Spisová značka: SMBO 30313/2025 OKT

Registrační číslo projektu: **CZ.31.2.0/0.0/0.0/23\_093/0008389**

**Příloha č. 2 Zadávací dokumentace**

**Specifikace předmětu plnění**

**„MěÚ Boskovice – Posílení kybernetické bezpečnosti Městského úřadu Boskovice“**

Obsah:

[1. Předmět veřejné zakázky 2](#_Toc200626232)

[2. Obecné požadavky 2](#_Toc200626233)

[3. Část 1. – Specifikace požadavků řešení 2](#_Toc200626234)

[3.1. Opatření ID 1 (§ 18 VyKB) – Bezpečnost komunikačních sítí 3](#_Toc200626235)

[3.1.1. Firewall NG – 1ks 3](#_Toc200626236)

[3.1.2. AKTIVNÍ PRVKY 7](#_Toc200626237)

[3.1.3. WiFi AP – 20 ks 17](#_Toc200626238)

[3.2. Opatření ID 2 (§ 19 VyKB) – Správa a ověřování identit 19](#_Toc200626239)

[3.2.1. 802.1X RADIUS – přístup do sítě – Server NAC (Network access) 19](#_Toc200626240)

[3.2.2. Více-faktorová autentizace a Single Sign-On (SSO) – pro 160 uživatelů 21](#_Toc200626241)

[3.3. Opatření ID 4 (§ 23 VyKB) – Detekce kybernetických bezpečnostních událostí 25](#_Toc200626242)

[3.4. Opatření ID 5 (§ 25 VyKB) – Aplikační bezpečnost 26](#_Toc200626243)

[3.5. Implementace 28](#_Toc200626244)

[4. Část 2. – Specifikace požadavků řešení 29](#_Toc200626245)

[4.1. Opatření ID 3 (§ 21 VyKB) – Ochrana před škodlivým kódem 29](#_Toc200626246)

[4.1.1. Centrální správa ochrany před škodlivým kódem 29](#_Toc200626247)

[4.1.2. Antivirus nové generace EDR pro klienty – 160 ks a pro servery – 20 ks 31](#_Toc200626248)

[4.2. Opatření ID 6 (§ 27 VyKB) – Zajišťování úrovně dostupnosti informací 40](#_Toc200626249)

[4.2.1. SERVER + OS – 1 ks 40](#_Toc200626250)

[4.2.2. Záložní zdroje – 4 ks 42](#_Toc200626251)

[4.2.3. Zálohovací SW pro 30 stávajících virtuálních serverů 43](#_Toc200626252)

[4.3. Implementace 45](#_Toc200626253)

[5. Požadavky na servisní podporu provozu a SLA 46](#_Toc200626254)

[6. Podmínky předání a převzetí – akceptace 46](#_Toc200626255)

[7. Harmonogram plnění 46](#_Toc200626256)

[8. Seznam zkratek 46](#_Toc200626257)

Seznam tabulek:

[Tabulka 1: Firewall NG – 1ks 3](#_Toc200626258)

[Tabulka 2: Aktivní prvky – L3 CORE – 2 ks 7](#_Toc200626259)

[Tabulka 3: Aktivní prvky – ACCESS – PoE – 10 ks 11](#_Toc200626260)

[Tabulka 4: Centrální management 14](#_Toc200626261)

[Tabulka 5: WiFi AP – 20 ks 17](#_Toc200626262)

[Tabulka 6: 802.1X RADIUS – přístup do sítě – Server NAC (Network access) 19](#_Toc200626263)

[Tabulka 7: Více-faktorová autentizace a Single Sign-On (SSO) – pro 160 uživatelů 21](#_Toc200626264)

[Tabulka 8: Detekce kybernetických bezpečnostních událostí 25](#_Toc200626265)

[Tabulka 9: Webový aplikační firewall 26](#_Toc200626266)

[Tabulka 10: Požadavky – Implementace nabízeného řešení 28](#_Toc200626267)

[Tabulka 12: Centrální správa ochrany před škodlivým kódem 29](#_Toc200626268)

[Tabulka 13: Antivirus nové generace EDR pro klienty – 160 ks a pro servery – 20 ks 31](#_Toc200626269)

[Tabulka 14: SERVER + OS – 1 ks 40](#_Toc200626270)

[Tabulka 15: Záložní zdroje – 4 ks 42](#_Toc200626271)

[Tabulka 16: Zálohovací SW pro 30 stávajících virtuálních serverů 43](#_Toc200626272)

[Tabulka 17: Požadavky – Implementace nabízeného řešení 45](#_Toc200626273)

# Předmět veřejné zakázky

Předmětem této veřejné zakázky je dodávka a implementace:

1. **Část: Posílení KB**
* Opatření ID 1 (§ 18 VyKB) – Bezpečnost komunikačních sítí
* Opatření ID 2 (§ 19 VyKB) – Správa a ověřování identit
* Opatření ID 4 (§ 23 VyKB) – Detekce kybernetických bezpečnostních událostí
* Opatření ID 5 (§ 25 VyKB) – Aplikační bezpečnost
1. **Část: HW a SW**
* Opatření ID 3 (§ 21 VyKB) – Ochrana před škodlivým kódem
* Opatření ID 6 (§ 27 VyKB) – Zajišťování úrovně dostupnosti informací

Včetně zajištění servisní podpory provozu předmětu veřejné zakázky po dobu 60 měsíců od předání předmětu veřejné zakázky.

# Obecné požadavky

Zadavatel požaduje, aby předmět plnění veřejné zakázky (veškeré dodané zboží) měl garantovanou plnou podporu a záruku výrobce. Za účelem prokázání tohoto požadavku předloží dodavatel k nabídce potvrzení výrobce, resp. jeho lokálního zastoupení, nebo jiný rovnocenný doklad ve smyslu § 45 odst. 2 ZZVZ, ze kterého bude jednoznačně vyplývat, že nabízené zboží disponuje plnou podporou a zárukou ze strany výrobce.

Zadavatel požaduje, aby byl předmět plnění veřejné zakázky (veškeré dodané zboží) nový a nepoužitý. Dodavatel tuto skutečnost prokáže nejpozději v rámci součinnosti před podpisem smlouvy ve smyslu § 122 ZZVZ předložením například potvrzení výrobce, oficiálního zastoupení výrobce nebo jiným dokladem ve smyslu § 45 odst. 2 ZZVZ, ze kterého bude jednoznačně vyplývat splnění tohoto požadavku zadavatele.

Je-li v zadávací dokumentaci stanoven požadavek na předložení datasheetu je tím myšleno produktový list vydaný samotným výrobcem zařízení nebo výrobcem předmětné technické komponenty, veřejně dostupný, především internetovým odkazem na www stránkách vlastního výrobce, produktový list či dokument, nejen s přehledovou, ale především podrobnou technickou specifikací vlastností výrobku, v časově aktuální verzi platné pro nabízený model zařízení a region jeho použití a dodání.

Je-li součástí produktů SW či FW, pak se musí jednat o verze, které jsou standardní, běžně dostupné a určené k produkčnímu použití. Není dovoleno použití beta verzí, neoficiálních verzí, ani SW/FW se zákaznickými úpravami.

Nabízený předmět veřejné zakázky, včetně všech interních komponent, musí být pokryt oficiální technickou podporou výrobce tak, aby v případě závady, kterou není dodavatel schopen odstranit, mohl zadavatel tuto závadu eskalovat přímo k technické podpoře výrobce. Servisní zásahy budou prováděny vždy v místě instalace předmětu veřejné zakázky.

Veškeré požadované funkce, vlastnosti, certifikace i výsledky testů, musí být dostupné nejpozději dnem podání nabídky.

# Část 1. – Specifikace požadavků řešení

V následujících podkapitolách je uvedena specifikace parametrů řešení nutných pro plnění této veřejné zakázky.

V době posuzování nabídek musí nabídka řešení účastníka dále splňovat níže specifikované požadavky.

Účastník nakopíruje do nabídky následující tabulku a popis splnění požadavků ve sloupci **„Účastníkem nabízená hodnota, výrobce a typ.“**, tak že tam nakopíruje text ze sloupce „Specifikace požadavků“ a **doplní výrobce a typ**, případně doplní nebo upraví popis nabízené hodnoty, ze kterého bude patrné, že splňuje požadavky.

Sloupec „Specifikace požadavků“ nesmí být účastníkem nijak měněn a účastník je oprávněn vyplnit pouze sloupec „Účastníkem nabízená hodnota, výrobce a typ.“.

Sloupec **„Splněno [ano/ne]“** účastník nevyplňuje, slouží pro zadavatele.

## Opatření ID 1 (§ 18 VyKB) – Bezpečnost komunikačních sítí

### Firewall NG – 1ks

Tabulka 1: Firewall NG – 1ks

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| **Základní technické požadavky** |
|  | Platforma postavená na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází) |  |  |
|  | Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu 5 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nejsou akceptovány. |  |  |
|  | Zařízení ve formátu HW appliance o velikosti 1RU. |  |  |
|  | Veškeré příslušenství (montážní prvky) pro montáž do RACKu. |  |  |
|  | Možnost rozšíření platformy o další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž cele řešení musí být podporováno výrobcem.  |  |  |
|  | Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality.  |  |  |
| **HW parametry** |
|  | Počet síťových rozhraní RJ45 10/100/1000 - min 16x. |  |  |
|  | Počet síťových rozhraní SFP – min. 6x a SFP+ min. 4x. |  |  |
|  | Konzolový port pro management. |  |  |
|  | Dedikovaný port RJ45 pro management. |  |  |
|  | Dedikovaný port RJ45 pro HA. |  |  |
|  | USB 3.0 port pro zálohu konfigurace. |  |  |
|  | Redundantní napájecí zdroj. |  |  |
|  | Zabudovaný pevný disk typu SSD pro účely logování o velikost min. 400 GB. |  |  |
| **Výkonnostní parametry** |
|  | Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B – min 37Gbps, 36Gbps, 25Gbps |  |  |
|  | Výkon firewallu – min. 40 000 000 paketů / s. |  |  |
|  | Počet současně otevřených spojení – min 3 M. |  |  |
|  | Počet nových spojení za sekundu – min. 125 000. |  |  |
|  | Podpora virtualizace (nativně min. 10 virtuálních kontextů bez dodatečné licence) |  |  |
|  | Počet firewall pravidel až 10 000. |  |  |
| **Funkce** |
|  | Networking a High Availibility. |  |  |
|  | Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nody v clusteru. |  |  |
|  | Režim fungování L2 – transparentní režim, L3 – NAT/Router. |  |  |
|  | Podpora VLAN. |  |  |
|  | Podpora multicast, vytváření politiky pro multicast routování. |  |  |
|  | Podpora 802.3ad link aggregation. |  |  |
|  | Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading. |  |  |
|  | Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace. |  |  |
|  | Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP. |  |  |
|  | Policy-based routing. |  |  |
|  | Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky. |  |  |
| **VPN** |
|  | Funkce SSL VPN:* Podpora klientského i bezklientského (portálového) režimu.
* Minimální počet současně navázaných SSL VPN tunelů: 450.
* Minimální propustnost SSL VPN: 1500 Mbps.
 |  |  |
|  | Funkce IPSEC VPN:* Podpora site-to-site VPN.
* Podpora klientských VPN.
* Dostupnost VPN klienta pro koncové stanice (kompatibilní pro stávající OS Windows a MacOS). (zadavatel umožňuje nabídnout rovnocenné řešení)
* Funkce klientských IPSec VPN nesmí být licencovaná na počet uživatel. V opačném případě bude dodána neomezená licence.
* Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 1900.
* Minimální počet klientských IPSEC VPN tunelů: 15000.
* Propustnost IPSec VPN min. 32Gbps (měřeno při AES256-SHA256).
* Podpora konfigurace redundantních IPSec VPN tunelů za pomoci statického směrování.
* Podpora konfigurace redundantních IPSec VPN tunelů za pomoci dynamického směrování.
* Podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace.
 |  |  |
|  | Podpora VXLAN. |  |  |
|  | Podpora L2TP, PPTP, GRE. |  |  |
|  | podpora dynamických routovací protokolů OSPF, BGP ve VPN IPsec. |  |  |
|  | Ochrana VPN pomocí MFA pro minimálně 50 uživatelů. |  |  |
| **UTM** |
|  | Funkce detekce aplikací na L7 (Application Control):* Detekce známých aplikací na základě signatur.
* Signaturový database automaticky aktualizované výrobcem.
* Alespoň 4000 podporovaných aplikací.
* Pro populární cloudové aplikace (minimálně kompatibilní pro stávající Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) (zadavatel umožňuje nabídnout rovnocenné řešení) pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login, atd. (relevantní k dané aplikaci).
* Možnost tvorby vlastních signatur.
* Detekované aplikace je možné: povolit, monitorovat, blokovat.
* Na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci.
* Funkce AppCtr se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše.
* Minimální propustnost funkce application control: 6Gbps.
 |  |  |
|  | Funkce detekce a potlačení narušení (IPS):* Signatury automaticky aktualizované výrobcem.
* Alespoň 11.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem.
* Možnost tvorby vlastních signatur.
* Funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
* Propustnost funkce IPS včetně logování min. 5 Gbps.
 |  |  |
|  | Funkce antivirové kontroly:* Ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem.
* Signatury automaticky aktualizované výrobcem.
* AV kontrola rozšířená o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky).
* Možnost rozšíření o inspekci tzv. sandbox technikou formou lokální HW appliance stejného výrobce.
* Deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 2,6 Gbps.
* Funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
* Podpora služby výrobce, která umožní́ detekovat malware, který byl objevený v době od poslední́ aktualizace AV signaturové databáze pomocí globální́ a rychle se aktualizující́ databáze hashů.
* Funkce odstranění́ aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu/bezpečnostní́ emailové bráně v reálném čase odstraní aktivní obsah z dokumentu. Dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky. Upravený dokument jde k původnímu příjemci, originální dokument se odešle do Sandboxu.
 |  |  |
|  | Funkce kategorizace webových stránek:* Založená na centrálně spravované databázi výrobce.
* Minimálně 50 filtračních kategorií.
* Možnost definice vlastních kategorií.
* Možnost definice vlastních seznamů zakázaných URL.
* Kategorizace musí zahrnovat I české a slovenské internetové stránky.
 |  |  |
|  | Funkce DNS filtru:* Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu).
* Možnost definovat vlastní tzv. blacklist domén.
* Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL.
* Možnost importu seznamu blokovaných domén do DNS filtru.
* Detekce a blokování komunikace do botnet sítí.
* Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty.
* Podpora SSL dekrypce/SSL inspekce s minimální propustností 3000 Mbps.
* DoS Policy prevence proti základním útokům typu DoS.
 |  |  |
| **Firewall** |
|  | Možnost nastavovat firewall politiku na základě geografických údajů. |  |  |
|  | Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem. |  |  |
|  | Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud. |  |  |
|  | Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru. |  |  |
|  | Viditelnost do provozu na aplikační úrovni. |  |  |
|  | Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo). |  |  |
|  | Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu. |  |  |
|  | Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření. |  |  |
|  | Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii. |  |  |
|  | Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu. |  |  |
|  | Podpora funkce reverzní proxy. |  |  |
|  | Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů. |  |  |
|  | Explicit proxy:* Podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl).
* Podpora transparentního ověřování uživatele proti stávající MS AD protokolem Kerberos (zadavatel umožňuje nabídnout rovnocenné řešení).
* Funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta.
* Funkce transparentního ověřování uživatelů pomocí stávající domény MS Active Directory (zadavatel umožňuje nabídnout rovnocenné řešení) včetně podpory autentizace uživatel na terminálovém serveru.
 |  |  |
| **Integrovaný kontroler bezdrátových sítí (Wi-Fi)** |
|  | Wifi kontroler integrovaný do NGFW platformy pro alespoň 48 AP. |  |  |
|  | Bezdrátová síť (SSID) může být reprezentována virtuálním síťovým rozhraním – provoz tunelován z AP do kontroleru. |  |  |
|  | Podpora bezpečnostních profilů (AV, AppControl, Webfilter) přímo na wifi kontroleru. |  |  |
|  | Podpora SSL dekrypce uživatelského provozu přímo na wifi kontroleru. |  |  |
|  | Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení. |  |  |
|  | Možnost volby z různých modelů (802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor, WiFi 6, WiFi 6e). |  |  |
|  | Podpora BSS Coloring. |  |  |
|  | On-wire rogue AP detekce a mitigace. |  |  |
|  | Podpora fast-roamingu (802.11 k,v,r). |  |  |
|  | Podpora více PSK u jednoho SSID. |  |  |
|  | Podpora IPSEC tunelu pro šifrování data plane (uživatelských dat). |  |  |
|  | Podpora WPA3 protokolu. |  |  |
| **Integrovaný switch kontroler** |
|  | Zařízení musí podporovat switch kontroler jenž umožní spravovat switche výrobce z jednoduchého GUI v počtu alespoň 25 přepínačů. |  |  |
|  | Možnost správy VLAN. |  |  |
|  | Spolu s NAC politikami musí nabídnout možnost automatické přiřazení VLAN pro konkrétní zařízení či skupinu zařízeních. |  |  |
|  | Z integrovaného switch kontroleru musí být obsluha schopna pomocí GUI jednoduše definovat VLAN na konkrétní port. |  |  |
|  | V případě správy switche s funkcí PoE musí být v GUI možnost resetování PoE pro vzdálený restart zařízení. |  |  |
| **Virtualizace** |
|  | Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp. |  |  |
|  | Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech). |  |  |
|  | Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů). |  |  |
| **Management** |
|  | FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici. |  |  |
|  | Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem. |  |  |
|  | Podpora otevřeného API. |  |  |
|  | **V nabídce doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry.** |  |  |

### AKTIVNÍ PRVKY

#### Aktivní prvky – L3 CORE – 2 ks

Tabulka 2: Aktivní prvky – L3 CORE – 2 ks

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
| **Základní vlastnosti** |
|  | Třída zařízení: L3 switch. |  |  |
|  | Formát zařízení do racku. |  |  |
|  | Velikost zařízení: 1U |  |  |
|  | Počet 10G portů s volitelným optickým rozhraním min. 24x SFP+ včetně 24 ks 10G SFP+ modulů. |  |  |
|  | Počet optických 10/25/50GE portů s volitelným fyzickým rozhraním min.: 4x 10/25/50 Gbit/s SFP56, včetně 8 ks 5m kabelů DAC.  |  |  |
|  | 2x Interní AC hot-swap napájecí zdroje. |  |  |
|  | Redundantní vyměnitelné ventilátory – hot swap. |  |  |
|  | Podpora Energy Efficient Ethernet (802.3az). |  |  |
|  | Celková přepínací propustnost přepínače min.: 880 Gbit/s |  |  |
|  | Celkový paketový výkon přepínače min.: 654 Mpps |  |  |
|  | Minimální paketový buffer: 8MB |  |  |
|  | Maximální hloubka přepínače: 39 cm |  |  |
| **Vlastnosti stohování** |
|  | Podporovaný počet přepínačů ve stohu min.: 10 |  |  |
|  | Kapacita stohovacího propojení min.: 200 Gbps |  |  |
|  | Stoh podporuje distribuované přepínaní paketů. |  |  |
|  | Podpora stohu na delší vzdálenost min. 100m. |  |  |
|  | Redundance řídícího prvku v rámci stohu. |  |  |
|  | Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor). |  |  |
|  | Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG). |  |  |
|  | Podpora stohování různých typů přepínačů (PoE, Non-PoE, 24port, 48port). |  |  |
|  | Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF. |  |  |
|  | Součástí každého přepínače je stohovací 50GE kabel s min. délkou 1m. |  |  |
| **Základní 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. |  |  |
|  | Počet LACP skupin/linek ve skupině min.: 256/16. |  |  |
|  | Minimální počet záznamů v tabulce MAC adres: 32 000 |  |  |
|  | Minimální počet záznamů v tabulce ARP: 45 000. |  |  |
|  | Protokol pro definici šířených VLAN: MVRP. |  |  |
|  | Podpora VLAN podle IEEE 802.1Q, minimálně 4000 aktivních VLAN. |  |  |
|  | VLAN translace - swap 802.1Q tagů na trunk portu. |  |  |
|  | Podpora zařazování do VLAN podle standardu 802.1v. |  |  |
|  | Podpora VLAN-group pro rozkládání klientů přes více VLAN ID. |  |  |
|  | Private VLAN. |  |  |
|  | IEEE 802.1s - Multiple Spanning Tree. |  |  |
|  | STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+). |  |  |
|  | Podpora protokolu ERPS (ITU G.8032) pro rychlou konvergenci do 100 ms v kruhových sítích. |  |  |
|  | Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED včetně LLDP over OoB management port. |  |  |
|  | Detekce jednosměrnosti optické linky (např. UDLD). |  |  |
|  | DHCP server. |  |  |
|  | DHCP relay pro IPv4 a IPv6. |  |  |
|  | Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace. |  |  |
|  | Podpora protokolu PTP. |  |  |
|  | Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subnety. |  |  |
|  | Statické směrování IPv4 a IPv6. |  |  |
|  | Minimální počet IPv4 záznamů ve směrovací tabulce: 60 000 |  |  |
|  | Minimální počet IPv6 záznamů ve směrovací tabulce: 60 000. |  |  |
|  | Dynamické směrování OSPFv2, OSPFv3 včetně podpory BFD. |  |  |
|  | Dynamické směrování BGP a MP-BGP včetně podpory BFD. |  |  |
|  | Podpora směrovacího protokolu RIP a RIPng. |  |  |
|  | OSPFv2 autentizace s podporou HMAC-SHA-384. |  |  |
|  | Podpora Layer-3 routed port včetně podpory L3 sub-interface. |  |  |
|  | Podpora minimálně 256 virtuálních směrovacích instancí (VRF). |  |  |
|  | IGMP v2 a v3, IGMP snooping. |  |  |
|  | Multicast Listener Discovery (MLD) v1 a v2, MLD snooping. |  |  |
|  | Směrování multicast: PIM-DM, PIM-SM, PIM6-SM, MSDP. |  |  |
|  | Hardware podpora IPv4 a IPv6 ACL. |  |  |
|  | ACL definice na základě skupiny fyzických portů. |  |  |
|  | IN a OUT ACL aplikovatelný na interface, LAG, VLAN. |  |  |
|  | BPDU a Root guard. |  |  |
|  | DHCP snooping pro IPv4 a IPv6. |  |  |
|  | HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps. |  |  |
|  | 802.1X ověřování včetně více současných uživatelů na port, min. 32 uživatelů/port. |  |  |
|  | Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou). |  |  |
|  | Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675. |  |  |
|  | 802.1X s podporou odlišných Preauth VLAN, Fail VLAN, Critical VLAN a Critical voice VLAN. |  |  |
|  | Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely. |  |  |
|  | Podpora uživatelských rolí definovaných lokálně v přepínači, jejich aplikace na základě výsledku autorizace. |  |  |
|  | Podpora uživatelských rolí dynamicky stahovatelných z RADIUS serveru, jejich aplikace na základě výsledku autorizace. |  |  |
|  | Podpora IPv6 RA Guard. |  |  |
|  | IP source guard / dynamic IP lockdown. |  |  |
|  | Možnost instalace vlastního certifikátu včetně podpory Enrollment over Secure Transport (EST). |  |  |
|  | Podpora Dynamic ARP protection. |  |  |
|  | Podpora bezpečného transportu Dynamic ACL během 802.1X, např. pomocí SSL. |  |  |
|  | Port security. |  |  |
|  | Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU. |  |  |
|  | Podpora IPv4 a IPv6 QoS. |  |  |
|  | IEEE 802.1p - minimální počet front: 8 |  |  |
|  | Energy Efficient Ethernet (EEE). |  |  |
| **SDN funkce** |
|  | Podpora service insertion včetně technologie VXLAN. |  |  |
|  | Podpora BGP EVPN s využitím VXLAN. |  |  |
|  | Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izolovat více koncových zařízení na jednom portu do unikátních tunelů. |  |  |
|  | Přiřazení koncového zařízení do tunelu na základě výsledku autorizace. |  |  |
|  | Podpora Group based policy pro VXLAN (VXLAN GPB). |  |  |
| **Analytické a automatizační nástroje** |
|  | Podpora REST API pro automatizaci nastavení sítě. |  |  |
|  | Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Integrovaný nástroj na odchyt paketů. |  |  |
|  | Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události. |  |  |
|  | Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů. Možnost vynášení stavu monitorovaných metrik do grafů. |  |  |
|  | Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase. |  |  |
|  | Interní úložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení. |  |  |
|  | Kapacita interního úložiště dat pro analytické účely minimálně 30 GB. |  |  |
| **Management** |
|  | USB-C konzolový port. |  |  |
|  | 1xRJ45 OoB management port s podporou ethernetu. |  |  |
|  | Konfigurace zařízení v člověku čitelné textové formě. |  |  |
|  | Podpora automatických i manuálních snapshotů konfigurace systému. |  |  |
|  | USB port pro diagnostiku, přenos konfigurace a firmware. |  |  |
|  | Přímé bezdrátové připojení ke konzoli zařízení skrze Bluetooth. |  |  |
|  | Podpora managementu přes IPv4 i IPv6. |  |  |
|  | SSHv2 a HTTPS pro IPv4 a IPv6. |  |  |
|  | SFTP nebo SCP pro šifrované kopírování. |  |  |
|  | Podpora SNMPv2c a SNMPv3. |  |  |
|  | Remote Network Monitoring (RMON). |  |  |
|  | Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL. |  |  |
|  | Možnost plánování automatického spouštění příkazů. |  |  |
|  | Lokálně vynucené Role-based access control (RBAC) na úrovni přepínače. |  |  |
|  | Dualní flash image |  |  |
|  | Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů. |  |  |
|  | Podpora RADIUS včetně RADIUS CoA (RFC3576). |  |  |
|  | Podpora Secure RADIUS (RadSec). |  |  |
|  | Podpora standardního Linux Shellu (BASH) pro debugging a skriptování. |  |  |
|  | Podpora TACACS+. |  |  |
|  | Analýza síťového provozu sFlow podle RFC 3176. |  |  |
|  | Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM chipu. |  |  |
|  | Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN. |  |  |
|  | Podpora IP SLA pro měření zpoždění provozu VoIP. |  |  |
|  | Podpora Cloud based management. |  |  |
|  | Podpora Zero Touch Provisioning (ZTP). |  |  |
|  | Hardware musí být dodán plně funkční a kompletní (včetně příslušenství). |  |  |
|  | Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů. |  |  |
|  | Podpora hardware s výměnou NBD v délce 60 měsíců. Tato podpora musí být garantovaná výrobcem zařízení. |  |  |
|  | Účastník je povinen s dodávkou doložit seznam sériových čísel dodávaných zařízení. |  |  |
|  | **V nabídce doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry.** |  |  |

#### Aktivní prvky – ACCESS – PoE – 10 ks

Tabulka 3: Aktivní prvky – ACCESS – PoE – 10 ks

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
| **Základní vlastnosti**  |
|  | Třída zařízení: přepínač  |  |  |
|  | Formát zařízení do racku  |  |  |
|  | Velikost zařízení: 1U  |  |  |
|  | Počet 1Gbit/s metalických portů min.: 48x 10/100/1000Mbps RJ45 |  |  |
|  | Počet optických 10GE portů s volitelným fyzickým rozhraním (SFP+) min. 4x, včetně 40 ks 10G SFP+ modulů. |  |  |
|  | Interní AC zdroj.  |  |  |
|  | Minimálně 370 W třídy 4 PoE / PoE+ podporující až 30 W na port. |  |  |
|  | Celková přepínací propustnost přepínače min.: 176 Gbit/s |  |  |
|  | Celkový paketový výkon přepínače min.: 130 Mpps |  |  |
|  | Minimální paketový buffer: 8MB  |  |  |
| **Vlastnosti stohování**  |
|  | Podporovaný počet přepínačů ve stohu min.: 8  |  |  |
|  | Kapacita stohovacího propojení min.: 80 Gbps  |  |  |
|  | Stoh podporuje distribuované přepínaní paketů. |  |  |
|  | Stohování přes standartní uplink porty (možnost zapojení stohu na minimálně 100m).  |  |  |
|  | Redundance řídícího prvku v rámci stohu. |  |  |
|  | Podpora stohování různých typů přepínačů (PoE, Non-PoE, 24port, 48port). |  |  |
|  | Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor). |  |  |
|  | Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG).  |  |  |
|  | Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF. |  |  |
|  | Součástí každého přepínače je stohovací kabel minimálně 10GE s minimální délkou 1m. |  |  |
| **Základní funkce a protokoly**  |
|  | Podpora "jumbo rámců" včetně velikosti 9198 Byte. |  |  |
|  | Podpora linkové agregace IEEE 802.1AX. |  |  |
|  | Konfigurovatelné rozkládání LACP zátěže podle L2, L3. |  |  |
|  | Počet LACP skupin/linek ve skupině: 32/8. |  |  |
|  | Minimální počet záznamů v tabulce MAC adres: 16 000.  |  |  |
|  | Minimální počet záznamů v tabulce ARP: 8 000. |  |  |
|  | Protokol pro definici šířených VLAN: MVRP.  |  |  |
|  | Podpora VLAN podle IEEE 802.1Q, minimálně 2000 aktivních VLAN. |  |  |
|  | Podpora zařazování do VLAN podle standardu 802.1v. |  |  |
|  | IEEE 802.1s - Multiple Spanning Tree. |  |  |
|  | STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+). |  |  |
|  | Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED. |  |  |
|  | Detekce jednosměrnosti optické linky (např. UDLD). |  |  |
|  | Podpora NTPv3. |  |  |
|  | Statické směrování IPv4 a IPv6. |  |  |
|  | Minimální počet IPv4 záznamů ve směrovací tabulce: 2 000. |  |  |
|  | Minimální počet IPv6 záznamů ve směrovací tabulce: 1 000. |  |  |
|  | Dynamické směrování OSPFv2, OSPFv3. |  |  |
|  | Podpora Layer-3 routed port. |  |  |
|  | IGMP v2 a v3. |  |  |
|  | IGMP snooping. |  |  |
|  | Multicast Listener Discovery (MLD) v1 a v2. |  |  |
|  | MLD snooping. |  |  |
|  | Hardware podpora IPv4 a IPv6 ACL. |  |  |
|  | ACL definice na základě skupiny fyzických portů. |  |  |
|  | ACL aplikovatelný na interface, LAG, VLAN. |  |  |
|  | BPDU a Root guard. |  |  |
|  | DHCP snooping pro IPv4 a IPv6. |  |  |
|  | HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps. |  |  |
|  | 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port. |  |  |
|  | Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou). |  |  |
|  | Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675. |  |  |
|  | Podpora Critical VLAN. |  |  |
|  | Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.  |  |  |
|  | Podpora uživatelských rolí definovaných lokálně v přepínači, jejich aplikace na základě výsledku autorizace. |  |  |
|  | Podpora uživatelských rolí dynamicky stahovatelných z RADIUS serveru, jejich aplikace na základě výsledku autorizace. |  |  |
|  | Podpora Dynamic ARP protection. |  |  |
|  | Port security. |  |  |
|  | Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU. |  |  |
|  | Podpora IPv4 a IPv6 QoS. |  |  |
|  | IEEE 802.1p - minimální počet front: 8  |  |  |
| **SDN funkce**  |
|  | Podpora technologie VXLAN. |  |  |
|  | Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izolovat více koncových zařízení na jednom portu do unikátních tunelů. |  |  |
|  | Přiřazení koncového zařízení do tunelu na základě výsledku autorizace. |  |  |
| **Analytické a automatizační nástroje**  |
|  | Podpora REST API pro automatizaci nastavení sítě.  |  |  |
|  | Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Integrovaný nástroj na odchyt paketů.  |  |  |
|  | Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události. |  |  |
|  | Grafické rozhraní pro zobrazení výsledků monitorování a analytických skriptů. Možnost zobrazení stavu monitorovaných metrik do grafů.  |  |  |
|  | Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase.  |  |  |
|  | Interní uložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení. |  |  |
|  | Kapacita interního úložiště dat pro analytické účely minimálně 14 GB. |  |  |
| **Management**  |
|  | Konzolový port. |  |  |
|  | 1xRJ45 OoB management port s podporou ethernetu. |  |  |
|  | Konfigurace zařízení v člověku čitelné textové formě. |  |  |
|  | Podpora automatických i manuálních snapshotů konfigurace systému. |  |  |
|  | USB port pro diagnostiku, přenos konfigurace a firmware. |  |  |
|  | Přímé bezdrátové připojení ke konzoli zařízení skrze Bluetooth. |  |  |
|  | Podpora managementu přes IPv4 i IPv6. |  |  |
|  | SSHv2 a HTTPS pro IPv4 a IPv6. |  |  |
|  | Podpora SNMPv2c a SNMPv3. |  |  |
|  | Remote Network Monitoring (RMON).  |  |  |
|  | Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL. |  |  |
|  | Lokálně vynucené Role-based access control (RBAC) na úrovni přepínače. |  |  |
|  | Dualní flash image. |  |  |
|  | Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů. |  |  |
|  | Podpora RADIUS včetně RADIUS CoA (RFC3576). |  |  |
|  | Podpora shellu pro debugging a skriptování.  |  |  |
|  | Podpora TACACS+. |  |  |
|  | Analýza síťového provozu sFlow podle RFC 3176. |  |  |
|  | Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM chipu. |  |  |
|  | Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN. |  |  |
|  | Podpora IP SLA pro měření zpoždění provozu VoIP. |  |  |
|  | Podpora Zero Touch Provisioning (ZTP). |  |  |
|  | Hardware musí být dodán plně funkční a kompletní (včetně příslušenství). |  |  |
|  | Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů. |  |  |
|  | Podpora hardware s výměnou NBD v délce 60 měsíců. Tato podpora musí být garantovaná výrobcem zařízení. |  |  |
|  | Účastník je povinen s dodávkou doložit seznam sériových čísel dodávaných zařízení. |  |  |
|  | **V nabídce doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry.** |  |  |

#### Centrální management

Tabulka 4: Centrální management

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
| **Základní vlastnosti** |
|  | Software nástroj pro centrální správu a monitoring aktivních síťových prvků. |  |  |
|  | Public cloud nativní aplikace dodávána formou služby. |  |  |
|  | Plně kompatibilní s nabízenými aktivními prvky. |  |  |
|  | Licence pro správu všech zařízení s možností flexibilního rozšiřování až do 1000 zařízení. |  |  |
|  | Vysoká dostupnost aplikace – nativní HA režim. |  |  |
|  | Komunikace se spravovanými zařízením přes zabezpečený protokol (HTTPS, SSL) |  |  |
|  | Hromadná aktualizace firmware s možností naplánovaní na definovaný čas a skupinu zařízení. |  |  |
|  | Automatické upozornění na aktualizaci firmware - návrh výrobcem doporučené verze. |  |  |
|  | Kontrola souladu firmware s definovanou verzí a vynucení aktualizace pro všechna zařízení ve skupině. |  |  |
|  | Možnost přímého přístupu do CLI aktivních prvku z portálu centrální správy. |  |  |
|  | Integrované diagnostické nástroje umožňují spouštět vzdáleně CLI příkazy. |  |  |
|  | RESTful API pro možnost integrace s externími systémy a možnost vyčítat provozní statistiky. |  |  |
|  | Možnost rozdělení zařízení do uživatelských skupin s jednotnou správou. |  |  |
|  | Hierarchická konfigurace: nad skupinou zařízení a individuálním zařízením. |  |  |
|  | Podpora přihlášení administrátorů s podporou dvoufaktorové autentizace. |  |  |
|  | Podpora různých administrátorských rolí s možností definice oprávnění. |  |  |
|  | Možnost přiřazení detailních oprávnění administrátorům, 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). |  |  |
|  | Možnost omezení přístupu k managementu pomocí definovaných povolených IP adres. |  |  |
|  | Instalační a monitorovací aplikace dostupná a kompatibilní pro stávající zařízení s OS Android a IOS (zadavatel umožňuje nabídnout rovnocenné řešení). Umožňuje naskenovat a přidat zařízení pod centrální správu. Dále umožňuje monitorovat stav zařízení a připojených klientů včetně objemu přeneseného provozu. |  |  |
|  | Provisioning zařízení do centrální správy probíhá automaticky po registraci zakoupených zařízení do nástroje centrální správy (vyplnění identifikačních údajů zařízení). |  |  |
|  | Konfiguračních audit - porovnání rozdílů skupinová vs. individuální konfigurace zařízení. |  |  |
|  | Audit příkazů zadávaných/odesílaných na aktivní prvek včetně administrátora který je zadával. |  |  |
|  | Modul pro vytváření souhrnných reportů z dat za poslední období. Minimálně reporty: PCI, bezpečnostní report, kapacitní plánování sítě, klient inventory, využití sítě klienty. |  |  |
|  | Real-time diagnostika událostí týkajících se konkrétního klienta – okamžité zobrazování stavů připojení, autentizace atp. bez nutnosti čekání na pravidelný update interval. |  |  |
|  | Grafický dashboard zobrazující aktuální a historické informace o připojených klientech. Informace o přeneseném objemu dat. |  |  |
|  | Dohled aktivních prvků, zobrazení událostí a alertů. |  |  |
|  | Nástroje pro ověření konektivity spouštěné přímo z management nástroje (ping, traceroute). |  |  |
|  | Možnost definování seznamu příkazů pro diagnostiku problémů a jejich hromadné spuštění. |  |  |
| **Správa a monitoring přepínačů** |
|  | Centrální správu a monitoring přepínačů |  |  |
|  | Definice společných konfiguračních elementů nad skupinou zařízení |  |  |
|  | Grafický editor s integrovanou validací syntaxe příkazů – příkazy identické jako v CLI přepínače |  |  |
|  | Automatická validace konfigurace na jednotlivých prvcích v síti před jejím nasazením. |  |  |
|  | Zobrazení stavu a konfigurace portů přepínače, zobrazení spotřeby PoE po jednotlivých portech, zobrazení stavu hardwaru (CPU, RAM, ventilátory, teplota, napájecí zdroje). |  |  |
|  | Zobrazení seznamu sousedních zařízení přepínače. |  |  |
|  | Měření zakončení a délky metalického kabelu (např. TDR nebo ekvivalentní) |  |  |
|  | Správa a monitoring přístupových bodů |  |  |
|  | Centrální správu a monitoring přístupových bodů.  |  |  |
|  | Definice společných konfiguračních elementů nad skupinou zařízení. |  |  |
|  | Grafický dashboard zobrazující aktuální a historické informace o WIFI AP, připojených klientech a jimi používaných aplikacích a webových obsazích včetně objemu provozu přeneseného těmito aplikacemi/weby. |  |  |
|  | Integrovaná diagnostika umožňující aktivní testy z pozice WIFI AP – iPerf testování |  |  |
|  | Centrální monitorování WIFI parametrů per AP a per jednotliví klienti – SNR, šum, přenosová rychlost, WIFI kanály, síla signálu atp.  |  |  |
|  | Monitorování síťových služeb jako je DNS, DHCP či RADIUS ověřování klientů, jejich chybovost a zpoždění. Volitelné rozdělení dat dle AP, klientů, pásma a SSID.  |  |  |
|  | Uchovávání roaming historie klienta včetně měření času roamingu (přechodu z AP na jiné AP či jinou frekvenci) a záznamu o metodě roamingu (standardní 802.11 WIFI deautentizace, OKC, 802.11r). Vizualizace roaming událostí v časovém grafu. |  |  |
|  | Podpora packet capture. |  |  |
|  | Podpora bezdrátové detekce a prevence průniku – detekování pokusů neoprávněného proniknutí do bezdrátové sítě a jejich zastavení je-li to technicky možné (např. deautentizačním útokem či cíleným zpožďováním rámců/tarpiting). Detekce a potlačení cizích AP připojených do domácí drátové sítě. |  |  |
|  | Typy autentizace: WPA/WPA2-PSK, WPA/WPA2-Enterprise, 802.1X, MAC autentizace, “captive portal”, 802.1X ověření s následným ověřením MAC |  |  |
|  | Typy autentizace: Enhanced Open (OWE), SAE (Simultaneous Authentication of Equals), WPA3 Enterprise Basic, WPA3-Enterprise SuiteB |  |  |
|  | Autentizace sdíleným klíčem s možnosti definovat několik různých PSK na jednom SSID (např. Identity PSK). Podpora externích i lokálních identit přímo v APOD. |  |  |
|  | Podporované autentizační/autorizační zdroje: RADIUS, LDAP, RFC 3576 Change of Authorization. |  |  |
|  | Funkce řízení a ochrany rádiového spektra s automatickou optimalizací sítě (přidělováni kanálů, fast roaming, rozdělení klientů na jednotlivá AP). |  |  |
|  | Automatizovaná migrace klientů na optimální frekvenci, AP či rádio s využitím min. těchto parametrů: kategorie daného klienta, SNR, schopnosti klienta, kvalita signálu. |  |  |
|  | Automatické ladění radiových kanálu i vysílacího výkonu v koordinaci s ostatními APOD. |  |  |
|  | Pokročilá optimalizace radiových kanálů i vysílacího výkon s využitím měřených charakteristik z celého předchozího dne. Možnost plánování spuštění optimalizace v čase mimo pracovní hodiny.  |  |  |
| **Správa a monitoring gateway**. |
|  | Centrální správu a monitoring gateway.  |  |  |
|  | Podpora automatické a i manuální konfigurace HA clusteru. |  |  |
|  | Vestavěný průvodce pro rychlou úvodní konfiguraci. |  |  |
|  | Monitoring clusteru. |  |  |
|  | Monitoring uživatelů připojených ke gateway.. |  |  |
|  | Podpora packet capture. |  |  |
| **Správa přístupu WiFi hostů.** |
|  | Možnost centrálního vytváření SSID pro hosty s cloud captive portálem. |  |  |
|  | Vytvoření upravitelného captive portálu pro hosty s možnostmi úpravy obrázku pozadí, loga, barvy pozadí a barvy elementů webové stránky. |  |  |
|  | Možnost přidávání podmínek použití captive portálu pro koncové uživatele a vynucení jejich akceptace před připojením přes portál. |  |  |
|  | Možnost přidávání reklamních sdělení formou bannerů či obrázků. |  |  |
|  | Lokalizace veškerých textových prvků stránky do jakéhokoliv jazyka. |  |  |
|  | Captive portál umožňuje hostům anonymní, autentizované a samoregistrační řízení přístupu. |  |  |
|  | V případě samoregistrace hosta portál podporuje ověření identifikační údajů pomocí SMS či mailu. Platba za SMS zprávy pro ověření telefonního čísla hosta je zahrnuta v ceně poplatku za cloud nástroj zprávy. |  |  |
|  | V případě autentizované metody přístupu je podporován lokální účet a popř. již vytvořené účty ve stávajících sítích LinkedIn, Facebook a Google (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
|  | Podpora MAC caching – systému, který zajistí, že po prvním přihlášení uživatele na captive portál již při dalších připojeních není nutné znovu zadávat přístupové údaje po dobu, kterou definuje administrátor portálu. |  |  |
| **Cloud autentizace** |
|  | Podpora Cloud autentizace s využitím metod jako 802.1X pro LAN i WiFi. |  |  |
|  | Cloud platforma podporuje bezpečnou autentizace s využitím protokolu RadSec. |  |  |
|  | Podpora autorizace s využitím stávajících identit v Google Workspace a Microsoft Azure AD (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
|  | Mapování bezpečnostních role uživatele podle stávající identity z Google Workspace a Microsoft Azure AD (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
|  | Záruka garantovaná přímo výrobcem zařízení v režimu 24x7. Možnost otevírat servisní požadavky přímo u výrobce. |  |  |
|  | **V nabídce doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry.** |  |  |

### WiFi AP – 20 ks

Tabulka 5: WiFi AP – 20 ks

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Třída zařízení: indoor přístupový bod  |  |  |
|  | Uzavřená konstrukce bez ventilátorů. |  |  |
|  | Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax. |  |  |
|  | Plnohodnotná certifikace Wi-Fi Aliance: IEEE 802.11a/b/g/n/ac. |  |  |
|  | Plnohodnotná certifikace Wi-Fi Aliance: WPA3-CNSA, WPA3-SAE, WPA3-OWE. |  |  |
|  | Pracovní režim AP bez kontroléru (autonomní). |  |  |
|  | Pracovní režim AP řízené kontrolérem (lightweight). |  |  |
|  | Pracovní režim AP v roli kontroléru s možností správy až 120 AP. |  |  |
|  | Minimální počet portů ethernet LAN: 1x 100/1000 Mbit/s RJ45.  |  |  |
|  | Podpora standardů IEEE 802.3af (PoE), IEEE 802.3at (PoE+). |  |  |
|  | Podpora standardního PoE IEEE 802.3af 15W bez nutnosti redukce výkonu libovolného rádia. |  |  |
|  | Podpora napájení z AC napájecího zdroje. |  |  |
|  | Vestavěná interní anténa MIMO, omni down-tilt. |  |  |
|  | Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz. |  |  |
|  | MIMO a počet nezávislých streamů na 2,4GHz rádio: 2x2:2. |  |  |
|  | MIMO a počet nezávislých streamů na 5GHz rádio: 2x2:2. |  |  |
|  | Podpora šířky kanálu 80 MHz. |  |  |
|  | HW podpora DL-OFDMA, UL-OFDMA a DL-MU-MIMO. |  |  |
|  | Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP. |  |  |
|  | Možnost nastavení vysílacího výkonu s krokem 0.5 dBm. |  |  |
|  | Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 5GHz: 1200 Mbps. |  |  |
|  | Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 2.4GHz: 570 Mbps. |  |  |
|  | Integrovaný TPM pro bezpečné uložení certifikátů a klíčů. |  |  |
|  | Podpora 802.11ac explicitního beamformingu. |  |  |
|  | Podpora airtime fairness. |  |  |
|  | Prioritizace jednotlivých SSID na základě vysílacího času. |  |  |
|  | USB port s podporou 3G/4G USB modemu jako WAN uplink. |  |  |
|  | Vypínatelné indikační LED diody informující o stavu zařízení. |  |  |
|  | Band Steering či obdobné (prioritizace 5GHz pásma v případě je-li podporováno). |  |  |
|  | Detekce Rogue APOD. |  |  |
|  | Minimální počet inzerovaných SSID (BSSID) na radio: 16. |  |  |
|  | Nastavitelný DTIM interval pro jednotlivé SSID. |  |  |
|  | Mapování SSID do různých VLAN podle IEEE 802.1Q. |  |  |
|  | VLAN Pooling. |  |  |
|  | HW Podpora wireless MESH funkcionality s protokolem pro optimální výběr cesty v rámci MESH stromu. |  |  |
|  | Podpora Layer-2 izolace bezdrátových klientů. |  |  |
|  | HW Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz. |  |  |
|  | Hardware filtry pro filtraci intermodulačního rušením pocházejícím z mobilních sítí. |  |  |
|  | Detekce a monitorování problémů WLAN odchytáváním provozu na AP ve formátu PCAP a jeho zasíláním do Ethernetového analyzátoru, schopnost zachytávat rámce včetně 802.11 hlaviček. |  |  |
|  | DHCP server, směrování a NAT pro bezdrátové klienty. |  |  |
|  | AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN. |  |  |
|  | Automatická identifikace připojeného zařízení a jeho operačního systému. |  |  |
|  | Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming. |  |  |
|  | Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními APOD. |  |  |
|  | Optimalizace provozu: multicast-to-unicast konverze. |  |  |
|  | Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace). |  |  |
|  | Filtrování přístupu na web. |  |  |
|  | Podpora RadSec (RADIUS over TLS). |  |  |
|  | 802.11w ochrana management rámců.  |  |  |
|  | Podpora Kensington lock (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
|  | Podpora MAC ověřování a 802.1X ověřování s využitím lokální DB v AP. |  |  |
|  | Podpora 802.1X suplicant, AP se ověřuje před připojením do LAN. |  |  |
|  | Volitelně možnost spravovat AP cloud management nástrojem. |  |  |
|  | CLI formou serial konsole port a serial over Bluetooth. |  |  |
|  | SSHv2, SNMPv2c a SNMPv3. |  |  |
|  | AP podporuje zero touch provisioning pomocí externího management SW jehož IP adresu získá z cloud aktivační služby poskytované výrobcem. |  |  |
|  | Integrované Bluetooth 5.0 Low Energy (BLE) rádio. |  |  |
|  | Integrované Zigbee 802.15.4 rádio (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
|  | Podpora režimu SLEEP s max. spotřebou energie do 4W. |  |  |
|  | Součástí AP je příslušenství pro montáž na zeď nebo strop. |  |  |
|  | Hardware musí být dodán plně funkční a kompletní (včetně příslušenství). |  |  |
|  | Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů. |  |  |
|  | Podpora hardware s výměnou NBD v délce 60 měsíců. Tato podpora musí být garantovaná výrobcem zařízení. |  |  |
|  | Účastník je povinen s dodávkou doložit seznam sériových čísel dodávaných zařízení. |  |  |
|  | **V nabídce doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry.** |  |  |

## Opatření ID 2 (§ 19 VyKB) – Správa a ověřování identit

### 802.1X RADIUS – přístup do sítě – Server NAC (Network access)

Tabulka 6: 802.1X RADIUS – přístup do sítě – Server NAC (Network access)

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
| **Základní funkce platformy** |
|  | Autentizační platforma (AAA) pro řízení přístupu uživatelů a zařízení do LAN a Wi-Fi. |  |  |
|  | On-premise appliance, nepřipouští se cloud řešení. |  |  |
|  | Virtuální appliance bez nutnosti dodatečných licencí např. pro OS nebo database. |  |  |
|  | Režimu vysoké dostupnosti – minimálně 2 autentizační node s jednotnou správou. |  |  |
|  | Podporované stávající hypervisory kompatibilní s: VMware (.OVA formát), Hyper-V, KVM (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
|  | Plná kompatibilita s infrastrukturou zadavatele na které bude probíhat ověřování. |  |  |
|  | Podpora 802.1X autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN. |  |  |
|  | Požadovaný počet licencí pro současně autentizovaná zařízení (pomocí 802.1X): 300. |  |  |
|  | Požadovaný počet licencí pro současně profilovaná zařízení: 300. |  |  |
|  | Možnost vytváření active-active clusterů. Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality a umožňovat navýšení počtu podporovaných uživatelů přidáním další instance. |  |  |
|  | Režim vysoké dostupnosti umožňuje v jednom clusteru kombinovat specializovanou HW a virtuální appliance. |  |  |
|  | Podpora minimálně následujících autentizačních metod: PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, Tunnel Extensible Authentication Protocol (TEAP), MAC autentizace. |  |  |
|  | Platforma musí umožňovat úplné oddělení autentizace a autorizace, např. autentizace proti stávající službě Active Directory, autorizace proti externí SQL databázi (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
|  | Autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, typ zařízení, osobní profil či členství ve skupině v Active Directory. |  |  |
|  | Podpora dalších způsobů autentizace a autorizace. Minimálně: LDAP, MS AD, Token, MAC auth, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta). |  |  |
|  | Podpora změny autorizačního stavu zařízení bez nutnosti změny definice autorizační politiky, např. pro odpojení nebo karanténu koncových zařízení. |  |  |
|  | Podpora autorizace pomocí externího Cloud zdroje identity pro: stávající Azure Active Directory (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
|  | Podpora RADIUS CoA podle RFC3576 pro změnu autorizace ověřeného zařízení. |  |  |
|  | Podpora RadSec (RADIUS over TLS) a RadSec proxy pro IPv4 a IPv6. |  |  |
|  | 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. |  |  |
|  | Sběr dodatečných informací o připojených zařízeních (profilování) jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace lze využít pro doplňkové ověření přístupu zařízení do sítě. |  |  |
|  | Sběr dodatečných informací o připojených IoT zařízeních (profilování), pomocí aktivních metod jako jsou: SNMP, WMI a NMAP scan. Tyto informace lze využít pro doplňkové ověření přístupu zařízení do sítě. |  |  |
|  | Automatická identifikace a označení privátních (randomizovaných) MAC adres koncových zařízení. |  |  |
|  | Platforma obsahuje funkci otestovaní autentizační politiky, včetně flexibilní volby typu autentizace, atributů klienta, atd. |  |  |
|  | Podpora REST API pro většinu základních úkonů AAA platformy. Podpora REST volání vyvolaného autentizační či autorizační událostí (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. |  |  |
|  | Možnost vlastní tvorby parseru/integrace SYSLOG hlášení pro možnost uživatelské integrace s libovolnými systémy třetích stran. |  |  |
|  | Podpora SYSLOG podle RFC 5424. |  |  |
|  | Možnost registrace zařízení pomocí MAC adresy pro non-IT uživatele - omezená funkce administračního rozhraní, se zařazením zařízení do skupiny s definovanou politikou přístupu. |  |  |
|  | Podpora TACACS+ autentizace správců síťových zařízení. |  |  |
|  | Možnost integrace s MDM (Mobile Device Management) platformami třetích stran (kompatibilní minimálně se stávajících: AirWatch, Citrix, MobileIron, JAMF) (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
|  | Funkce pro řízení přístupu hostů – LAN a WiFi Guest Captive portál. |  |  |
|  | Podpora HTTP a HTTPS web autentizace (Captive portál). |  |  |
|  | Podpora CAPPORT - RFC 8908. |  |  |
|  | Podpora autentizace hostů pomocí účtů stávajících sociálních sítí: Google, Google Plus, Facebook, Facebook WIFI, LinkedIn, Microsoft (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
|  | Podpora autentizace lokálními účty v rámci portálu, ověření pomocí jméno+heslo, autentizační kód. |  |  |
|  | Možnost samoobslužné registrace hosta do sítě se SMS a email ověřením. |  |  |
|  | Přístup zdarma pouze s akceptací podmínek užití. |  |  |
|  | Tarify lze omezit časově, z hlediska rychlosti připojení či objemu přenesených dat. |  |  |
|  | Vynucení odpojení zařízení ihned po naplnění jakéhokoliv z limitů. |  |  |
|  | Perzistence autentizace/registrace s využitím MAC cache a zobrazení jen uvítacích stránek s osobním oslovením hosta při opakovaných návštěvách. Konfigurovatelné hodnoty trvání MAC cache pro různé hosty v rámci jedné služby (např. jedno SSID). |  |  |
|  | Možnost vytváření účtů samoobslužnou registrací. |  |  |
|  | Možnost provozovat více graficky i obsahově unikátních portálů v rámci jedné instalace. |  |  |
|  | Redakční systém pro plnou grafickou a obsahovou úpravu jednotlivých captive portálů:* Úprava barev, fontů, pozadí a loga.
* Úprava registračních formulářů – přidávání a odebírání polí pro vstupní data formuláře včetně validace vkládaného obsahu.
* Možnost vkládání animací, videí a dalšího dynamického obsahu.
* Vytváření specifických stránek pro různé typy zařízení a operačních systémů.
 |  |  |
| **Management** |
|  | HTTPS rozhraní s podporou konfiguračních průvodců a předkonfigurovaných šablon. |  |  |
|  | Podpora SNMPv3. |  |  |
|  | NTP pro synchronizaci času. |  |  |
|  | Diagnostika problémů (systémová, údaje o chybách přihlašování, packet capture včetně filtrů). |  |  |
|  | Appliance podporuje šifrování disku nebo souborů. |  |  |
|  | Appliance podporuje CLI přístup a umožňuje v něm konfiguraci základních nastavení. |  |  |

### Více-faktorová autentizace a Single Sign-On (SSO) – pro 160 uživatelů

Tabulka 7: Více-faktorová autentizace a Single Sign-On (SSO) – pro 160 uživatelů

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
| **Funkční specifikace** |
|  | Klientská část řešení musí být kompatibilní a podporovat stávající MS Windows Desktop OS (MS Windows 10 a novější), Linuxové OS tenkých klientů a v případě mobilních klientských zařízení minimálně operační systémy rodiny MS Windows pro minimálně 160 uživatelů. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Řešení bude ve výchozím stavu navrženo a dodáno jako vysoce dostupné, s odolností vůči výpadku jednoho serverového prvku, s minimálně dvěma vzájemně zastupitelnými prvky. Při výpadku jednoho prvku zůstává řešení plně funkční, zbylý funkční prvek/prvky nadále poskytují plnou funkčnost. K překlopení na funkční prvek/prvky musí dojít automaticky, bez nutnosti ručního zásahu, maximálně v jednotkách sekund. Všechny prvky si vzájemně replikují nastavení a data, v případě výpadku prvku tedy nedojde ke ztrátě nastavení či dat. Všechny prvky řešení musí být spravovány jako jeden celek, jednotnou správou z webové konzoly, napříč datovými centry, případně cloudy. |  |  |
|  | Serverová část řešení bude nasazena ve formě virtuálních strojů (podpora a kompatibilní minimálně se stávajícím VMware vSphere, Microsoft Hyper-V). (zadavatel umožňuje nabídnout rovnocenné řešení) Virtuální stroje musí být možné, a ze strany výrobce podporované, provozovat v cloudu (podpora a kompatibilní minimálně se stávající Microsoft Azure) (zadavatel umožňuje nabídnout rovnocenné řešení). Řešení musí být možné nasadit také v hybridním režimu, kdy jeden nebo více virtuálních strojů je provozováno v místním datovém centru a další virtuální stroj nebo stroje v cloudu, formou SaaS. Minimálně jeden virtuální stroj však musí být provozován v místním datovém centru organizace zadavatele. |  |  |
|  | Řešení musí umožnovat definovat práva na činnosti ve správcovských nástrojích na základě členství v Active Directory skupinách. Řešení musí být schopno definovat různé úrovně administrátorských přístupů – delegování administrativních oprávnění – vytvořením kombinací (sad) oprávnění. |  |  |
|  | Řešení musí být integrováno a kompatibilní na jednu nebo více instancí adresářových služeb se stávající Microsoft Active Directory Directory Services (AD DS) (zadavatel umožňuje nabídnout rovnocenné řešení). Identita – uživatelský účet – uživatele dodaného řešení musí odpovídat identitě v AD DS. Změny v AD DS (změny stavu účtu, atributů, členství ve skupinách) musí být automaticky synchronizovány s dodaným řešením. Dodané řešení musí být možné integrovat na více samostatných AD DS bez nutnosti jejich propojení pomocí vztahů důvěryhodnosti (trustu), a dále musí být možné řešení integrovat na další adresářové (LDAP) služby jiných výrobců. |  |  |
|  | Komunikace mezi jednotlivými komponenty řešení v rámci HTTPS komunikace musí být šifrována TLS protokolem minimálně verze 1.2, uložená citlivá data - zejména přihlašovací údaje uživatelů - musí být chráněna FIPS 140-2 validovaným šifrováním AES 256. |  |  |
| **Více-faktorová autentizace** |
|  | Řešení musí umožňovat používání různých autentizačních předmětů pro více-faktorovou autentizaci, minimálně: kontaktní čipové karty (smart karty), bezkontaktní karty a předměty, bezkontaktní standard FIDO2 bezpečnostní karty a kontaktní FIDO2 USB klíče, USB tokeny, bezkontaktní RFID předměty, biometrické prvky (otisk prstu), login/heslo (s vazbou i bez vazby na adresářovou službu), a jejich vzájemné kombinace. Vyžádání druhého faktoru musí být možné definovat dynamicky, na základě splnění podmínky (např. uplynutí časového intervalu). |  |  |
|  | Řešení musí umožnit volbu parametrů autentizačního PIN kódu pro více-faktorové ověřování (podobně, jako u hesla kompatibilní ve stávající Active Directory) (zadavatel umožňuje nabídnout rovnocenné řešení). Délku PINu v rozmezí alespoň od 4 do alespoň 16 znaků, musí umožnit exspiraci PIN kódu po definovaném časovém intervalu, musí umožnit použití jak čistě numerického PINu, tak PINu obsahujícího čísla a písmena a speciální znaky. Řešení dále musí umožnit vynucení historie PINu a zamezit uživateli, aby si při obnově PINu zvolil dříve jím použitý PIN kód (je požadováno, aby si systém pamatoval alespoň 8 posledních PINů). Řešení musí volitelně umožnit vynutit nastavení, které uživateli zamezí nastavit si snadno uhodnutelný PIN (minimálně nedovolit opakování stejných po sobě jdoucích znaků, jako např. „1111“ a jednoduchou číselnou řadu, jako např. „1234“). |  |  |
|  | Řešení musí obsahovat technologii pro automatizaci přihlašovacího procesu, která uživateli umožní přihlášení do vzdálené plochy s využitím již zadaných přihlašovacích pověření, bez nutnosti opakovaně zadávat přihlašovací údaje, potvrzovat připojovací dialogy, znovu použít autentizační předmět, znovu zadávat PIN kód. |  |  |
|  | Řešení musí umožňovat režim redukovaného uživatelského rozhraní, tzv. "appliance mode", na tenkých klientech. V tomto režimu je běžné uživatelské rozhraní tenkého klienta nahrazeno přihlašovací obrazovkou pro více-faktorovou autentizaci. |  |  |
|  | Řešení musí umožnit nastavení různých kombinací přihlašovacích faktorů pomocí politik, a tyto politiky aplikovat na skupiny uživatelů, skupiny koncových zařízení, typy koncových zařízení s rozlišením minimálně: 1. koncová stanice kompatibilní se stávajícím OS MS Windows, 2. mobilní zařízení kompatibilní se stávajícím OS Android. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Řešení musí zajistit funkčnost více-faktorové autentizace pomocí bezkontaktních předmětů i v případě, kdy klientské zařízení není připojeno k síti (je offline) nebo není dostupná serverová strana řešení. |  |  |
|  | Řešení musí poskytnout funkce více-faktorové autentizace na koncových (klientských) zařízeních používaných jedním uživatelem, používaných více uživateli, a dále na sdílených koncových stanicích s častým střídáním uživatelů během pracovní doby. Řešení musí poskytnout funkce více-faktorové autentizace na koncovém (klientském) zařízení přihlášeném pomocí jmenného účtu, pomocí obecného (skupinového) Active Directory účtu a pomocí obecného (skupinového) lokálního účtu. Ve všech případech musí být více-faktorové ověření provedeno jménem konkrétního uživatele, tedy přihlašování musí být prováděno stávajícím uživatelským Active Directory účtem (zadavatel umožňuje nabídnout rovnocenné řešení) reprezentujícím konkrétní přihlašovanou osobu. Výše uvedené funkce musí být dostupné a kompatibilní také na koncových stanicích, které nejsou členy stávající Active Directory domény (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
| **Single Sign-On (SSO)** |
|  | Řešení musí poskytovat funkci automatického přihlášení SSO (Single Sign-On) alespoň do následujících stávajících aplikací:* Ginis, Czechpoint, IS pro provoz úřadu (MS Office365, Vita stavební úřad, Cevis docházkový systém od společnosti Ivar ID Poděbrady, s.r.o.) (zadavatel umožňuje nabídnout rovnocenné řešení). Zadavatel zajistí součinnost se stávajícími dodavateli.

V případě webových aplikací musí být pro funkci SSO podporovány a kompatibilní minimálně tyto stávající prohlížeče: Microsoft Edge Chromium verze 120 a vyšší, Google Chrome verze 120 a vyšší (zadavatel umožňuje nabídnout rovnocenné řešení). Dále musí být pro webové aplikace podporována autentizace pomocí protokolu standardu SAML a pomocí protokolu standardu OpenID Connect. |  |  |
|  | Řešení musí poskytovat funkci Single Sign-On do aplikací (popsaných v předchozím bodu) z koncových (klientských) zařízení používaných jedním uživatelem, používaných více uživateli, a dále na sdílených koncových stanicích s častým střídáním uživatelů v průběhu pracovní doby. Řešení musí poskytnout funkce SSO do aplikací (popsaných v předchozím bodu) na koncovém zařízení přihlášeném pomocí jmenného účtu, pomocí obecného (skupinového) stávajícího Active Directory účtu (zadavatel umožňuje nabídnout rovnocenné řešení) a pomocí obecného (skupinového) lokálního účtu. Ve všech případech musí být funkce SSO poskytovány jménem konkrétního uživatele, tedy přihlašování do aplikací musí být prováděno uživatelským účtem reprezentujícím konkrétní přihlašovanou osobu. Výše uvedené funkce musí být dostupné a kompatibilní také na koncových stanicích, které nejsou členy stávající Active Directory domény (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
|  | Řešení musí zajišťovat funkčnost SSO pro aplikace, jejichž klientská strana běží jak na fyzických stanicích, tak ve virtuální ploše – VDI, dále pro virtualizované aplikace a server vzdálené plochy. |  |  |
|  | Přihlašovací údaje do jednotlivých aplikací musí být dostupné jen příslušnému uživateli. Přihlašovací údaje do jednotlivých aplikací a systémů musí být šifrovány, a musí být ukládány na serverovou stranu řešení, aby byly dostupné na každé koncové stanici, ke které se uživatel přihlašuje. Systém musí umožnit, aby pro kritické aplikace bylo přihlášení pomocí SSO vynucováno. |  |  |
|  | Řešení musí umožnit kompatibilní funkci SSO přihlašování do aplikací jak identitou (účtem) ze stávající Active Directory (zadavatel umožňuje nabídnout rovnocenné řešení), tak účtem spravovaným danou aplikací. Řešení musí dále poskytovat funkcionalitu Identity Provider (IdP). |  |  |
|  | Řešení musí obsahovat integrovaný správce hesel (Password Manager) pro všechny uživatele, s možností uživatelské správy. IT správce musí mít možnost nastavit, zda uživatel může přihlašovací údaje editovat nebo jen zobrazit, a dále, zda může zobrazit heslo v čitelné podobě. Funkce zobrazení hesla v čitelné podobě musí být možné dodatečně zabezpečit (např. vyžádáním hesla, PINu apod.). |  |  |
|  | Řešení musí obsahovat grafické uživatelské rozhraní pro vytváření, editaci a správu Single Sign-On napojení (konektorů/profilů). Toto prostředí musí být intuitivní a uživatelsky přívětivé, bez nutnosti psát kód, programovat, používat řádkové příkazy a umožnit zadavateli vytvářet vlastní napojení (konektory/profily) na další aplikace uživatelsky, vlastními silami, bez nutnosti objednávání nových napojení u dodavatele a bez nutnosti úprav kódu těchto aplikací. |  |  |
| **Čtečky karet – 160 KS** |
|  | Požadované parametry stacionárních čteček bezkontaktních předmětů:* Pracovní frekvence: min. 13,56 MHz
* Podpora bezkontaktních karet/předmětů
* Rozhraní: připojitelná přes USB
* Typ: externí
* Napájení: přes USB rozhraní
* Formát: stolní
* Přenos dat: zabezpečený, přes API (nesmí simulovat klávesnici)
* Kompatibilita OS: stávající MS Windows 10 a vyšší. (zadavatel umožňuje nabídnout rovnocenné řešení)
 |  |  |
| **Autentizační předměty – 160KS** |
|  | Požadované parametry bezkontaktních předmětů:* Pracovní frekvence: min. 25 kHz a 13,56 MHz
* Formát: přívěšek (fob)
* Provedení: plastový, mechanicky odolný, možnost potisku nebo gravírování
 |  |  |
| **Implementace** |
|  | Instalace a konfigurace SW pro dvoufaktorovou autentizaci a SSO.Konfigurace přístupu uživatelů.Pilotní ověření a ostré nasazení. |  |  |

## Opatření ID 4 (§ 23 VyKB) – Detekce kybernetických bezpečnostních událostí

Tabulka 8: Detekce kybernetických bezpečnostních událostí

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
| **Funkční specifikace** |
| **Základní technické požadavky** |
|  | Nástroj pro bezpečnostní analýzu logů z NGFW zařízení se schopností jejich korelace včetně možnosti ukládání logů. |  |  |
|  | Podpora analýzy logů s využitím Indicators of Compromise, případná licence pro takovou funkci musí být součástí nabídky. |  |  |
|  | Podpora automatizace reakcí na bezpečnostní události detekované nabízeným řešením směrem k NGFW zařízení přímo v grafickém rozhraní nabízeného řešení včetně potřebné licence pro takovou funkci. |  |  |
|  | Virtuální appliance kompatibilní pro stávající platformu zadavatele VMWare, MS Microsoft Hyper-V a KVM (fyzické zařízení) (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
|  | Možnost nativní integrace s poptávaným zařízením typu NGFW, které bude sloužit jako zdroj dat pro analýzu (zařízení NGFW je poptáváno samostatně). |  |  |
|  | Kapacita úložiště logů je alespoň 5TB a minimální limit pro množství přijatých logů za jeden den je alespoň 10GB. |  |  |
|  | Možnost zvýšení denní kapacity analyzovaných logů nad 10GB za den pomocí licence. |  |  |
|  | Minimálně 4x vNIC. |  |  |
|  | Možnost provozovat poptávané řešení jakou prosté uložiště logů bez jejich další analýzy z dalších zařízení zákazníka. |  |  |
|  | Možnost tvorby komplexních reportů (Top X uživatelů/zařízení dle množství zjištěných hrozeb, přeneseného provozu atd.) nad analyzovanými daty z grafického rozhraní poptávaného nástroje. |  |  |
|  | Možnost generovat reporty na základě specifikace dotazů do databáze logů poptávaného řešení. |  |  |
|  | Formát generovaných reportů je HTML/CSV/XML/PDF s možností plánování pravidelné automatické tvorby reportů. |  |  |
|  | Možnost logické segmentace poptávaného nástroje s možností izolace jednotlivých segmentů z hlediska jejich administrace a zdroje dat. |  |  |
|  | Poptávané řešení obsahuje předdefinované vzory možných reportů a umožňuje upravit vzhled generovaných reportů prvky zákazníka (loga, hlavička) |  |  |
|  | Možnost zobrazení aktuálních logů z jednotlivých integrvaných NGFW zařízení v reálném čase |  |  |
|  | Možnost zpětného zobrazení a analýzy logů až 7 dnů zpět z důvodu možnosti zpětné analýzy provozu a možných uskutečněných bezpečnostních hrozeb |  |  |
| **Požadavky na management** |
|  | Plnohodnotná správa pomocí grafického rozhraní a CLI |  |  |
|  | Podpora SNMPv2 a SNMPv3 a REST API |  |  |
|  | Samostatná sekce v grafickém rozhraní pro zobrazní zjištěných hrozeb |  |  |
|  | Možnost šifrování přenášené komunikace mezi poptávaným řešením pro analýzu dat a poptávaným NGFW zařízením |  |  |
|  | Podpora výrobce v režimu 24x7 na systém i konfiguraci je součástí nabídky. |  |  |

## Opatření ID 5 (§ 25 VyKB) – Aplikační bezpečnost

Tabulka 9: Webový aplikační firewall

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
| **Základní technické požadavky** |
|  | Zařízení typu WAF (zařízení typu NGFW s integrovanou funkcí WAF není akceptovatelné). |  |  |
|  | Virtuální zařízení pro stávající virtualizační platformy VMWare, Hyper-V a KVM (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
|  | Podpora alespoň 2x vCPU spolu s případnou licencí pro počet vCPU. |  |  |
|  | Licenčně neomezená možnost přidělení paměti RAM. |  |  |
|  | Alespoň 10x virtuální síťové rozhraní. |  |  |
|  | Propustnost plnohodnotné WAF inspekce nad protokolem HTTP min. 100Mbps (výkonová hodnota musí být doložena oficiálním produktovým listem výrobce). |  |  |
|  | licenčně neomezená podpora režimu vysoké dostupnosti active/passive a active/active. |  |  |
|  | Podpora funkce synchronizace konfigurace mezi dvěma samostatnými WAF prvky v režimu vysoké dostupnosti. |  |  |
|  | Licenčně neomezený počet chráněných serverů a aplikací. |  |  |
|  | Podpora HTTP v1.0, v1.1 a TLS v1.0 - 1.3 |  |  |
|  | Nativní podpora HTTP/2. |  |  |
|  | Integrovaný průvodce/wizzard pro nejčastější typy konfigurací. |  |  |
| **Bezpečnostní funkce** |
|  | Požadujeme podporu následujících režimů nasazení WAF: Reverse proxy, Transparentní režim, Transparentní proxy režim (řešení je schopné filtrovat i modifikovat provoz v transparentním režimu nasazení) a pasivní režim (konfigurace na SPAN portu switche), WCCP. |  |  |
|  | Ochrana před OWASP TOP10 hrozbami. |  |  |
|  | Validace protokolu http (dle RFC). |  |  |
|  | Podpora funkce strojového učení (machine learning) - dvoúrovňová detekce anomálií a hrozeb za pomoci databáze vzorků výrobce a za pomoci strojového učení. |  |  |
|  | Podpora funkce ochrany API rozhraní s podporou schémat OpenAPI, XML a JSON. |  |  |
|  | Ochrana před klasickými typy útoků na web aplikace (XSS, SQL injection, Cross site request forgery, session hijacking, cookie poisoning, …). |  |  |
|  | Signatury pro ochranu před útoky na známé webové aplikace. |  |  |
|  | Ochrana před útoky typu brute-force. |  |  |
|  | Ochrana před útoky na OS & webserver. |  |  |
|  | Ochrana před útoky typu L7 DoS/DDoS. |  |  |
|  | Podpora geolokační databáze, automaticky aktualizované výrobcem. |  |  |
|  | Podpora reputační DB pro IP adresy. |  |  |
|  | Rozpoznání a ochrana před přístupem automatizovaných klientů/nástrojů (skenery, crawlery, skripty, …) včetně využití funkce strojového učení. |  |  |
|  | Funkce user tracking & scoring (uživatel je identifikován, jeho chování je následně dlouhodobě sledováno a je mu dynamicky upravována reputace na základě reálného chování. Při překročení hraničních hodnot je provedena předdefinovaná akce.). |  |  |
|  | Pokročilá ochrana před false positive IPS alerty pomocí ML s automatickým a opakovaným učením se na provozu. |  |  |
|  | Syntax based detection (signatura popisující útok je kombinována s inteligentní analýzou specifického/nestandardního chování s cílem minimalizovat množství false positives např. u SQL injection). |  |  |
|  | Antivirová/antimalware kontrola (kontrola uploadovaných souborů). |  |  |
|  | AV kontrola integrovaná do WAF appliance (nikoliv jako externí zařízení/služba). |  |  |
|  | Ochrana před škodlivým kódem (malware, ransomware, trojské koně, atp.) včetně ochrany před polymorfním kódem. |  |  |
|  | Signaturová databáze udržovan výrobcem a automaticky aktualizovaná. |  |  |
|  | Plná integrace s platformou sandbox pro ochranu před pokročilým malware, která bude s WAF plně funkčně integrovaná (řešení SandBox není součástí řešení). |  |  |
|  | Předdefinované politiky pro nejznámější aplikace (MS Exchange, MS SharePoint, OWA, WordPress). |  |  |
|  | Všechny signatury udržované výrobcem a automaticky aktualizované. |  |  |
|  | Ochrana proti únikům dat – DLP. |  |  |
|  | Detekce použití kompromitovaných přístupových údajů a zabránění autentizace takovými přístupovými údaji. |  |  |
|  | Možnost využití Cloud SandBox prostředí výrobce WAF pro analýzu přenášeného provozu. |  |  |
|  | Ochrana API. |  |  |
| **Požadavky na autentizační mechanismy** |
|  | Podpora autentizace klientským SSL certifikátem. |  |  |
|  | Podpora dvoufaktorové autentizace (radius access-challenge response). |  |  |
|  | LDAP, RADIUS, SAML, Kerberos, HTTP Basic. |  |  |
|  | Podpora SSO (single sign on) pomocí Kerberos a HTTP Basic / HTML Form. |  |  |
| **Síťové funkce** |
|  | Podpora IPv4 i IPv6. |  |  |
|  | Požadované algoritmy pro L7 load balancing: Round Robin, Weighted Round Robin, Least Connection, URI hash, Host hash, Domain hash, Source IP hash. |  |  |
|  | Požadované metody pro LB persistence: Source IP, http header, URL parameter, Insert cookie, Rewrite cookie, Persistent cookie, Session ID (ASP, PHP, JSP, SSL). |  |  |
|  | Požadované metody pro kontrolu stavu serverů (healthcheck metody): ICMP Ping, TCP, TCP half open, TCP SSL, HTTP, HTTPS. |  |  |
|  | URL rewriting. |  |  |
|  | Content routing. |  |  |
|  | HTTPS offloading, HTTPS inspekce. |  |  |
|  | Komprese HTTP. |  |  |
|  | Object caching. |  |  |
| **Skenování zranitelností** |
|  | Vulnerability scanner integrovaný do WAF appliance (možnost interní bezpečnostní kontroly vlastních web aplikací). |  |  |
|  | Výstup ve formátu PDF. |  |  |
|  | Definice automaticky aktualizované výrobcem. |  |  |
|  | Možnost automatického importu výsledků auditu pomocí externích nástrojů a následné automatické tvorby bezpečnostní politiky (tzv. virtual patching). |  |  |
|  | Minimální podpora těchto nástrojů: Acunetix, HP WebInspect, IBM AppScan, Qualys. |  |  |
| **Požadavky na management** |
|  | Plnohodnotná správa pomocí grafického rozhraní a CLI. |  |  |
|  | Management rozhraní provozované přímo na bezpečnostním prvku (bez nutnosti instalovat samostatný management server). |  |  |
|  | Správa pomocí web browseru, bez nutnosti instalovat management aplikaci. |  |  |
|  | Podpora SNMP včetně MIB souboru dodávaného výrobcem. |  |  |
|  | Virtualizace na úrovni mgmt rozhraní (možnost omezit přístup administrátorů pouze na vybraná pravidla resp. chráněné servery). |  |  |
|  | Podpora výrobce v režimu 24x7 na systém i konfiguraci je součástí nabídky. |  |  |

## Implementace

Tabulka 10: Požadavky – Implementace nabízeného řešení

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota**  | **Splněno [ano/ne]** |
|  | Součástí je zajištění instalace a konfigurace předmětu veřejné zakázky v návaznosti na stávající infrastrukturu zadavatele (tj. včetně dopravy, montáže, instalace a implementace do stávající IT infrastruktury) v sídle zadavatele. |  |  |
|  | Účastník zajistí:* instalace zařízení do standardní RACK skříně 19“ 42U,
* implementace Best Practice scénářů pro dané konfigurace,
* kontroly kompatibility verzí ovladačů a firmware jednotlivých zařízení a jejich aktualizace,
* registrace záruk u výrobců,
* umístění do racku a zapojení kabeláže vč. jejího označení,
* inicializace a konfigurace všech dodaných zařízení,
* nastavení IP adres,
* nastavení vysoké dostupnosti,
* zapojení do stávající LAN.
 |  |  |
|  | Účastník do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění předmětu veřejné zakázky jako logického a funkčního celku. |  |  |
|  | Součástí instalace musí být i zaškolení administrátorů (správců) – 3 osoby minimálně v rozsahu nutném pro samostatnou administraci předmětu zakázky. Administrací se rozumí zejména: konfigurace, monitoring činnosti, aktualizace, řešení problémů, zálohování konfigurace. Trvání zaškolení administrátorů je minimálně 40 hodin pro každého administrátora v sídle zadavatele. |  |  |
|  | Konzultační práce pro předmět veřejné zakázky v minimálním rozsahu 48 hodin, poskytnuté do konce realizace.  |  |  |
|  | Testování implementovaného předmětu veřejné zakázky na zkušebních datech. |  |  |
|  | Zahájení ostrého provozu (převedení předmětu veřejné zakázky do produkčního prostředí). |  |  |
|  | Vypracování a předání dokumentace popisující konečný skutečný stav předmětu veřejné zakázky.Dokumentace bude zahrnovat:* popis všech prvků/zařízení,
* popis způsobu zálohy a obnovy konfigurace všech prvků/zařízení
* veškeré požadavky na zachování záruky/podpory (např. kompatibilita)
* informaci o způsobu řešení servisních požadavků.
 |  |  |

# Část 2. – Specifikace požadavků řešení

V následujících podkapitolách je uvedena specifikace parametrů řešení nutných pro plnění této veřejné zakázky.

V době posuzování nabídek musí nabídka řešení účastníka dále splňovat níže specifikované požadavky.

Účastník nakopíruje do nabídky následující tabulku a popis splnění požadavků ve sloupci **„Účastníkem nabízená hodnota, výrobce a typ.“**, tak že tam nakopíruje text ze sloupce „Specifikace požadavků“ a **doplní výrobce a typ**, případně doplní nebo upraví popis nabízené hodnoty, ze kterého bude patrné, že splňuje požadavky.

Sloupec „Specifikace požadavků“ nesmí být účastníkem nijak měněn a účastník je oprávněn vyplnit pouze sloupec „Účastníkem nabízená hodnota, výrobce a typ.“.

Sloupec **„Splněno [ano/ne]“** účastník nevyplňuje, slouží pro zadavatele.

## Opatření ID 3 (§ 21 VyKB) – Ochrana před škodlivým kódem

### Centrální správa ochrany před škodlivým kódem

Tabulka 11: Centrální správa ochrany před škodlivým kódem

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Webová konzole.  |  |  |
|  | Možnost instalace a kompatibilní na stávající MS Windows i Linux.  |  |  |
|  | Předpřipravená virtual appliance kompatibilní pro stávající virtuální prostředí VMware, Microsoft Hyper-V a Microsoft Azure, Oracle Virtual Box. (zadavatel umožňuje nabídnout rovnocenné řešení)  |  |  |
|  | Server/proxy architektura pro síťovou pružnost – snížení zátěže při stahování aktualizací detekčních modulů výrobce.  |  |  |
|  | Možnost probuzení klientů pomocí Wake On Lan.  |  |  |
|  | Možnost konfigurace virtual appliance přes uživatelsky přívětivé webové rozhraní Webmin.  |  |  |
|  | Nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta. |  |  |
|  | Offline uplatňování politik a spouštění úloh při výskytu definované události (odpojení od sítě při nalezení škodlivého kódu).  |  |  |
|  | Administrace v nejpoužívanějších jazycích včetně češtiny. |  |  |
|  | Široké možnosti konfigurace oprávnění administrátorů (možnost správy pouze části infrastruktury, které konkrétnímu administrátorovi podléhá).  |  |  |
|  | Zabezpečení přístupu administrátorů do vzdálené správy pomocí 2FA.  |  |  |
|  | Informace o aktuálně přihlášených uživatelích na daném zařízení. |  |  |
|  | Podpora štítků/tagování pro snazší správu a vyhledávání. |  |  |
|  | Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce.  |  |  |
|  | Vzdálené získání zachyceného škodlivého souboru z klienta.  |  |  |
|  | Detekce nespravovaných (rizikových) počítačů komunikujících na síti.  |  |  |
|  | Instalace a odinstalace aplikací 3. stran.  |  |  |
|  | Vyčítání informací o verzích softwaru 3. stran.  |  |  |
|  | Možnost vyčítat informace o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty…).  |  |  |
|  | Odeslání zprávy na počítač / mobilní zařízení, které se následně zobrazí uživateli na obrazovce.  |  |  |
|  | Vzdálená odinstalace antivirového řešení 3. strany.  |  |  |
|  | Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku.  |  |  |
|  | Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny a automatickému uplatnění klientské úlohy  |  |  |
|  | Dynamické skupiny musí umět fungovat i v konkrétních časových slotech a uplatňovat podporované klientské úlohy |  |  |
|  | Automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů (například: 5 % všech počítačů / 50 klientů hlásí problémy).  |  |  |
|  | Podpora SNMP Trap, Syslogu a SIEM.  |  |  |
|  | Podpora instalace skriptem - \*.bat, \*.sh, \*.ini (GPO, SSCM…).  |  |  |
|  | Rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu.  |  |  |
|  | Reportování stavu klientů chráněných jinými bezpečnostními programy.  |  |  |
|  | Schopnost zaslat reporty a upozornění na e-mail.  |  |  |
|  | Řešení umožňuje odesílat notifikace o vybraných událostech prostřednictvím tzv. webhooků |  |  |
|  | Možnost integrace s řešením třetích stran podporující MDM funkcionalitu. |  |  |
|  | Možnost definice kontrolního součtu ve formátu SHA256. |  |  |
|  | Možnost řízení managementu konzole a jeho komponent prostřednictvím API pro:* Centrální správu samotnou.
* Komponenty antimalware řešení, jeho správy, politik a nastavení.
* EDR řešení.
 |  |  |
|  | Možnost exportu informací o detekcích, incidentech |  |  |
|  | Možnost úpravy detekčních pravidel EDR správy zařízení a jeho nastavení, instalačních balíčků, včetně možnosti automatizace jednotlivých úkonů. |  |  |
|  | Přidání zařízení do vzdálené správy pomocí:* synchronizace kompatibilní se stávající Active Directory (jedné nebo více Active Directory), včetně možnosti synchronizace počítačů a uživatelů,
* ruční přidání pomocí dle IP adresy nebo názvu zařízení,
* o pomocí síťového skenu nechráněných zařízení v síti.
 |  |  |

### Antivirus nové generace EDR pro klienty – 160 ks a pro servery – 20 ks

Tabulka 12: Antivirus nové generace EDR pro klienty – 160 ks a pro servery – 20 ks

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Instalátor pro podporované koncové body (PC) kompatibilní se stávajícím OS: MS Windows, Linux, MacOS, Android, vše v českém jazyce. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Instalátor pro stávající serverové platformy kompatibilní s OS: MS Windows server 2016 a vyšší, běžné unixové distribuce, v souladu s Filesystem Hierarchy Standard (FHS) - Ubuntu, Redhat, SUSe. Vše v českém jazyce. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  |  Antimalware, antiransomware, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb.  |  |  |
|  | Personální firewall pro zabránění neautorizovanému přístupu k zařízení se schopností automatického přebrání pravidel kompatibilní se stávající bránou MS Windows Firewall.  |  |  |
|  | Modul pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory.  |  |  |
|  | Ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému  |  |  |
|  | Aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb.  |  |  |
|  | Systém pro blokaci exploitů zneužívajících zero-day zranitelností, jenž pokrývá nejpoužívanější vektory útoku: * síťové protokoly,
* kompatibilní se stávající Flash Player,
* kompatibilní se stávající Java,
* kompatibilní se stávající Microsoft Office,
* webové prohlížeče,
* e-mailové klienty,
* PDF čtečky

(zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Systém pro detekci malwaru již na síťové úrovni poskytující ochranu i před zneužitím zranitelností na síťové vrstvě.  |  |  |
|  | Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS…).  |  |  |
|  | Anti-phishing se schopností detekce homoglyph útoků.  |  |  |
|  | Kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování.  |  |  |
|  | Cloud kontrola souborů pro urychlení skenování fungující na základě reputace souborů.  |  |  |
|  | Kontrola souborů v průběhu stahování pro snížení celkového času kontroly.  |  |  |
|  | Kontrola souborů při zapisování na disku a extrahování archivačních souborů. |  |  |
|  | Detekce s využitím strojového učení.  |  |  |
|  | Funkce ochrany proti zapojení do botnetu pracující s detekcí síťových signatur.  |  |  |
|  | Ochrana před síťovými útoky skenující síťovou komunikaci a blokující pokusy o zneužití zranitelností na síťové úrovni.  |  |  |
|  | Kontrola s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací.  |  |  |
|  | Lokální sandbox. |  |  |
|  | Modul behaviorální analýzy pro detekce chování nových typů ransomwaru. |  |  |
|  | Systém reputace pro získání informací o závadnosti souborů a URL adres.  |  |  |
|  | Cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur.  |  |  |
|  | Technologie pro detekci rootktitů obvykle se maskujících za součásti operačního systému.  |  |  |
|  | Skener firmwaru BIOSu a UEFI.  |  |  |
|  | Skenování souborů v cloudu OneDrive.  |  |  |
|  | Podpora odečítače obrazovky pro zrakově postižené. |  |  |
|  | Funkcionalita kompatibilní pro stávající klienty MS Windows – Antimalware, Antispyware, Personal Firewall, Personal IPS, Application control, Device control, Security Memory (zabraňuje útokům na běžící aplikace), kontrola integrity systémových komponent. (zadavatel umožňuje nabídnout rovnocenné řešení)  |  |  |
|  | Funkcionalita kompatibilní pro stávající klienty MacOS – Personal Firewall, Device control, autoupgrade. |  |  |
|  | Možnost aplikování bezpečnostních politik i v offline režimu na základě definovaných podmínek. |  |  |
|  | Ochrana proti pokročilým hrozbám (APT) a 0-day zranitelnostem. |  |  |
|  | Podpora automatického vytváření dump souborů na stanici na základě nálezů. |  |  |
|  | Okamžité blokování/mazání napadených souborů na stanici (s možností stažení administrátorem k další analýze). |  |  |
|  | Duální aktualizační profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (pro cestující uživatele s notebooky). |  |  |
|  | Možnost definovat webové stránky, které se spustí v chráněném režimu prohlížeče, pro bezpečnou práci s kritickými systémy nebo internetovým bankovnictví |  |  |
|  | Aktivní ochrany před útoky hrubou silou na protokol SMB a RDP. |  |  |
|  | Možnost zablokování konkrétní IP adresy po sérii neúspěšných pokusů o přihlášení pro protokoly SMB a RDP s možností výjimek ve vnitřních sítích. |  |  |
| **Integrovaná cloudová analýza neznámých vzorků** |
|  | Funkce cloudového sandboxu je integrována do produktu pro koncové a serverové zařízení, tzn. Cloudový sandbox nemá vlastního agenta, nevyžaduje instalaci další komponenty ať už v rámci produktu nebo implementace HW prvku do sítě. |  |  |
|  | Sandbox umožňující spuštění vzorků malwaru kompatibilní pro stávající OS MS Windows, Linux.(zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Možnost využití na koncových bodech a serverech pro aktivní detekci škodlivých souborů. |  |  |
|  | Analýza neznámých vzorků v řádu jednotek minut. |  |  |
|  | Reporty poskytují i nízkoúrovňové informace o vzorku - informace o konkrétním problematickém chování, detailní informace o procesech, API. |  |  |
|  | Optimalizace pro znemožnění obejití anti-sandbox mechanismy. |  |  |
|  | Schopnost analýzy rootkitů a ransomwaru. |  |  |
|  | Schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti. |  |  |
|  | Řešení pracuje s behaviorální analýzou. |  |  |
|  | Kompletní výsledek o zanalyzovaném souboru včetně informace o nalezeném i nenalezeném škodlivém chování daného souboru. |  |  |
|  | Manuální odeslání vzorku do sandboxu. |  |  |
|  | Možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu. |  |  |
|  | Neomezené množství odesílaných souborů. |  |  |
|  | Veškerá komunikace probíhá šifrovaným kanálem. |  |  |
|  | Okamžité odstranění souboru po dokončení analýzy v cloudovém sandboxu. |  |  |
|  | Možnost volby, jaké kategorie souborů do cloudového sandboxu budou odcházet (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty atp.). |  |  |
|  | Velikost odeslaných souborů do cloudového sandboxu může dosahovat až 64MB. |  |  |
| **Šifrování celých disků** |
|  | Podpora kompatibilní se stávajícími platformami MS Windows a MacOS. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Správa skrze centrální management. |  |  |
|  | Technologie kompatibilní se stávající platformou MS Windows a MasOS. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Podpora Pre-Boot autentizace. |  |  |
|  | Podpora TMP modulu. |  |  |
|  | Podpora Opal samošifrovacích disků. |  |  |
|  | Možnost definovat počet chybně zadaných pokusů. |  |  |
|  | Možnost definovat složitost a délku autentizačního hesla. |  |  |
|  | Možnost omezit platnost autentizačního hesla. |  |  |
|  | Podpora okamžitého smazání šifrovacího klíče a následné uzamčení počítače. |  |  |
|  | Recovery z centrální konzole. |  |  |
| **EDR řešení** |
|  | Možnost provozu centrálního serveru on-premise na stávající platformě kompatibilní s MS Windows Server. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Možnost provozu kompatibilní se stávajícími databázemi: MS SQL a MySQL.(zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Možnost provozu v offline prostředí.  |  |  |
|  | Možnost logování činností administrátora  |  |  |
|  | Podpora EDR agenta kompatibilní pro stávající prostředí MS Windows, MS Windows server, macOS a linuxové distribuce. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Možnost autentizace do managementu EDR pomocí 2FA. |  |  |
|  | Možnost řízení managementu EDR a EDR agentů prostřednictvím API, a to jak pro:* Přijímání informací z EDR serverů/agentů.
* Zasílání příkazů na EDR servery/agenty.
 |  |  |
|  | EDR řešení podporuje vzdálené pouštění příkazů přímo z EDR konzole. U jednotlivých stávajících OS požadujeme plnou podporu funkcionalit kompatibilní s: Powershell u OS MS Windows (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Vzdálené spouštění příkazů umožňuje vynucení 2FA ověření daného uživatele. |  |  |
|  | Možnost izolace zařízení od sítě prostřednictvím EDR agenta přímo z konzole. |  |  |
|  | Možnost tvorby vlastních IoC.  |  |  |
|  | Možnost škálování množství historických dat vyhodnocených v EDR, až 3 měsíce pro raw-data, 3 roky pro detekované incidenty. |  |  |
|  | Možnost aktivovat „učící režim“ pro automatizované vytváření výjimek k detekčním pravidlům. |  |  |
|  | Indikátory útoku pracující s behaviorální detekcí.  |  |  |
|  | Indikátory útoku pracující s reputací.  |  |  |
|  | Řešení umožnuje analýzu vektorů útoku. Schopnost detekce:* škodlivých spustitelných souborů,
* skriptů,
* exploitů,
* rootkitů,
* síťových útoků,
* zneužití WMI nástrojů,
* bezsouborového malwaru.
* pokusů o dumpování přihlašovacích údajů uživatele.
 |  |  |
|  | Schopnost detekovat laterální pohyb útočníka.  |  |  |
|  | Schopnost ukončit infikovaný proces.  |  |  |
|  | Možnost ruční analýzy procesů veškerých spustitelných souborů a DLL knihoven.  |  |  |
|  | Možnost náhledu na spuštěné skripty použitých v daném incidentu. |  |  |
|  | Možnost zabezpečeného vzdáleného spojení přes servery výrobce do konzole EDR. |  |  |
|  | Možnost vytváření automatizovaného response úkonu v podobě izolace stanice, blokace konkrétní hash, odhlášení uživatele, restartování počítače pro jednotlivá detekční pravidla. |  |  |
|  | Možnost automatického vyřešení incidentu definovaných administrátorem. |  |  |
|  | Schopnost prioritizace vzniklých incidentů.  |  |  |
|  | Schopnost stažení problémového souboru.  |  |  |
|  | Schopnost zobrazení detekcí provedených antimalware produktem.  |  |  |
|  | Řešení je schopno generovat tzv. forest / full execution tree model.  |  |  |
|  | Možnost vyhledávání pomocí nově vytvořených IoC nad historickými daty.  |  |  |
|  | Provázání s technikami popsanými v knowledge base MITRE ATT&CK. |  |  |
|  | Řešení umožňuje fungovat v offline režimu, a to konkrétně jeho detekční pravidla + předem definované komplexnější incidenty/set detekčních pravidel po sobě jdoucích.  |  |  |
|  | Průběžně aktualizovaná detekční pravidla EDR systému bez nutnosti aktualizace centrální správy/klienta. |  |  |
|  | Možnost definice vlastních komplexních "incidentů" spojující v chronologickém pořadí detekci vybraných událostí. |  |  |
|  | Pokročilý detekční mechanismy pro detekci útoku i při nedostupnosti cloudového/centrálního detekčního mozku výrobce. |  |  |
|  | Možnost exportu raw dat (veškerých dat) na externí úložiště. |  |  |
|  | Možnost definice kontrolního součtu ve formátu SHA256. |  |  |
|  | Možnost filtrování určitého typu dat zpracovávaného a odesílaného z klientské stanice/server do centrální správy. |  |  |
|  | U detekčních pravidel možnost definovat jako automatickou součást pravidla/remediace odeslat soubor na analýzu do cloudového sandboxu výrobce. |  |  |
| **Multi-faktorová autentizace** |
|  | Klientská část:* Doručení OTP:
* aplikací v mobilním zařízení,
* e-mailem,
* bezpečnostním tokenem,
* SMS zprávou,
* Možnost konfigurace vlastní SMS bránu pro doručení OTP kódu
* vlastní aplikací.
* Další možnosti ověření:
* FIDO
* Push Authnetication
* Aplikace výrobce s podporou Push-Notifications kompatibilní pro stávající platformy:
* iOS
* Android
* watchOS, wear OS
* (zadavatel umožňuje nabídnout rovnocenné řešení)
* Požadavky na aplikaci výrobce:
* Mobilní aplikace v češtině.
* Přístup do mobilní aplikace ochráněn PINem / biometrikou.
* Možnost generovat OTP v off-line prostředí (bez internetové připojení, bez GSM spojení)
* Další požadavky
* Hardwarové tokeny HOTP splňující standard OATH.
* Hardwarové tokeny certifikované výrobcem.
* Kompletně softwarové řešení – bez nutnosti nákupu dalšího hardwaru.
* Podpora time based hardwarových tokenů (PSKC)
* Self-enrollment uživatelů.
 |  |  |
|  | Chráněné služby:* Přihlášení kompatibilní pro stávající webové aplikace společnosti Microsoft (OWA, SharePoint).
* Přihlášení přes RDP.
* kompatibilní se stávajícím Exchange Control Panel & Exchange Administrator Center. (zadavatel umožňuje nabídnout rovnocenné řešení)
* kompatibilní se stávajícím VMware Horizon View. (zadavatel umožňuje nabídnout rovnocenné řešení)
* kompatibilní se stávajícím Citrix XenApp. (zadavatel umožňuje nabídnout rovnocenné řešení)
* VPN služby využívajících protokol RADIUS.
* kompatibilní se stávajícími cloudovými službami Office 365, G Suite, identity providerů (podpora SAML protokolu, podpora AD FS)
* kompatibilní se stávajícím lokálním přihlášením do MS Windows, Linux, macOS účtů.
* Vyžádání 2FA v nouzovém režimu kompatibilní se stávajícím MS Windows.
* Vyžádání 2FA při vyvolání UAC dialogu kompatibilní se stávajícím MS Windows.
* Vyžádání 2FA při uzamčeném účtu.
 |  |  |
|  | Požadavky na správu řešení:* Webové konzole provozována v cloudu výrobce.
* Přístup do konzole lze chránit 2FA ověřením.
* Podpora multitenantního provozu (možnost spravovat vícero uživatelských struktur v jedné konzoli).
* Podpora synchronizace uživatelských účtů kompatibilní se stávající Active Directory. (zadavatel umožňuje nabídnout rovnocenné řešení)
* Možnost tvorby výjimek pro vnitřní sítě, kde není 2FA vyžadováno.
* Umožnit uživatelům přihlášení bez použití 2FA pro vybrané služby.
* Konzole umožňuje generovat Master recovery klíče pro konkrétní chráněné služby.
* Centrální správa a přidělování hardwarových tokenů jednotlivým uživatelům.
* Možnost reportování o úspěšných/ neúspěšných přihlášení uživatelů, způsobu použité autentizace (SMS, Push, OTP).
 |  |  |
|  | Možnost implementace 2FA do vlastních systémů pomocí:* API
* SDK výrobce
 |  |  |
|  | Další požadavky na řešení:* Soulad s:
	+ ISO27001 Standard,
	+ PCI/DSS - The Payment Card Industry Data Security Standard,
	+ ISAE 3402 – International Standards for Assurance Engagements no. 3402,
	+ HIPAA - Health Insurance Portability and Accountability Act,
	+ FFIEC - Federal Financial Institutions Examination Council compliances,
* Možnost definovat maximální počet offline přihlášení.
* Technická podpora v češtině.
* Technická podpora zdarma 8/5 poskytující pomoc na telefonu / přes e-mail / vzdáleně.
* Možnost dokoupení technické podpory 24/7.
 |  |  |
| **Ochrana kompatibilní se stávajícími poštovními servery MS Exchange** (zadavatel umožňuje nabídnout rovnocenné řešení) |
|  | Společná víceúrovňová ochrana celého serveru - databáze schránek, transportu zpráv i souborového systému serveru. |  |  |
|  | Podpora kompatibilní se stávajícími MS Exchange 2013 a 2016, 2019. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Antivirus, antispyware a antispoofing technologie. |  |  |
|  | Antispam s funkcí graylisting. |  |  |
|  | Blokace nevyžádané pošty a phishingu bez potřeby manuálně upravovat SCL (Spam Confidenace Level) hodnoty. |  |  |
|  | Možnost vytváření vlastních pokročilých antispamových pravidel (vyhodnocení více podmínek v jenom pravidlu). |  |  |
|  | Kontrola jednotlivých MBX databází, případně konkrétní schránky uživatele. |  |  |
|  | Umožnit uživateli poštovní schránky pracovat pomocí samostatného prohlížeče se spamovými a potenciálně infikovanými zprávami, které nebyly doručeny do emailové schránky. |  |  |
|  | Možnost vlastních pravidel s vlastním hodnocením obsahu. |  |  |
|  | Podpora více serverového prostředí zajištění P2P komunikací, např. Ve skupině DAG. |  |  |
|  | Detekce škodlivých souborů v reálném čase. |  |  |
|  | Možnost správy přes příkazovou řádku (Podpora edice Windows Server Core). |  |  |
|  | Komplexní protokoly blokovaného spamu a zobrazení greylistingovaných odesílatelů …protokoly všech zpráv, nejen blokovaných. |  |  |
|  | Sledování výkonu serveru v reálném čase. |  |  |
|  | Možnosti pro nastavení pravidel inspekce souborů - mazání spustitelných souborů, skriptů. |  |  |
|  | Cloudová reputační služba pro kontrolu příloh emailových zpráv. |  |  |
|  | Možnost spravovat ochranu kompatibilní se stávajícím Exchange Serveru samostatně nebo prostřednictvím management konzole v cloudu. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Možnost exportu protokolu událostí produktu do protokolu operačního systému. |  |  |
|  | Tvorba pravidla "Z hlavičky" a vyhodnocovat pole From: pro přesnější detekci podvržených e-mailů. |  |  |
|  | Backscatter ochrana. |  |  |
|  | Synchronizace lokální karantény zpráv napříč uzly clusteru. |  |  |
|  | Podpora hybridního prostředí s možností kontroly poštovních schránek kompatibilní se stávajícím MS Office 365. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Možnost zasílání přehledů o zachycených e-mailových hrozbách koncovým uživatelům. |  |  |
|  | Možnost zabezpečit heslem ochranu poštovního serveru a jeho komponent proti náhodné či chtěné modifikaci neautorizovaného uživatele. |  |  |
|  | Možnost zabezpečení heslem musí být možné přes konzoli dočasně deaktivovat pro vybrané uživatele na základě ověření administrátora vůči doméně. |  |  |
|  | Správa karantény prostřednictvím webového portálu pro vybrané uživatele i administrátory. |  |  |
|  | Ochrana nastavení dodatečným heslem před neoprávněnou změnou konfigurace produktu. |  |  |
|  | Možnost editovat zasílané zprávy o stavu karantény a zachycených souborů v karanténě (editace těla emailu, předmětu a odkazu na blokovaný e-mail). |  |  |
|  | Technologie cloudového sandboxu musí umožňovat:* Funkce cloudového sandboxu je integrována do produktu pro e-mailovou ochranu kompatibilní se stávajícím MS Exchange, tzn. Cloudový sandbox nemá vlastního agenta, nevyžaduje instalaci další komponenty ať už v rámci produktu nebo implementace HW prvku do sítě. (zadavatel umožňuje nabídnout rovnocenné řešení)
* Data odesílané v rámci cloudového sandboxu jsou zpracovávány v rámci EU.
* Sandbox umožňující spuštění vzorků malwaru kompatibilní se stávajícími OS:
	+ MS Windows,
	+ macOS,
	+ Linux

(zadavatel umožňuje nabídnout rovnocenné řešení)* Možnost využití na koncových bodech a stávající MS Exchange serveru pro aktivní detekci škodlivých souborů v e-mailech.
* Analýza neznámých vzorků v řádu jednotek minut.
* Optimalizace pro znemožnění obejití anti-sandbox mechanismy.
* Schopnost analýzy rootkitů a ransomwaru.
* Schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti.
* Řešení pracuje s behaviorální analýzou.
* Kompletní výsledek o zanalyzovaném souboru dostupný v centrálním managementu včetně informace o nalezeném i nenalezeném škodlivém chování daného souboru.
* Možnost manuálního odeslání vzorku do sandboxu.
* Možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu.
* Neomezené množství odesílaných souborů.
* Veškerá komunikace probíhá šifrovaným kanálem.
* Možnost okamžitého odstranění souboru po dokončení analýzy z cloudovém sandboxu.
* Možnost volby, jaké kategorie souborů do cloudového sandboxu budou odcházet (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty).
* Velikost odeslaných souborů do cloudového sandboxu může dosahovat až 64MB.
 |  |  |
|  | Požadavky na management konzoli: * Webová konzole dostupná v cloudu a provozovaná výrobcem řešení.
* Možnost probuzení klientů pomocí Wake On Lan.
* Nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta.
* Offline uplatňování politik a spouštění úloh při výskytu definované události (například: odpojení od sítě při nalezení škodlivého kódu).
* Administrace v češtině.
* Široké možnosti konfigurace oprávnění administrátorů (například možnost správy pouze části infrastruktury, které konkrétnímu administrátorovi podléhá).
* Zabezpečení přístupu administrátorů do vzdálené správy pomocí 2FA.
* Podpora štítků/tagování pro snazší správu a vyhledávání.
* Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce.
* Vzdálené získání zachyceného škodlivého souboru z klienta.
* Detekce nespravovaných (rizikových) počítačů komunikujících na síti.
* Instalace a odinstalace aplikací 3. stran.
* Vyčítání informací o verzích softwaru 3. stran.
* Možnost vyčítat informace o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty…).
* Možnost získat informaci o posledním restartu počítače tzv. Boot time.
* Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku.
* Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny a automatickému uplatnění klientské úlohy.
* Automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů (například: 5 % všech počítačů / 50 klientů hlásí problémy).
* Podpora SNMP Trap, Syslogu a SIEM.
* Podpora instalace skriptem - \*.bat, \*.sh, \*.ini (GPO, SSCM…).
* Reportování stavu klientů chráněných jinými bezpečnostními programy.
* Schopnost zaslat reporty a upozornění na e-mail.
* Možnost synchronizace vícero struktur kompatibilní se stávající Active Directory do management konzole s možností nastavení granulárních oprávnění pro správce bezpečnostního řešení, tak aby jednotlivé struktury nebyli navzájem viditelné. (zadavatel umožňuje nabídnout rovnocenné řešení)
* Přidání uživatelů zařízení do vzdálené správy pomocí prostřednictvím:
* Importu XLS seznamu,
* Synchronizace kompatibilní se stávající Active Directory. (zadavatel umožňuje nabídnout rovnocenné řešení)
* Přidání stanic a serverů do vzdálené správy pomocí:
* synchronizace s Active Directory,
* ruční přidání pomocí dle IP adresy nebo názvu zařízení,
* pomocí síťového skenu nechráněných zařízení v síti,
* Import XLS seznamu.
 |  |  |
| **Bezpečnost cloudových aplikací** |
|  | Řešení poskytuje ochranu kompatibilní se stávajícími komponentami Microsoft 365:* Exchange Online
* OneDrive
* SharePoint Online
* Microsoft Teams

(zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Řešení poskytuje ochranu kompatibilní se stávajícími komponentami Google Workspace:* Gmail
* Google Drive

(zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Nezávislá cloudová správa pro vyhodnocení zachycených hrozeb. |  |  |
|  | Neinvazivní technologie – nesmí při nedostupnosti ovlivnit fungování samotného stávajícího MS 365 nebo Google tenantu. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Funkce Antimalware, Antispam, Antiphishing. |  |  |
|  | Možnost zasílání pravidelných reportů. |  |  |
|  | Možnost ochránit celý tenant nebo jednotlivé uživatele. |  |  |
|  | Automatická aplikace ochrany pro nově vzniklé uživatele kompatibilní se stávajícím MS 365 nebo Google Workspace. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Integrovaná funkce analýzy neznámých vzorků v prostředí cloudového sandboxu. |  |  |
| **Management zranitelností** |
|  | Řešení je součástí agenta poskytovatele bezpečnostní platformy bez nutnosti instalace. |  |  |
|  | Podpora kompatibilní se stávajícími operačními systémy MS Windows. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Patch managament je integrován jako součást centrální správy bezpečnostní řešení daného výrobce. |  |  |
|  | Všechny detekované zranitelnosti a jejich dostupné záplaty jsou spravované přes centrální správu výrobce bezpečnostního řešení. |  |  |
|  | informace o zranitelnosti je ve standardizovaném formátu CVE včetně datumu objevení zranitelnosti, její povahy a odkaz na zdroj popisující zranitelnost |  |  |
|  | každá zranitelnost musí mít "bezpečnostní skóre" dle databáze CVSS 3.0 či novější. |  |  |
|  | Možnost ručního spuštění záplaty podporované aplikace. |  |  |
|  | Možnost automatického spuštění záplaty podporované aplikace podle časových kritérií s možností vybrání aplikací logikou blacklist/whitelist. |  |  |
|  | Možnost automatizovaného spuštění záplaty vybrané aplikace podle vydefinované podmínky (např. podle skóringu zranitelnosti, podle konkrétních CVE, podle konkrétních verzí aplikací). |  |  |
|  | V případě potřeby restartu zařízení má uživatel možnost restart odložit. |  |  |
|  | V případě potřeby restartu aplikace je uživatel informován o této potřebě a aplikace není bez vyzvání rovnou restartována. |  |  |
|  | Automatické záplatování kompatibilní se stávajícím MS Windows OS s možností definice typ aktualizací kritických/důležitých updatů. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Možnost definovat minimální prostor na disku pro stáhnutí a aplikaci záplat. |  |  |
| **Správa mobilních zařízení** |
|  | Zařízení je možné centrálně spravovat pomocí management konzole:* Podpora stávajících OS Android, iOS a iPadOS. (zadavatel umožňuje nabídnout rovnocenné řešení).
* Možnost zaregistrovat zařízení v režimu vlastníka nebo ABM.
* Application control s možností vynucení požadovaných aplikací.
* Lokalizace zařízení.
* Podpora anti-theft akcí (siréna, zámek telefonu, vzdálené smazání dat).
* Detekce roamingu.
* Konfigurace restrikcí.
* Vynucení složitosti zámku obrazovky zařízení.
* Správa účtů (email, LDAP, stávající MS Exchange,..). (zadavatel umožňuje nabídnout rovnocenné řešení)
* Integrace s managementem zařízení Microsoft Intune a VMware Workspace ONE.
* WebControl s možností filtrování obsahu webu.
* Filtrování hovorů a SMS s definicí časových slotů pro uplatnění pravidel.
* Správa aktualizací systému.
* Ochrana před výměnou SIM karty (definice důvěryhodné SIM).
* Možnost definovat informace na zamčené obrazovce (kontaktní údaje společnosti).
 |  |  |
|  | Požadavky na antivirové zabezpečení: * Podpora antivirového zabezpečení pro stávající operační systém Android. (zadavatel umožňuje nabídnout rovnocenné řešení)
* Rezidentní ochrana běžící a chránící zařízení v reálném čase.
* Možnost definice naplánovaných kontrol.
* Možnost kontroly výměnných zařízení.
* Detekce potenciálně nechtěných aplikací.
* Definice aktualizačního serveru.
* Antiphishing ochrana.
* Detekce phishingových URL v SMS zprávách.
* Instalace a odinstalace aplikací 3. stran.
* Vyčítání informací o verzích softwaru 3. stran.
* Možnost vyčítat informace o hardwaru na spravovaných zařízeních.
 |  |  |

## Opatření ID 6 (§ 27 VyKB) – Zajišťování úrovně dostupnosti informací

### SERVER + OS – 1 ks

Tabulka 13: SERVER + OS – 1 ks

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Provedení, příslušenství:* Rackové provedení, min.. 2U.
* Pro přístup ke všem komponentám serveru není nutné nářadí.
* Barevně značené hot-plug vnitřní i vnější komponenty
 |  |  |
|  | CPU: 1x procesor o výkonu minimálně 62 000 bodů dle http://cpubenchmark.net, počet jader min. 32  |  |  |
|  | RAM minimálně 512 GB RAM v provedení min. DDR5, min. 4800 MHz |  |  |
|  | HDD: Server musí disponovat alespoň 2x diskovou hotswap šachtou pro disky. Osazení min. dvěma SSD s kapacitou min. 480GB s NVMe rozhraním, min. 1DWPD, připojené na hw řadič s podporou RAID0/1. |  |  |
|  | Vlastnosti :* 4 x 10/25GbE SFP28
* 1x Dual Port 32GB Fibre Channel karta
* Redundantní napájecí zdroje 230V, max. 700W (alespoň Platinum třída podle specifikace 80 Plus).
* Možnost provozu při okolní teplotě stabilně až do 40°C (provoz chlazení vzduchem)
* 1 x přední, 2x zadní a 1x vnitřní USB port (alespoň jeden zadní a vnitřní s podporou USB3.0)
* Interaktivní LCD display indikující základní informace o systému (min. IP adresa, model, chybové stavy, atd.), možnost nastavení IP konfigurace a čtení chybových stavů z out-of-band managementu, bez potřeby připojení monitoru a klávesnice
* Dedikovaný RAID slot pro RAID kartu
* OCP 3.0 slot
* Zásuvné ližiny pro rack
 |  |  |
|  | Management serveru nezávislý na operačním systému poskytující následující management funkce a vlastnosti:* web GUI a dedikovaná IP adresa, dedikovaný management LAN port s podporou VLAN.
* SW LAN adaptér pro management mapovaný prostřednictvím z předu přístupného USB portu, podpora přímého připojení USB kabelem z notebooku správce nebo servisního technika (není nutné zpřístupňovat management LAN).
* Agent-less hardware FW update vč. možnosti rollback při neúspěchu.
* Podpora asistovaného OS Deploymentu.
* LifeCycle Log
* sledování hardwarových sensorů (teplota, napětí, stav, chybové sensory).
* erroralerty (server reset, kritické sensorové hodnoty, atd.) za použití email traps, paging, atd.
* možnost failoveru management LAN portu na jinou síťovou kartu na desce serveru (LOM).
* podpora IPv6.
* podpora WS-MAN/SMASH-CLP.
* plná podpora a IPMI funkcionalita.
* vestavěný Unified Server Configurator GUI (není třeba asistenční/driverové nebo HW-test CD/DVD).
* vzdálená konfigurace RAID, přímo v OOB managementu.
* server remote reset, reboot, power-on/off/cycle.
* power management a powercaping.
* integrace managementu do ActiveDirectory a dvoufaktorováauthentikace (TFA), encryption)
* podpora RemotevirtualSerial support.
* BIOS recovery.
* Management serveru nepožaduje instalaci agenta jak pro monitoring, tak pro update SW/FW/BIOS v jednotlivých HW komponentech serveru.
* Podpora hromadné konfigurace více serverů pomocí XML souborů (z USB, nebo síťovým PXE bootem), hesla v takovém souboru musí být hashována proti zneužití (zerotouchdeployment).
* Management serveru ukládá nastavení komponent do vyhrazené paměti, která je neoddělitelnou součástí chassis. Tato konfigurace je pak použitelná po výměně kterékoliv HW komponenty.
* Interaktivní čelní informační panel. Panel musí umožňovat kontrolu a nastavení parametrů out-of-band vestavěné správy systemu, včetně přiřazení IP adres a přístupu do HW logu.
* management nástroje musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích.
 |  |  |
|  | Podpora na 5 let typu NBD, oprava v místě instalace serveru, servis je poskytován výrobcem serveru, možnost rozšíření záruky min. na 7 let. Podpora prostřednictvím internetu musí umožňovat stahování ovladačů a manuálů adresně pro konkrétní zadané sériové či produktové číslo každého serveru. Možnost provázání managementu serveru pro online spojení technickou podporou výrobce a automatickým otevíráním servisních požadavků včetně automatického odeslání HW a OS logů pro následný troubleshooting proces. |  |  |
|  | 1 ks licencí 64-bitového serverového operačního systému v aktuální verzi * Podpora min. 64 procesorových socketů.
* Podpora běhu v on-premise, hybrid a cloudovém prostředí.
* Podpora TPM 2.0 čipů.
* Podpora ochrany firmware před neoprávněným přepsáním.
* Podpora replikace úložišť.
* Vestavěná technologie serverové i desktopové virtualizace.
* Nativní podpora virtualizace sítí.
* Neomezený počet virtuálních serverů.
* Licence pro min. 32CORE.
* Operační systém musí být kompatibilní s již provozovanými OS. Aktuálně zadavatel provozuje operační systémy od společnosti MICROSOFT (zadavatel umožňuje nabídnout rovnocenné řešení).
 |  |  |
|  | **V nabídce doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry.** |  |  |

### Záložní zdroje – 4 ks

Tabulka 14: Záložní zdroje – 4 ks

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Kapacita výstupního výkonu [W]: 2 700 |  |  |
|  | Kapacita výstupního výkonu [VA]: 3 000 |  |  |
|  | Jmenovité výstupní napětí [V]: 230 |  |  |
|  | Topologie: Line interaktivní |  |  |
|  | Typ křivky: Sinusoida |  |  |
|  | Výstupní přípojky:(8) IEC 320 C13 (Záložní provoz na baterie)(3) IEC Jumpers (Záložní provoz na baterie)(1) IEC 320 C19 (Záložní provoz na baterie) |  |  |
|  | Port rozhraní: RJ-45 10/100 Base-T, RJ-45 Serial, SmartSlot, USB, Karta pro řízení přes web/SNMP |  |  |
|  | Ovládací panel – Luminiscenční diody zobrazují stav: * napájení ze sítě,
* napájení z baterie,
* vyměnit baterii,
* přetížení.
 |  |  |
|  | Multifunkční LCD stavová a kontrolní konzola |  |  |
|  | Zvukové upozornění: * upozornění na stav, kdy je systém napájen z baterie,
* zřetelné upozornění na nízkou kapacitu baterie, nastavitelná doba.
 |  |  |
|  | Provozní teplota [°C]: 0-40 |  |  |
|  | Typ baterie: Bezúdržbový olověný zatavený akumulátor se suspendovaným elektrolytem: netečeObvyklá doba nabíjení max [Hod]: 4Očekávaná životnost baterie: min 3roky |  |  |

### Zálohovací SW pro 30 stávajících virtuálních serverů

Tabulka 15: Zálohovací SW pro 30 stávajících virtuálních serverů

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
| **Obecné požadavky**  |
|  | Zálohovací řešení musí být kompatibilní a podporovat stávající infrastrukturu VMware ve verzích 6.x, 7.x a 8.0, včetně VMware Cloud Foundation, VMware Cloud on AWS, VMware cloud on Dell a Azure VMware Solution (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Řešení musí podporovat a být kompatibilní s hostiteli spravovanými stávajícím serverem VMware vCenter ve verzích 6.x, 7.x a 8.0 i samostatné ESXi hostitele. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Zálohovací řešení musí podporovat a být kompatibilní se stávajícími Windows Server Hyper-V 2012 až 2022 včetně Server Core, Azure Stack HCI i Microsoft Hyper-V Server (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Řešení musí podporovat a být kompatibilní se stávajícími hostiteli spravovanými pomocí Microsoft System Center Virtual Machine Manager 2012 R2 až 2019, klastrové i samostatné hostitele Hyper-V (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Řešení musí podporovat zálohování všech operačních systémů, které jsou podporovány pro provoz na těchto hypervizorech.  |  |  |
|  | Řešení musí podporovat a být kompatibilní se zálohováním stávající platformy Red Hat Virtualization 4.4 SP1 (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Řešení musí podporovat a být kompatibilní se zálohováním celých zařízení NAS, jednotlivých sdílených složek SMB a NFS a stávajících souborových serverů MS Windows a Linux. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Software musí být možné licencovat pomocí trvalé licence.  |  |  |
| **TCO** |
|  | Řešení nesmí být závislé na jednom poskytovateli HW, virtualizační, nebo cloudové platformy a to jak pro výpočetní část, tak pro část ukládání dat.  |  |  |
|  | Licence musí být přenositelná mezi různými fyzickými, virtuálními a cloudovými chráněnými objekty. |  |  |
|  | Všechny součásti řešení musí plně podporovat komunikaci po IPv6. |  |  |
|  | Řešení musí mít mechanismy k úspoře objemu úložného prostoru pro ukládání záloh. Jejich využití musí být volitelné a nesmí omezit žádné funkcionality zálohování a obnovy dat.  |  |  |
|  | Řešení musí poskytovat jednotnou konzoli pro přehled o zálohách fyzických, virtuálních, cloudových, NAS i Kubernetes open source prostředí. |  |  |
|  | Řešení musí umožnit vytvoření jednoho logického úložiště pro ukládání záloh z neomezeného počtu různorodých diskových úložišť. |  |  |
|  | Řešení musí umožňovat ukládání záloh do různých diskových úložišť, souborových systémů, objektových úložišť, nebo deduplikačních diskových zařízení. |  |  |
|  | Řešení musí umožňovat rozšíření logického úložiště o vrstvy pro automatické vytváření sekundární a archivní kopie záloh, zajišťující soulad s pravidlem 3-2-1 ukládání záloh.  |  |  |
|  | Řešení musí umožňovat "single pass backup“ s možností vyloučit zpracování jednotlivých souborů a složek. „Jednoprůchodová záloha“ je vyžadována pro všechny druhy obnovení včetně granulárních obnov na úrovni aplikačních položek. |  |  |
|  | Řešení musí umožňovat připojování a spouštění jakéhokoli skriptu pro zálohování před nebo po spuštěním zálohovací úlohy, nebo před a po snapshotu VM. |  |  |
|  | Řešení musí podporovat a být kompatibilní s technologiemi klonování datových bloků u souborových systémů pro stávající OS MS Windows i Linux pro zajištění dalších úspor konzumované kapacity. (zadavatel umožňuje nabídnout rovnocenné řešení)  |  |  |
| **Předcházení rizik** |
|  | Přístup do řídící konzole musí být chráněný vícefaktorovou autentizací bez nutnosti přístupu k internetu. |  |  |
|  | Řešení musí umožňovat vytváření záloh odolných vůči náhodnému, či úmyslnému smazání, nebo ransomware útokům na komoditním serverovém HW, nebo jakémkoliv S3-kompatibilním objektovém úložišti. |  |  |
|  | Řešení nesmí použít centrální databázi pro ukládání jakýchkoli metadat deduplikace. Ztráta databáze nemůže způsobit, že záložní soubory budou nestabilní. Metadata deduplikace musí být uložena v záložních souborech. |  |  |
|  | Řešení musí umožňovat pravidelné automatické testování obnovitelnosti záloh, včetně funkčnosi jednotlivých služeb a kontrolou obsahu na kybernetické hrozby pomocí řešení třetích stran.  |  |  |
|  | Řešení musí disponovat nástrojem pro analýzu konfigurace z pohledu bezpečnostních "Best Practices" doporučení.  |  |  |
|  | Řešení musí umožňovat v průběhu obnovy dat ověřovat obsah obnovovaných dat na kybernetické hrozby pomocí produktů třetích stran. |  |  |
|  | Řešení musí disponovat API pro zpřístupnění obsahu záloh aplikacím třetích stran. |  |  |
|  | Řešení musí umožňovat vytvářet a spouštět izolované "Sandbox" prostředí pro provoz skupin VM ze záloh, replik i snímků diskových polí.  |  |  |
|  | Řešení musí nabízet šifrování celého síťového provozu mezi všemi komponentami a také šifrování souborů záloh "na cíli" na diskovém, cloudovém nebo páskovém úložišti. |  |  |
|  | Řešení musí nabízet způsoby, jak omezit stres na úložišti zdrojových dat během zálohování tak, aby záloha kontrolovatelným způsobem ovlivňovala latenci produkčního úložiště.  |  |  |
|  | Zálohování NAS zařízení musí podporovat přímé ukládání záloh do S3-kompatibilních objektových úložišť s podporou ObjectLock funkce. |  |  |
|  | Řešení musí podporovat vytváření sekundárních kopií záloh z S3-kompatibilních objektových úložišť na datové pásky pro zajištění "off-line", či "air-gapped" sady záloh. |  |  |
|  | Součástí záloh musí být všechny informace, potřebné pro zajištění obnovy i v případě nedostupnosti původního zálohovacího serveru, nebo databáze s katalogem záloh.  |  |  |
| **Monitoring** |
|  | Řešení musí poskytovat dohled nad chráněnou virtualizační platformou, poskytující včasná varování před výpadkem, nebo omezením dostupnosti produkčního prostředí  |  |  |
|  | Řešení musí poskytovat možnost dohledu služeb a procesů provozovaných v GuestOS jednotlivých chráněných VM. |  |  |
|  | Řešení musí informovat, které VM nejsou chráněné dostatečně, nebo vůbec a zároveň kdy a jakým spůsobem byl naposledy vytvořen bod obnovy.  |  |  |
|  | Řešení musí poskytovat možnost automatizovaných řešení chybových stavů. |  |  |
|  | Řešení musí poskytovat funkce pro zasílání stavových hlášení do centrálního monitorovacího nástroje přes SNMP protokol. |  |  |
|  | Řešení musí podporovat a být kompatibilní s monitorováním stávajících virtualizovaných prostředí VMware vSphere a Microsoft Hyper-V bez nástrojů třetích stran. (zadavatel umožňuje nabídnout rovnocenné řešení)  |  |  |
|  | Řešení musí podporovat a být kompatibilní s dohledem následujících stávajících systémů: VMware, ESXi 6.x, 7.x a 8.0 pro placené i bezplatné edice ESXi. Podporovaní hostitelé mohou být spravováni pomocí vCenter serveru nebo pracovat v samostatném režimu. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Řešení musí podporovat a být kompatibilní s dohledem následujících stávajících systémů: Microsoft Server Hyper-V 2012, 2012R2, 2016, 2019 a 2022 pro placené i bezplatné edice. Podporovaní hostitelé mohou být spravováni SCVMM nebo pracovat v samostatném režimu. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Řešení musí být certifikováno jako „VMware ready“ (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |

## Implementace

Tabulka 16: Požadavky – Implementace nabízeného řešení

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota**  | **Splněno [ano/ne]** |
|  | Součástí je zajištění instalace a konfigurace předmětu veřejné zakázky v návaznosti na stávající infrastrukturu zadavatele (tj. včetně dopravy, montáže, instalace a implementace do stávající IT infrastruktury) v sídle zadavatele. |  |  |
|  | Účastník zajistí:* instalace zařízení do standardní RACK skříně 19“ 42U,
* implementace Best Practice scénářů pro dané konfigurace,
* kontroly kompatibility verzí ovladačů a firmware jednotlivých zařízení a jejich aktualizace,
* registrace záruk u výrobců,
* umístění do racku a zapojení kabeláže vč. jejího označení,
* Instalace SERVERU – rozšíření CLUSTERU (aktuálně 2NODY a diskové pole), konektivita 16Gb Fiber, stávající VMWARE virtualizace
* inicializace a konfigurace všech dodaných zařízení,
* nastavení IP adres,
* nastavení vysoké dostupnosti,
* konfiguraci datových prostor polí, integrace s hypervizorem, nastavení dohledu a instalace SW pro monitoring výkonu,
* zapojení do stávající LAN.
 |  |  |
|  | Účastník do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění předmětu veřejné zakázky jako logického a funkčního celku. |  |  |
|  | Součástí instalace musí být i zaškolení administrátorů (správců) – 3 osoby minimálně v rozsahu nutném pro samostatnou administraci předmětu zakázky. Administrací se rozumí zejména: konfigurace, monitoring činnosti, aktualizace, řešení problémů, zálohování konfigurace. Trvání zaškolení administrátorů je minimálně 40 hodin pro každého administrátora v sídle zadavatele. |  |  |
|  | Konzultační práce pro předmět veřejné zakázky v minimálním rozsahu 48 hodin, poskytnuté do konce realizace.  |  |  |
|  | Testování implementovaného předmětu veřejné zakázky na zkušebních datech. |  |  |
|  | Zahájení ostrého provozu (převedení předmětu veřejné zakázky do produkčního prostředí). |  |  |
|  | Vypracování a předání dokumentace popisující konečný skutečný stav předmětu veřejné zakázky.Dokumentace bude zahrnovat:* popis všech prvků/zařízení,
* popis způsobu zálohy a obnovy konfigurace všech prvků/zařízení
* veškeré požadavky na zachování záruky/podpory (např. kompatibilita)
* informaci o způsobu řešení servisních požadavků.
 |  |  |

# Požadavky na servisní podporu provozu a SLA

Požadavky na servisní podporu provozu a SLA jsou uvedeny ve smlouvě o dílo a poskytování servisní podpory v **příloze č. 3 pro 1. část a v příloze č. 8 pro 2. část** ZD.

# Podmínky předání a převzetí – akceptace

Předání a převzetí bude provedeno na základě podepsaného předávacího protokolu, ve kterém budou zaznamenány výsledky splnění předmětu smlouvy o dílo:

1. Dodávka předmětu plnění dle smlouvy o dílo – předávací protokol;
2. Dodávka technické dokumentace skutečného provedení díla (tj. administrátorská a uživatelská dokumentace) – předávací protokol;
3. Protokol o úspěšném provedení akceptačních testů.

Předávací protokol musí obsahovat minimálně:

- Úroveň technické podpory.

- Datum konce platnosti technické podpory.

- **Pro 2. část:** Seznam vyměnitelných interních komponent, jako jsou CPU, RAM, paměťová média, rozšiřující karty a napájecí zdroje.

Rozsah akceptačních testů je stanoven ve smlouvě o dílo a poskytování servisní podpory v **příloze č. 3 pro 1. část a v příloze č. 8 pro 2. část** ZD.

# Harmonogram plnění

Harmonogram plnění je uveden ve smlouvě o dílo a poskytování servisní podpory v **příloze č. 3** **pro 1. část** a v **příloze č.8 pro 2. část** ZD.

# Seznam zkratek

API Rozhraní pro programování aplikací (Application Programming Interface)

DHCP Protokol pro správu sítě vyžadovaný v sítích IP (Dynamic Host Configuration Protocol)

DNS Domain Name System

EDR Detekce a odpověď koncového bodu (Endpoint Detection and Response)

FC Fibre Channel

HA High Availability

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

HW Hardware

IS Informační systém

IT Informační technologie

LAN lokální síť (Local Area Network)

NFS Network File System

MP Management Packs

OOB Out-Of-Band

OS Operační systém

RAID Redundant Array of Independent Disks

SAS Serial Attached SCSI

SLA Dohoda o úrovni služeb servisní podpory (Service Level Agreement)

SSD Solid State Drive

SSH Secure Shell

SSL Secure Sockets Layer

SW Software