolver na straně školy
WAN: Podpora monitoringu a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení
WAN: Podpora DNSSEC a IPv6 protokolů pro služby školy dostupné online
WAN/LAN: U software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu.
(P9 - DOPORUČENÝ parametr) WAN: Zapojení poskytovatele připojení v bezpečnostním projektu FENIX resp. veřejné adresy využívané školou jsou zapojeny do infrastruktury FENIX nebo ISP splňuje alespoň technické standardy definované projektem FENIX – viz http://nix.cz/cs/file/NIX_PRAVIDLA_FENIX
LAN: Systém pro monitorování a sběr provozně-lokačních údajů (NetFlow kolektor) minimálně na úrovni rozhraní WAN (ideálně i LAN) s kapacitou pro uchování dat po dobu minimálně 2 měsíců.
LAN: 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.
LAN: Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel a to včetně ošetření v případě sdílených učeben (pracovních stanic apod.)
LAN – pevná část: Minimální konektivita stanic a dalších koncových zařízení 100Mbit/s fullduplex, minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení, NAS 1Gbit/s fullduplex
LAN – pevná část: Strukturovaná kabeláž pro připojení pracovních stanic a dalších zařízení (tiskárny, servery, AP,…).
LAN – pevná část: Páteřní rozvody mezi budovami v areálu realizovány prostřednictvím optických, metalických vláken, P9 - popř. bezdrátovými spoji v licencovaném pásmu (povolení ČTÚ).
LAN – Wi-Fi část - Návrh topologie wifi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů.
(P9 - DOPORUČENÝ parametr) LAN – Wi-Fi část - Minimálně pasivní zapojení do federovaného systému eduroam (www.eduroam.cz). Optimálně aktivní zapojení do systému eduroam pro zajištění národní i mezinárodní mobility žáků a učitelů.

Centrální systém řízení a monitorování sítě

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

Základní technická kritéria (povinné minimální parametry)

Popis
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.
Systém musí zajistit automatickou aktualizaci softwaru a instalaci bezpečnostních záplat do všech zařízení v systému a to v uživatelsky definovaném čase.

Systém musí umožnit změny konfigurace více zařízení stejného typu současně a konfigurace nových zařízení pomocí šablon.
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
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
Systém musí být schopen zobrazit seznam top žáků / studentů, kteří za dané období ve školní síti přenesli nejvíce dat.
Systém musí být schopen zobrazit polohu a stav všech síťových zařízení v systému v geografické mapě a také graficky zobrazit reálnou fyzickou topologii sítě školy.
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.
Systém musí v případě bezpečnostní brány umožnit konfiguraci FW L3-L7 a IDS/IPS bezpečnostních pravidel, NATu, celkové šířky pásma na uplinku a propustnosti pro klienty a jednotlivé rozpoznané aplikace.
Systém musí být provozován v režimu vysoké dostupnosti.
Základní konektivita a přístup do Internetu musí být pro klienty zachován i v případě, že je Centrální systém řízení a monitorování sítě dočasně nedostupný.
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.
Systém musí umožnit rozdělení administrátorů do skupin s různými právy přístupu.
Pro autentizaci administrátora přistupujícího přes webové rozhraní musí systém podporovat minimálně RADIUS protokol, SAML a dvoufaktorovou autentizaci.
Systém musí být schopen odesílat správcům emailové zprávy o důležitých systémových událostech.
Systém musí být schopen odesílat zprávy na vzdálený SYSLOG server.
Systém musí podporovat SNMP protokol pro vzdálenou správu a monitorování.
Systém musí podporovat XML API pro integraci s navazujícími systémy školy poskytující informace o připojených komponentách sítě a také klientských zařízeních.
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
Systém musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
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.

Integrovaná bezpečnostní brána

Integrovaná bezpečnostní brána je zařízení umožňující vynucení bezpečnostních politik školy, ochranu uživatelů před útoky a také centrální směrování IP paketů mezi různými VLAN školy a překlad adres směrem do Internetu.

Základní technická kritéria (povinné minimální parametry)

Popis
Zařízení musí být možné nainstalovat CAB komunikace 19" 1U rack
Zařízení musí mít minimálně 10x1GE rozhraní 1000BASE-T, 2x1GE rozhraní SFP
Propustnost firewallu musí být alespoň 500 Mbps.
Zařízení musí podporovat minimálně 250.000 současných připojení.
Zařízení musí podporovat minimálně 8.000 nově navázaných spojení za sekundu.
Zařízení musí obsahovat následující možnosti zabezpečení: FW, anti-virus, anti-phishing, IPS, antispoofing, filtrování http a ###https### provozu na základě kategorizace webových stránek (per skupina uživatelů) a web caching.
Kombinovaný výkon (současný běh FW, IPS, AV) musí být minimálně 320 Mbps.
Zařízení musí podporovat IPSec VPN pro připojení vzdálených lokalit.
Zařízení musí podporovat VPN připojení vzdálených klientů.
Zařízení musí podporovat statické směrování.
Zařízení musí podporovat 802.1Q VLAN.
Zařízení musí podporovat 1:1 a 1:N NAT pro překlad IP adres
Zařízení musí podporovat funkci DHCP serveru.
Zařízení musí podporovat funkce pro bezpečné vyhledávání a YouTube pro školy.
Zařízení musí podporovat funkci kontroly souborů pomocí reputační databáze a sandboxingu jako ochranu před malwarem.
Zařízení musí podporovat funkci rozpoznávání klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
Zařízení musí umožnit zakázat komunikaci vybraných klientů a to až dle rozpoznaných tříd aplikací (dle 7. vrstvy ISO/OSI).
Zařízení musí umožnit omezit celkovou propustnost na uplinku a také přístupovou rychlost vybraných klientů a to až dle rozpoznaných tříd aplikací (dle 7. vrstvy ISO/OSI).
Zařízení musí umožnit QoS klasifikaci paketů pomocí DSCP tagu a to až dle rozpoznaných tříd aplikací (dle 7. vrstvy ISO/OSI).

Zařízení musí podporovat redundantní WAN rozhraní s možností dynamické volby odchozího rozhraní per aplikace na základě ztrátovosti, zpoždění a časového rozptylu na příslušné WAN lince.
Zařízení musí umožnit 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) ve formátu NetFlow v9.
Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
Zařízení musí podporovat režim vysoké dostupnosti (pár zařízení) s automatickou obnovou konektivity v případě HW chyby primárního zařízení.
Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
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.
Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

LAN přepínače

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 1 - je inteligentní přepínač s 24x 10/100/1000Base-T porty (s podporou PoE/PoE+) a 4x 1 GE SFP porty k propojení s ostatními síťovými prvky školy.

Základní technická kritéria (povinné minimální parametry)

Popis
Zařízení musí být možné nainstalovat stojanu 19 ".
Zařízení musí mít minimálně 24x RJ-45 10/100/1000Base-T rozhraní.
Zařízení musí mít minimálně 4x 1 GE SFP rozhraní pro uplink/downlink.
RJ-45 rozhraní na zařízení musí podporovat funkci auto-MDIX.
Zařízení musí podporovat virtuální stohování více zařízení stejného typu.
Zařízení musí podporovat PoE (IEEE 802.3af-2003) na alespoň polovině RJ45 rozhraní.
Zařízení musí podporovat PoE+ (IEEE 802.3at-2009) na alespoň čtvrtině RJ45 rozhraní.
Zařízení musí podporovat jumbo frame 9600 bajtů.
Zařízení musí podporovat L2 protokoly: 802.1D, 802.1w, 802.1Q, 802.3ad.
Zařízení musí podporovat minimálně 16000 MAC adres.
Zařízení musí podporovat minimálně 4095 virtuálních sítí LAN (802.1Q).
Zařízení musí podporovat 802.1x na všech rozhraních.
Zařízení musí podporovat autentizaci pomocí MAC adres prostřednictvím protokolu RADIUS.
Propustnost zařízení musí být nejméně 56 Gb/s.
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).
Zařízení musí podporovat zachytávání klientského provozu per port s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
Zařízení musí podporovat funkci testování připojených UTP/STP kabelů – zjištění stavu jednotlivých párů a celkové délky kabelu.
Zařízení musí podporovat funkci rozpoznávání klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
Zařízení musí podporovat filtrování procházejících uživatelských dat dle zdrojových a cílových IP adres a UDP/TCP portů.
Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
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.
Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

LAN přepínač 2 - je inteligentní přepínač s 48x 10/100/1000Base-T porty (s podporou PoE/PoE+) a 4x 1 GE SPF porty k propojení s ostatními síťovými prvky školy.

Základní technická kritéria (povinné minimální parametry)

Popis
Zařízení musí být možné nainstalovat stojanu 19 ".
Zařízení musí mít minimálně 48x RJ-45 10/100/1000Base-T rozhraní.
Zařízení musí mít minimálně 4x 1 GE SFP rozhraní pro uplink/downlink.
Zařízení musí podporovat virtuální stohování více zařízení stejného typu.
RJ-45 rozhraní na zařízení musí podporovat funkci auto-MDIX.
Zařízení musí podporovat PoE (IEEE 802.3af-2003) na alespoň polovině RJ45 rozhraní.
Zařízení musí podporovat PoE+ (IEEE 802.3at-2009) na alespoň čtvrtině RJ45 rozhraní.
Zařízení musí podporovat jumbo frame 9600 bajtů.
Zařízení musí podporovat L2 protokoly: 802.1D, 802.1w, 802.1Q, 802.3ad.
Zařízení musí podporovat minimálně 32000 MAC adres.
Zařízení musí podporovat minimálně 4095 virtuálních sítí LAN (802.1Q).
Zařízení musí podporovat 802.1x na všech rozhraních.
Zařízení musí podporovat autentizaci pomocí MAC adres prostřednictvím protokolu RADIUS.
Propustnost zařízení musí být nejméně 104 Gb/s.
Zbytek jako tab pro typ 1a (od řádku 15 (včetně))

Bezdrátový přístupový bod

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

Základní technická kritéria (povinné minimální parametry)

Popis
Zařízení musí podporovat následující Wi-Fi standardy: 802.11b, 802.11g, 802.11a, 802.11n, 802.11ac Wave2.
Zařízení musí být schopno pracovat současně v pásmu 2,4 GHz a 5 GHz.
Zařízení musí v případě standardu 802.11ac podporovat šířku kanálu až 80MHz.
Zařízení musí podporovat centrálně řízené automatické nastavení výběru kanálu a vysílacích výkonů a to včetně dynamické reakce na změnu prostředí.
Zařízení musí podporovat 2x2:2 MU-MIMO a beamforming.
Zařízení musí podporovat PoE napájení dle standardu 802.3af.
Zařízení musí být dodáno s úchytem na stěnu a/nebo strop.
Zařízení musí být uzamykatelné proti krádeži.
Zařízení musí mít alespoň jedeno 100/1000Base-T rozhraní.
Zařízení musí umožnit konfiguraci minimálně 8 SSID na každém z 802.11 rádií.
Zařízení musí podporovat následující bezpečnostní standardy: WPA2-PSK, WPA2-Enterprise s 802.1X autentizací.
Zařízení musí podporovat šifrování AES.
Zařízení musí podporovat ověřování PEAP (MSCHAPv2)
Zařízení musí podporovat standardy 802.11r, 802.11k a 802.11v pro rychlý roaming klientů a rozložení zátěže mezi jednotlivými AP infrastruktury.
Zařízení musí podporovat VLAN tagging (802.1Q) na jeho ethernetovém rozhraní.
Zařízení podporuje principy QoS dle WMM, 802.1p a DSCP.
Zařízení musí podporovat funkci rozpoznávání tříd klientských aplikací (dle 7. vrstvy ISO/OSI) a identifikaci operačních systémů a hostname klientských zařízení.
Zařízení musí být schopné omezit šířku pásma pro každé jednotlivé SSID, pro každého z klientů a také dle rozpoznaných tříd aplikací (dle 7. vrstvy ISO/OSI).
Zařízení musí umožnit QoS klasifikaci paketů dle rozpoznaných tříd aplikací (dle 7. vrstvy ISO/OSI) pomocí DSCP a 802.1p tagu.
Zařízení musí podporovat BLE (Bluetooth Low Energy) dle specifikace Bluetooth 4.0.
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.
Zařízení musí umožnit filtrování procházejících uživatelských dat dle cílových IP adres a/nebo UDP/TCP portů.
Zařízení musí umožnit zakázat komunikaci vybraných klientů a to až dle rozpoznaných tříd aplikací (dle 7. vrstvy ISO/OSI) a v případě http i dle DNS jména cílového serveru.
Zařízení musí mít integrovánu 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.
Zařízení musí podporovat zachytávání klientského provozu s možností odeslání do ethernetového analyzátoru (např. Wireshark) pro vzdálené řešení problémů připojených klientů.
Zařízení musí podporovat L3 roaming klientských zařízení mezi různými subnety školy.
Zařízení musí umožnit tunelovat SSID pro návštěvy přímo na bezpečnostní bránu v DMZ školy.
Zařízení musí umožnit izolaci jednotlivých uživatelských zařízení tak, aby tato zařízení nemohla komunikovat mezi sebou (v rámci celého SSID školy).
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.
Zařízení musí umožnit spolu s Centrálním systémem řízení a monitorování sítě lokalizaci klientských zařízení v mapě jednotlivých podlaží na základě triangulace dle síly signálu.
Zařízení musí umožnit spolu s Centrálním systémem řízení a monitorování sítě poskytovat analytika na základě počtu bezdrátových klientů (i nepřipojených), síly jejich signálu a doby, kterou v dosahu zařízení strávily.
Zařízení musí být schopné odesílat zprávy na vzdálený SYSLOG server.
Zařízení musí zahrnovat všechny licence pro zajištění požadované funkcionality na období minimálně 60 měsíců.
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.
Zařízení musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

Systém správy mobilních zařízení (MDM)

Systém správy mobilních zařízení umožňuje centrální správu a dohled tabletů a PC v učebnách školy. Aplikace, bezpečnost, SSID profilu, vymazání v případě ztráty, lokalizace v mapě budovy nebo dle GPS

Základní technická kritéria (povinné minimální parametry)

Popis
Systém MDM musí umožňovat monitorování, vynucení bezpečnostních politik a celkovou správu zahrnutých koncových zařízení (tabletů, mobilních telefonů, PC a notebooků).
Systém MDM musí podporovat minimálně následující klientské platformy: - Microsoft Windows a Windows Phone - Apple iOS a OS X - Google Android a Chrome OS
Systém MDM musí umožnit vzdálenou instalaci a správu aplikací na všech podporovaných klientských platformách. V případě MS Windows musí být podporována instalace MSI balíčků přímo ze Systému MDM.
Systém MDM musí být schopen vynutit bezpečnostní politiky a restrikce použití na koncovém zařízení. V závislosti na klientské platformě musí Systém MDM podporovat:

- Vynucení způsobu přihlášení na zařízení (PIN, zamknutí zařízení) - Zakázání fotoaparátu, pořizování kopie obrazovky, instalaci nových aplikací, spouštění vybraných aplikací - Vzdálené vymazání zařízení v případě ztráty nebo krádeže
Systém MDM musí podporovat nástroje pro vzdálené řešení problémů na koncových zařízeních – v závislosti na klientské platformě musí Systém MDM umožnit monitorování využití systémových prostředků (CPU, paměť, disky), funkci vzdálené plochy, zaslání kopie obrazovky, vypsání běžících procesů a restart zařízení.
Systém MDM musí být schopen zobrazit ztracené koncové zařízení na mapě na základě lokalizačních dat z WiFi, GPS souřadnic nebo jeho IP adresy. V závislosti na poloze zařízení musí Systém MDM podporovat dynamickou změnu jeho bezpečnostního profilu.
Systém MDM musí umožnit vzdálenou správu síťových profilů koncového zařízení včetně nastavení přístupu do bezdrátové sítě a VPN konektivity.
Systém MDM musí být v kombinaci s ostatními komponentami sítě schopný vynutit MDM politiky při přístupu zařízení do sítě – nastavit / obnovit bezpečnostní politiky a restrikce určené pro dané koncové zařízení a případně i zajistit instalaci MDM klienta na nově připojené zařízení.
Systém MDM musí umožnit vzdálenou správu koncového zařízení i v případě, že je toto zařízení připojeno do Internetu mimo prostředí interní infrastruktury školy.
Systém MDM musí být schopen poskytnout analytika síťových aktivit klientů pomocí automatizovaného vytváření přehledů o připojených BYOD klientech, objemu jimi přenesených dat a procentuální zobrazení přenosů v kontextu všech ostatních klientů.
Systém MDM musí umožnit zasílání souhrnných přehledů sítě emailem a to i podle automatického rozvrhu.
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 MDM musí být v době prodeje výrobcem plně podporován a nesmí být pro něj vyhlášeno ukončení prodeje.
Systém MDM musí podporovat plnou správu a monitorování prostřednictvím Centrálního systému řízení a monitorování sítě.

Požadavky na sondu

Základní technická kritéria (povinné minimální parametry)

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	
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	
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	
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	
Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména	
Správa uživatelů a přístupových práv na zařízení	
Podpora vzdálené autentizace uživatelů	LDAP (Active Directory)
Plná zákaznická podpora v českém jazyce	

Firewall se službami

centrálně spravován pomocí programu management, který poskytuje bezpečnostním týmům komplexní přehled sítě a kontrolu nad činnostmi v ní. Takový přehled zahrnuje uživatele, zařízení, komunikaci mezi virtuálními stroji, slabiny, hrozby, aplikace na straně klienta, složky a webové stránky.

Bezpečnostní zařízení musí splňovat všechny parametry podle níže uvedené specifikace:

- Stavový aplikační firewall jako samostatné HW zařízení, který musí nabízet
  - Dynamický a statický NAT/PAT (překlad IP adres)
  - Podporu dynamických směrovacích protokolů RIP, OSPF (BGP výhodou)
  - Plnou podporou protokolu IPv6
  - Redundanci pro případ výpadku ve formě Active/Active failover, Active/Standby failover nebo cluster
- Aplikační firewall
  - Pokročilá hloubková analýza dat na aplikačních (L5-L7) vrstvách ISO modelu
  - Rozeznávání a kategorizace aplikací, geografických lokalit, uživatelů
  - Identifikace a zamezení přístupu na nedůvěryhodné či škodlivé webové stránky
  - Možnost omezení přístupu uživatele do Internetu na základě důvěryhodnosti či bezpečnosti kategorie cílové webové stránky s možností definice vlastních kategorií
- IPS senzor, který musí nabízet
  - Detekci a hloubkovou analýzu dat na aplikační (L2-L7) vrstvě ISO modelu
  - Aktivace licencí a (případně) přidáním softwarového modulu
  - Automatickou aktualizací signatur
  - Funkcionalitu NGIPS (senzor tzv. „nové generace“) schopného plně vnímat souvislosti (kontext) datové komunikace pomocí parametrů včetně, ale bez omezení na: kdo komunikuje (uživatel), odkud kam komunikuje (síť), z čeho komunikuje (zařízení), kdy komunikuje (čas), typ komunikace (aplikace), obsah komunikace apod.
  - Pokročilou podporu pro detekci, blokování, sledování, analýzu, opravu škodlivých datových toků (Advanced Malware Protection)
  - Zhodnocování dopadů a korelace událostí a následné automatické ladění politik
  - Globální korelace a možnost ovlivnit rozhodování s využitím dat z cizích systémů v reálném čase

- URL Filtrace
  - Možnost omezení přístupu uživatele do Internetu na základě URL filtrace s využitím předdefinovaných URL kategorií
  - Možnost omezení přístupu uživatele do Internetu na základě URL filtrace s využitím reputace URL definované od výrobce
- Fyzicky musí firewall mít
  - Minimálně 8 Gigabit Ethernet metalických rozhraní pro datovou komunikaci
  - Minimálně 1 Gigabit Ethernet metalických rozhraní pro management
  - Možnost rozšíření o optické nebo metalické Gigabit Ethernet porty formou externího modulu. Alespoň 6 portů v modulu
  - Alespoň 1 zdroj napájení
- VPN koncentrátor
  - Zakončení „full-tunnel“ IPSec nebo SSL VPN pro alespoň 300 současné připojených uživatelů
  - Možnost „odlehčené“ SSL VPN pro uživatele formou zabezpečeného přístupu na webový portál
  - Zakončení alespoň 300 současně připojených site-to-site IPsec tunelů
  - Implementace IPsec musí podporovat protokoly IKEv1 i IKEv2 a šifrovací standardy 3DES/AES a algoritmy nové generace popsané ve standardu NSA Suite-B
- Výkonnostní parametry
  - Minimální „hrubá“ propustnost firewallu 1.8 Gbps
  - Minimální propustnost firewallu (stateful IMIX provoz) – 900 Gbps
  - Minimální propustnost NGFW (hloubková inspekce) 850 Mbps
  - Minimální propustnost NGFW (hloubková inspekce + IPS modulem) minimálně 450 Mbps.
  - Počet současně procházejících spojení alespoň 250,000
  - Počet nově založených spojení alespoň 20,000 za sekundu
  - Alespoň 100 L3 virtuálních rozhraní (L3 zakončených VLAN)
  - Počet paketů (64 bytové) za sekundu minimálně 750,000
  - Minimální propustnost pro IPsec VPN komunikaci (šifrování 3DES/AES) 250 Mbps
  - Minimální počet souběžných VPN tunelů (IKEv1 nebo IKEv2) 300
  - Minimální počet podporovaných virtuálních kontextů 5
- Kompatibilita
  - Otevřené API pro integraci se systémy třetích stran
- Management
  - Správa pomocí příkazové řádky, SNMP a grafického rozhraní
  - Správa zařízení může být on-box i off-box
  - Napájení ze sítě střídavého napětí 230V

Maximální výška 1RU

Koordinační opatření

Během výstavby a montáže je nutné koordinovaně postupovat s ostatními profesemi a zamezovat zbytečným vícepracím. Veškeré projektové změny je nutno konzultovat se zástupcem investora nebo zodpovědným projektantem.

Bezpečnost a ochrana zdraví při práci

Při provádění stavebních prací je třeba dodržovat ze strany dodavatele všechny podmínky pro ochranu a bezpečnost zdraví podle zákona č. 309/2006 Sb, nařízení vlády č. 591/2006 Sb, nařízení vlády 101/2005 Sb, nařízení vlády 362/2005 Sb.

Zhodnocení stavby s ohledem na životní prostředí, nakládání s odpady.

Odpady vzniklé při provádění stavebních pracích budou vyvezeny na organizovanou skládku. Odpady vzniklé při pokládce trubek a montáže kabelů budou odevzdány k druhotnému zpracování do sběrných surovin. Veškeré trubky a kabely jsou vůči okolí fyzikálně neutrální.