

Registrační číslo projektu: **CZ.06.01.01/00/22\_009/0003519**

**Příloha č. 3 Zadávací dokumentace**

**Specifikace předmětu plnění – 2. část**

**„HW a SW“**

Obsah:

[1. Předmět 2. části veřejné zakázky 2](#_Toc189139942)

[2. Specifikace požadavků řešení 2. části 2](#_Toc189139943)

[2.1. Obecné požadavky 2](#_Toc189139944)

[2.2. Hardware 3](#_Toc189139945)

[2.2.1. Deduplikační diskové úložiště – 1ks 3](#_Toc189139946)

[2.2.2. Server – 2ks 5](#_Toc189139947)

[2.2.3. Diskové pole – 1ks 7](#_Toc189139948)

[2.2.4. Firewall – 2ks v HA 8](#_Toc189139949)

[2.2.5. Gigabitové přepínače – 2 ks 13](#_Toc189139950)

[2.3. Software 17](#_Toc189139951)

[2.3.1. Virtualizační a operační systém 17](#_Toc189139952)

[2.3.2. Databázový systém 17](#_Toc189139953)

[2.4. Implementace 17](#_Toc189139954)

[3. Požadavky na servisní podporu provozu 17](#_Toc189139955)

[4. Podmínky předání a převzetí – akceptace 18](#_Toc189139956)

[5. Harmonogram plnění 18](#_Toc189139957)

[6. Seznam zkratek 18](#_Toc189139958)

Seznam tabulek:

[Tabulka 1: Obecné požadavky 2](#_Toc189139959)

[Tabulka 2: Deduplikační diskové úložiště – 1ks 3](#_Toc189139960)

[Tabulka 3: Server – 2ks 5](#_Toc189139961)

[Tabulka 4: Diskové pole – 1ks 7](#_Toc189139962)

[Tabulka 5: Firewall – 2ks v HA 8](#_Toc189139963)

[Tabulka 6: Gigabitové přepínače – 2 ks 13](#_Toc189139964)

[Tabulka 7: Virtualizační a operační systém 17](#_Toc189139965)

[Tabulka 8: Databázový systém 17](#_Toc189139966)

[Tabulka 9: Požadavky – Dodávka a implementace nabízeného řešení 17](#_Toc189139967)

# Předmět 2. části veřejné zakázky

**Předmětem 2. části této veřejné zakázky je dodávka a implementace hardware a software nutného pro provoz „Transakčního portálu pro sdílení a výměnu dat mezi informačními systémy Nemocnice Letovice a jinými externími systémy“, který je předmětem 1. části VZ.**

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

# Specifikace požadavků řešení 2. části

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.

## Obecné požadavky

Tabulka 1: Obecné požadavky

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota.** | **Splněno [ano/ne]** |
|  | Veškerý nabízený hardware, musí být originální, nově vyrobený, nepoužitý, určen pro český trh.  V databázi výrobce, pokud taková existuje, musí být Zadavatel veden jako první uživatel předmětu veřejné zakázky. |  |  |
|  | 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. |  |  |
|  | Délku, úroveň a stav technické podpory pro servery, pole a switche musí být možné ověřit přímo na stránkách výrobce, po zadání výrobního čísla zařízení. |  |  |
|  | Nabízený předmět veřejné zakázky, včetně konfigurace interních komponent, musí splňovat požadavky ErP Lot 9 (EU 2019/424). |  |  |
|  | Veškeré požadované funkce, vlastnosti, certifikace i výsledky testů, musí být dostupné nejpozději dnem podání nabídky. |  |  |

## Hardware

### Deduplikační diskové úložiště – 1ks

Tabulka 2: Deduplikační diskové úložiště – 1ks

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
|  | Datové úložiště typu All Flash |  |  |
|  | Architektura   * All Flash diskové pole * Duální řadiče active-active * RAM Cache celkem min. 192 GB (96 GB per řadič) * Ochrana cache vůči výpadku napájení * Vysoká dostupnost, plná redundance, bez SPOF   Celková velikost max. 2U |  |  |
|  | Kapacita   * Min. 53 TiB (Tebibyte) čisté využitelné kapacity typu All-Flash * Osazení disky NVMe SSD Encryption Drive, všechny osazené disky musí být stejného typu a velikosti * Všechny SSD disky musí mít životnost minimálně s DWPD=1, technologie flash musí být TLC nebo lepší (nikoliv QLC) * Kapacita musí být ochráněna pomocí RAID6 * Pro výpočet kapacity se nesmí využít žádné technologie datové redukce (komprese/deduplikace) * Navíc musí být osazena hotspare kapacita odpovídající velikosti dat minimálně 1 disku * Hotspare kapacita musí být rovnoměrně distribuována na všech osazených discích * Možnost rozšíření čisté využitelné kapacity na min. 200 TiB   Doložit výstup z nástroje výrobce s kapacitním návrhem, kde bude patrný počet a typ disků, režim RAID, velikost čisté kapacity a počet hotspare |  |  |
|  | Konektivita   * Celkem min. 16 portů 10GE, osazené SFP+ optickými moduly (8 per řadič) * Celkem min. 8 portů 1GE RJ45 (4 per řadič) * Management porty 1GE RJ45 (1 per řadič) * Požadované protokoly pro blokový přístup: iSCSI * Požadované protokoly pro souborový přístup: SMBv3 a NFSv3/v4 * Možnost rozšíření o další port adaptéry: minimálně 1 adaptér pro každý řadič s volitelným typem konektivity (podpora ETH 25GE, FC 16/32Gbs) * Podpora direct připojení k serverům   Podpora připojení pomocí ETH switchů |  |  |
|  | Správa a management   * GUI pomocí standardního webového prohlížeče přes HTTPS * Podpora CLI, RESTful API * Výkonnostní a kapacitní monitoring s historií minimálně 12 měsíců * Predikce trendů obsazení kapacity * Podpora SNMP v3 a SNMP traps * Upgrade kódu a opravných patches online bez zastavení datových služeb * Podpora IPv4 i IPv6 * Funkce Audit Log pro záznamy a bezpečné uchování všech administrátorských operací   Zabudovaný nástroj pro správu šifrovacích klíčů |  |  |
|  | Funkcionalita pro blokový přístup   * Funkce ThinProvisioning na úrovni LUNů * Podpora online expanze LUNů * Funkce Snapshots * Funkce zabezpečených Snapshots s nastavením retenční periody a s ochranou nesmazatelnosti a nezměnitelnosti * Funkce plánování periodických snapshotů * Funkce Clones na úrovni LUNů * Funkce Quality of Service na úrovni LUNů s definicí SLA per IOPS nebo per MB/s a s možností prioritizace aplikací * Funkce synchronní replikace dat na úrovni LUNů * Funkce asynchronní replikace dat na úrovni LUNů * Funkce geografického storage metroclusteru pro LUNy * Funkce bezpečného mazání dat na úrovni LUNů * Funkce deduplikace a komprese dat pro LUNy   Podpora IO multipath |  |  |
|  | Funkcionalita pro souborový přístup   * Funkce nastavení kvót pro uživatele souborových služeb * Podpora online expanze filesystémů * Funkce multi-tenancy pro souborové služby * Funkce napojení na AD a LDAP * Funkce napojení na DNS * Funkce Audit Log pro souborové služby pro záznamy a bezpečné uchování uživatelů filesystémů a jejich činností s daty * Funkce WORM pro souborové služby se zabezpečením proti smazání a modifikaci dat a s nastavením retenční periody; zabezpečení systémového času; podpora režimů Enterprise WORM a Regulatory WORM * Funkce Snapshots na úrovni filesystémů * Funkce zabezpečených Snapshots na na úrovni filesystémů s nastavením retenční periody a s ochranou nesmazatelnosti a nezměnitelnosti * Funkce plánování periodických snapshotů filesystémů * Funkce Quality of Service na úrovni filesystémů s definicí SLA per IOPS nebo per MB/s s možností prioritizace aplikací * Funkce asynchronní replikace dat na úrovni filesystémů * Funkce geografického storage metroclusteru pro filesystémy * Funkce bezpečného mazání dat na úrovni filesystémů * Funkce deduplikace a komprese dat pro filesystémy * Podpora NDMP pro zálohování souborových služeb pomocí běžných zálohovacích SW   Podpora pro externí antivirus server |  |  |
|  | Výkonnost   * Minimálně 100000 IOPs   Výkonnost bude ověřena pro scénář modelové zátěže: protokol iSCSI, reads/writes 70%/30%, velikost bloků 8kB, random. 0% cache hit. Ověření pomocí nástroje vdbench na nakonfigurovaných 8 LUNech s velikostí 500GB per LUN |  |  |
|  | Kompatibilita a integrace   * Podpora pro nabídnutý serverový virtualizační systém * Podpora VMware * Podpora Hyper-V   Podpora Microsoft Windows, Linux |  |  |
|  | Ostatní   * Funkcionality popsané výše musí být pokryty příslušnými softwarovými licencemi typu „perpetual“ na celou dodávanou kapacitu diskového pole * Veškeré HW a SW komponenty musí být od jednoho výrobce   16 ks optických kabelů multi-mode o délce 3 metry |  |  |
|  | Záruka a podpora   * HW záruka 60 měsíců, 5x9 NBD onsite * SW záruka a podpora 60 měsíců, s právem na nové verze * Možnost ověření podpory na stránkách výrobce dle sériového čísla zařízení   Možnost zakládat servisní požadavky přímo u výrobce zařízení |  |  |

### Server ­– 2ks

Tabulka 3: Server – 2ks

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Form Factor a vnitřní uspořádání:  1U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty a místa pro uchopení.  LCD display pro základní diagnostiku serveru a uzamykatelný přední panel. |  |  |
|  | CPU Dvousocketový  Minimálně Floating Point Speed 204 a Integer Rates 284 dle Spec.org. ke dni zahájení zadávacího řízení. |  |  |
|  | RAM:  min. 8x 64GB na min. 5600MHz. Ideální rozložení paměťových modulů v návaznosti na technické požadavky paměťových kanálů daného typu serveru, paměť rozšiřitelná min. na 4096 GB min. typu DDR5 s možností osazení min. 16 slotů. |  |  |
|  | Diskový subsystém:  Diskless konfigurace BOSS karta osazená min. 2x 480GB M.2 v RAID1 |  |  |
|  | Síťové rozhraní:  min.: 2x 10/25GbE SFP28, 6x 1GbE BASE-T |  |  |
|  | Napájení:  Redundantní síťové napájecí zdroje min. 700W s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting) min. 96% účinnost při zatížení 50% (Titanium), včetně příslušných PDU kabelů C13/14 o délce 2M |  |  |
|  | Interface:  - min. 3 x USB (1 vpředu, 2 vzadu z toho min. 1x USB 3.0)  - min. 2 x VGA (1 vpředu, 1 vzadu) |  |  |
|  | Rozšiřující sloty:  - Min 1x PCIe Gen4 x16 a 1x PCIe Gen5 x8  - Osazeno 1x 12Gb SAS 4 portové HBA |  |  |
|  | Kolejnice  Zásuvné ližiny pro montáž do racku s ramenem pro vedení kabelů. |  |  |
|  | Management a vzdálená správa:   1. Nezávislá OOB karta s dedikovaným LAN RJ45 portem. 2. S podporou failoveru na jinou síťovou kartu v serveru, musí podporovat VLAN a LLDP Discovery síťové infrastruktury, protokolů IPv4 a IPv6 3. Monitoring jakékoliv komponenty serveru nesmí vyžadovat instalaci agenta do OS, OS se musí kompletně obejít bez AMS (Agentless Management Service). Tento požadavek se týká i diskového systému, včetně přístupu k nastavení RAID řadičů, SAS HBA či případných expansních diskových polic serveru. V případě síťových karet na desce či mezzanine kartě, musí být v managementu možnost monitorování až do úrovně případných optický modulů (SFP) osazených v těchto kartách. 4. Vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, platí i pro vzdálenou konzoli KVM over IP. 5. Management musí průběžně vyhodnocovat průměrné vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů v případě excesů. 6. Automatická instalace a obnova SSL certifikátu vestavěného serveru. 7. Přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE 8. Podpora multifaktorové autentizace, podpora stávajícího MS AD a generického LDAP. 9. Možnost streamingu údajů senzorů serveru, telemetrie a reportů o provozu pro účely prediktivního vyhodnocování provozu a zabezpečení s podporou pro Splunk nebo ELK stack. 10. Data logů musí být možné přesměrovat na sériový port RS232. Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů (stav, teplota, napětí, …) včetně událostí o přihlášení a změnách konfigurace. 11. Podpora uzamčení stavu serveru pro zvýšení bezpečnosti (System Lock Down), automatický Secure OS recovery včetně BIOS serveru a firmware BMC, firmware rollback. 12. Podpora dynamických změn nastavení externích USB portů systému, pro vzdálené povolení či zakázání portů, bez nutnosti restartu serveru či managementu. 13. Podpora serverových konfiguračních profilů pro kompletně automatický deployment serverů vzdáleně i lokálně (Zero Touch deployment) 14. Management musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) a hardware firmware update s možností ověření a stažení aktuálních verzí proti online repository výrobce, případně zabezpečenému lokálnímu repository pod správou administrátora. 15. Management musí umět poskytovat FW zařízením a kartám instalovaných v serveru, s možností automatické obnovy používané verze a konfigurace v případě výměny zařízení / karty z důvodu servisního zásahu, včetně konfigurace biosu a samotného managementu. Vzdálený mount úložiště není dostatečný, z důvodu případné nízké propustnosti správcova připojení. 16. OOB karta serveru musí být schopna utvořit management skupinu s dalšími servery, tak aby prostředí mohlo být dohlíženo z jedné IP adresy bez nutnosti instalace externí management aplikace. Databáze takové skupiny musí být minimálně na dvou místech tak aby v případě výpadku jedné OOB karty, převzala funkcionalitu druhá v jiném serveru. Funkcionalita musí být alespoň v režimu master-slave (či active-pasive) a podporovat min. 100 serverů ve skupině. 17. OOB karta musí mít vestavěnu funkcionalitu automatického odeslání hrozících či vzniklých chybových stavů na helpdesk výrobce serverů a automatického vytvoření servisního incidentu, na základě, kterého se automaticky rozběhne servisní zásah (call-home). 18. Možnost přístupu přes dedikovaný USB port s emulací síťového připojení. 19. Možnost přístupu přes wifi a BT rozhraní přes aplikaci podporující stávající OS Android a iOS. 20. Vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle). 21. Management musí umožnit bezpečné smazání dat ze serveru a jeho médií pro případ vyřazení nebo přesunu serveru. 22. Licence OOB managementu musí být pro server trvalá (life time), pokud je vyžadována. Výrobce udržuje databázi zakoupených licencí přístupnou kupujícímu, tak aby ji bylo možné v případě výměny HW kdykoliv obnovit, pokud dojte ke ztrátě. 23. Management umožňuje monitoring spotřeby el. energie na úrovni serveru / hosta / virtuálního serveru. 24. Konfigurace základních LAN parametrů managementu pomocí LCD na šasi / bezelu. |  |  |
|  | Podpora a servis:  Podpora na 5 let typu 24x7x365 s reakční dobou opravy následující pracovní den, oprava v místě instalace serveru, servis je poskytován výrobcem serveru. Jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému. Možnost stažení ovladačů a management software na webových stránkách výrobce po zadání unikátního sériového čísla.  Zdarma aktualizace firmware a ovladačů i po uplynutí doby platné podpory. |  |  |
|  | **V nabídce doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry.** |  |  |
|  | **Dodaný předmět veřejné zakázky musí být určen k distribuci v České republice, v nabídce doložte potvrzení lokálního zastoupení výrobce.** |  |  |

### Diskové pole – 1ks

Tabulka 4: Diskové pole – 1ks

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | HW a SW řešení určené pro musí obsahovat zálohovací SW a zálohovací diskové pole s pokročilou deduplikací. |  |  |
|  | Architektura   * Hybrid Flash diskové pole * Duální řadiče active-active * RAM Cache celkem min. 256 GB (128 GB per řadič) * Ochrana cache vůči výpadku napájení * Vysoká dostupnost, plná redundance, bez SPOF   Celková velikost max. 10U |  |  |
|  | Kapacita   * Min. 78 TiB (Tebibyte) čisté využitelné kapacity HDD * Osazení disky HDD, všechny osazené disky musí být stejného typu a velikosti * Kapacita musí být ochráněna pomocí RAID6 * Pro výpočet kapacity se nesmí využít žádné technologie datové redukce (komprese/deduplikace) * Navíc musí být osazena hotspare kapacita odpovídající velikosti min. 1 disku * Hotspare kapacita musí být rovnoměrně distribuována na všech osazených discích * Osazení disky SSD, min. 5 ks s min. velikostí 1.92 TB * Možnost rozšíření čisté využitelné kapacity na min. 200 TiB   Doložit výstup z nástroje výrobce s kapacitním návrhem, kde bude patrný počet a typ disků, režim RAID, velikost čisté kapacity a počet hotspare |  |  |
|  | Konektivita   * Celkem min. 12 portů 10GE osazených SFP+ optickými moduly (6 per řadič) * Celkem min. 8 portů 1GE RJ45 (4 per řadič) * Management porty 1GE RJ45 (1 per řadič)   Požadované protokoly: NFS, SMB |  |  |
|  | Správa a management   * GUI pomocí standardního webového prohlížeče přes HTTPS * Podpora CLI, RESTful API * Výkonnostní a kapacitní monitoring s historií minimálně 12 měsíců * Predikce trendů obsazení kapacity * Podpora SNMP v3 a SNMP traps * Upgrade kódu a opravných patches online bez zastavení datových služeb * Podpora IPv4 i IPv6   Funkce Audit Log pro záznamy a bezpečné uchování všech administrátorských operací |  |  |
|  | Funkcionalita řešení pro zálohování   * Deduplikace, komprese a kompakce dat * Funkce Snapshots * Funkce zabezpečených Snapshots s nastavením retenční periody a s ochranou nesmazatelnosti a nezměnitelnosti * Funkce plánování periodických snapshotů * Funkce replikace dat * Funkce šifrování dat včetně zabudovaného systému pro správu šifrovacích klíčů * Funkce deduplikace zálohovaných dat na zdroji pomocí akceleračního zálohovacího agenta * Funkce nastavení politiky WORM se zabezpečením proti smazání a modifikaci dat a s nastavením retenční periody * GUI pro podporu a volitelné nastavení politik zálohování dle typu zálohovaných prostředí, minimálně full backup, incremental backup, forever incremental backup, DB Log backup * Nastavení politik zálohování musí umožňovat časové plánování záloh, periodicitu záloh, retenci záloh, expiraci záloh, replikační politiky záloh * Funkce indexování uložených záloh pro rychlé globální vyhledávání a file-level recovery * Funkce live mount záloh a instant recovery * Možnost rozšíření o řízení životního cyklu záloh s volbou archivace do dalšího tieru, například páskové knihovny LTO * Možnost rozšíření o funkci replikace dat, včetně šifrování replikačního toku   Možnost rozšíření o funkci Air-Gap s politikami řízeného odpojování replikačních linek mezi lokalitami pro izolaci záloh v sekundární lokalitě |  |  |
|  | Kompatibilita a integrace   * Podpora zálohování pro nabídnutý serverový virtualizační systém * Podpora zálohování VMware * Podpora zálohování Hyper-V * Podpora zálohování databází, včetně příslušných Backup agentů: MS SQL Server, Oracle, MySQL, Exchange, PostgreSQL   Podpora zálohování fyzických serverů a OS |  |  |
|  | Ostatní   * Funkcionality popsané výše musí být pokryty příslušnými softwarovými licencemi typu „perpetual“ na celou dodávanou kapacitu diskového pole * Licence pro zálohovací SW musí pokrývat nabídnuté virtualizační prostředí a/nebo kapacitu zálohovacího pole (dle licenční politiky výrobce SW)   12 ks optických kabelů multi-mode o délce 3 metry |  |  |
|  | Záruka a podpora   * HW záruka 60 měsíců, 5x9 NBD onsite * SW záruka a podpora 60 měsíců, s právem na nové verze * Možnost ověření podpory na stránkách výrobce dle sériového čísla zařízení   Možnost zakládat servisní požadavky přímo u výrobce zařízení |  |  |
|  | **V nabídce doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry.** |  |  |
|  | **Dodaný předmět veřejné zakázky musí být určen k distribuci v České republice, v nabídce doložte potvrzení lokálního zastoupení výrobce.** |  |  |

### Firewall – 2ks v HA

Tabulka 5: Firewall – 2ks v HA

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Plně redundantní řešení tj. redundantní hardware a cluster řešení firewallu. |  |  |
|  | HW parametry:  2x Rack mount 1U, min. 32GB min. DDR4, min. 2x 512GB Enterprise SSD, min. 2x 10Gb SFP+, min. 6x 1GbE LAN, IPMI/KVM, redundantní zdroj |  |  |
|  | Firewall nové generace tzv. next generation firewall, který kombinuje vlastnosti paketových, stavových a aplikačních firewallů s tzv. „deep inspection“, hloubkovou inspekci.  Tento typ firewallu detailně zkoumá celý paket a jeho obsah a představuje tak účinnou ochranu před malwarovými útoky a jinými vnějšími hrozbami. |  |  |
| **Firewall** | | | |
|  | SPI – stateful packet instpection:  Sleduje relace procházejících síťových připojení. Stavová kontrola paketů, označovaná také jako dynamické filtrování paketů, je bezpečnostní funkce, která se používá k vyvolání jemných bezpečnostních zásad. Firewall ji provádí ve výchozím nastavení a lze ji nakonfigurovat tak, aby blokovala provoz na základě shody se zásadami. Alternativně lze provoz pouze kontrolovat a nebránit přidáním pravidel průchodu pro veškerý provoz na každém rozhraní z libovolného/do libovolného podle potřeby. |  |  |
|  | GeoIP blokace:  GeoIP filtrování může blokovat webový provoz z celých zemí. Síťová připojení jsou blokována na základě zeměpisné polohy (informace získané z IP adres), kterou lze následně použity k filtrování a zabránění odchozím a příchozím připojením do sítě a z ní. |  |  |
|  | Anti-Spoofing: detekuje pakety s falešnými adresami. |  |  |
|  | Captive Portal: autentizace nových uživatelů LAN sítě (bezdrátové nebo drátové) před přidělením přístupu do interní sítě. |  |  |
|  | Pravidla založená na čase: umožňuje aktivaci pravidel brány firewall v zadaných dnech a/nebo časových rozmezích. Pravidla založená na čase fungují stejně jako jakákoli jiná pravidla s tím rozdílem, že mimo naplánovaný čas nejsou v souboru pravidel přítomna. |  |  |
|  | Limit konexí: povoluje nebo zamítá přenosy na základě odpovídajícího setu: zdrojové adresy, cílové adresy a služby a počtu připojení, což umožňuje detekci anomálních požadavků na připojení. |  |  |
|  | NAT: Překlad síťových adres. |  |  |
| **Router** | | | |
|  | Routing:  Směrování založené na zásadách předává a směruje datové pakety na základě zadaných zásad nebo filtrů s použitím parametrů, jako je zdrojová a cílová IP adresa, zdrojový nebo cílový port, typ provozu, protokoly, seznam přístupů, velikost paketů atd., a pak směruje pakety po uživatelsky definovaných trasách. |  |  |
|  | IPv4 / IPv6: mapování NAT pro příchozí a odchozí provoz podporuje souběžně IPv4 a IPv6, což usnadní konfiguraci statických tras na směrovači. |  |  |
|  | Statické routy: plná podpora |  |  |
|  | Dynamické routy: OSPFv3, RIPV2, BGPv4 |  |  |
|  | IPv6 network prefix translation. |  |  |
|  | IPv6 router advertisment:  Používá se pro automatickou konfiguraci a směrování protokolu IPv6. Pokud je tato funkce povolena, směrovač pravidelně odesílá zprávy v reakci na výzvy. Hostitel se na základě těchto informací dozvídá prefixy a parametry místní sítě. |  |  |
|  | Více IP adres pro jedno rozhraní:  Umožňuje mapování mnoha názvů hostitelů (nezařazených), z nichž každý je přiřazen jedné IP adrese i v rámci jednoho serveru, přestože tento server může mít pouze jedno fyzické síťové rozhraní. |  |  |
|  | PPPoE Server:  Protokol PPPoE (Point-to-Point Protocol over Ethernet) je určen ke správě způsobu přenosu dat v sítích Ethernet a umožňuje rozdělit jedno připojení k serveru mezi více klientů pomocí sítě Ethernet. |  |  |
| **Obrana před útoky** | | | |
|  | IDS/IPS:  Systémy detekce narušení (IDS) analyzují síťový provoz a hledají signatury, které odpovídají známým kybernetickým útokům. Systémy prevence narušení (IPS) také analyzují pakety, ale mohou také zastavit jejich doručení a pomoci tak zastavit útok. |  |  |
|  | Detekce na 7 vrstvě:  Vrstva 7 je aplikační vrstva dle modelu OSI (Open System Interconnection), podporuje procesy aplikací a koncových uživatelů, například HTTP a SMTP. Útoky na této vrstvě představují bezpečnostní problém, protože škodlivý kód se může maskovat jako platné požadavky klienta a běžná data aplikace. |  |  |
|  | Mnohočetná pravidla, zdroje, kategorie: systém při konfiguraci IPS/IDS podporuje více zdrojů pravidel, včetně plovoucích pravidel, pravidel pro skupiny a pravidel pro rozhraní. |  |  |
|  | Databáze hrozeb: Řešení IDS/IPS lze nakonfigurovat tak, aby detekované síťové události pouze zaznamenávalo, nebo aby je zaznamenávalo i blokovalo. To se provádí pomocí detekčních signatur, tzv. pravidel. Pravidla si může uživatel vytvořit sám nebo lze povolit a stáhnout některou z několika předem připravených sad pravidel. Předpřipravené sady pravidel nabízejí dodatečnou detekci/ochranu před nově vznikajícími hrozbami. |  |  |
|  | Databáze IP blacklistů: možnost vytvářet si své blacklisty, stahovat předdefinované sady s blacklistovanými IP adresami. |  |  |
|  | Předefinovaná pravidla: systém je v základu vybaven řadou automaticky přidaných pravidel brány firewall. Mezi ně patří například anti-lockout, anti-spoofing, blokování privátních sítí, blokování sítí Bogon, používání protokolu IPsec a přístup k portům, výchozí pravidlo deny atd. |  |  |
|  | Konfigurace per interface: Systém umožňuje pro každé rozhraní LAN nebo WAN nezávisle konfigurovat pravidla brány firewall a další funkce pro jednotlivá rozhraní. |  |  |
|  | Eliminace falešných poplachů: Systém umožňí zvolit konkrétní sadu pravidel a zásady upozorňování pro jednotlivá rozhraní a nabízí také podrobné pokyny, jak eliminovat falešné poplachy. |  |  |
|  | DPI:  Hloubková kontrola paketů (DPI) musí umožnit bezpečnostním analytikům zachytit a vyhodnotit kompletní informace o záhlaví a užitečném zatížení paketů a identifikovat tak dodržování protokolů, spam, viry, narušení a další anomální nebo škodlivé přenosy. |  |  |
|  | Blokování aplikací:  Systém musí umožnit detekovat provoz zvolených aplikací, monitorovat jej a spravovat jejich chování v síti. |  |  |
| **VPN server** | | | |
|  | Firewall musí být integrovatelný s externími servery pro služby, které vyžadují ověření uživatele: IPsec, SSLVPN, IoT, secure VPN. Podporovány musí být vytáčené VPN i permanentní VPN konexe. |  |  |
|  | podpora IPsec |  |  |
|  | Řešení VPN, které umožňuje realizovat zabezpečená připojení typu point-to-point nebo site-to-site ve směrovaných nebo přemostěných konfiguracích a zařízeních pro vzdálený přístup. |  |  |
|  | Typy VPN: Podpora site-to-site VPN a remote-access VPN. |  |  |
|  | SSL: plná podpora v rámci VPN. |  |  |
|  | VPN klient pro různá prostředí:  VPN musí podporovat klienty stávajících operačních systémů: BSD, Linuxu, Androidu, Mac OS X, iOS, Windows a novějších a telefonů VoIP. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
|  | Podpora pro IPv6:  VPN může být současně přenášen provoz IPv4 i IPv6. Protokol IPv6 je podporován jak u klientů site-to-site, tak u mobilních klientů, a lze jej tak použít k doručení protokolu IPv6 do lokality, která má pouze připojení IPv4. |  |  |
|  | Split tunneling:  Musí umožnit uživateli přistupovat k různým bezpečnostním doménám, např. k veřejné síti a místní síti LAN nebo WAN, současně pomocí stejných nebo různých síťových připojení. |  |  |
|  | Vícenásobné VPN tunely:  Systém musí podporovat možnost vytvoření více tunelů VPN přes jedno fyzické rozhraní. |  |  |
|  | VPN tunel failover:  Podpora jak pro VPN, tak pro IPSec. |  |  |
|  | Autentizace:  Podporovaná musí být jak autentizace přes stávající MS AD, LDAP a RADIUS server tak lokální autorizace proti VPN serveru. (zadavatel umožňuje nabídnout rovnocenné řešení) |  |  |
| **Filtrování obsahu** | | | |
|  | HTTP a HTTPS proxy. |  |  |
|  | Transparentní proxy a podpora non-transparent proxy. |  |  |
| **Filtrování URL a domén** | | | |
|  | Filtrování domén a URL:  Musí být využíván black list pro kontrolu přístupu. Administrátor musí mít možnost tento list manuálně upravovat dle potřeby tj. přidávat i ubírat filtrované domény a IP. |  |  |
|  | Antivirus:  Systém musí být možno nakonfigurovat tak, aby fungoval jako antivirový proxy server pomocí HAVP (HTTP Antivirus Proxy). Antivirové proxy servery se musí chovat jako tradiční webové proxy server, pouze skenují veškerý obsah procházející přes proxy server na přítomnost virů nebo signatur malwaru. Pokud proxy server identifikuje obsah jako škodlivý, stahování bude zablokováno a klientský počítač bude přesměrován na chybovou stránku. |  |  |
|  | Ochrana před nežádoucími výsledky vyhledávání ve vyhledávačích na internetu. |  |  |
|  | Podpora HTTPS URL a obsahový screening. |  |  |
|  | Logování přístupu k webovým stránkám. |  |  |
|  | Musí provádět Domain Name blacklisting. |  |  |
|  | Reporty:  Systém musí umožnit sledovat používání internetu. Procházením protokolů o přístupu k proxy serverům lze vytvářet webové přehledy, které podrobně popisují adresy URL, k nimž každý uživatel v síti přistupoval podle data a času, využití šířky pásma a přehledy nejnavštěvovanějších stránek - aniž by o tom uživatelé sítě věděli. |  |  |
| **Síťové služby** | | | |
|  | Dynamic DNS |  |  |
|  | DHCP server |  |  |
|  | DNS forwarding |  |  |
| **Konfigurace** | | | |
|  | Konfigurace přes webový prohlížeč v českém a anglickém jazyce. |  |  |
|  | Sada předdefinovaných wizardů pro konfiguraci systému. |  |  |
|  | Možnost vzdálené administrace pomoci SSH protokolu. |  |  |
|  | Konfigurovatelné přehledové „dashboardy“. |  |  |
|  | Nástroje pro snadnou zálohu a obnovu systému. |  |  |
|  | Nástroje pro sledování změn v konfiguraci s možnosti porovnání těchto změn a návratu k funkční konfiguraci. |  |  |
|  | Velmi detailně nastavitelná práva pro administrátory systému. |  |  |
|  | Granulární definice politik per IP adresa/síť, uživatelská identita, IP adresa/síť/uživatel, odesílatel/příjemce/doména, výjimky v definici politik per soubor. |  |  |
|  | Systém udpdatů. |  |  |
| **Autentizace uživatelů** | | | |
|  | Ověřování proti lokální databázi stávající MS AD, LDAP anebo RADIUS serveru. |  |  |
|  | Možnost definic skupin uživatelů. |  |  |
|  | Možnost definice platnosti účtu. |  |  |
|  | Automatické blokování uživatelů po neplatném pokusu o přihlášení. |  |  |
|  | System Security Management. |  |  |
|  | Zabezpečení konfigurační konzole přes SSL protokol. |  |  |
|  | Cross-site Request Forgery ochrana. |  |  |
|  | Vynucování http odkazů. |  |  |
|  | DNS rebinding protection. |  |  |
|  | http Strict Transport Security. |  |  |
| **Odolnost a spolehlivost systému** | | | |
|  | Podpora high availability clusteringu. |  |  |
|  | Podpora multi-WAN pro loadbalancing a failover. |  |  |
|  | Reverzní proxy. |  |  |
|  | Automatický failover po ztrátě spojení. |  |  |
|  | Bandwidth throttling. |  |  |
|  | Traffic Shapping. |  |  |
|  | Traffic priority. |  |  |
| **Monitoring, reporting a podpora** | | | |
|  | Detailní analýza všech aktivit (zápisy do registrů, změny ve filesystem, síťové spojení, analýza systémových procesů). |  |  |
|  | Customizovatelné dashboardy s přehledy. |  |  |
|  | Real-time grafy provozu a charakteristik. |  |  |
|  | SNMP monitoring. |  |  |
|  | Systém notifikací. |  |  |
|  | Dostupné API. |  |  |
|  | Podpora pro firewall v rozsahu aktualizací produktu a bezpečnostních databází pro spolehlivý a bezpečný provoz po dobu 5ti let. |  |  |
|  | **V nabídce doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry.** |  |  |
|  | **Dodaný předmět veřejné zakázky musí být určen k distribuci v České republice v nabídce doložte potvrzení lokálního zastoupení výrobce.** |  |  |

### Gigabitové přepínače – 2 ks

Tabulka 6: Gigabitové přepínače – 2 ks

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Gigabitové přepínače, které podporují statické směrování, směrování OSPF a IP Layer 3 směrování.  Systém umožňuje vytvořit virtuální strukturu a tím spravovat více přepínačů jako jedno logické zařízení, které zvyšuje odolnost, výkon a dostupnost sítě a zároveň snižuje provozní složitost systému. |  |  |
|  | Porty, sloty:  min. 48x RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T);  Duplex: 10BASE-T/100BASE-TX: half or full; 1000BASE-T: full only |  |  |
|  | Paměť:  min. 256MB Flash  min. 512MB RAM |  |  |
|  | Formát:  Montovatelný do 19“ RACKu |  |  |
|  | Výkon:  1000 Mb Latency < 5 µs  10 Gbps Latency < 3 µs  Throughput min. 131 Mpps  Routing/Switching capacity min. 176 Gbps  Routing table size min. 1024 entries  MAC address table size 16384 entries |  |  |
|  | Pracovní podmínky:  Rozsah pracovních teplot: od -5°C do 45°C.  Povolená vlhkost pro provozní podmínky: od 10% do 90%, bez kondenzace. |  |  |
|  | PoE výkon:  min. 370 W PoE+  Automatická detekce zařízení PoE |  |  |
|  | Standard OpenFlow:  Podporuje specifikaci OpenFlow 1.3, která umožňuje SDN díky oddělení datových (předávání paketů) a řídicích (rozhodování o směrování) cest. |  |  |
|  | Standard QoS:  Umožňuje omezit rychlost vysílání, aby se snížil nežádoucí provoz vysílání v síti.  Služba QoS založená na klasifikátorech – zařízení klasifikuje provoz pomocí více kritérií na základě informací z 2., 3. a 4. vrstvy; aplikuje zásady QoS, jako je nastavení úrovně priority a omezení rychlosti pro vybraný provoz na portu, VLAN nebo celém přepínači.  Podpora následujících akcí při přetížení:  Řazení do fronty striktně dle prioritoy (SP), vážené řazení s kruhovou rotací (WRR) a SP+WRR  Podpora přístupové rychlosti (CAR) a linkové rychlosti. |  |  |
|  | Konektivita:  Poskytuje min. 48 pevných portů 10/100/1000BASE-T v přepínači vrstvy 2/vrstvy 3.  Na všech portech podporuje napájení přes Ethernet (PoE+) podle standardu IEEE 802.3at.  Auto-MDIX - automaticky se přizpůsobí pro přímé nebo křížené kabely na všech portech 10/100/1000  Zajišťuje zpětnou vazbu pomocí standardu IEEE 802.3x, čímž snižuje přetížení v situacích s velkým provozem.  Umožňuje detekci problémů na vrstvě datového spoje, které se vyskytly v "poslední míli", pomocí standardu IEEE 802.3ah OAM. |  |  |
|  | Vysoká dostupnost:  Zařízení musí mít redundantní napájení.  Podporuje Spanning Tree/MSTP, RSTP, PVST+, RPVST+ - redundance spojů s podporou protokolů, jako jsou Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), Per-VLAN Spanning Tree (PVST+), Rapid Per-VLAN Spanning Tree (RPVST+), Equal-Cost Multipath (ECMP) a Smart Link, pro zajištění vysoké dostupnosti.  Zařízení podporuje oddělení datových a management cest pro tj. udržuje je odděleně pro zvýšení bezpečnosti a výkonu.  Zařízení podporuje vytváření virtuálních sítí, kde dva nebo více přepínačů fungují jako jeden přepínač L2 a směrovač L3 přičemž přepínače nemusí být umístěny společně a mohou být součástí DRP;  Servery nebo přepínače lze připojit pomocí standardního protokolu LACP pro automatické vyrovnávání zátěže a vysokou dostupnost. |  |  |
|  | Routing na 3 vrstvě:  Zařízení musí podporovat:  Statické směrování IP, Protokol OSPF s podporou protokolů OSPFv1/v2 a OSPFv3, RIP - podporuje směrování RIPv1 a RIPv2 a obsahuje ochranu proti smyčkám. |  |  |
|  | Správa:  Zařízení umožňuje konfiguraci a správu prostřednictvím zabezpečeného webového prohlížeče nebo rozhraní CLI umístěného na vzdáleném zařízení.  Poskytuje bezpečné, snadno použitelné grafické rozhraní pro konfiguraci zařízení prostřednictvím protokolu HTTPS  Zařízení umí řídit oprávnění, tj. umí poskytnout přístup pouze pro čtení (operátor) a čtení/zápis (manažer) a to na rozhraních pro správu CLI a webového prohlížeče.  Využívá protokol TACACS k propojení vlastního seznamu příkazů CLI s přihlášením jednotlivého správce sítě; poskytuje auditní stopu provedených úkonů.  Zařízení provádí kompletní protokolování relací s tím, že poskytuje podrobné informace pro identifikaci a řešení problémů  Používá standardní protokol SNMP k monitorování základních síťových funkcí; podporuje skupiny událostí, alarmů, historie a statistik a privátní skupinu rozšíření alarmů.  Plně podporuje IEEE 802.1AB Protokol LLDP (Link Layer Discovery Protocol)  Podporuje sFlow (RFC 3176) tj. poskytuje škálovatelné monitorování sítě na bázi ASIC bez dopadu na výkon sítě a umožňuje shromažďovat informace o síti pro účely plánování kapacity a monitorování sítě v reálném čase.  Podpora VLAN umožňující segmentovat provoz do a z rozhraní pro správu, včetně rozhraníCLI/telnet, rozhraní webového prohlížeče a SNMP.  Umožňuje zrcadlit vstupní provoz vybraný pomocí ACL z portu přepínače nebo VLAN do místního nebo vzdáleného portu přepínače kdekoli v síti.  Podpora protokolu DLDP (Device Link Detection Protocol) - monitoruje trasu mezi dvěma kompatibilními přepínači a vypíná porty na obou koncích, pokud je kabel přerušen, což zabraňuje problémům v síti, jako jsou smyčky  Správa na úrovni protokolu IPv6 - přepínač lze spravovat bez ohledu na to, zda připojená síť používá protokol IPv4 nebo IPv6; podporuje protokoly pingv6, tracertv6, Telnetv6, TFTPv6, DNSv6, syslogv6, FTPv6, SNMPv6, DHCPv6 a RADIUS pro IPv6.  Zařízení monitoruje vstupní a výstupní porty a umožňuje řešení problémů v síti a podporuje virtuální testy kabelů,  Vestavěný nástroj pro správu sítě s webovým grafickým uživatelským rozhraním, který zjednodušuje provoz a usnadňuje centralizovanou správu. Nástroj umožňuje centralizované zálohování konfigurace, správu verzí softwaru a bezproblémovou výměnu přepínačů.  Vestavěný nástroj na identifikaci a správu poruch, konfiguraci prvků a monitorování sítě z centrálního bodu; správce sítě může centrálně spravovat všechny síťové prvky pomocí řady automatizovaných úloh, včetně zjišťování, kategorizace, základních konfigurací a imagů; software rovněž poskytuje nástroje pro porovnávání konfigurací, dohledávání verzí, alertování změn a další  Zařízení podporuje SNMP v1/v2c/v3, MIB-II s Traps a RADIUS Authentication Client MIB (RFC 2618); Zařízení obsahuje vestavěný nástroj pro správu HTML se zabezpečeným přístupem. |  |  |
|  | Bezpečnost:  Podporuje ACL (Access Control Lists) - poskytuje filtrování provozu na 2. až 4. vrstvě IP; podporuje globální ACL, VLAN ACL, port ACL a IPv6 ACL.  Podporuje IEEE 802.1X - standardní metoda ověřování uživatelů pomocí IEEE 802.1X na klientovi ve spojení se serverem RADIUS.  Podporuje ověřování na základě MAC, kdy je klient ověřován serverem RADIUS na základě MAC adresy.  Podporuje zabezpečení a řízení přístupu založené na identitě:  - Seznamy ACL pro jednotlivé uživatele: povoluje nebo zamítá přístup uživatelů ke konkrétním síťovým prostředkům na základě identity uživatele a denní doby, což umožňuje více typům uživatelů ve stejné síti přistupovat ke konkrétním síťovým službám, aniž by bylo ohroženo zabezpečení sítě nebo hrozil neoprávněný přístup k citlivým datům.  - Automatické přiřazování sítí VLAN: automaticky přiřazuje uživatele do příslušné sítě VLAN na základě jejich identity.  Zabezpečený přístup ke správě prvku:  Poskytuje bezpečné šifrování všech přístupových metod (CLI, GUI nebo MIB) prostřednictvím SSHv2, SSL, HTTPS a/nebo SNMPv3.  Zabezpečené FTP/ SCP: umožňuje zabezpečený přenos souborů do přepínače a z něj; chrání před nežádoucím stažením souboru nebo neoprávněným zkopírováním konfiguračního souboru přepínače.  VLAN pro hosty: poskytuje ověřeným klientům prostředí založené na prohlížeči, které je podobné IEEE 802.1X  Zabezpečení portů: umožňuje přístup pouze k určeným adresám MAC, které určí správce  Izolace portů: zabezpečuje a zvyšuje bezpečnost a zabraňuje útočníkům získat informace o připojených uživatelích.  Ochrana portu STP BPDU: blokuje datové jednotky protokolu mostu (BPDU) na portech, které nevyžadují BPDU, a zabraňuje tak útokům pomocí falešných BPDU.  Ochrana kořenového STP: Chrání kořenový STP před škodlivými útoky nebo chybami v konfiguraci.  Ochrana DHCP: blokuje pakety DHCP z neautorizovaných serverů DHCP, čímž zabraňuje útokům typu "denial-of-service".  Ochrana zdroje IP: pomáhá zabránit útokům na podvržení IP adresy  Dynamická ochrana ARP: blokuje broadcasty ARP od neautorizovaných hostitelů, čímž zabraňuje odposlechu nebo krádeži síťových dat.  RADIUS/HWTACACS: usnadňuje správu zabezpečení správy přepínače pomocí serveru pro ověřování hesla. |  |  |
|  | Výkon:  Systém využívá nonblocking architekturu: podporuje až 176 Gb/s a přepínací rychlost s propustností až 130,9 Mpps.  Hardware-based wiresppeed ACL:  Vysoká úroveň zabezpečení a snadná správa bez dopadu na výkon sítě s implementací ACL založené na TCAM. |  |  |
|  | Konvergence:  IEEE 802.1AB Protokol LLDP (Link Layer Discovery Protocol): usnadňuje mapování pomocí aplikací pro správu sítě s automatizovaným protokolem LLDP pro zjišťování zařízení.  LLDP-MED: umožňuje automaticky konfigurovat síťová zařízení, včetně IP telefonů podporujících protokol LLDP.  Kompatibilita s LLDP-CDP: přijímá a rozpoznává pakety CDP z IP telefonů Cisco pro bezproblémovou funkci.  Napájení přes Ethernet podle standardu IEEE 802.3at (PoE+): poskytuje až 30 W na port.  Přidělení výkonu PoE:  podpora více metod ­– automatickou, třídy IEEE 802.3af, LLDP-MED nebo zadanou uživatelem.  Hlasová síť VLAN: automaticky přiřazuje VLAN a priority pro IP telefony.  IP multicast snooping (datově řízený IGMP): Automaticky zabraňuje zahlcení přenosy IP multicast. |  |  |
|  | L2 Switching:  Zařízení podporuje:  min. 16K tabulku MAC adres  VLAN tagy:  podpora standardu IEEE 802.1Q s 4 094 současnými ID VLAN.  IEEE 802.1ad QinQ a selektivní QinQ.  Agregace 10GbE portů: umožňuje seskupení portů pro zvýšení celkové propustnosti dat do vzdáleného zařízení.  Protokol DLDP (Device Link Detection Protocol): monitoruje propojení linek a vypíná porty na obou koncích, pokud je zjištěn jednosměrný provoz, čímž zabraňuje vzniku smyček v sítích založených na STP  Jumbo Frame: zlepšuje výkon velkých datových přenosů; podporuje rámce o velikosti až 9 Kb. |  |  |
|  | L3 Switching  Zařízení podporuje:  Protokol ARP (Address Resolution Protocol): určuje MAC adresu jiného IP hostitele ve stejné podsíti; podpora statické ARP; ARP umožňuje detekci duplicitních IP adres.  Proxy ARP umožňuje normální provoz ARP mezi podsítěmi nebo v případě, že jsou podsítě odděleny na 2. vrstvě sítě.  Protokol DHCP (Dynamic Host Configuration Protocol): zjednodušuje správu rozsáhlých IP sítí; podpora klienta; DHCP Relay umožňuje provoz DHCP mezi podsítěmi.  Adresa rozhraní zpětné smyčky: definuje adresu, která je vždy dosažitelná, čímž zlepšuje diagnostické možnosti.  Pomocná funkce protokolu UDP (User Datagram Protocol): umožňuje směrovat UDP provoz přes rozhraní směrovače na konkrétní adresy IP unicast nebo subnet broadcast a zabraňuje podvržení serveru pro služby UDP, jako je DHCP.  Mapy tras: poskytuje větší kontrolu při redistribuci tras; umožňuje filtrování a změnu metrik tras  Server DHCP |  |  |
|  | **V nabídce doložte katalogový list produktu (datasheet) podrobně popisující hardwarové i softwarové parametry.** |  |  |
|  | **Dodaný předmět veřejné zakázky musí být určen k distribuci v České republice v nabídce doložte potvrzení lokálního zastoupení výrobce.** |  |  |

## Software

### Virtualizační a operační systém

Tabulka 7: Virtualizační a operační systém

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Součástí dodávky musí být serverový virtualizační systém v nejnovější dostupné verzi, licence musí být dodány s technickou podporou na minimálně 5 let. |  |  |
|  | Licence pro všechny dodávané CPU. |  |  |
|  | Funkce migrace běžících virtuálních serverů. |  |  |
|  | Operační systém kompatibilní se stávajícím OS MS Windows Server (zadavatel umožňuje nabídnout rovnocenné řešení) ve verzi odpovídající aktuálním potřebám dané infrastruktury pro každý server.  Dodavatel musí zajistit, že licencování operačního systému bude plně v souladu s licenčními podmínkami výrobce. |  |  |
|  | Operační systém pro dodaný počet CPU jader. |  |  |
|  | Neomezený počet virtuálních serverů. |  |  |

### Databázový systém

Tabulka 8: Databázový systém

| **č.** | **Specifikace požadavků.** | **Účastníkem nabízená hodnota, výrobce a typ.** | **Splněno [ano/ne]** |
| --- | --- | --- | --- |
|  | Nejnovější dostupná verze. |  |  |
|  | Kompatibilní se stávajícím používaným MS SQL (zadavatel umožňuje nabídnout rovnocenné řešení). |  |  |
|  | Licence umožňující provoz ve vysoce dostupném virtualizačním clusteru. |  |  |
|  | Pro minimálně 8 CPU jader a neomezený počet uživatelů. |  |  |

## Implementace

Tabulka 9: Požadavky – Dodávka a implementace nabízeného řešení

|  |  |  |  |
| --- | --- | --- | --- |
| **č.** | **Specifikace minimálních požadavků** | **Účastníkem nabízená hodnota** | **Splněno [ano/ne]** |
|  | Instalace a konfigurace veškerého dodaného předmětu veřejné zakázky. |  |  |
|  | Zaškolení správců systému (administrátorů) – 2 osoby v celém rozsahu a praktické správy předmětu veřejné zakázky.  Trvání minimálně 16 hodin 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. |  |  |

# Požadavky na servisní podporu provozu

Požadavky na servisní podporu provozu a SLA jsou uvedeny ve smlouvě.

# 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;
2. Dodávka technické dokumentace skutečného provedení díla (tj. administrátorská a uživatelská dokumentace);
3. Protokol o úspěšném provedení akceptačních testů pro příslušnou část.

Předávací protokol musí obsahovat minimálně:

- Úroveň technické podpory.

- Datum konce platnosti technické podpory.

- 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. 5 ZD.

# Harmonogram plnění

Harmonogram plnění je uveden ve smlouvě o dílo a poskytování servisní podpory v příloze č. 5 ZD.

# Seznam zkratek

API Rozhraní pro programování aplikací (Application Programming Interface)

AMS Agentless Management Service

BOSS Boot Optimized Storage Solution

CIFS Common Internet File System

DAS Direct-Attached Storage

DNS Domain Name System

DPI Deep Packet Inspection

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

OSI Open System Interconnection

PPPoE Point-to-Point Protocol over Ethernet

RAID Redundant Array of Independent Disks

SAN Storage Area Network

SAS Serial Attached SCSI

SCOM System Center Operations Manager

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

SSD Solid State Drive

SSH Secure Shell

SSL Secure Sockets Layer

SW Software

VTL Virtual Tape Library