Veřejná zakázka

**„Zvýšení kybernetické bezpečnosti města Pelhřimov – část B“**

**Zadavatel:**

**Město Pelhřimov**se sídlem Pelhřimov, Masarykovo náměstí 1, PSČ 393 01   
IČO: 00248801  
DIČ: CZ00248801

Osoba zastupující zadavatele: Ladislav Med, starosta

Detailní specifikace předmětu plnění

# **1. Rozsah dodávek a služeb**

Následující seznam požadavků vymezuje technické parametry pro jednotlivé komodity předmětu plnění z pohledu jejich minimálních požadavků.

Všechny výrobky, které budou součástí nabízeného plnění a následné dodávky zadavateli:

1. jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
2. mají plnou záruku od výrobce,
3. budou podporovány výrobcem a budou součástí servisního programu výrobce pro ČR,
4. obsahují licenci příslušného softwaru nezbytnou pro splnění požadovaných vlastností a parametrů,
5. jsou/budou v databázi výrobce uvedeny jako nabízená/prodaná zadavateli,
6. jsou určeny pro provoz v České republice.
7. pocházejí z oficiální distribuční sítě v rámci EU

Tyto skutečnosti uchazeč doloží čestným prohlášením výrobce, popř. uchazeče samotného, nelze-li prohlášení výrobce získat. Zadavatel si vyhrazuje právo na zjištění původu výrobků při jejich převzetí, a to dle příslušných sériových čísel a právo podpisu předávacího protokolu, osvědčujícího převzetí plnění, až po ověření původu výrobku u výrobce.

Součástí předmětu plnění části B jsou dále následující služby:

* předimplementační analýza, která zohlední i výstupy části A veřejné zakázky
  1. Výchozí stav IT infrastruktury a bezpečnostního prostředí
  2. Používané bezpečnostní prvky a jejich stav.
  3. Organizační zabezpečení (politiky, postupy, řízení přístupů).
  4. Zohlednění výstupů z GAP analýzy a auditu části A
  5. Návrh řešení (architektonický koncept)
  6. Specifikace implementačních aktivit
  7. Specifikace měřitelných výstupních indikátorů a jejich hodnot
* dodání zařízení na místo plnění, vybalení, osazení do racků a oživení, včetně nezbytného příslušenství (zejména veškeré kabeláže, zářičů, montážního materiálu apod.) pro propojení všech komponent,
* potřebné licence pro splnění požadovaných vlastností a parametrů.
* instalaci a základní konfiguraci zařízení včetně posledních bezpečnostních záplat,
* zapojení do stávající síťové infrastruktury a serverového prostředí zadavatele,
* konfiguraci segmentace, přístupových politik, zabezpečení managementu a logování,
* nastavení alertingu, záloh konfigurací a obnovy po havárii,
* předání instalační dokumentace v českém jazyce,
* provedení testu funkčnosti a provozuschopnosti (akceptační scénář),
* detailní školení správců systémů,
* zpracování dokumentace finálního vyhotovení,
* odvoz a likvidace obalového materiálu

# **Návaznost na cíle dotační výzvy**

Navržené řešení musí být procesně i funkčně provázáno na výstupy plnění části A a implementováno do následujících informačních systémů města Pelhřimov identifikovaných pro účely posílení jejich kybernetické bezpečnosti:

* IS FENIX (správní a ekonomické agendy),
* IS eSPIS (spisová služba),
* IS FLUXPAM 5 (personalistika a mzdy),
* IS Elektronická pošta,
* IS Portál občana,
* IS Doménové prostředí Windows serveru (AD, autentizace).

Řešení musí být v souladu s požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a vyhlášky č. 82/2018 Sb., zejména § 18 a § 20.

# **1.1 Servery pro virtualizaci – 3 ks**

Parametry pro 1 ks:

* Provedení: rackmount 19“, výška max. 2U, plnovýsuvné ližiny včetně ramena pro vedení kabeláže
* 1ks CPU - architektura x86 s 16 plnohodnotnými jádry. Taktovací základní frekvence min. 4,1 GHz, FSB min. 4800 MHz, min. 256 MB L3 cache celkem, nebo v testu na cpubenchmark.net minimálně 55000 bodů. Max. počet CPU je omezen na 1 a počet jader je omezen na 16 core z důvodu licencování OS a aplikací.
* RAM 768 GB, RDIMM, 5600MT/s, Dual Rank
* 2 ks disků 960GB pro instalaci OS - konfigurace RAID-1 na samostatném HW řadiči
* 1 ks Ethernet adapter Dual Port 10/25GbE SFP Adapter včetně příslušných zářičů 10/25Gbps
* 1 ks FC adapter 2x port 32Gbps včetně zářičů
* 1 ks Ethernet adapter 2x 1Gbps 1000BASE-T včetně příslušných zářičů
* 2 ks hot-swap zdroje napájení dimenzované pro plné osazení serveru CPU, RAM a PCIe zařízení, účinnost min. 94%
* Server musí být osazen TPM 2.0
* Redundantní hotswap ventilátory
* IPMI 2.0 popř. obdoba, možnost vzdáleného převzetí grafické konsole bez závislosti na OS, webový klient HTML5, vzdálený mount DVD media, USB, dedikovaný port (není součástí požadovaného počtu ethernet portů)
* řízení přístupových práv do managementu serveru pomocí účtů Active Directory domény a dvou-faktorové authentikace
* Součástí managementu serveru musí být vestavěná funkcionalita call-home (server musí být schopen automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce)
* Server vybavený alfanumerickým zobrazovačem stavu s možností nastavení management IP adresy.
* Vyčítání přes SNMP celkového zdraví serveru bez nutnosti instalovat OS – jeden parametr v MIB
* Kompatibilita všech komponent s OS VMWARE ESXi 8.x dle veřejně dostupného seznamu (např. <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=server>)
* Záruka 60 měsíců s opravou následující pracovní den (NBD) v místě instalace. Přístup k firmware a jeho aktualizacím po dobu trvání záruční lhůty.
* Windows Server Datacenter 2025 per Core – licence pro celkový počet jader osazených v serveru
* Windows Server CAL 2025 User CAL – licence pro 50 uživatelů (při pořízení 3 ks serverů budou dodány licence celkem pro 150 uživatelů)
* Veeam Data Platform Essentials, Enterprise Plus Edition – licence s platností min. 5 let pro CPU osazené v serverech, umožňující zálohování neomezeného počtu virtuálních serverů na něm běžících. Tato konkrétní licence je poptávaná z důvodu kompatibility se stávajícím zálohovacím software, který již zadavatel vlastní a používá.

**Implementace**

* Instalace pole v určeném místě zadavatele a zapojení do vyhrazené management sítě Instalace posledních stabilních firmware.
* Instalace a konfigurace serverové virtualizace VMware vSphere 8 Standard – licence poskytne zadavatel.
* Připojení napřímo k diskovému poli pomocí FC.
* Instalace VMware vCenter Server – licenci poskytne zadavatel.
* Rekonfigurace zálohování a nastavení replikací virtuálních serverů.
* Migrace cca 50 virtuálních serverů ze stávajících serverů na nově dodávané.

# **1.2 Diskové pole – 1 ks**

|  |  |
| --- | --- |
| Architektura | * modulární, minimálně dvou řadičové all flash / hybridní diskové pole active-active designu založené na NVMe architektuře, řešení je koncipováno jako HW, SW a FW od jednoho výrobce |
| Výkonnost | * škálování výkonnosti je možné nativním přidáváním dalších řadičů minimálně do osmi řadičové konfigurace a škálování kapacity pomocí expanzních jednotek. Škálování řadičů ani expanzních jednotek není povoleno řešit pomocí externí virtualizace nebo podvěšením dalšího pole a řadičů |
| Rozšiřitelnost, podporované disky a moduly | * celková velikost cache/RAM v jednom řadiči je minimálně 128GB s možností rozšíření až na dvojnásobek. * celková nativní rozšiřitelnost je minimálně 400 disků, v případě nasazení více řadičů minimálně dvojnásobek disků. * podpora 2,5” nebo 3,5” disků technologie SSD/flash s NVMe atchitekturou včetně rotačních disků. * podpora minimálně následujících režimů RAID - 1, 5, 6, 10 nebo minimálně DRAID 1 a 6 |
| Minimální požadovaná hrubá kapacita a ochrana dat | * minimálně 52 TB na SSD/Flash s NVMe atchitekturou ve variantě enterprise (DWPD 2 a vyšší, maximální velikost jednoho SSD nebo flash modulu je 5 TB) |
| Požadavky na velikost řešení | * Nabízené řešení nesmí přesáhnout 1U. |
| Konektivita k hostitelským serverům (front-end) | * diskové pole obsahuje připojení diskového pole blokovým přístupem pomocí 32Gbit FC a 10Gbit iSCSI. Jsou požadovány min. 4 porty 32Gb FC a 2 porty 10Gb iSCSI na řadič, tzn. minimálně 8x 32Gbit FC portů včetně osazených SFP transceiverů a 4x 10Gbit iSCSI portů na jedno dvouřadičové diskové pole s možností rozšíření 32Gbit FC portů na dvojnásobek. |
| Funkcionality pro efektivní ukládání a správu dat | * vytváření virtuálních logických disků * thin provisioning (včetně detekce a reklamace prázdného prostoru) * komprese dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou nabízenou kapacitu včetně patřičného HW akcelerátoru nebo na jednotlivých modulech * deduplikace dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence * šifrování dat minimálně pro flash kapacitu ve standardu minimálně FIPS 140-2 nebo 3 bez nutnosti přítomnosti speciálních pevných disků včetně příslušné licence. Pokud nabízené řešení neumožňuje šifrování dat nad úrovní disků, jsou požadovány SED disky pro celou nabízenou flash kapacitu, opět minimálně ve standardu FIPS 140-2 nebo 3 * inteligentní správa výkonnostních charakteristik (pro minimálně 3 tiery a to včetně SCM) virtualizovaných diskových prostorů (automatická migrace více utilizovaných dat na rychlejší disky nebo SSD/SCM) * podpora externí storage virtualizace pro stávající disková pole a možnost dalšího připojení externích diskových polí od různých výrobců min. pro účely migrace. Seznam podporovaných diskových systému je veřejně dostupný. * Podpora nástrojů pro sledování historických dat o vytížení datového úložiště (minimálně počet IOps, latence, propustnost, alokovaná kapacita, využití keší) s granularitou na hosta či LUN s historií minimálně 1 rok (možnost řešit externích SW nástrojem v rámci dodávky) * Microsoft VSS podpora * VMware VAAI, VVOL podpora, dále je požadován VASA provider přímo ve FW nabízeného diskového pole |
| Podpora operačních systémů a hypervizorů | * Oracle Enterprise Linux 8.x a vyšší * Oracle DB 11.x a 12.x a vyšší * RHEL 6.x a vyšší * VMware 7 a vyšší včetně VAAI a VASA integrací * Windows server 2016 a vyšší |
| Typ přístupu k datům | * blokový, standard FCP a iSCSI |
| Bezpečnost | * ochrana proti ransomware útokům nativní funkcionalitou nabízeného pole v rámci jeho funkcionalit – řešení z aplikační vrstvy pomocí aplikací třetích stran nebo za asistence zálohovacího SW není přípustné. Řešení musí být pro tento účel jasně popsané a určené, např. ochrana LUNu pouze nastavením do read-only modu není dostatečná pro splnění tohoto požadavku |
| * řešení musí umožňovat detekci ransomware v reálném čase na blokové úrovni před uložením na disky / flash moduly |
| * řešení musí umožňovat kontrolu zapsaných dat (bloků) přímo na jednotlivých SSD / flash modulech |
| Kopírovací funkce - licence musí být součástí nabídky a musí být na neomezenou kapacitu, počet disků, expanzích jednotek atd. | * zrcadlení virtuálního disku tzn. ochrana virtualizovaných dat v režimu RAID1 (s možností zdvojení dat virtuálního disku i na dvě pole) * možnost vytváření snapshotů (CoW a RoW) a klonů v následujících režimech: * snapshot se po určité době může automaticky stát klonem * inkrementální snapshoty, tzn. kopírují se jen rozdílová data mezi dvěma okamžiky iniciace klonu * reverzní snapshoty, tzn. lze provést zpětné přesunutí dat z klonu do původního originálního Volume * lze udržovat až 4 inkrementálně pořizované klony z jednoho originálu (s možností reverzních snapshotů) * interní/externí zrcadlení logického (virtuálního) disku z jednoho zdroje do dvou cílů pro zvýšení dostupnosti v případě výpadku jednoho cíle |
| Zajištění kontinuální dostupnosti dat (DR a HA řešení) - licence musí být součástí nabídky a musí být na neomezenou kapacitu, počet disků, expanzích jednotek atd. | * upgrade software a hardware u řadičů je proveditelné za chodu a bez ztráty přístupu hostitelských serverů k datum * diskové musí být možné spojit do clusteru, který umožňuje vytvoření jednoho funkčního celku, zrcadlení dat mezi jednotlivými poli apod. * vytvoření HA řešení s automatickým failover bez dalších vícenákladů, které je navíc nezávislé na běžných OS nebo virtualizační platformě včetně příslušných licencí * podpora replikace do třetí lokality * SW pro redundantní datové cesty v ceně řešení * Nabízené řešení musí být plně kompatibilní s VMware Metro Storage Cluster funkcionalitou, tzn. musí být dohledatelné v matici kompatibility na stránkách VMware |
| Migrace dat | * transparentní migrace (tzn. možnost zdarma migrovat data ze stávajících diskových polí na nová disková úložiště) s možnosti rozšíření o synchronní a asynchronní zrcadlení logických (virtuálních) disků v případě více lokalit |
| Počet hostitelských serverů připojovaných k diskovému poli | * řešení obsahuje licence na neomezený počet připojení hostitelských serverů |
| Správa diskového pole a další dostupné funkcionality | * SW pro plnohodnotnou správu diskového pole a diskových subsystémů, možnost ovládání přes CLI, GUI (ze std. web browseru) * Remote Service (call home) v ceně řešení * Příkazy prováděné v GUI jsou uchovávány v tzv. "AuditLogu" v podobě standardních CLI příkazů, které lze později snadno zkopírovat a aplikovat při programování uživatelských skriptů např. pro podporu automatizace zálohování atd. |
| Příslušenství | * Součástí dodávky je veškerá potřebná kabeláž pro plné zapojení všech portů do instalovaného prostředí a potřebná napájecí kabeláž kompatibilní s napájecími lištami v RACK skříních. |
| Záruka a servisní podpora | * Minimálně 60 měsíců v režimu 24x7 s opravou do 24 hodin v místě instalace, včetně SW podpory, která umožňuje např. přístup k novým verzím FW, opravným patchům atd. * Servisní podpora výrobce v českém jazyce |

**Implementace**

* Instalace pole v určeném místě zadavatele a zapojení do vyhrazené management sítě.
* Instalace posledního stabilního firmware.
* Konfigurace diskových oddílů a jejich publikace serverům/clusteru
* Nastavení pravidelných storage snapshotů včetně jejich retence a omezení je smazat.
* Konfigurace zabezpečeného přístupu k managementu.
* Nastavení monitoringu včetně call home a detekce ransomware.
* Migrace dat ze stávajících diskových polí na nově dodávané.

# **1.3 Deduplikační zálohovací jednotka s ochranou proti smazání dat – 1 ks**

**Výkon a škálovatelnost:**

* Řešení musí mít minimálně 72 TB využitelné (usable) lokální kapacity bez redukce dat včetně všech potřebných licencí pro tuto kapacitu.
* Řešení musí umožňovat rozšíření alespoň do úrovně 1,5 PB využitelné lokální kapacity bez redukce dat a bez nutnosti výměny jakékoliv dodávané součásti, cloudové uložiště jako rozšíření není uznatelné
* Propustnost při zálohování dodávaného řešení (skutečný počet disků a dalších komponent) alespoň 7TB/hodinu,
* Zařízení musí při ukládání dat využívat princip deduplikace,
* Úložiště nesmí vytvářet deduplikační pooly – musí disponovat globální deduplikací bez ohledu na typ dat, přenosový protokol a množství zálohovacích serverů/aplikací, které na něj data ukládají,
* Řešení musí být postaveno na fyzické instalaci operačního systému bez další virtualizace.

**Integrace a interoperabilita:**

* Zařízení musí podporovat minimálně následující protokoly: CIFS, NFS, S3 a musí umožnit jejich současné použití,
* Zálohovací řešení musí být univerzální z hlediska podpory datových typů zálohovaných dat, musí podporovat všechny datové typy používané v produkčním prostředí
* Řešení musí umožnit komprimaci ukládaných deduplikovaných dat
* Nabízený diskový úložný systém musí být plně podporován nabízeným zálohovacím SW. Nabízené řešení bude uvedeno na webu výrobce zálohovacího SW mezi kompatibilními deduplikačními appliance. Řešení musí být plně podporováno pro produkt Veeam Backup & Replication. Oficiálně podporovaná řešení jsou popsána zde: <https://helpcenter.veeam.com/docs/backup/vsphere/deduplicating_storage_appliances.html?ver=120>

**Replikace**

* Zařízení musí obsahovat potřebné licence pro nativní funkcionalitu replikace dat do dalšího zařízení stejného výrobce,
* Řešení musí posílat pouze deduplikovaná zkomprimovaná data
* Řešení musí podporovat alespoň následující scénáře pro replikaci: 1:1, M:1 a kaskádovou replikaci
* Řešení musí umožnit funkcionalitu šifrování replikačního toku data-in-flight
* Řešení musí umožnit kontrolu a správu využití pásma pro přenos dat (QoS)

**Spolehlivost, ochrana a obnova**

* Zařízení musí disponovat redundantními hot-swap napájecími zdroji a ventilátory
* Zařízení musí zajišťovat ochranu dat alespoň na úrovni duální diskové parity
* Zařízení musí umožňovat šifrování úložného prostoru a to bez omezení výkonu - dodání včetně potřebných licencí pro výše požadovanou kapacitu
* Zařízení musí zajišťovat výměnu všech disků za chodu – hot-swap,
* Zařízení musí obsahovat HotSpare disk pro všechny RAID skupiny v rámci zařízení,
* Zařízení musí obsahovat algoritmy pro kontrolu a verifikaci konzistence a čitelnosti uložených dat,
* Zařízení musí umožňovat nastavit ochranu dat proti nechtěnému smazání či modifikaci dat pomocí časových zámků. Po nastavenou dobu lze data číst, ale nelze je přepisovat. Tato funkce nesmí být závislá na zálohovacím software, přenosovém protokolu (CIFS, NFS, S3) či typu dat. To znamená, že tato funkce musí být plně funkční nejenom s nabízeným zálohovacím SW, ale také jakýmkoliv jiným. Časové zámky se musí aplikovat uvnitř zařízení, nikoliv pomocí externích nástrojů a zálohovacích SW.
* Zařízení musí mít integrovanou ochranu časové integrity.
* Zařízení musí disponovat síťovými kartami 2x1GbE a 2x10Gb SFP+ včetně příslušných zářičů.
* Zařízení musí být v provedení RACK (šíře 19”), výška maximálně 2U, výsuvné kolejnice pro instalaci do racku.

**Správa**

* Řešení musí umožnit centrální správu pro všechna dodávaná zařízení prostřednictvím webového rozhraní
* Řešení musí poskytovat funkcionalitu automatického reportingu, automatický call-home,
* Řešení musí umožnit správu na principu rolí s různými typy oprávnění (Role-based Access Control).
* Řešení musí umožnit vynucení přihlášení minimálně dvou typů účtů (administrátorský, bezpečnostní) pro změny spojené se změnou nastavení ochrany dat – časových zámků.
* Řešení musí umožňovat zasílat strukturovaná data provozních a bezpečnostních událostí přes Syslog a SNMP.
* Řešení musí umožnit dvoufaktorové ověřování účtů pro správu díky jednorázovým heslům (Time-based One-Time Password). Pokud je potřeba externí nástroj, musí být součástí nabídky všechny potřebné licence až pro 25 uživatelů včetně potřebného hardware pro zajištění vysoké dostupnosti. Licence musí být perpetuální a instalace v místě zadavatele.

**Záruka a podpora**

* Podpora na hardware a software musí být od jednoho výrobce,
* Součástí nabízeného řešení musí být služba ponechání si vadných disků.
* V rámci povýšení verze softwaru dochází zároveň ke změně verze firmware na kompatibilní úroveň pro důležité komponenty – minimálně pro diskový řadič.
* Záruka a technická podpora celého řešení (HW i SW) v délce 60 měsíců s odezvou následující pracovní den.

**Implementace**

* Instalace v určeném místě zadavatele a zapojení do vyhrazené management sítě.
* Prvotní inicializace zařízení a upgrade firmware.
* Konfigurace účtů včetně dvoufaktorového ověření.
* Nastavení monitoringu a bezpečnostního logování.
* Konfigurace ochrany proti nevyžádanému smazání či editaci.
* Publikace diskového prostoru pro zálohovací SW.
* Konfigurace zálohovacího SW a nastavení jednotlivých zálohovacích úloh.
* Nastavení call-home – zabezpečené vzdálené propojení s podporou výrobce.
* Provedení bezpečnostního hardening.

# **1.4 Páteřní switch LAN – 2 ks**

**Základní vlastnosti**

* Typ zařízení: L3 přepínač
* Maximální velikost zařízení: 1U
* Minimálně 48x 1/10 GbE SFP+ portů s volitelným fyzickým rozhraním
* Minimálně 4x 40/100GbE portů s volitelným fyzickým rozhraním
* Potřebný počet SFP+/SFP modulů a propojovacích patch cordů
* 2x interní hot-swap AC napájecí zdroj
* Redundantní hot-swap ventilátory
* Směr proudění vzduchu zařízením: předo-zadní
* Minimální přepínací výkon: 1,76 Tbps
* Minimální paketový výkon: 1309 Mpps
* Minimální paketový buffer: 32 MB

**Vlastnosti stohování**

* Podporovaný počet přepínačů ve stohu: 2
* Kapacita stohovacího propojení: 400 Gbps
* Stoh podporuje distribuované přepínání paketů
* Libovolný prvek stohu může být řídícím prvkem (1:1 redundance)
* Seskupení portů IEEE 802.3ad mezi různými prvky stohu (MC-LAG)
* Podpora upgrade OS ve stohu bez narušení provozu (ISSU/Live upgrade)
* Podpora automatizace upgrade OS ve stohu bez narušení provozu přes REST API

**Funkce a protokoly**

* Podpora jumbo rámců včetně velikosti 9198 Byte
* Podpora linkové agregace IEEE 802.1AX
* Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4
* Minimální počet LACP skupin/linek ve skupině: 54/8
* Podpora LACP Fallback (např. pro PXE boot)
* Minimální počet záznamů v tabulce MAC adres: 147 000
* Minimální počet záznamů v tabulce ARP: 65 000
* Protokol pro definici šířených VLAN: MVRP
* Minimálně 1000 aktivních VLAN podle IEEE 802.1Q
* Tunelování 802.1Q v 802.1Q
* VLAN translace - swap 802.1Q tagů na trunk portu
* Podpora zařazování do VLAN podle standardu 802.1v
* Private VLAN včetně primary, secondary, isolated a community VLAN
* IEEE 802.1s - Multiple Spanning Tree a IEEE 802.1w
* STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
* Podpora ERPS (ITU G.8032) pro rychlou konvergenci do 100ms v kruhových sítích
* 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
* Podpora zapouzdření: GRE over IPv4
* Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace
* Podpora NTP server
* Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subnety
* Podpora L3 routed port včetně L3 sub-interface - nadřazené L3 rozhraní lze rozdělit
* Statické směrování IPv4 a IPv6
* Dynamické směrování: RIP, RIPng, OSPFv2 včetně HMAC-SHA-384, OSPFv3, BGP, MP-BGP
* Funkce BGP konfederace a route reflector pro IPv4 a IPv6
* Podpora BGP MD5 autentizace a BGP TTL security
* Podpora police based routing
* Podpora VRRPv2 a VRRPv3
* Podpora route map
* ECMP včetně možnosti konfigurace rozkládání zátěže podle L3 a L4
* Podpora minimálně 62 virtuálních směrovacích instancí (VRF)
* IGMP v2 a v3, IGMP snooping
* MLD v1 a v2, MLD snooping
* Směrování multicast: PIM-DM, PIM-SM, IPv6 PIM-SM, PIM-SSM, IPv6 PIM-SSM, MSDP
* Hardware podpora IPv4 a IPv6 ACL
* DHCP snooping pro IPv4 a IPv6
* ACL klasifikace na úrovni zdrojová/cílová MAC adresa, zdrojová/cílová IPv4/IPv6 adresa, číslo zdrojového/cílového portu, protokol, TTL hodnota , číslo VLAN,
* HW ochrana proti zahlcení portu (broadcast/multicast/unicast) nastavitelná na kbps a pps
* IEEE 802.1p – Minimálně 8 front
* 802.1X ověřování včetně více současných uživatelů na port, minimálně 64 uživatelů/port
* Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
* Dynamické zařazování do VLAN
* 802.1X s podporou odlišných Preauth VLAN, Fail VLAN, Critical VLAN a Critical voice VLAN
* 802.1X a MAC ověřování pomocí odlišných RADIUS serverů aplikované na různé skupiny portů přepínače
* Uživatelské role definované lokálně v přepínači, jejich aplikace dle výsledku autorizace
* Uživatelské role dynamicky stahovatelné z RADIUS, jejich aplikace dle výsledku autorizace
* Ochrana ARP protokolu (Dynamic ARP protection nebo funkčně ekvivalentní)
* IP source guard / dynamic IP lockdown
* Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC
* Podpora IPv6 RA Guard, DHCPv6 Guard a IPv6 Destination Guard
* BPDU guard a Root guard
* Podpora service insertion včetně technologie VXLAN
* Podpora static a dynamic VXLAN s využítím BGP-EVPN
* Podpora VXLAN PBR
* Podpora Group based policy pro VXLAN (VXLAN GBP)
* Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU
* Vynucení zadat heslo administrátora a nastavitelná politika komplexity hesla přímo na přepínači
* Možnost instalace vlastního certifikátu včetně podpory Enrollment over Secure Transport (EST)
* TACACS+ a RADIUS klient pro AAA (autentizace, autorizace, accounting)
* Aktivní monitoring dostupnosti RADIUS a TACACS+ přednastaveným jménem a heslem
* Podpora Radius over TLS (RadSec)
* Podpora RADIUS CoA (RFC3576)
* 802.1x autentizace přepínače vůči nadřazenému přepínači s podporou EAP-TLS a EAP-MD5
* QoS ochrana před zahlcením WRED
* Podpora Data Center Bridging (PFC 802.1Qbb, ETS 802.1Qaz)
* IP Explicit Congestion Notification (ECN)
* Podpora RoCEv2

**Management**

* Bezdrátová sériová konzole pomocí Bluetooth
* Konfigurace zařízení v člověku čitelné textové formě
* OoB management formou portu RJ45 s podporou ethernetu
* USB port pro přenos konfigurace a firmware
* Podpora IPv4 a IPv6 management: SSHv2 server, HTTPS server, SFTP a SCP klient
* Dvou-faktorová autentizace pro SSH a WebGUI přihlášení
* Kryptografické SSH algoritmy: AES256, HMAC-SHA2-256, DH s klíčem 3072bit a vyšší
* Podpora SNMPv2c a SNMPv3
* Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
* Lokálně vynucené RBAC na úrovni přepínače
* Duální flash image - podpora dvou nezávislých verzí operačního systému
* Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)
* TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více SYSLOG serverů
* Podpora SYSLOG over TLS
* Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby
* Podpora standardního Linux Shellu (BASH) pro debugging a skriptování
* Podpora skripování v jazyce Python – lokální interpret jazyka v přepínači
* Možnost vytváření vlastních diagnostických a korelačních skriptů a jejich grafických interpretací v jazyce Python (korelace libovolných událostí a hodnot v podobě grafů)
* Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů - možnost vynášení stavu monitorovaných metrik do grafů atp.
* Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase
* Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)
* Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události
* Interní uložistě dat pro sběr provozních dat a pokročilou dignostiku zařízení: min. 30 GB
* Analýza síťového provozu sFlow podle RFC 3176 pro oba směry ingress a egress
* Analýza síťového provozu IPFIX
* Ochrana proti nahrání modifikovaného SW prostřednictvím image signing a secure boot, ověřující autentičnost a integritu OS prostřednictvím TPM chipu
* SPAN a ERSPAN port mirroring, alespoň 4 různé obousměrné session
* IP SLA pro měření dostupnosti a zpoždění provozu VoIP - režim responder i probe
* Podpora integrace s automatizačními nástroji (Ansible, NAPALM)
* Automatizace – podpora read-only a read-write REST API včetně volání CLI příkazů
* Podpora Cloud management software výrobce zařízení
* Podpora Zero Touch Provisioning (ZTP)

**Záruka a podpora:**

* Záruka a technická podpora výrobce v délce 60 měsíců a odezvou následující pracovní den a opravou formou výměny boxu.
* Softwarové aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců.

**Implementace**

* Instalace v určeném místě zadavatele a zapojení do vyhrazené management sítě.
* Instalace posledních stabilních firmware.
* Konfigurace vysoké dostupnosti
* Rekonfigurace routování, vytvořeních nových síťových segmentů a nastavení komunikačních pravidel.

# **1.5 Přístupový LAN switch A – 10 ks**

**Základní vlastnosti**

* Třída zařízení: L3 switch
* Formát zařízení do racku
* Velikost zařízení: 1U
* Počet 10/100/1000Mbit metalických portů: 48
* Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním: 4
* Potřebný počet SFP+/SFP modulů a propojovacích patch cordů
* 10GE interface zpětně kompatibilní s 1Gbit/s transceivery
* Všechny ethernet porty jsou dostupné zepředu
* Interní napájecí zdroj
* Celková propustnost přepínače: 176 Gb/s
* Celkový paketový výkon přepínače: 98 mpps
* Minimálně 12MB paketový buffer
* Maximální přípustná hloubka přepínače z důvodu osazení do stávajících rozvaděčů: 30 cm

**Základní funkce a protokoly**

* Podpora "jumbo rámců" včetně velikosti 9220 Byte
* Podpora linkové agregace IEEE 802.3ad
* Konfigurovatelné rozkládání LACP zátěže podle L3 a L4
* Minimální počet LACP skupin/linek ve skupině: 8/8
* Protokol pro definici šířených VLAN: MVRP
* Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN
* 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)
* NTP pro IPv4 a IPv6 včetně MD5 autentizace
* Statické směrování IPv4 a IPv6
* IGMP v2 a v3
* MLD v1 a v2
* Hardware podpora IPv4 a IPv6 ACL
* ACL definice na základě skupiny fyzických portů
* ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN
* BPDU guard a Root guard
* HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu
* ICMPv4 a ICMPv6 rate-limiting per port
* Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port
* Konfiguovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
* 802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN
* Dynamické zařazování do VLAN
* 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)
* Port security - omezení počtu MAC adres na port, statické MAC
* Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení
* Ochrana control plane (CPU) před útoky typu DoS
* Podpora IPv4 a IPv6 QoS
* Minimálně 8 front pro IEEE 802.1p

**Management**

* Konfigurace zařízení v člověku čitelné textové formě
* Podpora automatických i manuálních snapshotů konfigurace systému
* USB port pro diagnostiku, přenos konfigurace a firmware
* Podpora managementu přes IPv4 i IPv6
* SSHv2 a a SFTP
* Podpora SNMPv2c a SNMPv3
* RMON
* Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
* Lokálně vynucené RBAC na úrovni přepínače
* Dualní flash image
* TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
* Podpora Syslog over TLS
* Podpora RADIUS včetně RADIUS CoA (RFC3576)
* Podpora RADIUS IPSEC
* Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem
* Podpora TACACS+
* Analýza síťového provozu sFlow podle RFC 3176
* Port mirroring (SPAN), alespoň 4 různé obousměrné session
* Podpora Zero Touch Provisioning (ZTP)
* REST API pro automatizaci nastavení
* Automatická konfigurace portu podle připojeného zařízení
* Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů

**Záruka a podpora:**

* Záruka a technická podpora výrobce v délce 60 měsíců a odezvou následující pracovní den a opravou formou výměny boxu.
* Softwarové aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců.

**Implementace**

* Instalace v určeném místě zadavatele a zapojení do vyhrazené management sítě.
* Instalace posledních stabilních firmware.
* Konfigurace vysoké dostupnosti k páteřním switchům.

# **1.6 Přístupový LAN switch B – 5 ks**

**Základní vlastnosti**

* Třída zařízení: L3 switch
* Formát zařízení do racku
* Velikost zařízení: 1U
* Počet 10/100/1000Mbit metalických portů: 24
* Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním: 4
* Potřebný počet SFP+/SFP modulů a propojovacích patch cordů
* 10GE interface zpětně kompatibilní s 1Gbit/s transceivery
* Všechny ethernet porty jsou dostupné zepředu
* Interní napájecí zdroj
* Celková propustnost přepínače: 128 Gb/s
* Celkový paketový výkon přepínače: 95 mpps
* Minimálně 12MB paketový buffer
* Maximální přípustná hloubka přepínače z důvodu osazení do stávajících rozvaděčů: 30 cm

**Základní funkce a protokoly**

* Podpora "jumbo rámců" včetně velikosti 9220 Byte
* Podpora linkové agregace IEEE 802.3ad
* Konfigurovatelné rozkládání LACP zátěže podle L3 a L4
* Minimální počet LACP skupin/linek ve skupině: 8/8
* Protokol pro definici šířených VLAN: MVRP
* Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN
* 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)
* NTP pro IPv4 a IPv6 včetně MD5 autentizace
* Statické směrování IPv4 a IPv6
* IGMP v2 a v3
* MLD v1 a v2
* Hardware podpora IPv4 a IPv6 ACL
* ACL definice na základě skupiny fyzických portů
* ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN
* BPDU guard a Root guard
* HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu
* ICMPv4 a ICMPv6 rate-limiting per port
* Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port
* Konfiguovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
* 802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN
* Dynamické zařazování do VLAN
* 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)
* Port security - omezení počtu MAC adres na port, statické MAC
* Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení
* Ochrana control plane (CPU) před útoky typu DoS
* Podpora IPv4 a IPv6 QoS
* Minimálně 8 front pro IEEE 802.1p

**Management**

* Konfigurace zařízení v člověku čitelné textové formě
* Podpora automatických i manuálních snapshotů konfigurace systému
* USB port pro diagnostiku, přenos konfigurace a firmware
* Podpora managementu přes IPv4 i IPv6
* SSHv2 a a SFTP
* Podpora SNMPv2c a SNMPv3
* RMON
* Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
* Lokálně vynucené RBAC na úrovni přepínače
* Dualní flash image
* TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
* Podpora Syslog over TLS
* Podpora RADIUS včetně RADIUS CoA (RFC3576)
* Podpora RADIUS IPSEC
* Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem
* Podpora TACACS+
* Analýza síťového provozu sFlow podle RFC 3176
* Port mirroring (SPAN), alespoň 4 různé obousměrné session
* Podpora Zero Touch Provisioning (ZTP)
* REST API pro automatizaci nastavení
* Automatická konfigurace portu podle připojeného zařízení
* Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů

**Záruka a podpora:**

* Záruka a technická podpora výrobce v délce 60 měsíců a odezvou následující pracovní den a opravou formou výměny boxu.
* Softwarové aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců.

**Implementace**

* Instalace v určeném místě zadavatele a zapojení do vyhrazené management sítě.
* Instalace posledních stabilních firmware.
* Konfigurace vysoké dostupnosti k páteřním switchům.

# **1.7 Přístupový LAN switch C – 14 ks**

**Základní vlastnosti**

* Třída zařízení: L3 switch
* Formát zařízení do racku
* Velikost zařízení: 1U
* Počet 10/100/1000Mbit metalických portů: 12
* Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním: 2
* Potřebný počet SFP+/SFP modulů a propojovacích patch cordů
* 10GE interface zpětně kompatibilní s 1Gbit/s transceivery
* Všechny ethernet porty jsou dostupné zepředu
* Interní napájecí zdroj
* Podpora PoE+ dle standardu 802.3at
* Dostupný výkon pro PoE+ napájení: 139W
* Celková propustnost přepínače: 176 Gb/s
* Celkový paketový výkon přepínače: 98 mpps
* Minimálně 12MB paketový buffer
* Maximální přípustná hloubka přepínače z důvodu osazení do stávajících rozvaděčů: 30 cm
* Tiché provedení - bez ventilátorů

**Základní funkce a protokoly**

* Podpora "jumbo rámců" včetně velikosti 9220 Byte
* Podpora linkové agregace IEEE 802.3ad
* Konfigurovatelné rozkládání LACP zátěže podle L3 a L4
* Minimální počet LACP skupin/linek ve skupině: 8/8
* Protokol pro definici šířených VLAN: MVRP
* Podpora VLAN podle IEEE 802.1Q, minimálně 512 aktivních VLAN
* 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)
* NTP pro IPv4 a IPv6 včetně MD5 autentizace
* Statické směrování IPv4 a IPv6
* IGMP v2 a v3
* MLD v1 a v2
* Hardware podpora IPv4 a IPv6 ACL
* ACL definice na základě skupiny fyzických portů
* ACL aplikovatelný na rozhraní IN včetně virtuálních VLAN
* BPDU guard a Root guard
* HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na množství paketů za vteřinu
* ICMPv4 a ICMPv6 rate-limiting per port
* Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port
* Konfiguovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
* 802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN
* Dynamické zařazování do VLAN
* 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)
* Port security - omezení počtu MAC adres na port, statické MAC
* Ochrana proti opakovaným výpadkům linek (flapování) s možností konfigurace citlivosti a akce při překročení
* Ochrana control plane (CPU) před útoky typu DoS
* Podpora IPv4 a IPv6 QoS
* Minimálně 8 front pro IEEE 802.1p

**Management**

* Konfigurace zařízení v člověku čitelné textové formě
* Podpora automatických i manuálních snapshotů konfigurace systému
* USB port pro diagnostiku, přenos konfigurace a firmware
* Podpora managementu přes IPv4 i IPv6
* SSHv2 a a SFTP
* Podpora SNMPv2c a SNMPv3
* RMON
* Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
* Lokálně vynucené RBAC na úrovni přepínače
* Dualní flash image
* TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů
* Podpora Syslog over TLS
* Podpora RADIUS včetně RADIUS CoA (RFC3576)
* Podpora RADIUS IPSEC
* Aktivní monitoring dostupnosti RADIUS přednastaveným jménem a heslem
* Podpora TACACS+
* Analýza síťového provozu sFlow podle RFC 3176
* Port mirroring (SPAN), alespoň 4 různé obousměrné session
* Podpora Zero Touch Provisioning (ZTP)
* REST API pro automatizaci nastavení
* Automatická konfigurace portu podle připojeného zařízení
* Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů

**Záruka a podpora:**

* Záruka a technická podpora výrobce v délce 60 měsíců a odezvou následující pracovní den a opravou formou výměny boxu.
* Softwarové aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců.

**Implementace**

* Instalace v určeném místě zadavatele a zapojení do vyhrazené management sítě.
* Instalace posledních stabilních firmware.
* Konfigurace vysoké dostupnosti k páteřním switchům.

# **1.8 Nástroj pro centrální správu LAN switchů – 1 ks**

**Základní vlastnosti**

* Centrální správa a monitoring všech nabízených switchů (páteřních i přístupových)
* Plně kompatibilní s nabízenými switchi
* Forma appliance pro provoz v prostředí VMWare ESX nebo cloudové řešení - licence min. na dobu 5 let
* Vysoká dostupnost management nástroje - HA režim
* Definice společných konfiguračních elementů nad skupinou zařízení
* Hierarchická konfigurace nad skupinou a individuální konfigurace platná pro jednotlivá zařízení
* Konfigurační audit - možnost porovnat rozdíly skupinová vs. individuální konfigurace zařízení
* Hromadná aktualizace firmware, možnost plánovaných upgrade pro pouze definovanou podmnožinu
* Grafický dashboard zobrazující aktuální a historické informace o připojených klientech
* Podpora hromadné změny více zařízení konfigurací pomocí šablon
* Komunikace s přepínači přes zabezpečené HTTPS rozhraní
* Minimální datová retence monitorovacích dat a statistik 90 dnů
* RESTful API pro možnost integrace s externími systémy a možnost vyčítat provozní statistiky
* Streaming API umožňující proaktivní zasílání změn stavů a statistik bez nutnosti pravidelného načítání statistik skrze pasivní REST API.
* Integrované diagnostické nástroje, které umožňují spouštět vzdáleně CLI příkazy
* Možnost rozdělení zařízení do skupin a hromadná konfigurace zařízení ve skupině
* Zobrazení stavu a konfigurace portů přepínače, zobrazení spotřeby PoE po jednotlivých portech, zobrazení stavu hardwaru (CPU, RAM, chlazení, teplota, napájecí zdroje)
* Zobrazení seznamu sousedních zařízení přepínače
* Možnost přímého přístupu do CLI daného zařízení z portálu centrální správy
* Automatické upozornění na aktualizaci firmwaru přepínače
* Real-time diagnostika událostí týkajících se konkrétního klienta – okamžité zobrazování stavů připojení, autentizace atp. bez nutnosti čekání na pravidelný update interval.
* Podpora automatizovaného strojového učení systému pro automatické odhalování konkrétních zařízení či skupin zařízení, které mají společné negativní projevy některého z monitorovaných parametrů.
* Monitorování síťových služeb jako je DNS, DHCP či RADIUS ověřování klientů, jejich chybovost a zpoždění.
* Reportovací modul pro vytváření souhrných reportů z dat za poslední období. Minimálně tyto reporty: PCI, bezpečnostní report, kapacitní plánování sítě, Klient inventory, využití sítě klienty
* Dohled přepínačů, zobrazení událostí a alertů
* Záznam příkazů zadávaných/odesílaných na přepínač včetně uživatele, který je zadával (Audit)
* Nástroje pro ověření konektivity přepínače spouštěné přímo z management nástroje (ping, traceroute)
* Možnost definování seznamu příkazů pro diagnostiku problémů a jejich hromadné spuštění
* Export výsledků diagnostických příkazů, možnost odeslání na Email

**Řízení přístupu do administrace a provisioning prvků**

* Podpora různých uživatelských rolí, možnost definice oprávnění pouze ke skupinám zařízení
* Administrace do centrální správy s podporou dvoufaktorové autentizace
* Instalační a monitorovací aplikace dostupná pro Android a IOS. Umožňuje naskenovat a přidat zařízení pod centrální správu. Dále umožňuje monitorovat stav zařízení a připojených klientů včetně objemu přeneseného provozu.
* Provisioning přepínačů do centrální správy probíhá automaticky po registraci zakoupených zařízení do nástroje centrální správy (vyplnění identifikačních údajů zařízení)
* Možnost přiřazení detailních práv pro jednotlivé administrátory řešení minimálně s rozlišením úrovní čtení, zápisu a úplného zamezení přístupu pro jednotlivé hlavní moduly řešení (správa a hierarchie zařízení, správa sítí, monitoring sítí a správa přístupu hostů do sítě)

**Záruka a podpora:**

* Záruka a technická podpora výrobce v délce 60 měsíců.
* Softwarové aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců.

**Implementace**

* Instalace a konfigurace management nástroje.
* Přidání všech dodávaných switchů
* Nastavení konfiguračních šablon, záloh a monitoringu.
* Nastavení uživatelských oprávnění.

# **1.9 Nástroj pro ověřování přístupu do sítě LAN – 1 ks**

**Základní vlastnosti:**

* Podpora 802.1x autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN připojení
* Forma dodání: virtuální appliance pro VMware
* Kapacita řešení pro autentizaci min. 300 unikátních koncových zařízení
* Řešení musí poskytovat vysokou dostupnost tak, aby v případě výpadku primárního serveru převzal jeho roli sekundární server.
* Možnost vytváření clusteru více virtuálních appliance. Minimální počet podporovaných appliance v clusteru je 2.
* Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance.
* Podpora minimálně 20ti předních světových výrobců síťových zařízení (LAN switche, WiFi řešení, obecně přístupové datové sítě)
* Požadované metody autentizace uživatelů a zařízení: PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace
* Podpora RADIUS CoA
* Podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v AD
* 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
* Další požadované autentizační a autorizační zdroje a metody: LDAP, MS AD, Token, MAC, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta)
* Podpora REST API pro většinu základních úkonů platformy
* Podpora REST volání vyvolaného autentizační či autorizační událostí (minimálně pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.)
* 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.
* Administrátor systému musí mít možnost vlastní tvorby parseru/integrace syslog hlášení pro možnost uživatelské integrace s libovolnými systémy třetích stran.
* 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 musí podporovat možnost přihlašování přes účty minimálně těchto sociálních sítí – Linkedln, Facebook, Twitter, Google+. Portál musí umožňovat bohatou grafickou úpravu včetně možnosti přidávání videí a dalšího dynamického obsahu. Možnost samoobslužné registrace hosta do sítě s SMS, email ověřením nebo na elektronickou notifikaci a schválení pověřených pracovníků.
* Možnost licenčního rozšíření o bezpečnou registraci soukromých zařízení do interní sítě na základě uživatelských údajů z AD či LDAP. Uživatel musí být schopen jednoduchým uživatelským wizardem instalovat osobní certifikát a síťový profil na své soukromé zařízení (BYOD systém).
* Možnost licenčního rozšíření o certifikační autoritu pro vydávání certifikátů na soukromá zařízení musí být součástí platformy.
* Možnost licenčního rozšíření o samoobslužný portál pro hosty či interní uživatele s možností správy svých vlastních registrací.
* Možnost licenčního rozšíření o systém pro bezpečnostní kontrolu přistupujících zařízení před jejich vpuštěním do sítě pomocí software agenta na koncová zařízení.
* Možnost licenčního rozšíření o kontroly stavu registrů, spuštěných procesů, stavu síťových zařízení, nastavení firewallu, aktualizace antivirů, instalované VM, stav enkrypce disku.
* Možnost licenčního rozšíření o podporu jednorázového i permanentního klienta pro kontroly na koncových zařízeních. Podpora klienta pro kontrolu koncových zařízení na OS Windows, MAC OS a Linux
* Možnost licenčního rozšíření o integraci tohoto koncového klienta s VPN klientem
* Jakékoliv funkční rozšíření systému musí být vždy v rámci stejné virtuální appliance jako je systém.

**Záruka a podpora:**

* Záruka a technická podpora výrobce v délce 60 měsíců.
* Softwarové aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců.

**Implementace:**

* Instalace a konfigurace dvou VM do clusteru.
* LDAP připojení do domény.
* Konfigurace certifikační autority.
* Vytvoření templates na certifikační autoritě pro klienty a nastavení automatické instalace pro zařízení v doméně.
* Vydání certifikátu pro RADIUS.
* Revize zapojených zařízení v síti LAN.
* Vytvoření ověřovací matice – definice ověřování uživatelů, zařízení, jejich kombinace, druh autentikační metody a přiřazení definovaných rolí na základě splnění autorizačního procesu.
* Konfigurace podmínek ověřovacích služeb.
* Konfigurace a ověřování přístupu hostů do izolované sítě.
* Distribuce nastavení suplikanta pro zařízení ověřovaná metodou 802.1x.
* Ruční nastavení suplikanta a nahrání certifikátu pro zařízení, u kterých nelze toto zajistit pomocí hromadné distribuce.
* Konfigurace přístupových switchů – definice ověřovacích serverů a služeb, konfigurace DHCP relay a konfigurace portů.
* Ověření funkčnosti na vybraném vzorku zařízení a uživatelů.
* Po ověření funkčnosti kompletní nasazení pro celou síť.

# **2. Dokumentace a převzetí**

Součástí předání a převzetí plnění části B bude:

* Instalační listy ke každému zařízení,
* Konfigurační protokoly vč. nastavených parametrů a přístupových údajů,
* Schéma zapojení (topologie LAN, IP plán, VLAN tagging apod.),
* Souhrnné potvrzení o provozuschopnosti systému,
* Přehled licencí, sériových čísel a podmínek podpory výrobce.
* Ověření redundantních zapojení dodávaných zařízení. Ověření, že monitoring tyto pokusy zaznamenal.
* Ověření funkčnosti ověřování přístupu do sítě na vybraných typech zařízení.
* Ukázka přidání aktivního prvku do sítě a managementu
* Ukázka automatizované kontroly obnovitelnosti ze záloh
* Ověření ochrany proti smazání záloh