Příloha č.1

Technická specifikace

smlouvy s názvem:

„Dodávka HW zařízení a SW aplikací – Městský úřad Jičín“

1. Identifikační údaje zadavatele

Název:	Město Jičín
Sídlo:	Žižkovo náměstí 18, 506 01 Jičín
Zastoupený:	JUDr. Jan Malý, starosta města
IČO:	00271632

2. Identifikace účastníka

Název:	Aricoma Systems a.s.
Sídlo:	Hornopolní 3322/34, 702 00 Ostrava
Osoba oprávněná za účastníka jednat:	Jaroslav Dvořák, člen představenstva Tomáš Ječmínek, člen představenstva
IČ:	04308697

3. Předmět veřejné zakázky – technická specifikace HW zařízení a SW aplikací

Pro zajištění vysoké dostupnosti serverové infrastruktury bude ke stávající serverovně v hlavní budově MěÚ Jičín na adrese: Žižkovo náměstí čp. 18, doplněna druhá serverovna v budově „Aris“, na adrese: 17. listopadu 16, čímž vznikne plnohodnotná, geograficky oddělená serverovna s redundantním prostředím.

Dojde k rozšíření stávající virtuální infrastruktury o 2 nody (servery) a dvě disková úložiště v režimu tzv. „metro clusteru“. Jedno diskové pole bude umístěno v lokalitě Žižkovo náměstí a druhé diskové pole bude umístěno v budově „Aris“. Pro správnou funkci metro clusteru bude ve třetí lokalitě instalován tzv. Quorum/Witness server (svědek/rozhodčí).

Stávající dva nody budou doplněny o kompatibilní 10GE síťové karty dle specifikace ve výkazu/výměr.

Součástí dodávky bude licenční rozšíření stávající virtualizační infrastruktury pro nové nody v budově „Aris“. Nové nody se tak začlení do stávající virtualizační infrastruktury se shodnou správou, zálohováním atd. (stávající nody mají licenci VMware Enterprise).

Serverovny „Aris“ a Žižkovo nám. budou vybaveny záložními zdroji napájení (UPS) o min. výkonu 8 kW a nezbytným počtem baterií.

Stávající řešení zálohování na platformě Veeam bude rozšířeno o specializované úložiště tzv. Hardened Repository ve formě dedikovaného serveru s dostatečnou kapacitou storage. Zadavatel vlastní licenční pokrytí zálohovacího SW Veeam Data Platform Essentials Standard pro 4 sockety, které již výrobce nenabízí. Podpora této licence vyprší 30. 8. 2025. Součástí projektu je prodloužení podpory výrobce o 36 měsíců a migrace na nový licenční model výrobce.

Stávající virtualizační infrastruktura bude rozšířena o dva nové nody v budově „Aris“. Tyto dva nody budou zalicencovány kompatibilním OS Windows Server 2025 DataCenter, nezbytným počtem uživatelských CAL licencí a licencí External Connector pro přístup uživatelů mimo doménu MěÚ Jičín.

Jako databázový server bude využit Microsoft SQL server 2025 Standard tak, aby mohla v lokalitě běžet veškerá agenda.

Stávající síťová infrastruktura bude modernizována tak, aby bylo zajištěno řízení přístupu k síťovým zdrojům na bázi protokolu 802.1x.

Přístup k síťovým zdrojům bude řízen specializovaným SW – Autentizační platformou (AAA), který bude implementován jako virtuální appliance pro platformu VMware.

Protokol 802.x bude implementován na drátovou i bezdrátovou část sítě. V bezdrátové části sítě bude vytvořena zabezpečená a logicky oddělená sít pro návštěvníky.

Součástí modernizace sítě bude mimo jiné zajištění vysoké dostupnosti páteřních přepínačů, které budou fyzicky umístěny v lokalitách Žižkovo náměstí a „Aris“. Dva páteřní přepínače budou vzájemně propojeny 2x 100GE optickými SM propoji tak, že vytvoří jeden logický páteřní přepínač.

K tomuto logickému páteřnímu přepínači budou redundantně (4x 25GE) připojeny oba stohy datacentrových přepínačů v lokalitách Žižkovo náměstí a „Aris“. Takové zapojení, spolu s validní konfigurací všech přepínačů zajistí vysokou dostupnost síťové infrastruktury, kdy při výpadku jednoho fyzického přepínače (páteřního nebo datacentrového) nebude ohrožena páteřní síťová komunikace.

Stejným způsobem tzn. také redundantně (2x 10 GE) budou k logickému páteřnímu přepínači připojeny oba NGFW v HA zapojení.

Stávající řešení zabezpečení perimetru sítě bude nahrazeno dvojicí NGFW v HA zapojení, tak, aby v případě HW výpadku jednoho boxu nebyla ohrožena komunikace do sítě Internet.

Jeden box bude umístěn v lokalitě Žižkovo náměstí, kam má zadavatel přivedenu Internetovou konektivitu, druhý box bude umístěn v lokalitě Aris. Internetová konektivita do lokality „Aris“ bude přivedena jedním optickým SM vláknem ve vlastnictví zadavatele z lokality Žižkovo náměstí.

ISP poskytuje zadavateli v lokalitě Žižkovo náměstí min. 2x SFP rozhraní na zařízení JUNIPER SRX340, které je pod správou ISP.

Oba NGFW zadavatele budou k ISP připojeny pomocí single mode single fiber (WDM) tranceiverů a pomocí stejné technologie single mode single fiber budou oba boxy propojeny 1GE optickým spojem (Heart beat).

Zapojení NGFW do sítě LAN bude v obou lokalitách obdobné. Každý box NGFW bude připojen redundantně pomocí metalických 2x10GE DAC kabelů, k páteřním přepínačům dané serverovny.

Součástí řešení perimetru sítě bude specializovaný logovací nástroj – Analyzer, pro cílené vyhodnocení logovaných událostí z NGFW včetně retrospektivní analýzy logů. Tento specializovaný nástroj s omezenou retencí logovaných událostí bude integrován s centrálním log managementem, který zajistí dlouhodobé uložení logů, jejich korelaci s událostmi z jiných systémů, reporting apod.

Pro ochranu webových aplikací bude v DMZ nasazen Webový aplikační FW (WAF).

Na koncových stanicích bude implementováno pokročilé centrálně řízené XDR řešení, které zajistí proaktivní ochranu koncových zařízení.

Stávající nesystémové opensource řešení sběru logů pomocí dvou virtuálních systémů AlienVault a Greylog není centralizované, nemá dostatečný výkon, nemá připojeny všechny potřebné zdroje a neumožňuje dlouhodobou retenci a centralizované vyhodnocení nasbíraných bezpečnostních událostí.

Do infrastruktury proto bude implementován specializovaný systém pro centrální sběr, dlouhodobou retenci a vyhodnocení bezpečnostních událostí provozovaných IT systémů a aplikací.

Systém bude umožňovat rychlé prohledávání, korelaci a reporting uložených dat. Nezbytnou součástí implementace bude nastavení jednotného času pro všechny dotčené systémy.

Zadavatel pořídil v roce 2024 200 ks hybridních čipových karet a 130 ks čteček CT30. Součástí dodávky je implementace Certifikační Autority (CA) na platformě Windows Server a implementace SW pro správu životního cyklu karet a certifikátů s licencí na dobu neurčitou. Využití hybridních čipových karet zajistí 2faktorovou autentizaci uživatelů (MFA), pomocí PKI uživatelských certifikátů uložených v kontaktním čipu karty.

Podrobnou technickou specifikaci (k jednotlivým částem plnění této veřejné zakázky uvádí zadavatel níže.

Zadavatel požaduje, aby dodavatelem nabízené zboží splňovalo **veškeré** níže uvedené **minimální** požadavky (funkcionality a parametry) a tyto byly zahrnuty v jeho nabídce a v celkové ceně.

1. Nod virtualizační infrastruktury (server) – 2 ks

- Jednosocketový server o velikosti 1U včetně ramena pro vedení kabelů umožňujícího vysunutí zapnutého serveru z racku pro servisní účely.
- Podpora procesorů 3-tí generace AMD EPYC Processors (kompatibilní se stávajícími dvěma nody).
- 1 procesor o frekvenci 3GHz, 16 core, podpora HT, min. výkon CPU dle PassMark - CPU Mark celkové hodnocení jednoho je min. 41000 bodů, 1-vláknová operace min. 2600 bodů.
- Podpora pamětí DDR-4 3200 MT/s.
- Možnost maximálního rozšíření operační paměti na minimálně 16x DIMM
- Osazeno 768GB DDR-4 RAM
- Osazeno 2x 480GB M.2 NVMe v RAID1 pro boot operačního systému
- 4 porty USB 3.0, z toho 1x interní pro aplikační klíče
- 2x 10/25Gb port Ethernet s rozhraním SFP+, včetně 2x 3m DAC, s podporou technologií VLAN tagging, adaptive interrupt coalescing, MSI-X, NIC teaming (bonding), Receive Side Scaling (RSS), jumbo frames, PXE boot a virtualizační technologie jako VMware NetQueue a Microsoft VMQ nezabírající rozšiřující PCIe sloty.
- 2x 10/25Gb port Ethernet s rozhraním SFP+ včetně 2x 3m DAC, s podporou technologií VLAN tagging, adaptive interrupt coalescing, MSI-X, NIC teaming (bonding), Receive Side Scaling (RSS), jumbo frames, PXE boot a virtualizační technologie jako VMware NetQueue a Microsoft VMQ.
- Ventilátory v serveru jsou vyměnitelné za provozu a redundantní
- 2x napájecí zdroje s redundancí napájení 1+1, min. požadovaný výkon jednoho zdroje je 1000 W
- Zdroje podporují řízení spotřeby CPU instalovaných v poptávaných serverech
- Zdroje splňují požadavky na certifikaci energetické účinnosti, např. ECOS Consulting 80 Plus (min. Titanium).
- Všechny základní nástroje, ovladače a agenti nutné pro instalaci a administraci serveru budou obsaženy uvnitř serveru bez nutnosti jejich instalace z externího zařízení. Server obsahuje

vestavěný nástroj pro update systému, který je schopný si nejnovější ovladače stáhnout od výrobce.

- Technická podpora výrobce po dobu 36 měsíců od převzetí zboží v režimu 24x7 se zahájením opravy v místě instalace nejpozději do 4 hodin po nahlášení závady.
- Telefonická podpora v režimu 24x7 se zpětným zavoláním nejpozději do 15 minut pro incidenty kritické závažnosti a do 1 hodiny pro ostatní incidenty.
- Přítomnost serveru na VMware Compability Guide pro Servers pro ESXi vSphere 7.0 update 3, 8.0 update 3
- Integrovaná vzdálená správa prostřednictvím dedikovaného 1G portu:
  - úložiště pro firmware, ovladače a další sw komponenty
  - konfigurovatelné úložiště pro vytváření instalačních sad s možností rollback/patch při pádu aktualizace
  - bezagentový vzdálený management
  - podpora pro standardní webové prohlížeče pro Java free grafickou vzdálenou konzoli
  - grafické „tlačítko“ pro Virtual Power
  - podpora pro vzdálený boot z DVD/CD/USB zařízení
  - uložení historických dat o sw upgradech a patchích
  - podpora pro vícefaktorovou autentikace
  - monitoring změny v HW a systémové konfiguraci
  - rychlá diagnostika
  - přístup min. 5 uživatelům během pre-OS a OS runtime operací
  - schopnost uchovat video z poslední zásadní poruchy a posledního bootovacího procesu
  - podpora MS TS integrace včetně 128bitové SSL enkrypce
  - podpora pro Secure Shell Version 2
  - podpora AES a 3DES na prohlížeči
  - vzdálený firmware update
  - podpora RESTFull API integrace
  - podpora automatického předávání HW událostí přímo výrobci serveru.
- Server management
  - rychlý pohled na spravované serverové zdroje
  - minimální zobrazované položky Dashboardu jsou Server Profiles, Server Hardware a Appliance Alerts
  - přístup do managementu je řízen pomocí rolí
  - management SW musí být integrovatelný minimálně do VMware vCenter a Microsoft SCVMM
  - proaktivní notifikace o aktuálních nebo hrozících selháních kritických komponent jako jsou procesory, paměť a disky
  - management dostupný přes vlastní portál odkudkoliv
  - upozornění na out-of-date BIOS, ovladače a agenty server managementu
  - vzdálený update těchto komponent
  - server management SW od stejného výrobce, jako je výrobce serveru

2. Diskové úložiště - 2 ks

- all NVMe architektura
- active-active replikace a funkce Metro Clusteru pro nulové RPO a RTO tak, aby daný pár svazků mezi primární a DR lokalitou mohl mít souběžný přístup k operacím čtení i zápisu.

- replikace typu active-active je podporována pro běžné operační systémy, jako je VMware, RHEL, SLES, Windows.
- podpora pro obvyklé platformy operačních systémů a cluster funkcí včetně Windows Server 2019/2022, VMware ESXI 7/8, Red Hat Enterprise Linux (RHEL) a SUSE Enterprise Server (SLES) atd.
- dva redundantní řadiče
- užitná kapacita minimálně 16TiB bez započtení redukčních mechanismů s použitím min. 12ks šifrovaných disků a alespoň RAID 6 ochranou.
- poměr datové a paritní kapacity není větší než 10D+2P
- doložení úložné kapacity výstupem z konfigurátoru výrobce
- úložiště je odolné proti výpadku nejméně 2 disků současně v rámci jedné RAID skupiny
- šifrované disky s příslušnými šifrovacími licencemi
- šifrování není založené na řadiči nebo softwaru
- aktivní architektura tak, že každý logický disk je rozložen na všechny disky a všechny disky přispívat IO do obou řadičů současně
- redundantní komponenty (tzv. No Single Point of Failure), minimálně řadiče pole, cache, ventilátory, zdroje napájení
- 512GB paměti celkem na obou řadičích
- 8 portů 10/25GE, včetně 8 ks 10GE DAC
- rozšiřitelné připojení na 25 Gb/s pouze výměnou DAC nebo SFP+ transcieverů
- distribuovaný globální rezervní prostor (global spare)
- inline engine s redukčními technologiemi pro efektivní ukládání dat (podpora Thin Zero detect and re-claim, De-duplication a Compression)
- funkce Thin Provisioning, Thin Re-claim, Snapshot, deduplikace, komprese, vzdálené replikace, monitoring výkonu a kvality služeb pro dodanou kapacitu pole
- nativní cloud konzole pro správu neomezeného počtu polí
- nativně cloudová aplikace pro správu tak, že během životního cyklu smlouvy o podpoře je nabízena jako služba a není třeba aplikaci pro správu konfigurovat, aktualizovat a záplatovat
- úložiště má jako součást nabídky monitoring s podporou cloudu, AI a analytický engine pro proaktivní správu úložiště a zmírnění rizik
- úložiště podporuje kvalitu služeb (QoS) pro kritické aplikace, aby bylo možné definovat vhodnou a požadovanou dobu odezvy pro logické jednotky aplikací v úložišti
- je možné definovat různé služby/doby odezvy pro různé aplikační logické jednotky
- online aktualizace firmwaru řadičů a diskových jednotek bez nutnosti restartu řadiče.
- technická podpora výrobce po dobu 36 měsíců od převzetí zboží v režimu 24x7
- telefonická podpora v režimu 24x7 se zpětným zavoláním nejpozději do 15 minut pro incidenty kritické závažnosti a do 1 hodiny pro ostatní incidenty

3. Quorum/Witness server (tzv. „svědek“) – 1 ks

- CPU 4 core 2,6GHz
- 32GB RAM s možností rozšíření až na 128GB
- 2x 480GB SSD DWPD1 v RAID1
- 2x 1Gbit Base-T
- TPM2.0
- Integrovaná vzdálená správa prostřednictvím dedikovaného 1G portu:
  - úložiště pro firmware, ovladače a další sw komponenty

- konfigurovatelné úložiště pro vytváření instalačních sad s možností rollback/patch při pádu aktualizace
- bezagentový vzdálený management
- podpora pro standardní webové prohlížeče pro Java free grafickou vzdálenou konzoli
- grafické „tlačítko“ pro Virtual Power
- podpora pro vzdálený boot z DVD/CD/USB zařízení
- uložení historických dat o sw upgradech a patchích
- podpora pro vícefaktorovou autentikace
- monitoring změny v HW a systémové konfiguraci
- rychlá diagnostika
- přístup min. 5 uživatelům během pre-OS a OS runtime operací
- schopnost uchovat video z poslední zásadní poruchy a posledního bootovacího procesu
- podpora MS TS integrace včetně 128bitové SSL enkrypce
- podpora pro Secure Shell Version 2
- podpora AES a 3DES na prohlížeči
- vzdálený firmware update
- podpora RESTFull API integrace
- podpora automatického předávání HW událostí přímo výrobci serveru
- technická telefonická podpora výrobce po dobu 36 měsíců od převzetí zboží v režimu 24x7 se zpětným zavoláním nejpozději do 15 minut pro incidenty kritické závažnosti a do 1 hodiny pro ostatní incidenty

4. Hardened Repository – 1 ks

- Dvousocketový server o velikosti 2U včetně ramena pro vedení kabelů umožňujícího vysunutí zapnutého serveru z racku pro servisní účely.
- Podpora procesorů 5. generace Intel Xeon Processors
- 1x procesor o frekvenci 2GHz, 16 core
- TPM 2.0.
- Podpora pamětí DDR-5 5800 MT/s.
- Možnost maximálního rozšíření operační paměti na minimálně 32x DIMM.
- Osazeno 64GB DDR-5 RAM
- Osazeno 2x 480 GB M.2 NVMe v RAID1 pro boot operačního systému
- Osazeno 16x12TB SAS 7.2k RAID6, min. 2 sloty volné pro další rozšíření.
- 12Gb/s SAS, 16G NVMe Raid řadič s RAID 0/5/50/6/60/1, 8GB battery backed write cache. Diskový řadič podporuje Secure encryption/data at rest Encryption.
- 4 porty USB 3.0, z toho minimálně 1x interní pro aplikační klíče
- 2x 10Gb port Ethernet s rozhraním SFP+ včetně 2x 3m DAC, s podporou technologií VLAN tagging, adaptive interrupt coalescing, MSI-X, NIC teaming (bonding), Receive Side Scaling (RSS), jumbo frames, nezabírající rozšiřující PCIe sloty.
- Ventilátory v serveru jsou vyměnitelné za provozu a redundantní
- 2x napájecí zdroje s redundancí napájení 1+1, min. požadovaný výkon jednoho zdroje je 1000 W
- Zdroje podporují řízení spotřeby CPU instalovaných v poptávaných serverech
- Zdroje splňují požadavky na certifikaci energetické účinnosti, např. ECOS Consulting 80 Plus (min. Titanium).
- Všechny základní nástroje, ovladače a agenti nutné pro instalaci a administraci serveru jsou obsaženy uvnitř serveru bez nutnosti jejich instalace z externího zařízení. Server obsahuje

vestavěný nástroj pro update systému, který je schopný si nejnovější ovladače stáhnout od výrobce.

- Integrovaná vzdálená správa prostřednictvím dedikovaného 1G portu:
  - úložiště pro firmware, ovladače a další sw komponenty
  - konfigurovatelné úložiště pro vytváření instalačních sad s možností rollback/patch při pádu aktualizace
  - bezagentový vzdálený management
  - podpora pro standardní webové prohlížeče pro Java free grafickou vzdálenou konzoli
  - grafické „tlačítko“ pro Virtual Power
  - podpora pro vzdálený boot z DVD/CD/USB zařízení
  - uložení historických dat o sw upgradech a patchích
  - podpora pro vícefaktorovou autentikaci
  - monitoring změny v HW a systémové konfiguraci
  - rychlá diagnostika
  - přístup min. 5 uživatelům během pre-OS a OS runtime operací
  - schopnost uchovat video z poslední zásadní poruchy a posledního bootovacího procesu
  - podpora MS TS integrace včetně 128bitové SSL enkrypce
  - podpora pro Secure Shell Version 2
  - podpora AES a 3DES na prohlížeči
  - vzdálený firmware update
  - podpora RESTFull API integrace
  - podpora automatického předávání HW událostí přímo výrobci serveru.
- Server management
  - rychlý pohled na spravované serverové zdroje
  - minimální zobrazované položky Dashboardu jsou Server Profiles, Server Hardware a Appliance Alerts
  - přístup do managementu musí být řízen pomocí rolí
  - management SW je integrovatelný minimálně do VMware vCenter a Microsoft SCVMM
  - proaktivní notifikace o aktuálních nebo hrozících selháních kritických komponent jako jsou procesory, paměť a disky
  - management dostupný přes vlastní portál odkudkoliv
  - upozornění na out-of-date BIOS, ovladače a agenty server managementu
  - vzdálený update těchto komponent
  - server management SW od stejného výrobce, jako je výrobce serveru
- Technická podpora výrobce po dobu 36 měsíců od převzetí zboží v režimu 24x7
- Telefonická podpora v režimu 24x7 se zpětným zavoláním nejpozději do 15 minut pro incidenty kritické závažnosti a do 1 hodiny pro ostatní incidenty

5. Virtualizační software - soubor

- Virtualizační software ve verzi Enterprise Plus, licence pro 32 procesorových jader
- Licence na min. 36 měsíců
- Hypervizor instalovaný přímo na fyzické železo
- Podpora Guset OS Windows, Linux, Solaris nad x86/x64 instrukční sadou
- Možnost přidělit VM více RAM než má fyzický server
- Možnost přidělit VM více diskového prostoru
- Maximální velikost virtuálního disku 62TB
- Podpora migrace VM za běhu mezi fyzickými servery
- Podpora migrace VM za běhu mezi diskovými úložišti

- Správa z jednoho místa, bez ohledu na to, na kterém fyzickém serveru VM běží
- Podpora pro použití Šablon VM, pro rychlejší vytváření VM
- Podpora pro offloading některých funkcí na úroveň diskového pole (kopírování, TRIM/UNMAP, zamykání bloků)
- Podpora knihovny obsahu - centralizovaná správa pro šablony virtuálních strojů, virtuální zařízení, obrazy ISO a skripty
- Podpora virtuálních Volumes - Virtualizace externích úložišť (SAN a NAS) a poskytuje správu úložiště založenou na zásadách VM
- Podpora optimalizace uhlíkové stopy energeticky náročných pracovní zátěže a využití prostoje ke konsolidaci zátěže
- Podpora společné správy napříč vrstvami úložiště a dynamická automatizace třídy služeb úložiště prostřednictvím roviny řízené zásadami.

6. UPS záložní zdroj – 2 ks

- Provedení tower
- Hloubka 80 cm, výška 150 cm, šířka max. 80 cm
- Výkon 8 kW rozšiřitelný na 15 kW
- Pevné připojení vstupu (3 fáze)
- Vstupní jmenovité napětí 400V (380/400/415V)
- Napájecí moduly vyměnitelné za provozu
- Pevné připojení výstupu (1 fáze)
- Výstupní napětí 220-240V
- Výstupní frekvence 50 Hz
- Online topologie
- Interní údržbový bypass
- Doba běhu při plné zátěži 45 minut
- Vzdálené monitorování a řízení UPS
- Vzdálená správa min. SSH v2, HTTPS, SNMP v3, telnet
- Součástí dodávky každé UPS je i protokolová datová jednotka (PDU) s montáží do datového rozvaděče min. 12x zásuvka C13 a min. 12x zásuvka C39
- Záruka 60 měs.

7. Doplnění stávajících serverů – soubor

- 2x HPE DL325 Gen10+ x16 LP PCIe Riser Kit
- 2x BCM 57412 10GbE 2p SFP
- Adaptér vč. 2x 3m DAC kabelů

8. Sada licencí software – soubor

- 2x operační serverový systém v nejnovější verzi, plně kompatibilní se současnými serverovými operačními systémy zadavatele. Licence na minimálně 16 procesorových jader. Licence pro neomezený počet provozovaných virtuálních serverů.
- 1x operační serverový systém v nejnovější verzi, plně kompatibilní se současnými serverovými operačními systémy zadavatele. Licence na minimálně 16 procesorových jader. Licence pro 2ks provozovaných virtuálních serverů.
- 205x klientská licence pro serverový operační systém v nejnovější verzi a plně kompatibilní se současnými i nově dodávanými serverovými operačními systémy zadavatele.

- 1x MS SQL Server 2025 v edici Standard pro 4 Core včetně SA na 3 roky pro běh ve virtuálním prostředí.
- 1x přístupová licence pro serverový operační systém. Licence pro přístup k serveru pro neomezený počet externích anonymních uživatelů.

9. Autentizační platforma (AAA) – soubor

- Autentizační platforma (AAA) pro řízení přístupu uživatelů a zařízení do LAN a WiFi
- Virtuální appliance pro on-premise prostředí VMware
- Virtuální appliance bez nutnosti dodatečných licencí např. pro OS nebo databáze.
- Podpora řešení vysoké dostupnosti tak, aby v případě výpadku primárního AAA serveru převzal jeho roli sekundární server
- Možnost vytváření clusteru více virtuálních appliance
- Cluster poskytuje vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance
- Celková kapacita řešení současně autentizovaných zařízení (pomocí 802.1x): 1 000
- Metody autentizace uživatelů a zařízení:
  - PEAP-MSCHAPv2,
  - EAP-TLS,
  - EAP-TTLS,
  - MAC autentizace
- Podpora RADIUS pro autentizaci, autorizaci, zaznamenávání a proxy funkci pro externí RADIUS
- Podpora RadSec (RADIUS over TLS)
- Podpora RADIUS CoA dle RFC3576
- Podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v MS Active Directory
- Možnost autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. za účelem omezení celkového času online či objemu přenesených dat za delší časové období
- Možnost TACACS+ autentizace správců síťových zařízení
- Řízení konfiguračních nebo přehledových příkazů na prvcích infrastruktury podle role administrátora
- Možnost definice sad příkazů a jejich přiřazení podle role administrátora
- Možnost integrace vícefaktorové autentizace pro řízení přístupu k prvkům sítě
- Okamžité informace o prováděných příkazech na síťových zařízeních
- Další požadované autentizační a autorizační zdroje a metody
- Ověření uživatelů heslem nebo certifikátem
- Interní databáze pro uživatele i koncová zařízení
- Zaznamenávání aktivity uživatelů a zařízení připojených k síti
- Snadné vytváření časově omezených oprávnění pro přístup k síti nebo do internetu pro hosty, externí spolupracovníky apod.
- Samoobslužný portál pro uživatele
- Registrace zařízení pomocí MAC adresy pro non-IT uživatele - omezená funkce administračního rozhraní, se zařazením zařízení do skupiny s definovanou politikou přístupu.
- Systém pro bezpečnostní kontrolu přistupujících zařízení před jejich vpuštěním do sítě pomocí software agenta na koncová zařízení. Lincence pro 500 takto kontrolovaných zařízení
- Možnost kontroly stavu registrů, spuštěných procesů, stavu síťových zařízení, nastavení firewallu, aktualizace antivirů, instalované VM, stav enkrypce disku

- Podpora jednorázového i permanentního klienta pro kontroly na koncových zařízeních.
- Podpora klienta pro kontrolu koncových zařízení na OS Windows, MAC OS a Linux
- Podpora REST API pro většinu základních úkonů AAA platformy
- Řízení přístupu k síti pomocí filtrů nebo přiřazením do VLAN sítě podle:
    - uživatele (role, skupiny),
    - stavu a typu koncového zařízení,
    - místa připojení,
    - historie připojení
- Omezení přístupu k síti pomocí filtrů aplikovaných na vstupu do sítě
- Zpracovávání syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení.
- Sběr dodatečných informací o připojených zařízeních ("profiling") jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě.
- LAN a WLAN Guest portál. Portál obsahuje možnost přihlašování přes účty minimálně těchto sociálních sítí – Linkedln, Facebook, Twitter. Portál umožňuje bohatou grafickou úpravu včetně možnosti přidávání videí a dalšího dynamického obsahu. Možnost samoobslužné registrace hosta do sítě pomocí SMS, email ověřením nebo na elektronickou notifikaci a schválení pověřených pracovníků.
- Centralizovaná správa s grafickým rozhraním
- Definice rolí administrátorů a úrovní přístupu k ověřovacímu systému
- Zjednodušení správy vytvářením skupin uživatelů, koncových a síťových zařízení
- Zaznamenávání událostí na externí syslog server
- Podpora SNMPv3
- NTP pro synchronizaci času
- Certifikace Common Criteria a FIPS 140-2
- Automatické zakázání non-FIPS autentizačních protokolů (např. PAP/ASCII, CHAP, and MS-CHAPv1) při aktivaci FIPS módu
- Systém podporuje funkce na poptávaném bezdrátovém řešení a přepínačích
- Jakékoliv funkční rozšíření systému je vždy v rámci stejné virtuální appliance jako je AAA systém
- Servisní podpora výrobce, včetně bezplatných aktualizací a přístupu na servisní portál výrobce po dobu 36 měsíců

10. Páteřní přepínač – 2 ks

- Typ přepínače: L3 switch
- Montáž do racku, velikost max. 1U
- Počet 1/10/25Gbps portů s volitelným fyzickým rozhraním: 16
- Počet 40/100Gbp portů s volitelným fyzickým rozhraním: 2
- Podpora rozdělení 40GE portů na 4x10GE a 100GE portů na 4x25GE
- Redundantní interní hot-swap napájecí zdroj
- Redundantní hot-swap ventilátory
- Směr proudění vzduchu zařízením: předo-zadní
- Celková přepínací propustnost přepínače: 1,2 Tbps
- Celkový paketový výkon přepínače: 540 Mpps
- Podporovaný počet přepínačů ve stohu: 2
- Kapacita stohovacího propojení: až 200 Gbps

- Redundance řídícího prvku v rámci stohu
- Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)
- Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)
- Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF
- Podpora upgrade OS ve stohu bez narušení provozu (ISSU/Live upgrade)
- Podpora automatizace upgrade OS ve stohu bez narušení provozu přes REST API
- Podpora "jumbo rámců" včetně velikosti 9198 Byte
- Podpora linkové agregace IEEE 802.1AX
- Počet LACP skupin/linek ve skupině: 52/16
- Počet záznamů v tabulce MAC adres: 210 000
- Počet záznamů v tabulce ARP: 140 000
- Protokol pro definici šířených VLAN: MVRP
- Podpora VLAN podle IEEE 802.1Q, počet aktivních VLAN: 4 000
- Podpora zařazování do VLAN podle standardu 802.1v
- IEEE 802.1s - Multiple Spanning Tree a IEEE 802.1w
- STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
- Podpora NTPv3
- Statické směrování IPv4 a IPv6
- Počet záznamů ve směrovací tabulce IPv4 unicast: 600 000
- Počet záznamů ve směrovací tabulce IPv6 unicast: 600 000
- Dynamické směrování: RIP, RIPng, OSPFv2, OSPFv3 a BGP
- Podpora police based routing
- Podpora VRRPv2 a VRRPv3
- Podpora route map
- Podpora minimálně 256 virtuálních směrovacích instancí (VRF)
- IGMP v2 a v3, IGMP snooping
- DHCP snooping pro IPv4 a IPv6
- Směrování multicast: PIM-DM, PIM-SM, IPv6 PIM-SM, PIM-SSM, IPv6 PIM-SSM, MSDP
- Hardware podpora IPv4 a IPv6 ACL
- ACL definice na základě skupiny fyzických portů
- ACL aplikovatelný na interface, LAG, VLAN
- Port security
- Podpora IPv4 a IPv6 QoS
- IEEE 802.1p - minimální počet front: 8
- 802.1X ověřování včetně více současných uživatelů na port, minimálně 259 uživatelů/port
- Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
- Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675
- Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.
- Podpora uživatelských rolí dynamicky stahovatelných z RADIUS serveru, jejich aplikace na základě výsledku autorizace
- Detekce protilehlého zařízení pomocí LLDP, včetně LLDP over OoB management port
- Detekce jednosměrnosti optické linky (např. UDLD nebo ekvivalentní)
- DHCP server a relay pro IPv4 a IPv6 včetně podpory VRF
- BPDU guard a Root guard

- Podpora service insertion včetně technologie VXLAN
- Podpora static a dynamic VXLAN s využitím BGP-EVPN
- Podpora VXLAN přes IPv6 (underlay)
- Podpora PBR VXLAN
- Podpora Group based policy pro VXLAN (VXLAN GBP)
- Podpora Data Center Bridging (PFC 802.1Qbb, ETS 802.1Qaz) S4B20A
- Konfigurace zařízení v člověku čitelné textové formě
- OoB management formou portu RJ45 s podporou ethernetu
- SSHv2 a HTTPS pro IPv4 a IPv6
- Podpora SNMPv2c a SNMPv3
- Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
- TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)
- Podpora RADIUS CoA (RFC3576)
- Port mirroring, alespoň 4 různé obousměrné session
- Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
- Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)
- Interní úložiště dat pro sběr provozních dat a pokročilou dignostiku zařízení: 24 GB
- Analýza síťového provozu sFlow podle RFC 3176
- Export síťového provozu formátem IPFIX
- Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM čipu
- Záruka a servisní podpora výrobce s výměnou vadného HW (včetně vestavěných zdrojů a ventilátorů) v režimu NBD (Next Bussiness Day) na 36 měsíců. Součástí servisní podpory musí být bezplatný nárok na běžně dostupné nové verze SW a přístup na servisní portál výrobce.

11. Datacentrový přepínač – 2 ks

- Typ přepínače: L3 switch
- Montáž do racku, velikost max. 1U
- Počet 10GE optických portů s volitelným fyzickým rozhraním SFP/SFP+: 24
- Počet optických 10/25/50GE portů s volitelným fyzickým rozhraním SFP/SFP+/SFP28/SFP56: 4
- Redundantní interní hot-swap napájecí zdroj
- Vyměnitelné ventilátory – hot swap
- Celková přepínací propustnost přepínače: 880 Gbps
- Celkový paketový výkon přepínače: 650 Mpps
- Podporovaný počet přepínačů ve stohu: 10
- Kapacita stohovacího propojení: až 200 Gbps
- Redundance řídícího prvku v rámci stohu
- Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)
- Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)
- Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF
- Podpora "jumbo rámců" včetně velikosti 9198 Byte
- Podpora linkové agregace IEEE 802.1AX
- Počet LACP skupin/linek ve skupině: 256/8
- Počet záznamů v tabulce MAC adres: 29 000
- Počet záznamů v tabulce ARP: 28 000
- Protokol pro definici šířených VLAN: MVRP

- Podpora VLAN podle IEEE 802.1Q, počet aktivních VLAN: 4 000
- Podpora zařazování do VLAN podle standardu 802.1v
- IEEE 802.1s - Multiple Spanning Tree
- STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
- Podpora NTPv3
- Statické směrování IPv4 a IPv6
- Počet záznamů ve směrovací tabulce IPv4 unicast: 64 000
- Počet záznamů ve směrovací tabulce IPv6 unicast: 32 000
- Dynamické směrování OSPFv2, OSPFv3 a BGP včetně podpory BFD
- Podpora Layer-3 routed port
- Hardware podpora IPv4 a IPv6 ACL
- ACL definice na základě skupiny fyzických portů
- ACL aplikovatelný na interface, LAG, VLAN
- 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port
- Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
- Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675
- Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.
- Podpora uživatelských rolí dynamicky stahovatelných z RADIUS serveru, jejich aplikace na základě výsledku autorizace
- Port security
- Podpora IPv4 a IPv6 QoS
- IEEE 802.1p - minimální počet front: 8
- Konfigurace zařízení v člověku čitelné textové formě
- SSHv2 a HTTPS pro IPv4 a IPv6
- Podpora SNMPv2c a SNMPv3
- Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
- TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)
- Podpora RADIUS CoA (RFC3576)
- Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN
- Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
- Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)
- Analýza síťového provozu sFlow podle RFC 3176
- Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM čipu
- Záruka a servisní podpora výrobce s výměnou vadného HW (včetně vestavěných zdrojů a ventilátorů) v režimu NBD (Next Bussiness Day) po 36 měsíců. Součástí servisní podpory musí být bezplatný nárok na běžně dostupné nové verze SW a přístup na servisní portál výrobce

12. Přístupový přepínač (typ 1) – 8 ks

- Třída zařízení: L2/L3 přepínač
- Formát zařízení do racku
- Velikost zařízení: 1U
- Počet 1Gbit/s metalických portů: 48
- Počet optických 10GE portů s volitelným fyzickým rozhraním (SFP+): 4
- Interní AC zdroj

- Podpora PoE+ dle standardu IEEE 802.3af, 802.3at
- Dostupný výkon pro PoE napájení: 370W
- Celková přepínací propustnost přepínače: 176 Gbps
- Celkový paketový výkon přepínače: 130 Mpps
- Minimální paketový buffer: 8MB

Vlastnosti stohování:

- Podporovaný počet přepínačů ve stohu: 8
- Kapacita stohovacího propojení: 40 Gbps
- Stoh podporuje distribuované přepínaní paketů
- Stohování přes standartní uplink porty (možnost zapojení stohu na minimálně 100m)
- Redundance řídícího prvku v rámci stohu
- Podpora stohování různých typů přepínačů (PoE, Non-PoE, 24port, 48port)
- Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)
- Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)
- Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF

Základní funkce a protokoly:

- Podpora "jumbo rámců" včetně velikosti 9198 Byte
- Podpora linkové agregace IEEE 802.1AX
- Konfigurovatelné rozkládání LACP zátěže podle L2, L3
- Počet LACP skupin/linek ve skupině: 32/8
- Počet záznamů v tabulce MAC adres: 16 000
- Počet záznamů v tabulce ARP: 8 000
- Protokol pro definici šířených VLAN: MVRP
- Podpora VLAN podle IEEE 802.1Q, minimálně 2000 aktivních VLAN
- Podpora zařazování do VLAN podle standardu 802.1v
- IEEE 802.1s - Multiple Spanning Tree
- STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
- Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
- Detekce jednosměrnosti optické linky (např. UDLD)
- Podpora NTPv3
- Statické směrování IPv4 a IPv6
- Minimální počet IPv4 záznamů ve směrovací tabulce: 2 000
- Minimální počet IPv6 záznamů ve směrovací tabulce: 1 000
- Dynamické směrování OSPFv2, OSPFv3
- Podpora Layer-3 routed port
- IGMP v2 a v3
- IGMP snooping
- MLD v1 a v2
- MLD snooping
- Hardware podpora IPv4 a IPv6 ACL
- ACL definice na základě skupiny fyzických portů
- ACL aplikovatelný na interface, LAG, VLAN
- BPDU a Root guard
- DHCP snooping pro IPv4 a IPv6
- HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps

- 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port
- Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
- Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675
- Podpora Critical VLAN
- Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.
- Podpora uživatelských rolí definovaných lokálně v přepínači, jejich aplikace na základě výsledku autorizace
- Podpora uživatelských rolí dynamicky stahovatelných z RADIUS serveru, jejich aplikace na základě výsledku autorizace
- Podpora Dynamic ARP protection
- Port security
- Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU
- Podpora IPv4 a IPv6 QoS
- IEEE 802.1p - minimální počet front: 8
- Podpora technologie VXLAN
- Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izolovat více koncových zařízení na jednom portu do unikátních tunelů
- Přiřazení koncového zařízení do tunelu na základě výsledku autorizace
- Podpora REST API pro automatizaci nastavení sítě.
- Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači
- Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)
- Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události
- Grafické rozhraní pro zobrazení výsledků monitorování a analytických skriptů. Možnost zobrazení stavu monitorovaných metrik do grafů atp.
- Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase.
- Interní uložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení
- Kapacita interního úložiště dat pro analytické účely minimálně 14 GB
- Konzolový port
- 1xRJ45 OoB management port s podporou ethernetu
- Konfigurace zařízení v člověku čitelné textové formě
- Podpora automatických i manuálních snapshotů konfigurace systému
- USB port pro diagnostiku, přenos konfigurace a firmware
- Přímé bezdrátové připojení ke konzoli zařízení skrze bluetooth
- Podpora managementu přes IPv4 i IPv6
- SSHv2 a HTTPS pro IPv4 a IPv6
- Podpora SNMPv2c a SNMPv3
- RMON
- Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
- Lokálně vynucené RBAC na úrovni přepínače
- Dualní flash image
- Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
- Podpora RADIUS včetně RADIUS CoA (RFC3576)
- Podpora standardního Linux Shellu (BASH) pro debugging a skriptování

- Podpora TACACS+
- Analýza síťového provozu sFlow podle RFC 3176
- Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM chipu
- Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN
- Podpora IP SLA pro měření zpoždění provozu VoIP
- Podpora Zero Touch Provisioning (ZTP)
- Doživotní záruka výrobce, tzn. min. 5 let od ukončení prodeje, včetně vestavěných zdrojů a ventilátorů a bezplatného nároku na běžně dostupné nové verze SW.

13. Přístupový přepínač (typ 2) – 6 ks

- Třída zařízení: L2/L3 přepínač
- Formát zařízení do racku
- Velikost zařízení: 1U
- Počet 1Gbit/s metalických portů: 48
- Počet optických 10GE portů s volitelným fyzickým rozhraním (SFP+): 4
- Interní AC zdroj
- Dostupný výkon pro PoE napájení: 370W
- Celková přepínací propustnost přepínače: 176 Gbps
- Celkový paketový výkon přepínače: 130 Mpps
- Minimální paketový buffer: 8MB

Vlastnosti stohování:

- Podporovaný počet přepínačů ve stohu: 8
- Kapacita stohovacího propojení: 40 Gbps
- Stoh podporuje distribuované přepínaní paketů
- Stohování přes standartní uplink porty (možnost zapojení stohu na minimálně 100m)
- Redundance řídícího prvku v rámci stohu
- Podpora stohování různých typů přepínačů (PoE, Non-PoE, 24port, 48port)
- Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)
- Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)
- Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF

Základní funkce a protokoly:

- Podpora "jumbo rámců" včetně velikosti 9198 Byte
- Podpora linkové agregace IEEE 802.1AX
- Konfigurovatelné rozkládání LACP zátěže podle L2, L3
- Počet LACP skupin/linek ve skupině: 32/8
- Počet záznamů v tabulce MAC adres: 16 000
- Počet záznamů v tabulce ARP: 8 000
- Protokol pro definici šířených VLAN: MVRP
- Podpora VLAN podle IEEE 802.1Q, minimálně 2000 aktivních VLAN
- Podpora zařazování do VLAN podle standardu 802.1v
- IEEE 802.1s - Multiple Spanning Tree
- STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
- Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
- Detekce jednosměrnosti optické linky (např. UDLD)
- Podpora NTPv3

- Statické směrování IPv4 a IPv6
- Minimální počet IPv4 záznamů ve směrovací tabulce: 2 000
- Minimální počet IPv6 záznamů ve směrovací tabulce: 1 000
- Dynamické směrování OSPFv2, OSPFv3
- Podpora Layer-3 routed port
- IGMP v2 a v3
- IGMP snooping
- MLD v1 a v2
- MLD snooping
- Hardware podpora IPv4 a IPv6 ACL
- ACL definice na základě skupiny fyzických portů
- ACL aplikovatelný na interface, LAG, VLAN
- BPDU a Root guard
- DHCP snooping pro IPv4 a IPv6
- HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps
- 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port
- Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
- Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675
- Podpora Critical VLAN
- Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.
- Podpora uživatelských rolí definovaných lokálně v přepínači, jejich aplikace na základě výsledku autorizace
- Podpora uživatelských rolí dynamicky stahovatelných z RADIUS serveru, jejich aplikace na základě výsledku autorizace
- Podpora Dynamic ARP protection
- Port security
- Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU
- Podpora IPv4 a IPv6 QoS
- IEEE 802.1p - minimální počet front: 8
- Podpora technologie VXLAN
- Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izolovat více koncových zařízení na jednom portu do unikátních tunelů
- Přiřazení koncového zařízení do tunelu na základě výsledku autorizace
- Podpora REST API pro automatizaci nastavení sítě.
- Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači
- Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)
- Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události
- Grafické rozhraní pro zobrazení výsledků monitorování a analytických skriptů. Možnost zobrazení stavu monitorovaných metrik do grafů atp.
- Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase.
- Interní uložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení
- Kapacita interního úložiště dat pro analytické účely minimálně 14 GB
- Konzolový port

- 1xRJ45 OoB management port s podporou ethernetu
- Konfigurace zařízení v člověku čitelné textové formě
- Podpora automatických i manuálních snapshotů konfigurace systému
- USB port pro diagnostiku, přenos konfigurace a firmware
- Přímé bezdrátové připojení ke konzoli zařízení skrze bluetooth
- Podpora managementu přes IPv4 i IPv6
- SSHv2 a HTTPS pro IPv4 a IPv6
- Podpora SNMPv2c a SNMPv3
- RMON
- Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
- Lokálně vynucené RBAC na úrovni přepínače
- Dualní flash image
- Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
- Podpora RADIUS včetně RADIUS CoA (RFC3576)
- Podpora standardního Linux Shellu (BASH) pro debugging a skriptování
- Podpora TACACS+
- Analýza síťového provozu sFlow podle RFC 3176
- Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM chipu
- Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN
- Podpora IP SLA pro měření zpoždění provozu VoIP
- Podpora Zero Touch Provisioning (ZTP)
- Doživotní záruka výrobce, tzn. min. 5 let od ukončení prodeje, včetně vestavěných zdrojů a ventilátorů a bezplatného nároku na běžně dostupné nové verze SW.

14. Přístupový přepínač (typ 3) – 5 ks

- Třída zařízení: L2/L3 přepínač
- Formát zařízení do racku
- Velikost zařízení: 1U
- Počet 1Gbit/s metalických portů: 24
- Počet optických 10GE portů s volitelným fyzickým rozhraním (SFP+): 4
- Interní AC zdroj
- Dostupný výkon pro PoE napájení: 370W
- Celková přepínací propustnost přepínače: 128 Gbps
- Celkový paketový výkon přepínače: 95 Mpps
- Minimální paketový buffer: 8MB

Vlastnosti stohování:

- Podporovaný počet přepínačů ve stohu: 8
- Kapacita stohovacího propojení: 40 Gbps
- Stoh podporuje distribuované přepínaní paketů
- Stohování přes standartní uplink porty (možnost zapojení stohu na minimálně 100m)
- Redundance řídícího prvku v rámci stohu
- Podpora stohování různých typů přepínačů (PoE, Non-PoE, 24port, 48port)
- Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)
- Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)
- Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF

Základní funkce a protokoly:

- Podpora "jumbo rámců" včetně velikosti 9198 Byte
- Podpora linkové agregace IEEE 802.1AX
- Konfigurovatelné rozkládání LACP zátěže podle L2, L3
- Počet LACP skupin/linek ve skupině: 32/8
- Počet záznamů v tabulce MAC adres: 16 000
- Počet záznamů v tabulce ARP: 8 000
- Protokol pro definici šířených VLAN: MVRP
- Podpora VLAN podle IEEE 802.1Q, minimálně 2000 aktivních VLAN
- Podpora zařazování do VLAN podle standardu 802.1v
- IEEE 802.1s - Multiple Spanning Tree
- STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
- Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
- Detekce jednosměrnosti optické linky (např. UDLD)
- Podpora NTPv3
- Statické směrování IPv4 a IPv6
- Minimální počet IPv4 záznamů ve směrovací tabulce: 2 000
- Minimální počet IPv6 záznamů ve směrovací tabulce: 1 000
- Dynamické směrování OSPFv2, OSPFv3
- Podpora Layer-3 routed port
- IGMP v2 a v3
- IGMP snooping
- MLD v1 a v2
- MLD snooping
- Hardware podpora IPv4 a IPv6 ACL
- ACL definice na základě skupiny fyzických portů
- ACL aplikovatelný na interface, LAG, VLAN
- BPDU a Root guard
- DHCP snooping pro IPv4 a IPv6
- HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps
- 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port
- Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
- Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675
- Podpora Critical VLAN
- Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.
- Podpora uživatelských rolí definovaných lokálně v přepínači, jejich aplikace na základě výsledku autorizace
- Podpora uživatelských rolí dynamicky stahovatelných z RADIUS serveru, jejich aplikace na základě výsledku autorizace
- Podpora Dynamic ARP protection
- Port security
- Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU
- Podpora IPv4 a IPv6 QoS
- IEEE 802.1p - minimální počet front: 8
- Podpora technologie VXLAN

- Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izolovat více koncových zařízení na jednom portu do unikátních tunelů
- Přiřazení koncového zařízení do tunelu na základě výsledku autorizace
- Podpora REST API pro automatizaci nastavení sítě.
- Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači
- Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)
- Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události
- Grafické rozhraní pro zobrazení výsledků monitorování a analytických skriptů. Možnost zobrazení stavu monitorovaných metrik do grafů atp.
- Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase.
- Interní uložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení
- Kapacita interního úložiště dat pro analytické účely minimálně 14 GB
- Konzolový port
- 1xRJ45 OoB management port s podporou ethernetu
- Konfigurace zařízení v člověku čitelné textové formě
- Podpora automatických i manuálních snapshotů konfigurace systému
- USB port pro diagnostiku, přenos konfigurace a firmware
- Přímé bezdrátové připojení ke konzoli zařízení skrze bluetooth
- Podpora managementu přes IPv4 i IPv6
- SSHv2 a HTTPS pro IPv4 a IPv6
- Podpora SNMPv2c a SNMPv3
- RMON
- Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
- Lokálně vynucené RBAC na úrovni přepínače
- Dualní flash image
- Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
- Podpora RADIUS včetně RADIUS CoA (RFC3576)
- Podpora standardního Linux Shellu (BASH) pro debugging a skriptování
- Podpora TACACS+
- Analýza síťového provozu sFlow podle RFC 3176
- Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM chipu
- Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN
- Podpora IP SLA pro měření zpoždění provozu VoIP
- Podpora Zero Touch Provisioning (ZTP)
  Doživotní záruka výrobce, tzn. min. 5 let od ukončení prodeje, včetně vestavěných zdrojů a ventilátorů a bezplatného nároku na běžně dostupné nové verze SW.

15. Přístupový přepínač (typ 4) – 1 ks

- Třída zařízení: L2/L3 přepínač
- Formát zařízení do racku
- Velikost zařízení: 1U
- Počet 1Gbit/s metalických portů: 24
- Počet optických 10GE portů s volitelným fyzickým rozhraním (SFP+): 4
- Interní AC zdroj

- Podpora PoE+ dle standardu IEEE 802.3af, 802.3at
- Dostupný výkon pro PoE napájení: 370W
- Celková přepínací propustnost přepínače: 128 Gbps
- Celkový paketový výkon přepínače: 95 Mpps
- Paketový buffer: 8MB

Vlastnosti stohování:

- Podporovaný počet přepínačů ve stohu: 8
- Kapacita stohovacího propojení: 40 Gbps
- Stoh podporuje distribuované přepínaní paketů
- Stohování přes standartní uplink porty (možnost zapojení stohu na minimálně 100m)
- Redundance řídícího prvku v rámci stohu
- Podpora stohování různých typů přepínačů (PoE, Non-PoE, 24port, 48port)
- Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)
- Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)
- Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF

Základní funkce a protokoly:

- Podpora "jumbo rámců" včetně velikosti 9198 Byte
- Podpora linkové agregace IEEE 802.1AX
- Konfigurovatelné rozkládání LACP zátěže podle L2, L3
- Počet LACP skupin/linek ve skupině: 32/8
- Minimální počet záznamů v tabulce MAC adres: 16 000
- Minimální počet záznamů v tabulce ARP: 8 000
- Protokol pro definici šířených VLAN: MVRP
- Podpora VLAN podle IEEE 802.1Q, minimálně 2000 aktivních VLAN
- Podpora zařazování do VLAN podle standardu 802.1v
- IEEE 802.1s - Multiple Spanning Tree
- STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
- Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED
- Detekce jednosměrnosti optické linky (např. UDLD)
- Podpora NTPv3
- Statické směrování IPv4 a IPv6
- Počet IPv4 záznamů ve směrovací tabulce: 2 000
- Počet IPv6 záznamů ve směrovací tabulce: 1 000
- Dynamické směrování OSPFv2, OSPFv3
- Podpora Layer-3 routed port
- IGMP v2 a v3
- IGMP snooping
- MLD v1 a v2
- MLD snooping
- Hardware podpora IPv4 a IPv6 ACL
- ACL definice na základě skupiny fyzických portů
- ACL aplikovatelný na interface, LAG, VLAN
- BPDU a Root guard
- DHCP snooping pro IPv4 a IPv6
- HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps

- 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port
- Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
- Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675
- Podpora Critical VLAN
- Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.
- Podpora uživatelských rolí definovaných lokálně v přepínači, jejich aplikace na základě výsledku autorizace
- Podpora uživatelských rolí dynamicky stahovatelných z RADIUS serveru, jejich aplikace na základě výsledku autorizace
- Podpora Dynamic ARP protection
- Port security
- Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU
- Podpora IPv4 a IPv6 QoS
- IEEE 802.1p - minimální počet front: 8
- Podpora technologie VXLAN
- Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izolovat více koncových zařízení na jednom portu do unikátních tunelů
- Přiřazení koncového zařízení do tunelu na základě výsledku autorizace
- Podpora REST API pro automatizaci nastavení sítě.
- Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači
- Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)
- Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události
- Grafické rozhraní pro zobrazení výsledků monitorování a analytických skriptů. Možnost zobrazení stavu monitorovaných metrik do grafů atp.
- Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase.
- Interní uložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení
- Kapacita interního úložiště dat pro analytické účely minimálně 14 GB
- Konzolový port
- 1xRJ45 OoB management port s podporou ethernetu
- Konfigurace zařízení v člověku čitelné textové formě
- Podpora automatických i manuálních snapshotů konfigurace systému
- USB port pro diagnostiku, přenos konfigurace a firmware
- Přímé bezdrátové připojení ke konzoli zařízení skrze bluetooth
- Podpora managementu přes IPv4 i IPv6
- SSHv2 a HTTPS pro IPv4 a IPv6
- Podpora SNMPv2c a SNMPv3
- RMON
- Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
- Lokálně vynucené RBAC na úrovni přepínače
- Dualní flash image
- Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
- Podpora RADIUS včetně RADIUS CoA (RFC3576)
- Podpora standardního Linux Shellu (BASH) pro debugging a skriptování

- Podpora TACACS+
- Analýza síťového provozu sFlow podle RFC 3176
- Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM chipu
- Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN
- Podpora IP SLA pro měření zpoždění provozu VoIP
- Podpora Zero Touch Provisioning (ZTP)
  Doživotní záruka výrobce, tzn. min. 5 let od ukončení prodeje, včetně vestavěných zdrojů a ventilátorů a bezplatného nároku na běžně dostupné nové verze SW.

16. Bezdrátový přístupový bod – 30 ks

- Třída zařízení: indoor přístupový bod (AP)
- Integrované antény
- Uzavřená konstrukce bez ventilátorů
- Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax
- Plnohodnotná certifikace Wi-Fi Aliance: Wi-Fi CERTIFIED 6E™ a WPA3™-Enterprise
- Pracovní režim AP bez kontroléru (autonomní)
- Pracovní režim AP řízené kontrolérem (lightweight)
- Pracovní režim AP v roli kontroléru s možností správy až 120 AP
- Počet portů ethernet LAN: 1x 100/1000/2500 Mbit/s RJ45
- Podpora multigigabit ethernet 2.5 Gbps IEEE 802.3bz
- Možnost 802.3at (PoE+) napájení z přepínače nebo injectoru
- Podpora standardního PoE IEEE 802.3af bez nutnosti redukce výkonu libovolného rádia
- Podpora napájení z AC napájecího zdroje
- Rozsah provozních teplot 0° až +50°C bez nutnosti redukce vysílacího výkonu nebo omezení funkcí
- Ochrana proti přehřátí - vestavěný teplotní senzor, který automaticky krátkodobě vypne AP
- Vestavěná interní anténa MIMO, omni down-tilt
- Radiová část: dual-radio / tri-band, podpora pásem 2,4GHz 5GHz a 6GHz
- MIMO a počet nezávislých streamů pro každé rádio: 2x2:2
- Podpora TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax
- HW podpora OFDMA
- Možnost nastavení vysílacího výkonu s krokem 0.5 dBm
- Max data rate: 2400 Mbit/s pro 6GHz, 1200 Mbit/s pro 5GHz a 574 Mbit/s pro 2,4GHz
- 16 inzerovaných BSSID na rádio
- Nastavitelný DTIM interval pro jednotlivé SSID
- Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP
- Integrovaný TPM pro bezpečné uložení certifikátů
- Podpora WPA3-CNSA, WPA3-SAE, OWE
- Podpora 802.11ac explicitního beamformingu
- Podpora airtime fairness
- Prioritizace jednotlivých SSID na základě vysílacího času
- USB port s podporou 3G/4G USB modemu jako WAN uplink
- Vypínatelné indikační LED diody informující o stavu zařízení
- Prioritizace 6GHz a 5GHz pásma – Band Steering či obdobné
- Automatická detekce Rogue AP
- Mapování SSID do různých VLAN podle IEEE 802.1Q

- VLAN Pooling
- Podpora Wireless MESH s protokolem pro optimální výběr cesty v rámci MESH stromu
- Podpora Layer-2 izolace bezdrátových klientů
- HW podpora spektrální analýzy v pásmech 2,4GHz a 5GHz (detekce zdroje rušivého signálu)
- Hardware filtry proti intermodulačnímu rušením z mobilních sítí (Advanced Cellular Coexistence nebo obdobné)
- DHCP server, směrování a NAT pro bezdrátové klienty
- AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN
- Automatická identifikace připojeného zařízení a jeho operačního systému
- Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming
- Dynamické vyvažování klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP
- Optimalizace provozu: multicast-to-unicast konverze
- Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace)
- Podpora filtrování přístupu na web
- Podpora RadSec (RADIUS over TLS)
- 802.11w ochrana management rámců
- Podpora Kensington lock
- Podpora MAC a 802.1X autentizace Wi-Fi klientů s využitím lokální databáze v AP
- AP se ověřuje před připojením do LAN pomocí 802.1X - podpora PEAP a EAP-TLS suplicant
- CLI formou serial konsole port a serial over bluetooth
- SSHv2, SNMPv3
- Integrované Bluetooth 5.0 Low Energy (BLE) rádio
- Integrované Zigbee 802.15.4 rádio
- Podpora režimu SLEEP s max. spotřebou energie do 2W
- Součástí AP je příslušenství pro montáž na zeď nebo strop
- Doživotní záruka výrobce, tzn. min. 5 let od ukončení prodeje.

17. Software pro správu sítě – 60 ks

- Software pro správu sítě / management nástroj s podporou správy produktů nabízeného výrobce a nejméně dvou dalších předních světových dodavatelů networking řešení
- Správa autonomních AP, “tenkých” AP, fyzických i virtuálních WiFi kontrolérů a přepínačů
- Licence pro správu, možnost flexibilního rozšiřování až do 1.500 zařízení
- Software bude dodán ve formě virtuální appliance (OVA nebo podobný formát) bez nutnosti pořizovat další licence např pro OS nebo databáze pro prostředí VMware
- Manuální a automatické discovery síťových zařízení pomocí SNMP, HTTP a CDP skenování
- Monitorovací nebo plný-managed režim pro nově objevená zařízení jako ochrana před nechtěným přepsáním konfigurace
- RBAC pro jednotlivé síťové operátory na úrovni síťových zařízení a jejich funkcí. Možnost plného oddělení tak aby se v rámci jednoho systému dalo spravovat více samostatných entit s vlastními procesy
- Webové uživatelské rozhraní s podporou HTTPS
- Možnost přizpůsobení prostředí ovládací obrazovky (webový dashboard), zvlášť pro každého síťového operátora
- Vyhledávání koncových uživatelů na základě MAC adresy, IP adresy, uživatelského jména a LAN hostname

- Real-time monitoring každého uživatele v síti včetně charakteristik jako jsou: kvalita RF signálu, utilizace pásma (in/out), autentizační status a čas, historie roamingu, délka trvání připojení, typ klientského zařízení, asociace s SSID, objem a seznam používaných L7 aplikací a navštívených webových kategorií.
- Podpora alarmování s možností nastavitelných prahů pro jednotlivé událostí. Podporované události: odchylka od baseline konfigurace, RF metrika, nově objevené zařízení, Radius autentizace, Rogue AP, nadměrné utilizace AP (bandwidth), počet připojených klientů, nadměrná utilizace klientem (bandwidth), Up/Down zařízení, Up/Down Radio, IDS událost
- Konfigurace formou politik aplikovatelných na všechna zařízení, jejich skupinu nebo jednotlivé zařízení.
- Možnost tvorby konfiguračních šablon, jak nových, tak z běžících zařízení jako jsou AP nebo kontroléry.
- Podpora konfigurační změn a upgrade firmware pomocí jednorázových nebo opakujících se pracovních úloh (scheduled-job).
- Kontrola provedených konfiguračních změny, v případě nesouladu definice a runtime stavu konfigurační rollback
- Archivace konfiguraci
- Audit konfigurace, porovnávání rozdílů proti přednastaveným politikám individuálně pro jednotlivá a hromadně proti skupině zařízení
- Možnost funkčního rozšíření o monitorování stability a odezvy ostatních síťových služeb pro jednotlivé klienty jako je průměrný čas odpovědi na DNS dotaz nebo průměrný čas zpracování RADIUS autentizace
- Vizualizace umístění prvků sítě ve fyzických mapách. Zobrazení bezdrátových klientů na mapě a jejich signálu a využívaných L7 aplikací
- Možnost monitorování bezdrátových IDS událostí z více samostatných systémů současně.
- Podpora systému pro automatizované bezzásahové zprovoznění připojeného zařízení
- Monitoring a detekce síťových anomálií jako je např. nadměrné a neobvyklé navýšení objemu provozu a upozorňování na tyto stavy pomocí alarmů
- Servisní podpora výrobce, včetně bezplatných aktualizací a přístupu na servisní portál výrobce po dobu 36 měsíců

18. Optimalizace provozu WiFi sítě – 1 ks

- Umístění bezdrátových AP bude provedeno na základě analýzy pokrytí WiFi signálem v zadavatelem definovaných prostorách.
- Analýza optimalizace provozu WiFi sítě bude realizována pomocí profesionálního nástroje na základě mapových podkladů dodaných zadavatelem (DWG).
- Takto vygenerovaný návrh rozmístění AP bude konzultován se zadavatelem a upraven dle možností skutečného umístění AP v budovách.
- Finálním výstupem optimalizace provozu WiFi sítě budou grafické reporty a zpráva ve formátu PDF minimálně v rozsahu:
    - Návrh rozmístění AP
    - Heat mapa bezdrátové sítě
    - Síla signálu (pokrytí) pro pásmo 5GHz
    - Síla signálu (pokrytí) pro pásmo 2,4 GHz
    - Překryv kanálů
    - Poměr síly signálu a šumu pro 5 GHz a 2,4 GHz

19. Firewall (NGFW) – 2 ks

- HW appliance (VM appliance) s montáží do datového rozvaděče, velikost max. 1RU
- Duální napájení tzn. osazen redundantní zdroj
- Počet 10GE SFP+ sítových rozhraní: 4
- Počet 1GE SFP sítových rozhraní: 4
- Počet 1GE RJ-45 sítových rozhraní: 8
- Management rozhraní 1 GbE RJ45 a sériový konzolový port
- Podpora režimu vysoké dostupnosti minimálně jako active/active a active/passive, cluster o dvou fyzických zařízeních
- Minimální propustnost firewallu pro IPv4 i IPv6 provoz (měřeno na UDP komunikaci o paketech s velikostí 512 byte): 35 Gbps
- Počet současně navázaných spojení firewallu: 2 mil.
- Počet nových spojení za sekundu: 0,1 mil.
- Propustnost IPSEC VPN (AES256-SHA256, 512byte): 0,1 mil.
- Propustnost SSL VPN (RSA-2048 certifikát): 1 Gbps
- Propustnost SSL inspekce: 3 Gbps
- Propustnost funkce IPS min. (reálná hodnota, měřeno na běžném provozu – real world traffic, včetně logování): 5 Gbps
- Propustnost funkcí next generation firewallingu (zapnutý stavový firewall, IPS, analýza aplikací, reálná hodnota, měřeno na běžném provozu – real world traffic): 3 Gbps
- Propustnost funkcí ochrany před hrozbami (stavový firewall, IPS, analýza aplikací, ochrana před škodlivým kódem reálná hodnota, měřeno na běžném provozu – real world traffic): 2,5 Gbps
- Výrobcem udávaná latence firewallu (64 byte, UDP provoz): Max. 4 µs
- Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů
- Bezpečnostní funkce obecně označovaných jako Next Generation FireWall
- Podpora virtualizace na daném HW, vytváření a provozování tzv. virtuálních kontextů – min. 10 virtuálních kontextů (logických FW) v ceně zařízení
- Každý virtuální kontext pracuje izolovaně, má možnost propojovat jednotlivé virtuální kontexty pomocí interních virtuálních propojů, bez nutnosti použití fyzických rozhraní.
- Podpora stavového firewallingu pro IPv4 i IPv6, podpora NAT 64/46
- Možnost nasazení ve všech z následujících režimech: L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline)
- Plnohodnotná správa z lokálního management rozhraní (a to i v případě využití nástroje centrální správy, neboť i v takovém případě musí být možné firewall, resp. firewall cluster, plnohodnotně konfigurovat ve chvíli, kdy z jakéhokoliv důvodu centrální správa nebude dostupná)
- Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On
- Podpora lokální databáze a vzdálené databáze pro ověřování uživatelů: RADIUS, LDAP, TACACS+, SAML, KERBEROS
- Ověřování uživatelů pomocí SSO funkcionality pomocí RADIUS SSO a AD pollingu
- Funkce QoS, traffic shaping a SD-WAN min. v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek.
- Podpora funkcí VPN brány

- - IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran);
- SSL VPN pro klientský přístup s tunelovacím režimem včetně klienta pro osobní počítače i mobilní platformy a portálový režim pro bezklientský přístup
- VPN klient pro neomezený počet přistupujících zařízení součástí nabídky
- Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3
- Antivirový engine bude vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků
- Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče
- Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace: 4 000 aplikací
- Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů
- Funkce kategorizace a blokace provozu založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne
- Funkce antispamové a antivirové inspekce elektronické pošty
- Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů, součástí nabídky musí být min. 2 testovací HW/mobilní tokeny a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN
- Podpora ICAP rozhraní pro obousměrnou integraci s externími servery
- Podpora tunelování provozu pomocí technologie GRE
- Podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí
- Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu
- Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algoritmů pro rozklad zátěže (round robing, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí, podpora funkce ssl offloading a ssl inspekce pro rozkládaný provoz
- Rozšířená podpora výrobce v režimu 24x7 včetně pravidelné aktualizace signaturových databází a výměny vadného HW v režimu NBD po dobu 36 měsíců

20. Analyzer – 1 ks

- Virtuální apliance pro platformu VMware
- Příjem logů a vytváření reportů pro nabízené řešení NGFW

- Obousměrná integrace s NGFW, tedy data se přenáší jednak z firewallu na logovací a reportovací platformu, ale zároveň je možné přímo v GUI firewallu přistupovat k log údajům na logovací a reportovací platformě
- Podpora pro Syslog kompatibilní zařízení
- Výkon logování: 6 GB/den
- Kapacita storage (uložení historických dat):
- Real-time prohledávání logovaných dat: 3TB
- Vyhledávání historických dat podle typu události nebo typu provozu
- Funkce zpětné kontroly logů až 7 dnů zpět a zjištění, jestli systém nebyl napaden při přístupu na škodlivou webovou stránku
- Vyhledávání podle zařízení
- Uživatelská definice reportů (vzhled, obsah apod.)
- Automatické generování reportů v daném čase a periodě
- Automatické odesílání reportů emailem
- Rozšířená podpora výrobce v režimu 24x7 včetně pravidelných aktualizací a pravidelných aktualizací signaturových databází po dobu 36 měsíců

21. Webový aplikační FW (WAF) – 1 ks

- Virtuální apliance pro platformu VMware
- Funkce web aplikačního firewallu (WAF)
- Podpora režimu vysoké dostupnosti (A-A i A-P; pokud je tato funkce licencovaná, tak licence musí být součástí dodávky)
- Podpora HTTP v1.0, v1.1
- Nativní podpora HTTP/2
- Integrovaný průvodce/wizzard pro nejčastější typy konfigurací
- Ochrana před OWASP TOP10
- Validace protokolu http (dle RFC)
- Podpora funkce strojového učení (machine learning) - dvoúrovňová detekce anomálií a hrozeb za pomocí databáze vzorků výrobce a za pomoci strojového učení
- Podpora funkce ochrany API rozhraní s podporou schémat OpenAPI, XML a JSON
- Ochrana před klasickými typy útoků na web aplikace (XSS, SQL injection, Cross site request forgery, session hijacking, cookie poisoning, …)
- Signatury pro ochranu před útoky na známé webové aplikace
- Ochrana před útoky typu brute-force
- Ochrana před útoky na OS & webserver
- Ochrana před útoky typu L7 DoS/DDoS
- Podpora geolokační databáze, automaticky aktualizované výrobcem
- Podpora reputační DB pro IP adresy
- Rozpoznání a ochrana před přístupem automatizovaných klientů/nástrojů (skenery, crawlery, skripty, …) včetně využití funkce strojového učení
- Funkce user tracking & scoring (uživatel je identifikován, jeho chování je následně dlouhodobě sledováno a je mu dynamicky upravována reputace na základě reálného chování. Při překročení hraničních hodnot je provedena předdefinovaná akce.)
- Pokročilá ochrana před false positive
- Syntax based detection (signatura popisující útok je kombinována s inteligentní analýzou specifického/nestandardního chování s cílem minimalizovat množství false positives např. u SQL injection)

- Antivirová/antimalware kontrola (kontrola uploadovaných souborů)
- AV kontrola integrovaná do WAF appliance (nikoliv jako externí zařízení/služba)
- Ochrana před škodlivým kódem (malware, ransomware, trojské koně, atp.) včetně ochrany před polymorfním kódem
- Signaturová databáze udržovaná výrobcem a automaticky aktualizovaná
- Předdefinované politiky pro nejznámější aplikace (MS Exchange, MS SharePoint, OWA, WordPress)
- Ochrana proti únikům dat - DLP
- Ochrana API
- Podpora autentizace klientským SSL certifikátem
- Podpora dvoufaktorové autentizace (radius access-challenge response)
- LDAP, RADIUS, SAML
- Kerberos
- HTTP Basic / HTML Form
- Podpora SSO (single sign on)
- Podpora IPv4 i IPv6
- Algoritmy pro L7 load balancing: Round Robin, Weighted Round Robin, Least Connection, URI hash, Host hash, Domain hash, Source IP hash
- Požadované metody pro LB persistence: Source IP, http header, URL parameter, Insert cookie, Rewrite cookie, Persistent cookie, Session ID (ASP, PHP, JSP, SSL)
- Požadované metody pro kontrolu stavu serverů (healthcheck metody): ICMP Ping, TCP, TCP half open, TCP SSL, HTTP, HTTPS
- URL rewriting
- Content routing
- HTTPS offloading, HTTPS inspekce
- Komprese HTTP
- Object caching
- Podpora IPv4 i IPv6
- Vulnerability scanner integrovaný do WAF appliance (možnost interní bezpečnostní kontroly vlastních web aplikací)
- Plnohodnotná správa pomocí grafického rozhraní a CLI
- Správa pomocí web browseru, bez nutnosti instalovat management aplikaci
- Podpora SNMP včetně MIB souboru dodávaného výrobcem
- Otevřené API pro integraci do stávajícího management prostředí
- Virtualizace na úrovni mgmt rozhraní (možnost omezit přístup administrátorů na vybraná pravidla resp. chráněné servery)
- Propustnost plnohodnotné WAF inspekce nad protokolem HTTP min. 25 Mbps (výkonová hodnota musí být doložitelná oficiálním produktovým listem výrobce)
- Licenčně neomezený počet chráněných serverů
- Rozšířená podpora výrobce v režimu 24x7 včetně pravidelných aktualizací a pravidelných aktualizací signaturových databází po dobu 36 měsíců

22. Antimalware (EDR/XDR) pro stanice – 205 ks

- Antimalware řešení pro komplexní zabezpečení koncových stanic s OS Windows, Mac a Linux, fyzických a virtuálních serverů s OS Windows a Linux a mobilních zařízení s OS Android a iOS.
- Konzole pro správu nasazena v cloudu výrobce

- Možnost kdykoli migrovat konzoli pro správu do on-premise prostředí bezplatně, bez změny platnosti licence
- Konzole pro centrální správu je kompletně multi-tenantní
- Možnost zasílat upozornění napojením na Syslog server
- Možnost využití napojení jakékoli třetí aplikace za pomocí zdokumentované veřejné API
- Řešení umožňuje integraci se strukturami Microsoft Active Directory za účelem správy ochrany zařízení v těchto inventářích.
- Řešení je schopno odhalit stroje, které nejsou vedeny v Active Directory pomocí Network Discovery
- Možnost vzdálené instalace a odinstalace klienta přímo z konzole centrální správy
- Možnost upravit úroveň skenovacích úloh a jejich spouštění a plánování, přímo z konzole centrální správy
- Přiřazení bezpečnostních pravidel pro koncové stanice je možné granulárně na každé úrovni struktury inventáře, včetně kořenu a listů stromu (tzn. jakékoli OU, případně až přímo konkrétní stanici)
- Přiřazení pravidel minimálně podle:
    - uživatele či skupiny v Active Directory
    - OU v Active Directory
    - síťové lokality (IP adresa, rozsah IP adres, DNS server, WINS server, výchozí brána, typ sítě, název hostitele, DHCP přípona apod.)
- Možnost nastavení dědičnosti mezi bezpečnostními pravidly granulárně
- Vzdálená obnova či smazání souboru v karanténě
- Možnost automaticky přidat soubor do výjimky při obnově z karantény
- Po každé aktualizaci bezpečnostního obsahu jsou automaticky znovu proskenovány soubory v karanténě
- Instalace na koncové zařízení minimálně:
    - stáhnutím instalačního balíčku a instalace přímo na koncové stanici
    - instalace vzdáleně přímo z konzole správy
    - distribuce instalačního balíčku pomocí GPO či SCCM
    - instalace z již nainstalovaného klienta (např. vzdálená lokalita apod.)
- Možnost vytvářet instalační balíčky pro 32-bit a 64-bit operační systémy, včetně samoinstalačního balíčku, který obsahuje kompletní aplikaci a není nutné pro jeho instalaci přístup k síti
- Instalační balíček umožňuje tzv. „tichou“ instalaci (nevyskočí žádné okno, nevyžaduje žádnou uživatelskou interakci)
- Konzole správy musí obsahovat detailní informace o chráněných strojích minimálně:
    - název
    - IP adresa
    - operační systém
    - instalované moduly
    - aplikovaná pravidla
    - informace o aktualizacích
- Více administrátorských rolí min. 3 samostatné role pro:
    - správu komponent celého řešení
    - správu bezpečnostní pravidel a inventář koncových zařízení
    - správu a tvorbu reportů
- Podpora MFA ověření a možnost jeho vynucení

- Pro rozdílné skupiny uživatelů lze granulárně nastavit, jaké skupiny zařízení mají právo spravovat
- Logování uživatelských akcí
- Reporting včetně možnosti nastavení intervalu, ve kterém jsou reporty automaticky generovány a možnost vytvořit report okamžitě
- Možnost zasílání vygenerovaných reportů e-mailem
- Podpora min. operačních systémů:
    - Windows 10 1507 a vyšší
    - Windows Server 2019 a vyšší
    - Ubuntu 14.04 LTS a vyšší
    - Red Hat Enterprise Linux
    - CentOS 6.0 a vyšší
    - SUSE Linux Enterprise Server 11 SP4 a vyšší
    - Debian 8.0 a vyšší
    - Mac OS X El Capitan (10.11) a vyšší
- Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů nebo na maximální velikost souboru
- Aktualizace bezpečnostního obsahu alespoň jednou za hodinu
- Detekce na základě virových definicí (tzn. signatur)
- Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)
- Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)
- Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)
- Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení
- Detekce 0-day útoků na základě odhalování anomálního chování
- Dynamická detekce 0-day útoků, botnetových sítí, DDOS a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení
- Detekce 0-day bezsouborových útoků
- Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)
- Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností
- Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích, apod.)
- Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně
- Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno
- Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky
- Možnost automatické detonace podezřelých souborů v Sandboxu
- Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu
- Možnost ručního vložení vzorku do Sandboxu
- Řešení obsahuje funkce EDR / XDR integrované do jedné klientské aplikace spolu s EPP
- Řešení podporuje možnost izolace infikované koncové stanice.

- Řešení je schopno logování systémového, procesového a síťové aktivity v době zachyceného incidentu pro další investigaci.
- Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.
- Řešení generuje detekce na základě automatizovaného hledání IoCs v syrových datech sbíraných EDR senzorem
- Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku
- Řešení umožňuje analýzu vektoru útoku
- Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování
- Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR)
- Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů
- Ochrana proti podvodným a phishingovým webovým stránkám
- Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID
- Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)
- Podpora produktu výrobcem je poskytována v českém jazyce
- Možnost blokovat skenování portů
- Firewall, který obsahuje systém IDS včetně funkce odhalování neznámých hrozeb
- Možnost vypnout IDS
- Kontrola přístupu k Internetu:
    - zablokování přístupu pro specifické stanice / skupiny stanic
    - zablokování přístupu ke konkrétním webům pro specifické koncové stanice / skupiny stanic
    - zablokování přístupu k Internetu v určený čas
    - zamezení přístupu k různým kategoriím webových stránek (např. násilí, hazard a jiné)

<u>Ochrana poštovních schránek:</u>

- Cloudový firemní e-mail na vlastní doméně
- Webová, mobilní i desktopová aplikace pro Windows/Mac
- Licence desktopové aplikace až pro 3 zařízení na uživatele
- Kalendář, kontakty a úkoly, plná integrace s desktopovou aplikací
- Velikost email schránky min. 50 GB
- Antivirus, antispyware a antispoofing technologie
- Kontrola DKIM, DMARC and SPF
- Vestavěná ochrana proti spamu, phishingu, malwaru a neautorizovanému přístupu, včetně automatického filtrování a blokace škodlivých příloh bez potřeby manuálně upravovat SCL (Spam Confidence Level) hodnoty
- Možnost vytváření vlastních pokročilých antispamových pravidel (vyhodnocení více podmínek v jenom pravidlu)
- Umožnit uživateli poštovní schránky pracovat pomocí samostatného prohlížeče se spamovými a potenciálně infikovanými zprávami, které nebyly doručeny do emailové schránky
- Možnost vlastních pravidel s vlastním hodnocením obsahu
- Možnost správy přes příkazovou řádku
- Komplexní protokoly blokovaného spamu
- Možnosti pro nastavení pravidel inspekce souborů – mazání spustitelných souborů, skriptů

- Tvorba pravidla "Z hlavičky" a vyhodnocovat pole From: pro přesnější detekci podvržených e-mailů
- Backscatter ochrana
- Možnost zasílání přehledů o zachycených e-mailových hrozbách koncovým uživatelům
- Podpora šifrování
- Centrální správa identity, přístupových práv a uživatelských účtů až pro 300 zaměstnanců
- Správa karantény prostřednictvím webového portálu pro vybrané uživatele i administrátory
- Cloudové úložiště min. 1TB pro bezpečné sdílení a ukládání souborů, které lze snadno propojit s e-mailem (např. posílání odkazů na dokumenty místo příloh)
- Plná integrace s aplikacemi Microsoft 365
- Možnost rozšíření o AI nástroje
- Licence SW pro ochranu před škodlivým softwarem pro 205 uživatelů na 36 měsíců

23. Antimalware (EDR/XDR) pro servery – 10 ks

- Antimalware řešení pro komplexní zabezpečení koncových stanic s OS Windows, Mac a Linux, fyzických a virtuálních serverů s OS Windows a Linux a mobilních zařízení s OS Android a iOS.
- Konzole pro správu nasazena v cloudu výrobce
- Možnost kdykoli migrovat konzoli pro správu do on-premise prostředí bezplatně, bez změny platnosti licence
- Konzole pro centrální správu je kompletně multi-tenantní
- Možnost zasílat upozornění napojením na Syslog server
- Možnost využití napojení jakékoli třetí aplikace za pomocí zdokumentované veřejné API
- Řešení umožňuje integraci se strukturami Microsoft Active Directory za účelem správy ochrany zařízení v těchto inventářích.
- Řešení je schopno odhalit stroje, které nejsou vedeny v Active Directory pomocí Network Discovery
- Možnost vzdálené instalace a odinstalace klienta přímo z konzole centrální správy
- Možnost upravit úroveň skenovacích úloh a jejich spouštění a plánování, přímo z konzole centrální správy
- Přiřazení bezpečnostních pravidel pro koncové stanice je možné granulárně na každé úrovni struktury inventáře, včetně kořenu a listů stromu (tzn. jakékoli OU, případně až přímo konkrétní stanici)
- Přiřazení pravidel minimálně podle:
    - uživatele či skupiny v Active Directory
    - OU v Active Directory
    - síťové lokality (IP adresa, rozsah IP adres, DNS server, WINS server, výchozí brána, typ sítě, název hostitele, DHCP přípona apod.)
- Možnost nastavení dědičnosti mezi bezpečnostními pravidly granulárně
- Vzdálená obnova či smazání souboru v karanténě
- Možnost automaticky přidat soubor do výjimky při obnově z karantény
- Po každé aktualizaci bezpečnostního obsahu jsou automaticky znovu proskenovány soubory v karanténě
- Instalace na koncové zařízení minimálně:
    - stáhnutím instalačního balíčku a instalace přímo na koncové stanici
    - instalace vzdáleně přímo z konzole správy
    - distribuce instalačního balíčku pomocí GPO či SCCM
    - instalace z již nainstalovaného klienta (např. vzdálená lokalita apod.)

- Možnost vytvářet instalační balíčky pro 32-bit a 64-bit operační systémy, včetně samoinstalačního balíčku, který obsahuje kompletní aplikaci a není nutné pro jeho instalaci přístup k síti
- Instalační balíček umožňuje tzv. „tichou“ instalaci (nevyskočí žádné okno, nevyžaduje žádnou uživatelskou interakci)
- Konzole správy musí obsahovat detailní informace o chráněných strojích minimálně:
    - název
    - IP adresa
    - operační systém
    - instalované moduly
    - aplikovaná pravidla
    - informace o aktualizacích
- Více administrátorských rolí min. 3 samostatné role pro:
    - správu komponent celého řešení
    - správu bezpečnostní pravidel a inventář koncových zařízení
    - správu a tvorbu reportů
- Podpora MFA ověření a možnost jeho vynucení
- Pro rozdílné skupiny uživatelů lze granulárně nastavit, jaké skupiny zařízení mají právo spravovat
- Logování uživatelských akcí
- Reporting včetně možnosti nastavení intervalu, ve kterém jsou reporty automaticky generovány a možnost vytvořit report okamžitě
- Možnost zasílání vygenerovaných reportů e-mailem
- Podpora min. operačních systémů:
    - Windows 10 1507 a vyšší
    - Windows Server 2019 a vyšší
    - Ubuntu 14.04 LTS a vyšší
    - Red Hat Enterprise Linux
    - CentOS 6.0 a vyšší
    - SUSE Linux Enterprise Server 11 SP4 a vyšší
    - Debian 8.0 a vyšší
    - Mac OS X El Capitan (10.11) a vyšší
- Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů nebo na maximální velikost souboru
- Aktualizace bezpečnostního obsahu alespoň jednou za hodinu
- Detekce na základě virových definicí (tzn. signatur)
- Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně)
- Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům)
- Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům)
- Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení
- Detekce 0-day útoků na základě odhalování anomálního chování
- Dynamická detekce 0-day útoků, botnetových sítí, DDOS a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení
- Detekce 0-day bezsouborových útoků

- Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka)
- Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností
- Možnost varování před rizikovým chováním uživatele (přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích, apod.)
- Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně
- Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno
- Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky
- Možnost automatické detonace podezřelých souborů v Sandboxu
- Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu
- Možnost ručního vložení vzorku do Sandboxu
- Řešení obsahuje funkce EDR / XDR integrované do jedné klientské aplikace spolu s EPP
- Řešení podporuje možnost izolace infikované koncové stanice.
- Řešení je schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.
- Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.
- Řešení generuje detekce na základě automatizovaného hledání IoCs v syrových datech sbíraných EDR senzorem
- Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku
- Řešení umožňuje analýzu vektoru útoku
- Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování
- Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR)
- Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů
- Ochrana proti podvodným a phishingovým webovým stránkám
- Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID
- Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci)
- Podpora produktu výrobcem bude poskytována v českém jazyce
- Možnost blokovat skenování portů
- Firewall, který obsahuje systém IDS včetně funkce odhalování neznámých hrozeb
- Možnost vypnout IDS
- Kontrola přístupu k Internetu:
    - zablokování přístupu pro specifické stanice / skupiny stanic
    - zablokování přístupu ke konkrétním webům pro specifické koncové stanice / skupiny stanic
    - zablokování přístupu k Internetu v určený čas
    - zamezení přístupu k různým kategoriím webových stránek (např. násilí, hazard a jiné)
- Licence pro 10 zařízení na dobu min. 36 měsíců

24. Síťová sonda XDR – 1 ks

- Samostatná virtuální appliance pro platformu VMware
- Sonda obsahuje minimálně jeden port pro zpracování síťového provozu
- Sonda umožňuje připojení prostřednictvím TAP/SPAN portu
- Sonda analyzující provoz na síťové vrstvě, která je plně integrovaná do nabízeného XDR řešení
- Sonda obohacuje incidenty bezpečnostního řešení o informace získané z datové sítě
- Sonda není na monitorovacím portu detekovatelná, nezasahuje do síťového provozu

25. Nástroj pro zaznamenávání logů – 1 ks

- HW appliance (montáž do běžného 19‘‘ datového rozvaděče, výška max. 1U) pro zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.
- Redundantní zdroje a ventilátory za provozu vyměnitelné.
- Síťové rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému.
- Průměrný trvalý příjem událostí/s. (průměrná délka zprávy min. 700Byte)
- Minimálně dvojnásobný (4000 událostí/s) špičkový příjem bez ztráty dat alespoň po dobu 5 minut
- Čistá velikost integrované databáze
- Jedna webová console pro všechny administrátorské i operátorské činnosti
- Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 200 GB uložených událostí za den.
- Příjem a zpracování logů, události a další strojově generovaná data prostřednictvím protokolů
- Bezagentový sběr událostí, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů
- Pro systémy s OS Windows je současně podporován jak monitoring interních windows logů, tak monitoring textových souborových logů.
- V případě využití Windows agenta je agent instalován prostřednictvím MS AD Group Policy a jeho konfigurace je kompletně realizována centrálně v grafickém rozhraní systému.
- Windows agent podporuje centralizovanou konfiguraci Microsoft Sysmon pro obohacení logů, včetně globálního a selektivního zapínaní/vypínaní služby Sysmon.
- Komunikace Windows agenta a centrálního systému je zabezpečena TLS 1.2 a výše a podporuje ověřování certifikátem.
- Pro systémy s OS Windows je podporován sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířené Sysmonem.
- Ke všem odesílaným událostem ze systémů Windows je automaticky doplněn jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. K významným bezpečnostním událostem je doplňována značka a popis dle MITRE ATT&CK® matrice a k takto detekovaným procesům a souborům musí být automaticky vytvářen SHA256 hash.
- V případě využití Windows agenta není tento licenčně a časově omezen. Pokud je Windows agent licenčně nebo časově omezen, dodání licencí na Windows agenty v množství 300 na dobu předpokládané morální životnosti produktu – 7 let.
- Výrobcem vytvářené parsery pro běžné systémy.
- Uživatelsky definované parsery - systém umožňuje dopsání parserů pro další zdroje log zařízení uživatelem pomocí tzv. vizuální programování, bez nutnosti spolupráce s výrobcem.

- Standardizace přijatých logů do jednotného formátu a jejich normalizace (rozdělení) do příslušných polí dle jejich typu. Vytvoření vlastního důvěryhodného časového razítka ke každému logu.
- Uchování originální verze přijatých logů/zpráv včetně původní časové značky události.
- Okamžitá a automatická indexace umožňující okamžité prohledávání událostí.
- Podporované formáty
- Systém neumožňuje mazání nebo modifikování již uložených logů v rámci požadované retence. (ani libovolnou konfigurační změnou)
- Automatické doplňování reverzních DNS záznamů, čísel a jmen ASN systému a geolokace ke všem přijatým událostem a všem polím, obsahujícím IP adresy
- Nativní získávání logů z Office365 prostředí s licencí E3 bez nutnosti instalovat dodatečné externí komponenty
- Ověřování uživatele na externím LDAP serveru resp. ověření lokálního účtu v případě výpadku LDAP.
- Grafické rozhraní umožňuje filtraci nerelevantních událostí, snadné vyhledávání událostí, vytváření reportů a dynamickou vizualizaci událostí.
- Reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů
- Uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování
- Podpora základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity.
- Výrobcem předpřipravené sety/vzory alertů a korelací.
- Monitoring stavu systému - alertování při překročení prahových hodnot
- REST-API pro integraci s externím monitorovacím systémem
- Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba
- Dedikované síťové rozhraní pro management HW
- Uživatelské role definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému
- Aktualizace systému přes centrální webovou správcovskou konzoli v jednom balíku.
- Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém.
- Podpora komprese ukládaných dat
- Podpora důvěryhodného zálohování komprimovaných dat na externí systém.
- Servisní podpora na HW s opravou v místě instalace appliance, s garantovanou NBD od nahlášení závady.
- Servisní podpora na SW v rozsahu aktualizaci systému a parserů, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.

26. Hybridní čipové karty – soubor

- Zjednodušení životního cyklu karet a certifikátů
- Automatizovaná obnova kvalifikovaných i komerčních certifikátů od minimálně dvou externích poskytovatelů kvalifikovaných certifikátů. Automatizovaná obnova interních certifikátů z doménové CA
- Aplikace pro automatizovanou obnovu certifikátů umožňuje uživatelsky komfortní zážitek, aplikace prochází obsah čipové karty, pokud nastane čas obnovy certifikátu na kartě, aplikace v grafickém rozhraní vyzve uživatele k obnově. V opačném případě (není třeba certifikáty obnovovat) není uživatel aplikací informován o její činnosti:

- aplikace pro automatizovanou obnovu certifikátů je spuštěna automaticky při vložení čipové karty nebo po přihlášení certifikátem do operačního systému

- Aplikace, která prostřednictvím e-mailové notifikace upozorní uživatele na blížící se konec platnosti certifikátu:
  - notifikační profil lze konfigurovat podle potřeb, tj. vzhled a textace mailu, pravidla notifikace podle vlastností certifikátu (např. na základě vydavatele certifikátu, šablony certifikátu (pro MS CA), atp.
  - notifikační zprávu lze zároveň odesílat na mail správců, aby byli informování o blížící se expiraci certifikátů v organizaci
  - notifikace pro uživatelské i technické certifikáty
  - pokud byl předchozí certifikát obnoven, tak se notifikace s výzvou k obnově nezasílá
  - notifikaci lze odeslat nejen při blížící se expiraci certifikátů, ale také po jejich vydání
- Aplikace pro podporu činností spojených se správou životního cyklu čipových karet a certifikátů:
  - aplikace umožní v rámci jednoho scénáře připravit čipovou kartu pro uživatele: zvolit držitele, potisknout kartu údaji držitele, vydat certifikát z interní certifikační autority, nastavit do karty PIN, vytisknout hodnoty autorizačních kódů do diskrétní zóny PIN-formuláře
  - aplikace čerpá údaje o držitelích karet z Active Directory
  - podpora vydání certifikátů v zastoupení, alespoň pro certifikáty z interní CA
  - podpora archivace šifrovacích certifikátů a klíčů, pomocí technologie Key Recovery Agent
  - aplikace před vystavením certifikátu správce karet zobrazí varování, že bude vystaven certifikát Správce karet
  - aplikace před odvoláním certifikátu správce karet zobrazí varování, že bude odvolán certifikát správce karet
  - po dokončení scénáře vystavení čipové karty bude zobrazena informace, že bylo dokončeno vystavení čipové karty pro uživatele Jméno, Příjmení, Osobní číslo uživatele získané z AD
  - při vyhledávání karty např. před provedením evidence ztráty karty, kdy čipová karta nebude připojena ke čtečce a nebude dostupná, bude možné kartu vyhledat podle jednoznačného identifikátoru, případně podle AD atributů držitele karty.
- Aplikace pro zápis certifikátů na kartu plně komunikuje se stávajícím HW Zadavatele na tisk karet a to jak lokálně (USB) tak síťově
- Webová aplikace, určená správcům karet. Řízení přístupových oprávnění na základě členství ve skupině Active Directory. Možnost vyhledávat a prohlížet informace o čipových kartách – jejich držitelích, stavech čipové karty, datového obsahu čipové karty včetně aktuálních certifikátů, prohlížení statistik karet v organizaci a generování a prohlížení reportů
- Webová aplikace pro správce certifikátů, pro správu certifikátů z interní CA. Řízení přístupových oprávnění na základě členství ve skupině Active Directory. Možnost vyhledání a filtrace certifikátů podle různých vlastností certifikátů. Možnost zneplatnění vybraných certifikátů (uživatelských i technických).
- Aplikace pro online interní CA. Výstupy CA (žádosti, certifikáty, stavy zneplatnění) musí být v reálném čase ukládány do záložního úložiště (mimo interní databázi CA). Součástí řešení musí být i aplikace, která v případě havárie CA obnoví všechny chybějící certifikáty, a také všechny provedené stavy zneplatnění.
- Aplikace pro zjednodušení práce s kvalifikovanými certifikáty

<u>Systémové práce – min. požadavky:</u>

- Implementace CA
- Implementace dodaných systémů a vyškolení příslušných osob odběratele na obsluhu všech dodaných systémů

Servisní podpora:

- Přijetí požadavku do 2 hodin od nahlášení.
- Dočasné řešení do 1 pracovního dne od přijetí požadavku.
- Vyřešení požadavku do 5 pracovních dnů od dodání dočasného řešení.
- Reakční doby jsou garantovány pro serverové komponenty řešení.
- Poskytuje servisní podporu pro plnou funkčnost dodaného zboží a SW aplikací. Servisní podpora zahrnuje upgrade a update zboží a software a zároveň garantovanou technickou podporu.
- Základní servis nabízeného řešení zahrnuje podporu po dobu min. 36 měsíců ode dne podpisu předávacího protokolu (delší podpora je volitelná a zadavatel ji nemusí využít):
    - operačních systémů na klientských stanicích Windows 10 a vyšší
    - serverových operačních systémů Windows Server 2016 a vyšších
    - čipových karet do konce životnosti
    - čteček pro práci s kartou
    - mobilní metody multifaktorové autentizace
    - instalovaných aplikací pro správu životního cyklu karet a certifikátů
    - formou Service Desku v režimu 5 x 8, jehož provozní doba je od 8:00 do 16:00 v pracovní dny.

27. Instalace a implementace – soubor

- Rozbalení veškerého dodaného HW, kontrola bezvadného stavu, likvidace přepravního a obalového materiálu a spolupráce s dodavatelem na evidenci HW (případné opatření evidenčními štítky)
- Montáž síťových přepínačů a WiFi přístupových bodů
- Aktualizace FW
- L2 propojení a základní nastavení (IP adresace, NTP, SNMP apod.)
- Konfigurace L3 páteřních prvků a vysoké dostupnosti datových center
- Instalace a konfigurace SW pro správu sítě
- Testy vysoké dostupnosti páteřních a datacentrových přepínačů
- Instalace a zprovoznění veškerého serverového HW do stávajících 19“ rozvaděčů a provedení funkčních testů
- Instalace a oživení UPS
- Propojení LAN, SAN, kabelový management
- Aktualizace FW, BIOS apod.
- Osazení NIC karet do stávajících serverů
- Instalace diskových polí a implementace „Metro Clusteru“
- Integrace serverů do stávající VMware infrastruktury, oživení druhého datového centra
- Instalace VM (OS a SQL)
- Testy vysoké dostupnosti / trhací testy / testy UPS
- Začlenění Hardened Repository do stávajícího systému zálohování
- Úprava zálohovacích plánů
- Migrace stávajících dat
- Instalace AAA platformy
- Napojení na Radius server

- Konfigurace bezpečnostních pravidel pro přístup do sítě LAN
- Pilotní konfigurace 802.1x na 5 koncových stanic
- Montáž a propojení NGFW
- Aktualizace FW, napojení na aktualizační služby výrobce
- Zapojení vysoké dostupnosti (HA)
- Migrace a revize stávajících bezpečnostních pravidel
- Úpravy a doplnění bezpečnostních pravidel
- Nastavení VPN
- Testy redundance, komunikace a automatických aktualizací
- Instalace specializovaného logovacího nástroje a jeho integrace s NGFW
- Nastavení pravidel pro sběr událostí, přeposílání vybraných událostí na centrální logmanagement
- Otestování obousměrné komunikace
- Instalace a konfigurace Webového aplikačního FW
- Otestování komunikace
- Instalace a inicializace centrální EDR/XDR platformy
- Instalace síťové XDR sondy a její napojení na centrální management
- Integrace s MS Active Directory
- Postupná migrace koncových stanic a serverů ze stávajícího AV řešení do EDR
- Nastavení bezpečnostních politik, scanů, aktualizací atd.
- Konfigurace ochrany klientských mailboxů
- Migrace dat a služeb
- Nastavení reportingu
- Montáž nástroje pro zaznamenávání logů do racku
- Aktualizace FW a OS
- Napojení a sběr významných log zdrojů stávající infrastruktury, minimálně v rozsahu:
    - Stávající aplikace GINIS (Gordic spol. s r.o.), AIS (VITA Software), ESA (YAMACO Software), Mzdy a personalistika (VEMA) a GIS
    - MS Active Directory včetně základních služeb DNS, DHCP, PKI apod.
    - 1x Virtualizační systém VMware
    - 60x Windows Server
    - Xx Linux Server
    - 2x NGFW
    - 30x L2/L3 přepínač
    - 6x Management fyzických serverů
    - 2x diskové pole
    - Xx NAS
    - 1x 802.1X autentizační systém
    - 1x zálohovací systém Veeam
    - 1x XDR systém
    - 2x UPS
- Nastavení reportingu
- Nastavení alertů
- Dodávka hybridních čipových karet
- Implementace Certifikační Autority (CA)
- Implementace dodaných aplikací pro obsluhu čipových karet
- Vyškolení příslušných osob odběratele na obsluhu všech dodaných systémů

- Konfigurace datového centra tak, aby stávající produkční prostředí a služby jím poskytované byly provozovány, monitorovány, zálohovány a zabezpečeny na nově dodaném HW a SW;
- Dodání elektronické dokumentace (pdf) ke všem použitým SW komponentám (user guide, admin guide, config guide atp.)
- Vytvoření a předání dokumentace o konkrétním provedení a nastavení celého zálohovacího prostředí. (otevřený editovatelný formát ODF např. *.odt nebo MS Office formát např. *.docx)
- Zanesení dokumentace prostředí do Redmine objednatele popř. předání formou dokumentů ve formátech odt, docx či pdf;
- Kompletní instalace bezpečnostního software na všechna zařízení v jeho vlastnictví, které určí jeho pověření odborní (IT) zaměstnanci
- Dokumentace jednotlivých HW a SW komponent obsahuje část věnující se instalaci, konfiguraci, běžné administraci a užívání.

28. Zaškolení obsluhy – soubor

- Zaškolení 2 zaměstnanců zadavatele v obsluze a údržbě zařízení v rozsahu 24 pracovních hodin na dodaném zařízení v místě plnění (s rozsahem 8 pracovních hodin na zařízení LOG management).

Č.	Kritérium	Splněno	Popis řešení
1.	Nod virtualizační infrastruktury (server)	ANO	**Server HPE DL325 Gen11** **P54199-B21 HPE DL325 G11 8SFF CTO Server v konfiguraci:** 1x P53702-B21 AMD EPYC 9124 CPU for HPE 12x P50312-B21 HPE 64GB 2Rx4 PC5-4800B-R Smart Kit 2x P26262-B21 BCM 57414 10/25GbE 2p SFP28 Adptr 2x P03178-B21 HPE 1000W FS Ti Ht Plg PS Kit 1x BD505A HPE iLO Adv 1-svr Lic 3yr Support 1x S1A05A HPE Cmp Cloud Mgmt Srv FIO Enablement 2x P48183-B21 HPE NS204i-u Gen11 Ht Plg Boot Opt Dev 1x R7A12AAE HPE COM Std 5yr Up ProLiant SaaS Podpora: 1x HU4A6A5 HPE 5Y Tech Care Essential SVC

Č.	Kritérium	Splněno	Popis řešení
2.	Diskové úložiště	ANO	**HPE Alletra Storage MP S0B84A v konfiguraci:** 1x S3Q02A HPE Alletra Stg ArcusOS /TB 5yr LTU 1x R7C75A HPE Alletra STG MP 10000 2U Chassis 2x S0S38A HPE Alletra STG MP B10120 Cntrl Node 2x R7C82A HPE Alletra STG MP 10/25GbE 4p HBA 2x R9Z97A HPE Alletra STG MP C14 2200W AC PS 14x R9H66A HPE Alletra STG MP 1.92TB NVMe SED SSD 27x S3Q02AAE HPE AL STG MP B10000 /TB 5yr SW/Sup SaaS 12x 487655-B21 HPE BLc 10G SFP+ SFP+ 3m DAC Cable 2x HU4A6A5008M HPE Alletra StgMP 8C Swtchless Node Supp 2x HU4A6A5008Q HPE Alletra Stg 10/25GbE 4-port HBA Supp 14x HU4A6A5008R HPE Alletra Stg MP 1.92TB NVMe SSD Supp 1x HA124A1#VZW HPE Alletra Storage Arcus OS Startup SVC 1x HA124A1#VZS HPE Alletra STG MPB10000 2NFld Srtup SC Podpora: 1x HU4A6A5 HPE 5Y Tech Care Essential SVC
3.	Quorum/Witness server (tzv. „svědek“)	ANO	**HPE Microserver Gen 11 P71850-B21 v konfiguraci:** 1x P65225-B21 INT Xeon E-2414 FIO CPU for HPE 1x P64339-B21 HPE 32GB 2Rx8 PC5-4800B-E STND Kit 2x P65272-B21 HPE 480GB SATA RI SFF RW MV SSD 1x BD505A HPE iLO Adv 1-svr Lic 3yr Support 2x 870213-B21 HPE MicroSvr Gen10 NHP Converter Kit 1x P74395-B21 PE MicroSvr Gen11 180W Ext Pwr Adptr 1x R7A12AAE HPE COM Std 5yr Up ProLiant SaaS Podpora: 1x HU4B2A5 HPE 5Y Tech Care Basic SVC
4.	Hardened Repository	ANO	**Server HPE DL380 Gen11 P52533-B21 konfiguraci:** 1x INT Xeon-S 4514Y CPU for HPE 2x P64706-B21 HPE 32GB 2Rx8 PC5-5600B-R Smart Kit

Č.	Kritérium	Splněno	Popis řešení
			1x P48809-B21 HPE DL380 G11 4LFF SAS/SATA LP Kit 16x 881781-B21 HPE 12TB SAS 7.2K LFF LP He 512e HDD 1x P47781-B21 HPE MR416i-o Gen11 SPDM Storage Cntlr 1x P26256-B21 BCM 57412 10GbE 2p SFP+ OCP3 Adptr 2x P03178-B21 HPE 1000W FS Ti Ht Plg PS Kit 1x BD505A HPE iLO Adv 1-svr Lic 3yr Support 1x S1A05A HPE Cmp Cloud Mgmt Srv FIO Enablement 1x P48183-B21 HPE NS204i-u Gen11 Ht Plg Boot Opt Dev 1x R7A12AAE HPE COM Std 5yr Up ProLiant SaaS 10x 487655-B21 HPE BLc 10G SFP+ SFP+ 3m DAC Cable 2x P17264-B21 HPE DL325 Gen10+ x16 LP PCIe Riser Kit 2x P26259-B21 BCM 57412 10GbE 2p SFP+ Adptr Podpora: 1x HU4A6A5 HPE 5Y Tech Care Essential SVC **Součástí dodávky je SW pro zálohování:** V-ESSVUL-4S-BS5MG-40 Veeam Data Platform Essentials Universal 40 instance License v trvání 5 let
5.	Virtualizační software	ANO	**VMware vSphere Enterprise Plus** VCF-VSP-ENT-PLUS VMware vSphere Enterprise Plus – Multiyear, 32 core (licence celkem na 3 roky)
6.	UPS záložní zdroj	ANO	**Eaton 91PS UPS** 3/1fáze, 8kW - 91PS-8(15)-15-1x9Ah-MBS-6 2x EBC-A-2x32-9AH-BB-63A Externí bateriová skříň, typ A, 2x32-9AH 63A jistič + 24V ST (8-20kW) EVMAF132X ePDU G4: Řízené IEC 0U, In: IEC60309 32A 1P - Out: 24xC13:18xC39 Záruka: 5 let
7.	Doplnění stávajících serverů	ANO	**Serverové komponenty HPE** 2x P17264-B21 HPE DL325 Gen10+ x16 LP PCIe Riser Kit 2x 487655-B21 BCM 57412 10GbE 2p SFP P26259-B21 BCM 57412 10GbE 2p SFP+ Adptr včetně 2x 3m DAC kabelů
8.	Sada licencí software	ANO	**OS Windows Server Datacenter** 2x EP2-25015 Win Server DC Core 2025 SLng 16L **OS Windows Server** 1x EP2-24969 Win Server Standard Core 2025 SLng 16L

Č.	Kritérium	Splněno	Popis řešení
			Přístupové licence CAL 205x EP2-24898 Win Server CAL 2025 SLng UCAL **SQL server licence** 2x 7NQ-00300 SQL Server Standard Core SLng LSA 2L **MS External Connector** 1x EP2-25038 Win Server External Connector 2025 SLng
9.	Autentizační platforma (AAA)	ANO	**Aruba ClearPass** 2x JZ399AAE Aruba ClearPass Cx000V VM Appl E-LTU JZ402AAE Aruba ClearPass NL AC 1K CE E-LTU H9XH9E Aruba 5Y FC SW CP NL AC 1K CE E-L SVC JZ473AAE Aruba ClearPass NL OG 500 EP E-LTU H9WZ9E Aruba 5Y FC SW CP NL OG 500 EP E-L SVC
10.	Páteřní přepínač	ANO	**HPE Aruba 8325H** S4B20A HPE ANW 8325H 18Y 4C FB 4Fs 2PS Sw S2T44A HPE ANW 8325H 2-post Rack Mount Kit Podpora: H06MKE HPE ANW FC 3Y NBD Exch 8325H Sw SVC [for S4B20A] Příslušenství: 2x S3N89A HPE ANW 100G LR QSFP28 LC 10km SMF 4x S1C96A Aruba 25G BiDi 10km-Downstream 1330/1270 Transceiver 2x SPB-2910WHPE SFP+ WDM transceiver 10GBASE-BX, multirate, SM 10km, TX1330/RX1270nm, LC simp., DMI , HP komp. 2x J9283D Aruba 10G SFP+ to SFP+ 3m DAC Cable
11.	Datacentrový přepínač	ANO	**HPE Aruba 6300M** JL658A HPE Aruba Networking 6300M 24SFP+ 4SFP56 Switch Podpora: HR4C2E HPE ANW FC 3Y NBD Exch 8325H Sw SVC [for S4B20A] 2x JL085A Aruba X371 12VDC 250W PS HR4C2E Aruba 3Y FC NBD Exch 6300M 24SFP SVC Příslušenství:

Č.	Kritérium	Splněno	Popis řešení
			4x S1C98A Aruba 25G BiDi 10km-Downstream 1270/1330 Transceiver 2x R0M46A Aruba 50G SFP56 to SFP56 0.65m DAC Cable
12.	Přístupový přepínač - typ 1	ANO	**HPE Aruba 6200F** JL727B HPE ANW 6200F 48G C4 4SFP+370W Switch
13.	Přístupový přepínač - typ 2	ANO	**HPE Aruba 6200F** JL726B HPE ANW 6200F 48G 4SFP+ Switch
14.	Přístupový přepínač Typ 3	ANO	**HPE Aruba 6200F** JL725B HPE ANW 6200F 24G C4 4SFP+370W Switch
15.	Přístupový přepínač Typ 4	ANO	**HPE Aruba 6200F** JL724B HPE ANW 6200F 24G 4SFP+ Sw Příslušenství: 22x SPB-2810WHPE SFP+ WDM transceiver 10GBASE-BX, multirate, SM 10km, TX1270/RX1330nm, LC simp., DMI, HP komp. 22x SPB-2910WHPE SFP+ WDM transceiver 10GBASE-BX, multirate, SM 10km, TX1330/RX1270nm, LC simp., DMI , HP komp. 4x J9150D Aruba 10G SFP+ LC SR 300m MMF XCVR 3x J9283D Aruba 10G SFP+ to SFP+ 3m DAC Cable 12x J9281D Aruba 10G SFP+ to SFP+ 1m DAC Cable 2x S3N89A Aruba 100G LR QSFP28 LC 10km SMF XCVR
16.	Bezdrátový přístupový bod	ANO	**Přístupový bod (AP) Aruba AP-615** 1x R7J49A Aruba AP-615 (RW) Campus AP + 1x R3J18A AP-MNT-D AP mount bracket individual D
17.	Software pro správu sítě	ANO	**Aruba AirWave** JW546AAE 60x Aruba AirWave 1 Device Lic E-LTU H2YW0E 60x Aruba 5Y FC SW AW 1 Dev E-L SVC
18.	Optimalizace provozu WiFi sítě	ANO	• Umístění bezdrátových AP bude provedeno na základě analýzy pokrytí WiFi signálem v zadavatelem definovaných prostorách. • Analýza optimalizace provozu WiFi sítě bude realizována pomocí profesionálního nástroje Ekahau na základě mapových podkladů dodaných zadavatelem (DWG).

Č.	Kritérium	Splněno	Popis řešení
			• Takto vygenerovaný návrh rozmístění AP bude konzultován se zadavatelem a upraven dle možností skutečného umístění AP v budovách. • Finálním výstupem optimalizace provozu WiFi sítě budou grafické reporty a zpráva ve formátu PDF minimálně v rozsahu: o Návrh rozmístění AP o Heat mapa bezdrátové sítě o Síla signálu (pokrytí) pro pásmo 5GHz o Síla signálu (pokrytí) pro pásmo 2,4 GHz o Překryv kanálů o Poměr síly signálu a šumu pro 5 GHz a 2,4 GHz
19.	Firewall (NGFW)	ANO	**FortiGate FG-120G** FG-120G-BDL-950-36 FortiGate 120G, HW s licencí, HW + FortiCare Premium and FortiGuard Unified Threat Protection (UTP) 3YR Příslušenství: 3x SPB-2810WHPE SFP+ WDM transceiver 10GBASE-BX, multirate, SM 10km, TX1270/RX1330nm, LC simp., DMI , HP komp. 3x SPB-2910WHPE SFP+ WDM transceiver 10GBASE-BX, multirate, SM 10km, TX1330/RX1270nm, LC simp., DMI , HP komp.
20.	Analyzer	ANO	**FortiAnalyzer** FAZ-VM-GB1 FortiAnalyzer VM, Licence, 1 GB Logs/Day Add-on FAZ-VM-GB5 FortiAnalyzer VM, Licence, 5 GB Logs/Day Add-on FC1-10-LV0VM-248-02-36 FortiAnalyzer VM, SW podpora, FortiCare Premium (for 1-6 GB Logs/Day) 3YR FC1-10-LV0VM-661-02-36 FortiAnalyzer, FortiAnalyzer-VM IOC and Outbreak Detection Service 3YR
21.	Webový aplikační FW (WAF)	ANO	**FortiWeb** FWB-VM01 FortiWeb VM01, virtual apliance FC-10-VVM01-734-02-36 FortiWeb, FortiWeb-VM01 Enterprise Bundle - Advanced bundle plus Advanced Bot Protection (200,000 monthly requests) and Data Loss Prevention service
22.	Antimalware (EDR/XDR) pro stanice	ANO	**Bitdefender GravityZone Business Security Enterprise (Ultra)**

Č.	Kritérium	Splněno	Popis řešení
			Bundle – 205x Licence Bitdefender GravityZone Business Security Enterprise (Ultra) - 60 M vč. implementace a zaškolení
23.	Antimalware (EDR/XDR) pro servery	ANO	**Bitdefender GravityZone Business Security Enterprise (Ultra)** Bundle – 10x Licence Bitdefender GravityZone Business Security Enterprise (Ultra) - 60M
24.	Síťová sonda XDR	ANO	**BitDefender XDR Sensor** Add-On - Bitdefender XDR Sensor – Network – XDR virtuální sonda – 60M
25.	Nástroj pro zaznamenávání logů	ANO	**LogManager M** LOGM-M-5Y Logmanager M (Logmanager M, 1U server, 5 let HW a SW support, 4x4TB disky)
26.	Hybridní čipové karty	ANO	**Řešení MONET+ ProID** **CMS licence pro max. 250 uživ.** Card management system (CMS) je základním modulem pro správu čipových karet. (webová aplikace pro správce a webové služby na pozadí pro synchronizaci dat do centrální DB) Informace o kartách (a jejich datovém obsahu) používaných v rámci organizace. Informace o držitelích karet Využití pro správu životního cyklu čipových karet **Kartové centrum** Desktopová aplikace pro správu životního cyklu karet. Instaluje se na pracovišti správce karet a úzce spolupracuje s webovou aplikací CMS. Pomocí kartového centra může správce karet řídit životní cyklus karet a certifikátů v organizaci. **ACEx licence pro max. 250 uživ.** Zajišťuje automatické obnovení certifikátů, kterým končí platnost, na pozadí - v závislosti na nastavení. Zaměstnanci mohou obnovovat všechny své certifikáty téměř nezávisle přímo ze svého počítače. V případě blížící se expirace vyzve uživatele k obnovení certifikátu. ACEx dále může sloužit pro automatizované vystavení nových doménových certifikátu držitelům na základě

Č.	Kritérium	Splněno	Popis řešení
			členství v doménové skupině. ACEX také kontroluje volné místo na čipové kartě a v případě splnění podmínek odstraňuje neplatné a nepotřebné certifikáty. Nedochází tedy k postupnému zaplnění čipové karty nepotřebnými daty. **NTFMail** Informuje včas uživatele o blížícím se vypršení platnosti uživatelských nebo technologických certifikátů Informace o certifikátech ze SaRS, popřípadě CMS databáze, informace o uživatelích z Active Directory. Odesílá e-maily s blížící se expirací držitelům certifikátů/správcům. Ochrana pro případ, že by aplikace ACEx z nějakého důvodu včas neobnovila certifikáty uživatelů, nebo správcové nestihli obnovit certifikáty technologických prvků. Je možné notifikovat certifikáty vydávané z doménového PKI i externích certifikikačních autorit, např eIdentity, nebo PostSignum. Je možné notifikovat jak vydání certifikátu tak například blížící se konec platnosti. **Cache PIN licence pro max. 250 uživ.** **SaRS licence pro max. 250 uživ.** **Servisní podpora na 3 roky pro karty, čtečky, moduly** Implementace CA a dodaných systémů a vyškolení příslušných osob odběratele na obsluhu všech dodaných systémů
27.	Instalace a implementace	ANO	• Rozbalení veškerého dodaného HW, kontrola bezvadného stavu, likvidace přepravního a obalového materiálu a spolupráce s dodavatelem na evidenci HW (případné opatření evidenčními štítky) • Montáž síťových přepínačů a WiFi přístupových bodů • Aktualizace FW • L2 propojení a základní nastavení (IP adresace, NTP, SNMP apod.) • Konfigurace L3 páteřních prvků a vysoké dostupnosti datových center • Instalace a konfigurace SW pro správu sítě

Č.	Kritérium	Splněno	Popis řešení
			• Testy vysoké dostupnosti páteřních a datacentrových přepínačů • Instalace a zprovoznění veškerého serverového HW do stávajících 19“ rozvaděčů a provedení funkčních testů • Instalace a oživení UPS • Propojení LAN, SAN, kabelový management • Aktualizace FW, BIOS apod. • Osazení NIC karet do stávajících serverů • Instalace diskových polí a implementace „Metro Clusteru“ • Integrace serverů do stávající VMware infrastruktury, oživení druhého datového centra • Instalace VM (OS a SQL) • Testy vysoké dostupnosti / trhací testy / testy UPS • Začlenění Hardened Repository do stávajícího systému zálohování • Úprava zálohovacích plánů • Migrace stávajících dat • Instalace AAA platformy • Napojení na Radius server • Konfigurace bezpečnostních pravidel pro přístup do sítě LAN • Pilotní konfigurace 802.1x na 5 koncových stanic • Montáž a propojení NGFW • Aktualizace FW, napojení na aktualizační služby výrobce • Zapojení vysoké dostupnosti (HA) • Migrace a revize stávajících bezpečnostních pravidel • Úpravy a doplnění bezpečnostních pravidel • Nastavení VPN • Testy redundance, komunikace a automatických aktualizací • Instalace specializovaného logovacího nástroje a jeho integrace s NGFW • Nastavení pravidel pro sběr událostí, přeposílání vybraných událostí na centrální logmanagement • Otestování obousměrné komunikace

Č.	Kritérium	Splněno	Popis řešení

			• Instalace a konfigurace Webového aplikačního FW
			• Otestování komunikace
			• Instalace a inicializace centrální EDR/XDR platformy
			• Instalace síťové XDR sondy a její napojení na centrální management
			• Integrace s MS Active Directory
			• Postupná migrace koncových stanic a serverů ze stávajícího AV řešení do EDR
			• Nastavení bezpečnostních politik, scanů, aktualizací atd.
			• Konfigurace ochrany klientských mailboxů
			• Migrace dat a služeb
			• Nastavení reportingu
			• Montáž nástroje pro zaznamenávání logů do racku
			• Aktualizace FW a OS
			• Napojení a sběr významných log zdrojů stávající infrastruktury, minimálně v rozsahu:
			  ○ Stávající aplikace GINIS (Gordic spol. s r.o.), AIS (VITA Software), ESA (YAMACO Software), Mzdy a personalistika (VEMA) a GIS
			  ○ MS Active Directory včetně základních služeb DNS, DHCP, PKI apod.
			  ○ 1x Virtualizační systém VMware
			  ○ 60x Windows Server
			  ○ Linux Server
			  ○ 2x NGFW
			  ○ 30x L2/L3 přepínač
			  ○ 6x Management fyzických serverů
			  ○ 2x diskové pole
			  ○ NAS
			  ○ 1x 802.1X autentizační systém
			  ○ 1x zálohovací systém Veeam
			  ○ 1x XDR systém
			  ○ 2x UPS
			• Nastavení reportingu
			• Nastavení alertů
			• Dodávka hybridních čipových karet

Č.	Kritérium	Splněno	Popis řešení
			• Implementace Certifikační Autority (CA) • Implementace dodaných aplikací pro obsluhu čipových karet • Vyškolení příslušných osob odběratele na obsluhu všech dodaných systémů • Konfigurace datového centra tak, aby stávající produkční prostředí a služby jím poskytované byly provozovány, monitorovány, zálohovány a zabezpečeny na nově dodaném HW a SW; • Dodání elektronické dokumentace (pdf) ke všem použitým SW komponentám (user guide, admin guide, config guide atp.) • Vytvoření a předání dokumentace o konkrétním provedení a nastavení celého zálohovacího prostředí. (otevřený editovatelný formát ODF např. *.odt nebo MS Office formát např. *.docx) • Zanesení dokumentace prostředí do Redmine objednatele popř. předání formou dokumentů ve formátech odt, docx či pdf; • Kompletní instalace bezpečnostního software na všechna zařízení v jeho vlastnictví, které určí jeho pověření odborní (IT) zaměstnanci • Dokumentace jednotlivých HW a SW komponent bude mít část věnující se instalaci, konfiguraci, běžné administraci a užívání.
28.	Zaškolení obsluhy	ANO	Zaškolení 2 zaměstnanců zadavatele v obsluze a údržbě zařízení v rozsahu 24 pracovních hodin na dodaném zařízení v místě plnění (s rozsahem 8 pracovních hodin na zařízení LOG management).

Prohlašuji, že veškeré shora uvedené údaje (parametry) jsou úplné, pravdivé a odpovídají skutečnosti. Jsem si vědom/a právních následků v případě uvedení nesprávných nebo nepravdivých údajů (parametrů).

Za Dodavatele:

Ve Smiřicích v den elektronického podpisu

……

Jaroslav Dvořák, člen představenstva

Tomáš Ječmínek, člen představenstva