Příloha č. 1 smlouvy č. j. 05/13-2025

1 Technická specifikace zadavatele (kupujícího)

Zadavatel (dále též „kupující“) požaduje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v níže uvedené minimální specifikaci.

Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice.

Součástí dodávky níže uvedených technologií budou i dále uvedené služby.

Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí kupujícího k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího. Implementační práce budou naceněny samostatně.

Nabízené zboží musí být standardní, běžně dostupné a určené k produkčnímu použití.

Není dovoleno použití beta-verzí, kódu s custom úpravami či neoficiálních verzí.

Veškeré nabízené zboží musí být pokryto oficiálním supportem, přičemž požadavek na provedení bezplatného servisního zásahu musí být možné kdykoliv vznést přímo na výrobce zařízení.

Veškeré deklarované funkce a technické parametry nabízeného zboží musí být dostupné nejpozději dnem podání nabídky.

Deklarované funkce a technické parametry nabízeného zboží musí být ověřitelné prostřednictvím oficiálních datasheetů, release notes či manuálů vydaných výrobcem.

Užité pojmy níže:

- NBD – další pracovní den, tzn. například realizace opravy zařízení nejpozději další pracovní den od nahlášení
- x BD – x pracovních dnů, tzn. například realizace opravy zařízení nejpozději poslední pracovní den dané lhůty od nahlášení
- on-site – realizace například opravy zařízení v místě dodávky

Z důvodu kompatibility se stávající infrastrukturou a proškolených správců počítačové sítě, mohou být v zadávací dokumentaci uvedeny konkrétní značky výrobků, nebo určitý výrobce. Tyto důvody jsou vždy uvedeny v konkrétní části specifikace tam, kde dochází k uvedení konkrétního produktového názvu. V souladu s § 89 odst. 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, zadavatel připouští možnost dodávky rovnocenného řešení, které však musí zajistit celý komplex služeb, který je kompatibilitou vyžadován, tedy komplexní řešení agendových informačních systémů nad touto platformou vybudovaných a provozovaných, které předmětnou infrastrukturu užívají a slouží k výkonu veřejné správy zadavatele.

Obsah

2 Požadavky na jednotlivé technologie (prvky)

2.1 Zdůvodnění požadavku na kompatibilitu pro síťové prvky

Kupující (zadavatel) provozuje centrální firewally (NGFW) značky FortiGate typu 100F, se kterými požaduje provést integraci aktivních prvků v rámci plnění této specifikace tak, aby mohlo být dosaženo centrálního řízení všech aktivních prvků z jednoho technologického prostředí, včetně vizualizace a společného nastavování pravidel těchto prvků.
Tímto způsobem kupující (zadavatel) sleduje cíl zvýšení kybernetické bezpečnosti, když politiky jednotlivých zařízení budou provázané a budou vždy odpovídat centrálnímu nastavení, na rozdíl od situace, kdy je v technologickém prostředí provozováno několik typů technologií od různých výrobců, bez kompatibilního centrálního řízení a správy a dochází tak k individuální konfiguraci každého prvku administrátory individuálně. Pak nejenže dochází ke zvýšení rizika chybné konfigurace, ale současně není možné užít synergie a technologické specifičnosti jednotlivého produktu a předmětné konfigurace musejí být nastavovány spíše šířeji tak, aby bylo zajištěno, že budou vycházet z obecných standardů po ověření jejich shodné implementaci napříč portfoliem technologií provozovaných v prostředí kupujícího (zadavatele).
V případě sjednoceného prostředí řízení a správy aktivních prvků je dále možné využívat synergického efektu i v případě útoku, nebo automatizovaných činností, které je možné v takovém případě nastavit pro zjištění nežádoucího stavu nebo automatizované bezpečnostní kroky v případě automatizované identifikace bezpečnostní incidentu v prostředí umístění technologií.
Zadavatel (kupující) na tomto místě transparentně uvádí, že za účelem realizace plnění je možné dodat jakékoliv aktivní prvky, které budou plnit specifikaci dle této technické specifikace, při dodržení možnosti jejich centrálního řízení a správy společně se stávajícími firewally (dodavatel v rámci své nabídky popíše nabízené technologické řešení) nebo v případě nemožnosti na straně dodavatele takové řešení nalézt zadavatel dále připouští nahrazení stávajících firewallů za zařízení minimálně stejné nebo vyšší kvality, funkcionality a výkonu. V případě nahrazení musí být součástí ceny plnění dle této technické specifikace zohledněna i cena za náhradu těchto zařízení, včetně jejich nasazení (migrace a konfigurace pravidel nasazených na stávajících firewallech; export pravidel pro prodávajícího provede kupující). Součástí příslušenství v případě náhrady stávajících firewallů musí být i prodloužená záruka a záruční servis na 5 let a zajištění služeb na aktualizace balíčků zabezpečení pro tyto firewally a odstranění jejich zranitelností ze strany jejich výrobce v délce 5 let. Rozhodné informace o typu firewallu a jeho příslušenství v případě nabídky dodavatele na jejich náhradu musí být uvedeno v nabídce prodávajícího za účelem posouzení splnění předmětných požadavků kupujícím (zadavatele) už ve fázi podání a kontroly nabídky.

2.2 Páteřní přepínač s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

Parametr	Popis parametru
Základní parametry	Minimálně 48x 10G/1G SFP+/SFP portů Minimálně 6x 40G QSFP+ nebo 4x 100G/40G QSFP28/QSFP+ portů Samostatný konzolový port, L3 mgmt port a USB port Velikost maximálně 1 RU Minimální přepínací kapacita 1760 Gbps Propustnost minimálně 1518 Mpps Latence menší než 800ns Velikost bufferu pro zpracování paketů je alespoň 12MB per port Minimální počet LAG skupin odpovídá celkovému počtu portů přepínače (bez konzolového, mgmt a USB portu) Minimální počet podporovaných VLAN alespoň 4000 Minimální velikost MAC tabulky alespoň 144000 záznamů

Parametr	Popis parametru
	Minimálně dva redundantní zdroje napájení s možností výměny za chodu přepínače, které jsou součásti dodávky včetně přívodních kabelů pro CZ Průtok vzduchu přes čelní porty s odvodem přes zadní část přepínače
Funkce	L2/L3 přepínač Podpora IEEE 802.3ad Podpora IEEE 802.1q Podpora IEEE 802.1ab Podpora IEEE 802.1s Podpora IEEE 802.1w Podpora IEEE 802.1p Podpora IPv4 a IPv6 Podpora ACL (IPv4 a IPv6) až 4000 záznamů Podpora L2 ACL Podpora ECMP Podpora 802.1x Podpora MAB Podpora QoS pro IPv4 a IPv6 včetně 802.1p, prioritních front, WRED, čítačů QoS statistik Alespoň 8 prioritních QoS front per port Podpora Radius CoA Podpora Radius Accounting Podpora ARP inspekce Podpora IGMP, DHCP a MLD snooping Podpora protokolů RIPv2, BGP, OSPFv2, IS-IS, VRRP ve verzích IPv4 a IPv6 Podpora BFD pro protokoly RIPv2, BGP, OSPFv2, IS-IS, VRRP ve verzích IPv4 a IPv6 Podpora BGP EVPN s využitím VxLAN Možnost definovat alespoň 64 VRF domén Podpora multicast PIM-SM protokolu Podpora Jumbo Frame o velikosti alespoň 9000B Podpora SPAN, RSPAN a ERSPAN Podpora Multi-Chassis Link Aggregation protokolu Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS Podpora REST API pro konfiguraci a monitoring prvku Podpora duálního firmwaru Podpora SNMP v1/v2c/v3, sFlow, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu Podpora centrální správy z NGFW zařízení stejného výrobce s možností vynutit L2 inspekci provozu přes NGFW per VLAN Podpora kontroly validity instalovaného firmware z pohledu shody s oficiálním vydáním dané verze firmware výrobcem Podpora uložení až dvou verzi firmware na zařízení a volby, který načíst při startu zařízení Podpora sFlow pro IPv4 Integrovaný nástroj pro packet capture
Centrální správa	Jednotná centrální správa, monitorování a aktualizace firmware z centrální webové grafické konzole obsažené ve firmware nabízených síťových prvků nebo prostřednictvím samostatné appliance kompatibilní s virtualizovaným prostředím provozovaným zadavatelem dle této specifikace (přepínače). Centrální správa musí podporovat zejména: • Podpora centrální správy z NGFW s možností vynutit L2 inspekci provozu

Parametr	Popis parametru
	přes NGFW per VLAN • Podpora úzké integrace s NGFW pro aplikaci pokročilých funkcionalit, jako interVLAN blocking, NAC, virtual patching, Visibility • Detekce a zasílání telemetrických údajů o připojených zařízení do centrální správy, nebo NGFW • Možnost karantény koncového zařízení na základě pokynu z centrální správy, nebo NGFW • Podpora automatické detekce přepínače a přidání do centrální správy, nebo NGFW • Možnost logování přepínačů do centrální správy, nebo NGFW • Podpora vzdálené zprávy pomocí SSH prostřednictvím centrální správy, nebo NGFW • Automatická konfigurace trunk rozhraní na základě detekce připojených přepínačů v topologii
Záruka a záruční servis	Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den

2.3 Přístupový přepínač typu 1 s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

Parametr	Popis parametru
Základní parametry	Minimálně 48x GE/RJ45 portů Minimálně 4x 10 GE SFP+ a 2x 40 GE QSFP+ portů PoE budget alespoň 1440W a podpora napájení dle 802.3af/at na všech 48xRJ-45 portech Samostatný konzolový port, L3 mgmt port a USB port Velikost maximálně 1RU Minimální přepínací kapacita 336 Gbps Propustnost minimálně 512 Mpps Latence menší než 2us Velikost bufferu pro zpracování paketů je alespoň 4MB per port Minimální velikost MAC tabulky alespoň 36000 záznamů Minimální počet podporovaných VLAN alespoň 4000 Dva napájecí zdroje a přívodní elektrický kabel pro CZ jsou součástí dodávky
Funkce	L2/L3 přepínač Podpora IEEE 802.3ad Podpora IEEE 802.1q Podpora IEEE 802.1ab Možnost propojení s prvkem podporující IEEE 802.1s Podpora IEEE 802.1w Podpora IPv4 a IPv6 Podpora ACL IPv4 a IPv6 Podpora 802.1x Podpora MAB Podpora Radius CoA Podpora Radius Accounting

Parametr	Popis parametru
	Podpora ARP inspekce Podpora QoS pro IPv4 a IPv6 včetně 802.1p, prioritních front, WRED, čítačů QoS statistik Alespoň osm prioritních QoS front per port Podpora IGMP a DHCP snooping Podpora SPAN a RSPAN Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS Podpora REST API pro konfiguraci a monitoring prvku Podpora SNMP v1/v2c/v3, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu pro autentizaci administrátorů Podpora protokolů RIPv2, BGP, OSPFv2, IS-IS, VRRP ve verzích IPv4 a IPv6 Možnost definovat alespoň 64 VRF domén Podpora BFD pro protokoly RIPv2, BGP, OSPFv2, IS-IS, VRRP ve verzích IPv4 a IPv6 Podpora multicast PIM-SM protokolu Podpora Jumbo Frame o velikosti alespoň 9000B Podpora SPAN, RSPAN a ERSPAN Podpora Multi-Chassis Link Aggregation protokolu Podpora centrální správy z NGFW zařízení stejného výrobce s možností vynutit L2 inspekci provozu přes NGFW per VLAN Podpora kontroly validity instalovaného firmware z pohledu shody s oficiálním vydáním dané verze firmware výrobcem Podpora uložení až dvou verzi firmware na zařízení a volby, který načíst při startu zařízení Podpora sFlow pro IPv4 Minimální počet LAG skupin odpovídá celkovému počtu portů přepínače (bez konzolového, mgmt a USB portu) Integrovaný nástroj pro packet capture
Centrální správa	Jednotná centrální správa, monitorování a aktualizace firmware z centrální webové grafické konzole obsažené ve firmware nabízených síťových prvků nebo prostřednictvím samostatné appliance kompatibilní s virtualizovaným prostředím provozovaným zadavatelem dle této specifikace (přepínače). Centrální správa musí podporovat zejména: • Podpora centrální správy z NGFW s možností vynutit L2 inspekci provozu přes NGFW per VLAN • Podpora úzké integrace s NGFW pro aplikaci pokročilých funkcionalit, jako interVLAN blocking, NAC, virtual patching, Visibility • Detekce a zasílání telemetrických údajů o připojených zařízení do centrální správy, nebo NGFW • Možnost karantény koncového zařízení na základě pokynu z centrální správy, nebo NGFW • Podpora automatické detekce přepínače a přidání do centrální správy, nebo NGFW • Možnost logování přepínačů do centrální správy, nebo NGFW • Podpora vzdálené zprávy pomocí SSH prostřednictvím centrální správy, nebo NGFW • Automatická konfigurace trunk rozhraní na základě detekce připojených přepínačů v topologii

Parametr	Popis parametru
Záruka a záruční servis	Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den

2.4 Přístupový přepínač typu 2 s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

Parametr	Popis parametru
Základní parametry	Minimálně 48x GE RJ45 portů Minimálně 4x 10GE SFP+ portů PoE budget alespoň 772W a podpora napájení dle 802.3af/at na všech 48xRJ-45 portech Samostatný konzolový port, L3 mgmt port a USB port Velikost maximálně 1RU Minimální přepínací kapacita 176 Gbps Propustnost minimálně 262 Mpps Latence menší než 1us Velikost bufferu pro zpracování paketů je alespoň 4MB per port Minimální velikost MAC tabulky alespoň 32000 záznamů Minimální počet podporovaných VLAN alespoň 4000 Dva napájecí zdroje a přívodní elektrický kabel pro CZ jsou součástí dodávky
Funkce	L2/L3 přepínač Podpora IEEE 802.3ad Podpora IEEE 802.1q Podpora IEEE 802.1ab Možnost propojení s prvkem podporující IEEE 802.1s Podpora IEEE 802.1w Podpora IPv4 a IPv6 Podpora ACL IPv4 a IPv6 Podpora 802.1x Podpora MAB Podpora Radius CoA Podpora Radius Accounting Podpora ARP inspekce Podpora QoS pro IPv4 a IPv6 včetně 802.1p, prioritních front, WRED, čítačů QoS statistik Alespoň 8 prioritních QoS front per port Podpora IGMP a DHCP snooping Podpora SPAN a RSPAN Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS Podpora REST API pro konfiguraci a monitoring prvku Podpora SNMP v1/v2c/v3, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu pro autentizaci administrátorů Podpora protokolů RIPv2, BGP, OSPFv2, IS-IS, VRRP ve verzích IPv4 a IPv6 Podpora BFD pro protokoly RIPv2, BGP, OSPFv2, IS-IS, VRRP ve verzích IPv4 a IPv6 Podpora multicast PIM-SM protokolu Podpora Jumbo Frame o velikosti alespoň 9000B Podpora SPAN, RSPAN a ERSPAN Podpora Multi-Chassis Link Aggregeation protokolu Podpora kontroly validity instalovaného firmware z pohledu shody s oficiálním vydáním dané verze firmware výrobcem Podpora uložení až dvou verzi firmware na zařízení a volby, který načíst při startu

Parametr	Popis parametru
	zařízení Podpora sFlow pro IPv4 Minimální počet LAG skupin odpovídá celkovému počtu portů přepínače (bez konzolového, mgmt a USB portu) Integrovaný nástroj pro packet capture
Centrální správa	Jednotná centrální správa, monitorování a aktualizace firmware z centrální webové grafické konzole obsažené ve firmware nabízených síťových prvků nebo prostřednictvím samostatné appliance kompatibilní s virtualizovaným prostředím provozovaným zadavatelem dle této specifikace (přepínače). Centrální správa musí podporovat zejména: • Podpora centrální správy z NGFW s možností vynutit L2 inspekci provozu přes NGFW per VLAN • Podpora úzké integrace s NGFW pro aplikaci pokročilých funkcionalit, jako interVLAN blocking, NAC, virtual patching, Visibility • Detekce a zasílání telemetrických údajů o připojených zařízení do centrální správy, nebo NGFW • Možnost karantény koncového zařízení na základě pokynu z centrální správy, nebo NGFW • Podpora automatické detekce přepínače a přidání do centrální správy, nebo NGFW • Možnost logování přepínačů do centrální správy, nebo NGFW • Podpora vzdálené zprávy pomocí SSH prostřednictvím centrální správy, nebo NGFW • Automatická konfigurace trunk rozhraní na základě detekce připojených přepínačů v topologii
Záruka a záruční servis	Záruka a servisní podpora výrobce min. 60 měsíců, výměna či odeslání náhradního zařízení následující pracovní den

2.5 Síťové příslušenství k aktivním prvkům a zařízením v této oblasti/části (cenu příslušenství dodavatel zohlední v ceně zařízení v této části/oblasti plnění)

Parametr	Popis parametru
Optické moduly	4x 100GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 Slots, včetně diagnostiky, kompatibilní s nabízenými přepínači 24x QSFP+ 40Gb, SM, LC, min. 1 km, kompatibilní s nabízenými přepínači 50x SFP+ 10Gb, SM, LC, min. 1 km, kompatibilní s nabízenými přepínači
Optické kabely	4× DAC kabely 100Gb kompatibilní s porty dodávaných páteřních přepínačů – délky min. 0,5 metru 6× DAC kabely 40Gb kompatibilní s porty dodávaných přepínačů typu 1 – délky min. 0,5 metru 78× Propojovací kabely SFP umožňující využití plných rychlostí transceiverů délky min. 2 metry
Záruka	36 měsíců

2.6 Archivační úložiště záloh

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Parametr	Popis parametru

Parametr	Popis parametru
Základní parametry	1 ks deduplikačního diskového úložiště. Diskové úložiště musí disponovat alespoň 39TB čisté využitelné kapacity (kapacita před deduplikací a kompresí dat, která je dostupná pro uložení dat a lze ji zkontrolovat prostřednictvím management nástrojů). Nabízené uložiště musí umožňovat licenční rozšíření kapacity po 4TB krocích bez nutnosti dokoupení dodatečného HW kapacity, až do velikosti min. 100TB. Dále musí obsahovat N+1 zdroje vyměnitelné za provozu, rack provedení včetně potřebného materiálu pro montáž do racku. Diskové úložiště musí umožnit rozšiřování minimálně do 170TB čisté kapacity. Minimální propustnost pro zápis 20 TB/h. Každé úložiště musí být osazeno minimálně: • 4x 10Gbps ETH Base-T • 4x 10Gbps SFP+ včetně 10G-SR modulů Podpora až 270 konkurenčních zálohovacích úloh per fyzický systém, zařízení musí při ukládání dat využívat princip in-line deduplikace na cíli na principu variabilní délky bloku, architektura diskové úložiště musí pro deduplikace využívat procesorový výkon a nesmí být závislá na počtu a typu backendových disků, zálohovací diskové úložiště musí konsolidovat a centralizovat zálohovací prostředí (lokální i vzdálené) – všechna data budou deduplikována v rámci jednoho boxu (žádné separátní množiny deduplikovaných úložišť).
Funkce integrace a interoperability	Zařízení musí podporovat minimálně následující protokoly: CIFS, NFS, VTL, FC; a musí umožnit jejich současné použití, zařízení musí být umožňovat přímou integraci s různými typy zálohovacích SW (minimálně Microfocus Data Protector, IBM TSM, Veritas NetBackup, Dell Data Protection Suite, Quest, Microsoft DPM, Oracle RMAN, MS SQL Studio), zálohovací diskové úložiště musí být univerzální z hlediska podpory datových typů zálohovaných dat, musí podporovat všechny datové typy, používané v produkčním prostředí – soubor a tisk, databáze, emaily, VMware, Oracle, MS Exchange, deduplikace musí být prováděna přes celé zálohovací prostředí – jak přes všechny aplikace, tak přes cílová úložiště, zařízení musí umožnit současnou podporu standardních aplikací, platforem a protokolů bez nutnosti změny instalované infrastruktury (zejména nutnost výměny zálohovacího SW, změny topologie sítě), diskové úložiště musí být kompatibilní se standardem OpenStorage, diskové úložiště musí umožnit ukládat data i pro archivní účely s funkcionalitou nastavení retenčních politik, diskové úložiště musí být certifikováno podle SEC 17a-4f nebo ekvivalentní evropské nebo české normy, diskové úložiště musí umožnit případnou distribuci deduplikačního algoritmu z cílového (deduplikačního úložiště) na zdrojové zařízení (backup klienta nebo backup server) z důvodu výkonu a škálovatelnosti prostředí a z důvodu úspor na slabých datových linkách, diskové úložiště musí disponovat funkcí multitenancy (umožnit logické dělení diskového prostoru pro různé skupiny uživatelů s právy pouze na tyto logické jednotky s možností definice tenant administrator).
Replikace	Diskové úložiště musí obsahovat licenci pro replikaci do záložní lokality, diskové úložiště musí posílat pouze deduplikovaná zkomprimovaná data diskové úložiště musí podporovat alespoň následující scénáře pro replikaci: 1:1,

Parametr	Popis parametru
	M:1 a kaskádovou replikaci, replikaci musí být možno spustit ve stejném čase jako zálohu bez dopadu na výkon zálohy, diskové úložiště musí umožnit řízení replikace v prostředí zálohovacího SW, diskové úložiště musí umožnit funkcionalitu šifrování replikačního toku data-in-flight, diskové úložiště musí podporovat replikaci dat do cloudu.
Spolehlivost, ochrana a obnova	Zařízení musí disponovat interním algoritmem pro neustálou kontrolu zdraví uložených dat a v případě poškození jejich automatickou obnovu tak, aby bylo možno zálohy kdykoliv obnovit k jakémukoliv okamžiku, zařízení musí obnovovat data vždy z deduplikovaného a komprimovaného stavu, není přípustný mezikrok (např. externí disková cache), zařízení musí disponovat funkcionalitou pro šifrování ukládaných data metodou data-at-rest, zařízení je možné osadit HotSpare diskem, zařízení musí obsahovat kompletní verifikace dat – okamžitá verifikace záloh a kontrola integrity právě ukládaných dat.
Pokročilá ochrana dat (ochrana před ransomware)	Nabízené zařízení musí umožňovat šifrovat data a musí disponovat i nástroji pro správu klíčů. Úložiště musí umožňovat nastavit retenční lhůty uložených data, granulárně podle definovaných politik řízených zálohovacím SW. Retenční zámek úložiště musí ochránit data před změnou, nebo smazáním před vypršením retenční lhůty. Úložiště musí disponovat mechanismem ochrany dat a samotného úložiště před napadením útočníkem z prostředí zadavatele i mimo toto prostředí (např. hackerský útok, ransomware apod.). Úložiště musí umožnit tzv. HW hardening – tedy takové nastavení, aby nebylo možno jedním uživatelem s dostatečnými právy manipulovat s uloženými daty nebo systémovým nastavením (např. princip čtyř očí). Diskové úložiště musí být možno instalovat na separátním segmentu sítě, který je určen pouze pro replikaci dat pro ochranu proti ransomware. Tento segment musí být možno automaticky zpřístupnit pouze pro potřeby replikace dat a řízení tohoto přístupu bude probíhat nezávisle na zbytku běžné infrastruktury pro zálohování a obnovu z bezpečného místa prostřednictvím speciální management konzole.
Správa (management)	Diskové úložiště musí umožnit správu prostřednictvím jednotného webového rozhraní, diskové úložiště musí poskytovat funkcionalitu automatického reportingu, automatický call-home, diskové úložiště musí umožnit správu na principu rolí s různými typy oprávnění, zařízení musí být plně kompatibilní se stávajícím zálohovacím systémem kupujícího (podpora jednotné správy se stávajícími prvky), diskové úložiště musí umožnit přímou správu z managementu aktuálně používaného SW řešení pro zálohování (řízení replikací, nastavení multitenancy, využití funkcionalit jako jsou change block tracking backup pro prostředí VMware, souborových systémů Windows a Linux, MS Exchange, Oracle VM).
Záruka a záruční servis	Záruka a servisní podpora výrobce min. 60 měsíců, podpora 24x7 s reakcí na nahlášení kritické závady (znemožňující užívání zařízení) do 4 hodin

2.7 Nástroj pro komplexní správu logů

Parametr	Popis parametru
Základní funkce	Integrovaný systém zpracování logů a událostí z definovaných zdrojů napříč výrobci aplikací, operačních systémů a síťového hardware
Ovládání	Grafická webová konzole pro administrátory i operátory, umožňuje kompletní správu systému včetně úvodního nastavení
Autentizace	Autentizace uživatelů vůči Active Directory nebo LDAP serveru. V případě výpadku AD/LDAP musí systém umožnit autentizaci z lokální databáze
Uživatelské role	Podpora uživatelských rolí obsahujících přístupová práva k uloženým událostem a jednotlivým ovládacím částem systému
Sběr dat (logů)	Bezagentový sběr logů s výjimkou systémů Windows
Windows agent	Kompletní správa a aktualizace z administrátorské konzole, sběr dat z textových i Event logů (včetně rozšířených) , šifrovaná komunikace, buffer pro případ ztráty komunikace, překlad kódů na text (např. Logon type 2 => "Interactive" apod.) a textový popis události shodný s Windows Event Viewerem
Protokoly	Příjem a zpracování logů, událostí a další strojově generovaných dat minimálně protokoly UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně)
Formáty logů	Min. RAW, Syslog, CEF, LEEF, JSON RFC7159, Windows EventLog
Třídění logů	Podpora příjmu logů na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv
Zpracování logů	Integrované parsování a normalizace přijatých událostí/logů bez nutnosti instalovat externí aplikace nebo systémy
Ochrana logů	Zamezení mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor pro jeho jednoznačnou identifikaci
Vizualizace logů	Grafická vizualizace logů, událostí a strojových dat (grafy událostí). Dynamická vizualizace - změnou volby (např. filtru) v jednom grafu se ostatní svázané grafy upraví automaticky dle požadované volby. Integrované podpora zobrazení TOP X událostí za zvolené časové období
Pracovní plochy	Předpřipravené pohledy (dashboardy) na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění, průběžná aktualizace pohledů výrobcem. Integrovaná podpora tvorby uživatelských dashboardů včetně ukládání
Zajištění logů	Ochrana proti ztrátě logů při přetížení systému. Ukládání nezpracovaných logů/událostí do vyrovnávací paměti o kapacitě min. 25 GB, notifikace správce systému při riziku zaplnění vyrovnávací paměti
Doplňování logů	Integrovaná podpora doplňování logů dalšími údaji - např. umístění zařízení, typ zařízení, kritičnost zařízení apod. - k jednotlivým zdrojům dat, aplikacím, zařízením, IP rozsahů apod.
Archivace	Integrovaná archivace logů včetně zajištění integrity archivů, obnova
Rozpoznávání IP,	Automatické doplňování reverzních DNS záznamům k IP adresám a výrobce

Parametr	Popis parametru
MAC	podle MAC adresy
Časová razítka	Podpora doplňkové značky (razítka) navíc k časovému údaji zaznamenané události/logu, slouží jako výchozí časový údaj pro systém
Vyhledávání	Snadné multikriteriální vyhledávání událostí bez nutnosti speciálních znalosti (např. SQL dotazů apod.) napříč všemi typy dat a zařízení
Rychlé vyhledávání	Rychlé vyhledávání i v aktuálně uložených položkách (průběžné indexování)
Geolokace	Automatické doplňování geolokačních informací k událostem a jejich grafické znázornění na mapě bez služeb třetích stran
Reporty	Integrovaný reportovací nástroj s přednastavenými obvyklými reporty a možností vlastních úprav a vytvoření nových pohledů bez potřeby speciálních znalostí (např. SQL dotazů apod.). Průběžná aktualizace přednastavených reportů výrobcem
Integrace	Integrované REST API rozhraní musí umožnit autorizovaný přístup ke strukturované databázi logů
Parsery	Integrovaný grafický (vizuální) nástroj pro tvorbu vlastních parserů logů včetně testování a ladění - okamžitého zobrazení rozparserovaných testovacích dat včetně případných chyb
Konektory	Konektory (specifické parsery) pro stávající technologie - min. Active Directory, Vmware, Windows (vč. DNS, DHCP), Exchange, MS SQL, Fortinet, HPE/Aruba, Dell servery, Synology, Linux, Apache, nabízený Systém pro analýzu síťového provozu
Alerty, notifikace	Předpřipravené alerty a integrovaný grafický (vizuální) nástroj pro vytváření automatických notifikací/alertů generovaných při splnění definovaných podmínek v přijatých datech. Odesílání alertů min SMTP, Syslog, TCP
Výkon	Min. 2000 EPS (events per second), krátkodobá (min. 10 min) přetížitelnost systému až 200%
Úložiště logů	Logy musí být ukládány do databáze (příslušná licence musí být součástí dodávky) s podporou komprese ukládaných dat
Aktualizace	Integrovaná aktualizace systému prostřednictvím administrátorské konzole včetně podpory downgrade
Zálohování	Integrované zálohování a obnova konfigurace
Škálovatelnost	Systém lze propojit s dalšími systémy stejného výrobce. Spojením systémů dojde ke zvýšení kapacity, výkonu (včetně vyhledávání) a dostupnosti. Navenek se propojené systémy chovají jako jeden
Dokumentace	Plnohodnotná (tj. shodná s originální) dokumentace v českém jazyce
Podpora	Min. 60 měsíců včetně nároku na nové verze firmware/software a aktualizace

2.7.1 Úložiště pro komplexní správu logů

Parametr	Popis parametru

Parametr	Popis parametru
Základní funkce	Úložiště a výpočetní zdroje pro software systému centrálního logování - software systému centrálního logování
Architektura	Integrovaná appliance (hw se specializovaným firmware/software) nebo server se specializovaným software včetně operačního a podpůrných systémů (databáze apod.), samostatně funkční nezávisle na infrastruktuře zadavatele
Provedení	Určené pro montáž do serverového datového rozvaděče 19", výška max. 2U
Kapacita	Využitelná diskové kapacita pro ukládání data min. 12 TB, disky musí být chráněny min. RAID 5
Řízení diskového systému	Hardwarový řadič RAID se zálohovanou vyrovnávací pamětí (zápis i čtení) o kapacitě min. 2 GB
Napájení	Systém musí mít redundantní napájení (min. 2 nezávislé zdroje)
LAN konektivita	Min. 2x LAN 1 Gb + 1x 1Gb nezávislý port pro správu hardware prostřednictvím KVM konzole s grafickým rozhraním, zabezpečeným přístupem a detailním přehledem o stavu hardware včetně okamžité a dlouhodobé spotřeby elektrické energie a stavu dílčích komponent
Záruka	Min. 60 měsíců s opravou hardware do druhého pracovního dne v místě instalace, včetně nároku na nové verze firmware/software a aktualizace

2.8 Monitoring infrastruktury

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Parametr	Popis parametru
Základní funkce	Požadujeme dodávku nástroje pro monitoring infrastruktury s podporou výrobce technologie. Podpora min. 300 koncových bodů – zejména serverů fyzických nebo virtuálních, přepínačů, diskových poli, firewallů. Technologie musí umožnit provoz monitoringu na stejných prostředcích, ve stejné lokalitě, jakou jsou provozovány monitorované technologie. Nástroj musí umožňovat následující funkcionality: • Požadavky na prozkoumávání infrastruktury ○ Řešení musí umět scanovat síť podle IP adresy, podsítě nebo různých rozsahů IP adres ○ Řešení musí umožňovat scanování podle hostitele serveru a zdroje SNMP ○ Řešení musí být schopné scanovat všechny virtuální stroje a hostitelské servery ○ Během skenování nebo po něm musí být možné získat detailní výkonnostní data prostřednictvím protokolů SNMP - v1, v2, v3, WMI, ADO, Telnet, SSH, VMware, JMX, SMIS, AWS nebo Meraki Cloud ○ Systém musí ve výchozím nastavení obsahovat šablony skenování a naplánované úlohy automatického skenování

Parametr	Popis parametru
	• Požadavky na monitoring o Jakékoliv zařízení v infrastruktuře musí být možné sledovat jak pomocí seznamu názvů zařízení, tak pomocí mapy zařízení o Monitoring musí umožňovat filtrování podle kritérií jako je název/IP, Mac adresa, umístění, značka, role zařízení (zejména server, směrovač, úložiště), typ pověření, operační systém, stav monitoringu (zejména spuštění/vypnutí, údržba) o Monitorované zařízení vybrané na hlavní monitorovací obrazovce se musí zobrazit se souhrnnými informacemi o zařízení, aniž by bylo nutné přejít do jeho vlastností o Na hlavní monitorovací obrazovce (a volitelně v zobrazení mapy) musí být možné monitorovat zařízení s různými ikonami a s názvy virtuálních, bezdrátových a L2 rozhraní a typů připojení a funkcí závislosti zařízení o Monitorovací nástroj musí umět zobrazit pro každé zařízení vlastní obrazovku, kde je uveden název hostitele, IP adresa, role zařízení, SNMP OID, typy dle monitoringu (aktivní, pasivní, výkonnostní), výstrahy, atributy, inventář, odkaz a aplikační úlohy o Mapu zařízení musí být možné přizpůsobit pomocí obrázků, snímků a tvarů o Výběrem role zařízení, názvu hostitele/systému/sítě/adresy IP/podsítě musí být možné zařízení monitorovat pomocí automaticky vytvořených skupin prostřednictvím funkce dynamické skupiny L2 o Nástroj musí být schopen monitorovat zařízení s automaticky vytvořenými skupinami výběrem aktivního sledování (minimálně DNS, FAN, IIS, monitor napájení), atributů zařízení, názvu, WMI/SNMP nebo SNMP OID, IP adres • Požadavky na analýzu o Nástroj musí umět zobrazit, zda zařízení žije (zejména zapnuto/vypnuto/údržba), dále rozložení zařízení v síti podle jejich rolí, podle stavu aktivních monitorů a zobrazení souhrnu o Seznam 10 top zařízení v síti se musí zobrazovat podle důležitosti výkonnostních kritérií, jako je využití procesoru/paměti/disku/provozu na rozhraní/dostupnosti odpovídání na ping o Musí být možné sledovat zpětně i okamžitě informace o systému, zařízení, síti a lozích (logy). Dále tyto informace musí být možné sledovat podle různých úrovní důležitosti (minimálně kritická, vysoká, informační) o Monitorování a reportování zařízení v síti musí být možné klasifikovat podle následujících kategorií: ▪ Výkonnostní charakteristiky

Parametr	Popis parametru
	• Top 10 • Využití procesoru • Využití disku • Využití paměti • Vlastní monitor (vlastní monitory výkonu, které lze přidat ke standardním výchozím monitorům) • Prediktivní trendy (poskytuje předběžné informace o potřebách hardwaru s analýzou založenou na hlavních statistikách využití) ▪ Podle síťových parametrů • Dostupnost služby Ping • Doba odezvy pingu • Chyby síťového rozhraní • Ztráty na síťovém rozhraní • Provoz na rozhraní ▪ Na bázi stavu zařízení • Dostupnost aktivního monitoru • Výpadky aktivního monitoru • Položky z alertovacího centra • Zařízení v údržbě • Stav zařízení • Doba provozu zařízení • Přehled využití zařízení • Vypnuté aktivní monitory • Vypnutá rozhraní • Použité monitory • Čtvrtletní přehled dostupnosti zařízení • Potvrzení o změně stavu • Časová osa změn stavu • Souhrn stavu • Webové alarmy ▪ Upozornění a akce • Použité akce • Alertovací centrum • Položky z alertovacího centra • Logy z alertovacího centra ▪ Inventář • Soupis aktiv • Instalovaný software • Konektivita zařízení • Využití portu přepínače • Zobrazení VLAN

Parametr	Popis parametru
	• Zobrazení podsítě • Operační systém počítače • BIOS • Aktualizace softwaru • Windows Services ▪ Logování • Konsolidované logy • Akce • Aktivity • Alertovací centrum • Souhrn výpadku • Historie skenování • Obecná chyba • Zprávy o stavu logování • Chyba pasivního monitoru • Chyba monitoru výkonnosti • Opakující se akce • Plánované hlášení • Provoz SNMP • Syslog • Aktivita uživatele na webu • Windows Event o Pro výše uvedené reporty musí řešení umožnit výstup/export v pdf, csv či txt souboru. Reporty musí obsahovat také funkcionalitu automatického plánování za vybrané časové období.
Požadavky na konfiguraci a nastavení	Minimální možnosti nastavení monitorovacího nástroje • Systémové služby v navrženém řešení musí být možné zobrazit a spravovat (zastavit/spustit/restartovat). • Obecné nastavení monitorovacího nástroje musí být možné konfigurovat centrálně a musí umožnovat následující nastavení: o Doba uchovávání dat v alert centru o Nastavení e-mailových oznámení z alert centra o Obecné nastavení pro e-maily z monitorovacího nástroje o Nastavení externího ověřování (doména, LDAP, Cisco ACS) o Nastavení doby uchovávání záznamů dat a údajů o změnách stavu souvisejících s výkonem, aktivním a pasivním monitorováním o Nastavení Syslog, SNMP trap a Windows Event Log / protokolu událostí systému Windows požadovaná pro pasivní monitorování musí být dostupná centrálně o Soubory SNMP MIB od různých dodavatelů (zejména Cisco, HP, Aruba, Juniper, EMC) musí být snadno spravovatelné (min.

Parametr	Popis parametru
	import, export) • Nastavení Discovery tak, aby se zabránilo skenování stejných zařízení, musí být možné nastavit vyloučení IP adresy nebo MAC adresy. • Musí být k dispozici uživatelé a skupiny a zásady omezení musí být možné vytvořit podle různých kritérií (oddělení, správce, oprávnění uživatelů). • Nastavení akcí o Pro aktivní monitoring ▪ a) aktivní skript ▪ b) Beeper ▪ c) Správa konfigurace ▪ d) incident ServiceNow ▪ e) Email ▪ f) Logování do textového souboru ▪ g) správa alertů OpsGenie ▪ h) Pager ▪ i) Post to IFTT ▪ j) Post to Slack ▪ k) PowerShell ▪ l) Program ▪ m) restart služby ▪ n) SMS ▪ o) Zvuk ▪ p) Syslog ▪ q) Text to Speech ▪ r) Vmware ▪ s) Webový Alarm, ▪ t) Windows Event Log ▪ u) For performance monitoring ▪ v) Email, ▪ w) generování SMS o Pro alerty ▪ Možnost definovat e-mail a SMS ▪ Musí být možné definovat různé intervaly podle různých kritérií pro analýzu síťového provozu, pasivní monitory, monitory výkonu a bezdrátové monitory ▪ Alarmy vytvořené pro různé pracovní intervaly musí být dostupné na centrální monitorovací obrazovce výstrah (dashboard) ▪ Alarmy (e-mail a sms) a zásady alarmů musí být dostupné po stanovené intervaly ▪ V zásadách alarmů musí být možné provádět postupné definice varování (eskalace) • Knihovna

Parametr	Popis parametru
	○ Musí zahrnovat úlohy týkající se pověření, monitoru (aktivního, pasivního, výkonnostního), role a podrole zařízení a systémové úlohy • Požadavky na monitoring provozu v síti ○ Nástroj musí podporovat podrobné monitorování a analýzu stávající sítě a síťového provozu ○ Nástroj musí umět klasifikovat síťový provoz procházející v určitém časovém období podle parametrů, jako je odesílatel, příjemce, aplikace, protokol, port, rychlost provozu, využití provozu ○ Aby byla analyzovaná data srozumitelná, musí podporovat shromáždění informací o výkonnostních kritériích ze zařízení sledovaných na síti pomocí protokolů jako je SNMP/WMI a klasifikovat informace o používaných aplikacích dle IEEE či aplikačních detailů ○ Nástroj musí podporovat zobrazení provozu load balanceru, aplikačního serveru nebo webového serveru nebo peer-to-peer aplikací s možností reportování (i podle počtu přijatých dat na hosta) ○ Monitorovací nástroj musí podporovat vytvoření reportů – top příjemci s nejvíce neúspěšnými připojeními, dále skenování portů, penetrační testování, bezpečnostní testy a informace o zranitelnostech, které využívají hackeři, nebo o pokusech o útoky DoS ○ Nástroj musí podporovat zobrazení reportů uživatelů, kteří generují největší síťový provoz. ○ Nástroj musí podporovat vytváření sestav dle parametrů standardu NBAR (Network Based Application Recognition) nebo QoS ○ Nástroj musí podporovat klasifikaci odeslaného a přijatého provozu podle zeměpisné polohy její analýzou podle domén, měst a zemí ○ Nástroj musí umět podporovat nahlášení podezřelých připojení pomocí knihovny reputace IP vytvořené pomocí databází Tor • Požadavky monitorování bezdrátových sítí ○ V rámci řízení sítě bezdrátovým kontrolérem musí monitorovací nástroj všechny prvky na bezdrátové síti infrastruktury zobrazit a zmapovat
Požadavky na provoz	Monitoring bude provozovaný prostřednictvím virtuální appliance ve virtualizačním prostředí (VMware vSphere) kupujícího. Pokud monitoring SW vyžaduje další licence (např. OS apod.), je dodavatel povinen takové další licence zohlednit do své nabídky a učinit je tak její součástí
Technická podpora	Nárok na maintenance a opravné balíčky software od výrobce software po dobu 60 měsíců

2.9 Ochrana před škodlivým kódem

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Parametr	Popis parametru
Platforma	Možnost plně on-prem nasazení Možnost plně cloudového nasazení Hybridní možnost nasazení (kombinace on-prem a cloud) Podpora multitenancy pro minimálně 3 tenanty (včetně licence, pokud je třeba)
Systémové vlastnosti a správa řešení	Podpora OS Windows 10/11 Podpora starších Windows OS (Windows XP SP2, Windows 7) Podpora Windows Server 2003 SP2-2022 Podpora Mac OS Podpora Linux OS (Ubuntu LTS 16.04 a vyšší, RHEL) Podpora VDI prostředí (VMware Horizons 6-7, Citrix Xendesktop 7) Lightweight agent pro koncové stanice (do 3% CPU a 400MB RAM) Lokální administrátorské účty centrální administrace Administrátorské účty navázané na LDAP centrální administrace Administrátorské účty navázané na SAML (Entra ID) centrální administrace Napojení na SIEM/Syslog Plnění standardu GDPR (odstranění citlivých uživatelských údajů) Správa koncových stanic dle skupin Oddělené politiky pro skupiny koncových stanic Možnost vytvoření předkonfigurovaného instalačního balíčku Instalace agenta koncové stanice bez uživatelské interakce Možnost globálního preventivního nebo simulačního módu vynucování politik Nemožnost ukončení procesu agenta koncové stanice ani s právy administrátora
Antivirus	Moderní antivirový engine s využitím strojového učení Real-time antivirové ochrana koncové stanice Možnost připojení na sandboxu výrobce nebo přes ICAP protokol na sandbox třetí strany Periodický a ad-hoc sken stanic
Ochrana aplikací	Přehled instalovaných aplikací na koncových stanicích Klasifikace a reputační ohodnocení aplikací Vyhodnocení zranitelností aplikací a odkaz na CVE Zákaz síťové komunikace zranitelných aplikací (virtual patching) Definice politik pro zákaz síťové komunikace na základě reputace Definice politik pro zákaz síťové komunikace na základě výrobce Definice politik pro zákaz síťové komunikace na základě zranitelnosti Zákaz spouštění konkrétních aplikací
Detekce útoků a malware	Behaviorální analýza bez použití signatur Grafický agregovaný přehled detekovaných událostí s možností forenzní analýzy Detekce a mapování útoků dle MITRE ATT&CK framework Možnost kontroly podezřelých souborů přes VirusTotal Ochrana před exfiltrací dat Ochrana před ransomware Možnost prevenčního nebo simulačního módu per politika Podpora definice výjimek pro konkrétní procesy Podpora definice výjimek na základě chování aplikace (application flow)
Odpověď na detekované útoky	Definice automatických reakcí na útoky (playbook) Možnost izolace koncové stanice pomocí agenta Terminace detekovaného procesu Odstranění persistentních dat vytvořených detekovaným procesem

Parametr	Popis parametru
	Odstranění podezřelého nebo škodlivého souboru Notifikace emailem, SIEM/syslog Možnost napojení na tiketovací systém pomocí API nebo emailu (ServiceNow a podobně) Možnost zablokování uživatelského účtu kompromitovaného uživatele Možnost resetu hesla kompromitovaného uživatele Možnost připojení na kompromitovanou stanici pomocí remote shell, možnost zadávat systémové příkazy
Kontrola zařízení	Kontrola USB zařízení dle jejich typu Detekce IoT zařízení v lokální síti pomocí agenta koncové stanice (pasivní sken)
Proaktivní vyhledávání hrozeb – Threat hunting	Proaktivní vyhledávání hrozeb (Threat Hunting) Uchovávání threat hunting dat minimálně 30 dní Možnost rozšíření kapacity threat hunting databáze Zaznamenávání a ukládání informací o procesech: - vytvoření, spuštění a terminace procesu - načtení ovladače a knihovny Zaznamenávání a ukládání informací o souborech: - vytvoření, smazání, změna, přejmenování - změna oprávnění, vlastníka a atributů Zaznamenávání a ukládání informací o síťových spojeních: - HTTP request - DNS dotaz - otevření, zavření a spojení v rámci síťového socketu (spojení) - detekce a reputace cílových IP adres komunikace Zaznamenávání a ukládání informací o registrech (Windows): - Vytvoření, změna, načtení, smazání klíče - Vytvoření, změna, načtení, smazání hodnoty klíče Možnost konfigurace zaznamenávaných informací pomocí profilů Možnost tvorby výjimek ze zaznamenávaných událostí Tvorba a ukládání vlastních dotazů do threat hunting databáze (IOC) IOC poskytované výrobcem Periodické spouštění IOC Definice akcí v případě pozitivního nálezu Identifikace MITRE ATT&CK taktik a technik Agregovaná data pro rychlou orientaci Možnost vyhledávat a filtrovat data na základě: - Koncové stanice - Procesu (jméno, ID) - Verze operačního systému - Verze jádra operačního systému - Data a Času - Časové zóny - MITRE taktiky, techniky - Zdrojové a cílové IP Podpora automatického doplňování nebo dynamické nápovědy v rámci vyhledávání
Podpora	Nárok na podporu v podobě nových balíčků zranitelností a aktualizace software po dobu 60 měsíců

2.10 Nástroj pro ověřování identity uživatelů a správců

Řešení musí splňovat následující minimální požadavky na parametry a funkcionalitu:

Parametr	Popis parametru
Platforma	Centrální autentizační server s podporou 2 faktorové autentizace
Obecné požadavky	VM appliance pro virtualizační platformu zadavatele management identit, plnohodnotná AAA funkcionalita, integrované funkce AAA pro připojení z VPN Podpora nabízených funkcí pro minimálně 100 uživatelů Licenčně rozšiřitelné Možnost automaticky synchronizovat uživatele z Active Directory Možnost vytvářet lokální uživatele a skupiny Podpora 2FA pomocí tokenů (aplikace pro iOS a Android, HW token) Možnost přidání min. 100 tokenů s možností rozšíření Podpora 2FA pomocí SMS a emailu Podpora ověřováni ze sociálních sítí (facebook, linkedin) Možnost definovat zařízení na základě MAC adresy Funkce LDAP/LDAPS serveru Možnost automatického importu identit ze vzdálených LDAP serverů Funkce TACACS+ serveru Funkce Radius serveru Podpora radius accountning v proxy režimu Funkce SAML 2.0 IdP, IdP proxy Možnost napojení a ověřování z externího Radius, LDAP SAML a OAuth server Podpora SSO autentizace uživatelů v prostředí domény MS Windows Podpora Kerberos podpora EAP metod EAP-MSCHAPv2, EAP-TLS, PEAP, EAP-GTC Funkce certifikační autority Možnost přidání min. 500 uživatelských certifikátů Podpora SCEP a CRL Podpora captive portálu Podpora samoobslužných portálů (reset hesla, editace uživatelských údajů, přidělení tokenů) Podpora 2FA pro Outlook Web Access pomocí nativního klienta Podpora mechanismu 2FA pro koncové stanice a přihlášení do systému Windows Podpora FIDO2 ověření Podpora push notifikací pro 2FA a mobilní aplikaci Podpora REST API (pokud tato funkce vyžaduje licenci, tak musí být součástí dodávky) Podpora active-pasive HA Podpora Config sync HA
Varianty provedení	HW i SW token

3 Požadavky na instalační a implementační práce

Dodané řešení bude sloužit jako rozšíření vysoce dostupné hyperkonvergované infrastruktury pro chod agendových IS úřadu a jeho zálohování.

Implementace dodávaného řešení bude provedena po odsouhlasení zadavatelem a v souladu s „best practice“ a dle doporučení výrobců jednotlivých komponent dodávaného řešení k datu realizace plnění.

Náklady na provedení implementačních služeb musí být uvedeny v nabídkové ceně a musí být je vyčísleny zvlášť.

Dodavatel je povinen zahrnout do nabídky i veškeré další činnosti a prostředky, které jsou nezbytné pro řádné provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

3.1 Specifikace konkrétních instalačních a implementačních požadavků

V rámci předmětu plnění kupující požaduje provedení minimálně následujících služeb pro následující oblasti plnění:

- zpracování předimplementační analýzy
- zpracování prováděcí dokumentace
- zajištění projektového vedení realizace předmětu plnění
- dodávku hardware a software
- likvidace obalů
- kompletní implementaci řešení splňující povinné a nabízené parametry technického řešení
- zpracování dokumentace skutečného provedení
- zaškolení administrátorů
- zajištění zkušebního provozu
- provedení akceptačních testů
- předání do ostrého provozu
- zajištění ostatních služeb potřebných pro realizaci projektu

Zadavatel požaduje, aby práce mající dopad do fungování IT prostředí kupujícího, byly prováděny výhradně mimo pracovní dobu (tedy byly prováděny v časech 17:00 – 6:00, případně mimo pracovní dny kdykoliv).

Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (např. MS Office) používaných kupujícím na datovém nosiči a 1× kopii v papírové formě.

<u>Implementační služby pro jednotlivé oblasti plnění:</u>

- Implementační služby pro přepínače
    - analýza současného stavu
    - instalace a konfigurace dodaných zařízení (instalace mimo běžnou pracovní dobu úřadu)
    - přenesení konfigurace na nové zařízení
    - otestování nakonfigurovaných vlastností (802.1x, vysoká dostupnost, logování)

- zabezpečení přístupu ke správě jednotlivých zařízení, konfigurace synchronizace jejich času, konfigurace SNMP parametrů pro možnost vzdáleného dohledu, konfigurace SMTP pro zasílání e-mailové notifikace o stavu zařízení
- sestohování páteřních přepínačů a přístupových přepínačů a jejich propojení
- zprovoznění managementu síťového prostředí, včetně zavedení 802.1x
- konfigurace agregačních skupin (LACP) na přepínačích pro propojení přepínačů, připojení serverů
- konfigurace VLAN, analýza a prohloubení segmentace dle doporučení a metodik výrobce zařízení, trunk portů a přístupových portů na jednotlivých přepínačích
- nasazení Spanning-Tree protokolu (MSTP) na síťových prvcích
- konfigurace VPN agregátoru v rámci páteřních přepínačů
- Integrace se systémem centrální správy sítě a provozního monitoringu
- konfigurace centrální správy sítě dodaných přepínačů a NGFW
  - Analýza současného stavu
  - Import politik v integrovaných zařízení
  - Provedení kompletního nasazení
  - Vytvoření přístupových pravidel a integrace ověřování uživatelů s MS AD
  - Integrace se systémem provozního monitoringu, který je součástí plnění dle této specifikace

- Implementační práce pro archivační úložiště
  - Instalace a konfigurace HW a SW vybavení do serverovny zadavatele na adrese Žižkovo Náměstí 2, 390 01 Tábor, přesné umístění jednotlivých komponent bude upřesněno kupujícím do 5 dnů od uzavření smlouvy na dodávku plnění dle této specifikace.
  - Implementace a integrace HW a SW vybavení do stávajícího zálohovacího prostředí (konfigurace v softwarové části DELL EMC AVAMAR) a předání do rutinního provozu.
  - Implementace musí být prováděna osobou s certifikací výrobce technologie prokazující její kvalifikaci v části instalace a implementace. Kupující si vyhrazuje právo vyžádat potvrzení o certifikaci osob provádějících implementaci před jejím zahájením.
  - Dodání dokumentace pro obsluhu.
- Implementační služby pro nástroj pro komplexní správu logů
  - analýza a detailní identifikace zdrojů dat, jejichž provozně bezpečnostní informace bude nutné, popř. vhodné sbírat. Bude obsahovat i návrh způsobu zpracování získaných informací a vhodných proaktivních i reaktivních akcí
  - návrh a vybudování systému centrálního logování pro zaznamenávání činnosti informačního a komunikačního systému, jeho uživatelů a administrátorů
  - monitoring a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení (ve spolupráci s firewallem)

  - logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených pracovních stanic (aplikační virtualizace) apod.
  - monitorování IP datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) dle RFC3954 nebo ekvivalentu (např. netflow) – minimálně na úrovni rozhraní WAN
  - provedení souvisejících konfigurací monitorovaných systémů
  - návrh a provedení akceptačních testů, musí zahrnovat i testy archivace a obnovy logů
- Implementační práce pro monitoring infrastruktury
  - Analýza současného stavu
  - Začlenění všech relevantních zařízení v rámci této dodávky
  - Vytvoření politik prahových hodnot provozních stavů jednotlivých zařízení
  - Vytvoření politik závislostí jednotlivých zařízení
  - Vytvoření notifikačních politik
    - online sledování – filtrování pohledů na události podle zařízení, uživatele nebo dalších atributů, vyhledávání
    - upozornění (alerty) – na základě definovaných pravidel budou generována upozornění, která mohou být odeslána emailem nebo zobrazena interaktivně v grafickém rozhraní systému
- Implementační práce pro ochranu před škodlivým kódem
  - Analýza současného stavu
  - Vytvoření politik pro dílčí typy koncových zařízení
  - Otestování politik
  - Vytvoření plánu nasazení na všech zařízeních úřadu
  - Provedení kompletního nasazení
- Implementační služby pro nástroj pro ověřování identity uživatelů a správců
  - analýza prostředí se zaměřením na zavedení vícefaktorové autentizace
  - vybudování interní PKI (Public Key Infrastructure) včetně certifikační autority, návrh a implementace šablon certifikátů
  - vybudování systému vícefaktorové autentizace s využitím dodávaných identifikačních prostředků (SW a HW tokenů). Instalace podpůrného software na koncová zařízení, pokud je pro dané řešení potřeba
  - návrh a vybudování systému pro správu kompletního životního cyklu identifikačních prostředků (doménových i veřejných certifikátů) včetně uživatelské běžné správy a obnovy platnosti
  - návrh procesů souvisejících se řízením životního cyklu tokenů a certifikátů včetně jejich vystavování a přidělování zaměstnancům
  - návrh a realizace zálohování
  - provedení potřebných konfigurací souvisejících systémů

- návrh a provedení akceptačních testů včetně výkonových testů

3.2 Požadavky na předimplementační analýzu

Dodavatel před implementací řešení zpracuje předimplementační analýzu, minimálně pro následující oblasti:

- způsob začlenění nabízeného řešení do stávajícího ICT prostředí
- analýza požadavků na síťovou infrastrukturu
- analýza požadavků na ukládání a zálohování dat, obnovu dat, toky a objemy dat
- požadavky na rekonfigurace stávajících systémů ve vztahu k plánovanému využití
- dopady implementace na dostupnost a funkčnost stávajících služeb
- další podklady relevantní pro návrh řešení
- požadovaná součinnost Zadavatele
- návrh opatření k odstranění neshod zjištěných v průběhu analýzy

Výstupem předimplementační analýzy bude písemná zpráva podléhající schválení kupujícím.

3.3 Požadavky na zpracování prováděcí dokumentace

Dodavatel před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.

Prováděcí dokumentace musí být před zahájením prací písemně schválena kupujícím.

Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:

- detailní popis cílového stavu včetně popisu funkcionalit jednotlivých HW a SW částí systému
- způsob zajištění koordinace realizace předmětu plnění s běžným provozem
- detailní návrh a popis postupu implementace předmětu plnění
- detailní popis zajištění bezpečnosti informací
- detailní harmonogram projektu včetně uvedení kritických milníků
- návrh designu úložiště a jeho konfigurace
- návrh designu síťového řešení a jeho konfigurace
- návrh monitorování řešení monitorovacími nástroji
- vazby na stávající systémy a jejich konfigurace
- návrh akceptačních kritérií a akceptačních testů
- detailní popis navrhovaných školení

Dokumentace skutečného provedení bude před akceptací plnění aktualizována na skutečně provedenou podobu, včetně konečné podoby provedených konfigurací.

3.4 Požadavky na provozní dokumentaci

Provozní dokumentace bude zpracována a předána v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat všechny dodané systémy.

3.5 Požadavky na zaškolení

Dodavatel zajistí zaškolení zaměstnanců zadavatele – administrátorů – na zařízení a systémy, v rámci tohoto plnění, a to minimálně v rozsahu předávané provozní dokumentace.

- Zaškolení zajistí seznámení specialistů IT kupujícího se všemi podstatnými částmi plnění v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
- Minimální rozsah zaškolení je 8 hodin.
- Zaškolení bude probíhat v sídle kupujícího.
- Předpokládá se účast 3 administrátorů.
- Náklady na zaškolení musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují.

3.6 Požadavky na provedení zkušebního provozu a akceptačních testů

- Dodavatel zajistí pro realizovanou část zkušební provoz v délce minimálně 10 dnů se zajištěním technické podpory specialistů na dodané řešení s možností nahlášení požadavku v pracovní den v době od 8 hod. do 16 hod. a dobou reakce od nahlášení požadavku do 4 hod.
- Dodavatel navrhne způsob a provedení akceptačních testů, který bude podléhat schválení ze strany kupujícího.
- Součástí akceptačních testů musí být minimálně kompletní ověření funkčnosti celého řešení dle této specifikace, a to minimálně v následujícím rozsahu
    - Ověření (otestování) požadovaných funkcí a parametrů.
    - Provedení zátěžových testů a změření výkonových parametrů (rychlost, odezvy aplikací) na testovacím prostředí.
    - Otestování vysoké dostupnost řešení na testovacím prostředí.
    - Provedení zálohy a ukázkové obnovy dat na testovacím prostření.
    - Testovací prostředí pro ověření funkčnosti a schopností nově implementovaných technologií bude navrženo prodávajícím v rámci prováděcí dokumentace a musí respektovat omezení plynoucí z nutnosti zachovat plný provoz stávajících technologií do okamžiku převzetí činností nově nasazenou technologií. Jeho rozsah a forma provedené bude podléhat schválení kupujícím jako součást odsouhlasení prováděcí dokumentace.
- O provedení akceptace a jejím výsledku musí být vyhotoven písemný protokol.
- Přechodem do ostrého provozu se rozumí okamžik úspěšné akceptace plnění včetně vypořádání všech vad a nedodělků.

3.7 Další požadavky na záruky, záruční servis a další podmínky v rámci záruky

- Nabídne-li dodavatel v rámci svého řešení HW, na něž výrobce standardně (tj. v rámci standardní dodávky a ceny) poskytuje horší záruku, popř. podporu, požaduje kupující zahrnout do nabídky cenu povýšení záruky, popř. podpory na jím požadovanou úroveň.
- Kupující požaduje přístup k aktualizacím software a firmware dodaného HW v kupní ceně minimálně po dobu záruky.
- Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro kupujícího.
- Není-li uvedeno u dané položky požadovaného HW jinak, požaduje zadavatel provedení záruční opravy do deseti pracovních dnů.

4 Harmonogram plnění

Kupující požaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro realizaci dodávky. Údaj D značí datum nabytí účinnosti kupní smlouvy. Čísla značí počet kalendářních dnů.

Aktivita	Začátek	Termín splnění
Nabytí účinnosti smlouvy (uveřejnění v registru smluv)	D	D
Zahájení projektu – úvodní projektová schůzka	D	D+7
Předimplementační analýza – zpracování	D+7	D+17
Předimplementační analýza – připomínkové řízení, schválení	D+17	D+24
Prováděcí dokumentace – zpracování	D+24	D+34
Prováděcí dokumentace – připomínkové řízení, schválení	D+34	D+40
Realizace předmětu plnění	D+40	D+60
Školení administrátorů	D+60	D+65
Zkušební provoz	D+65	D+75
Akceptační testy	D+75	D+80
Zahájení ostrého provozu	D+80	-

Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb. V takovém případě detailní harmonogram plnění uvede ve své nabídce.

Maximální lhůty trvání nesmí dodavatel při tvorbě detailního harmonogramu prodloužit.

Dodavatel uvede potřebnou součinnost kupujícího pro splnění harmonogramu plnění ve své nabídce.