# Střední škola Edvarda Beneše Břeclav

# **TECHNICKÁ SPECIFIKACE**

**KYBERBEZPEČNOST**

1. Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky a dodavatel splnění těchto podmínek potvrdí samostatným čestným prohlášením:
   1. jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
   2. mají plnou záruku od výrobce,
   3. jsou podporovány výrobcem a jsou součástí servisního a podpůrného programu výrobce,
   4. obsahují všechny nezbytné licence na používání příslušného softwaru,
   5. jsou určeny pro provoz v České republice.

Tyto skutečnosti dodavatel doloží:

1. potvrzením výrobce daného zařízení, nebo
2. čestným prohlášením distributora, nelze-li prohlášení výrobce získat, nebo
3. jiným rovnocenným dokladem (doklady) v případě, že doklady dle předchozích písm. a) a b) není dodavatel z důvodů, které mu nelze přičítat, schopen předložit (takové důvody musí dodavatel doložit).
4. Zadavatel si vyhrazuje právo na ověření všech dodaných informací od výrobce daného zařízení a zjištění původu výrobků nejpozději při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.

Dodavatel doloží toto potvrzení ke všem nabídnutým technologiím v níže uvedeným kapitolám technické specifikace:

1. Nástroje pro ochranu integrity komunikačních sítí

* Firewall – 6 ks
* Centrální a přístupové switche – 43 ks
* WiFi AP – 80 ks
* Analýza síťového provozu – 1 ks

1. Nástroj pro zajišťování úrovně dostupnosti informací

* Virtualizační server
* Zálohovací server
* Diskové pole

1. Rozsah migrace zahrnuje dva stávající fyzické servery s operačním systémem Windows Server 2008 R2, které poskytují následující služby:

* Active Directory (AD)
* DNS
* DHCP
* File server

Požadujeme migraci tohoto prostředí na novou virtualizační platformu dodávanou v rámci této veřejné zakázky a zároveň aktualizaci operačního systému na Windows Server 2022 nebo Windows Server 2025 (podle dostupnosti v době implementace).

Upřesnění rozsahu migrace:

1. **Vytvoření nového virtuálního prostředí** na dodávané infrastruktuře dle požadavků v technické specifikaci.
2. **Migrace služeb AD, DNS, DHCP a souborových služeb** ze stávajících fyzických serverů na nové virtuální servery.
3. **Upgrade operačního systému** z Windows Server 2008 R2 na Windows Server 2022/2025.
4. **Zachování stávajícího nastavení všech služeb** včetně uživatelských účtů, skupinových politik, DNS záznamů, DHCP rozsahů a rezervací.
5. **Migrace dat souborového serveru** včetně zachování struktury adresářů a oprávnění.
6. **Testování funkčnosti** a ověření správné funkcionality všech migrovaných služeb.

Dodavatel v rámci implementační fáze provede podrobnou analýzu stávajícího prostředí před zahájením migrace pro zjištění detailních parametrů stávajících serverů a služeb.

Během migrace požadujeme minimalizaci výpadků služeb a provedení migrace mimo běžnou provozní dobu školy (optimálně o víkendu nebo během školních prázdnin) po předchozí dohodě s IT oddělením školy.

**(4)** Na základě dokumentů (Zadávací dokumentace, Smlouva o dodávce, implementaci a technické podpoře řešení a Technická specifikace) dodavatel dodá požadovanou dokumentaci:

**1. Projektová dokumentace kybernetické bezpečnosti**

1.1 Prováděcí projekt

* Právní základ: Bod 5 článku II smlouvy, vyžadující písemný projekt
* Obsah:
  + Popis dodávaného řešení (specifikace HW a SW, funkční schéma)
  + Popis způsobu a postupu implementace do infrastruktury
  + Popis zabezpečení dodávaného řešení včetně zabezpečení informačních a komunikačních systémů během implementace
  + Plán zálohování a obnovy síťové infrastruktury
  + Plán zkušebního provozu a akceptačních testů
  + Plán zaškolení administrátorů a uživatelů
  + Harmonogram postupu prací

1.2 Analýza rizik

* Právní základ: Vyhláška č. 82/2018 Sb., § 5
* Obsah:
  + Identifikace a hodnocení aktiv (s vazbou na dodávané komponenty)
  + Hodnocení hrozeb a zranitelností
  + Stanovení míry rizik a jejich akceptovatelnosti
  + Návrh opatření pro zvládání rizik

**2. Dokumentace provozních bezpečnostních opatření**

2.1 Dokumentace síťové bezpečnostní architektury

* Právní základ: Vyhláška č. 82/2018 Sb., § 19-21
* Obsah:
  + Architektura sítě s popisem bezpečnostních zón
  + Popis implementovaných nástrojů (firewall, switche, analýza síťového provozu)
  + Dokumentace bezpečnostních politik firewallů
  + Dokumentace segmentace sítě a jednotlivých segmentů
  + Popis konfigurace a nastavení NAC
  + Dokumentace monitorovacích politik nástrojů pro analýzu síťového provozu

**2.2 Dokumentace nástrojů pro zajištění integrity komunikačních sítí**

* Právní základ: Vyhláška č. 82/2018 Sb., § 20, Technická specifikace bod "nástroje pro ochranu integrity komunikačních sítí"
* Obsah:
  + Konfigurační dokumentace firewallů (6 ks)
  + Konfigurační dokumentace centrálních a přístupových switchů (43 ks)
  + Konfigurační dokumentace WiFi AP (80 ks)
  + Konfigurace nástroje pro analýzu síťového provozu (1 ks)
  + Popis implementovaných bezpečnostních politik

**2.3 Dokumentace monitorování kybernetické bezpečnosti**

* Právní základ: Vyhláška č. 82/2018 Sb., § 22, Technická specifikace požadavků na monitoring
* Obsah:
  + Dokumentace implementované analýzy síťového provozu
  + Konfigurace systému pro sběr dat a vyhodnocení
  + Popis monitorovacích politik
  + Dokumentace a postupy pro vyhodnocování bezpečnostních událostí
  + Konfigurace sběru a analýzy metrik (RTT, jitter atd.)

**3. Dokumentace technických bezpečnostních opatření**

3.1 Dokumentace virtualizačního prostředí

* Právní základ: Vyhláška č. 82/2018 Sb., § 25, Technická specifikace v části virtualizace
* Obsah:
  + Architektura virtualizačního prostředí
  + Bezpečnostní konfigurace virtualizace
  + Dokumentace nasazení a konfigurace virtuálních systémů
  + Dokumentace migrace stávajícího prostředí virtuálních serverů

3.2 Dokumentace zálohování a obnovy

* Právní základ: Vyhláška č. 82/2018 Sb., § 26, Technická specifikace v části zálohování
* Obsah:
  + Konfigurace zálohovacího serveru
  + Dokumentace zálohovacích politik serverové infrastruktury
  + Konfigurace a implementace HARDENED REPOSITORY
  + Postupy pro ověření zálohování a obnovu
  + Dokumentace použitých nástrojů (zálohovací server, diskové pole)

3.3 Dokumentace fyzické bezpečnosti

* Právní základ: Vyhláška č. 82/2018 Sb., § 27
* Obsah:
  + Popis fyzické bezpečnosti serverového HW
  + Implementace UPS a její konfigurace
  + Dokumentace fyzického rozmístění síťových prvků

**4. Dokumentace testů a auditu**

4.1 Dokumentace akceptačních testů

* Právní základ: Smlouva, bod 5.5, povinnost provedení akceptačních testů
* Obsah:
  + Protokol z testu výpadku jednoho fyzického nodu
  + Protokol z testu výpadku napájení
  + Protokol z testu obnovy libovolného serveru či dat ze zálohy
  + Výsledky ověření monitorovacích pravidel a testovacího provozu

**5. Dokumentace pro akceptaci a provoz**

5.1 Zákaznická dokumentace

* Právní základ: Společné požadavky - "Zákaznická dokumentace bude zahrnovat"
* Obsah:
  + Popis všech prvků/zařízení
  + Popis způsobu zálohy a obnovy konfigurace všech prvků/zařízení
  + Veškeré požadavky na zachování záruky/podpory
  + Informace o způsobu řešení servisních požadavků

**5.2 Provozní a administrátorská dokumentace**

* Právní základ: Společné požadavky - "Součástí instalace musí být i zaškolení IT administrátorů"
* Obsah:
  + Dokumentace ke konfiguraci všech komponent
  + Dokumentace k monitoringu činnosti
  + Postupy pro aktualizace všech komponent
  + Dokumentace řešení problémů
  + Postupy zálohování konfigurace

**Souhrnné požadavky na bezpečnostní dokumentaci**

Dokumentace musí:

1. Být v souladu s požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti
2. Odpovídat vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti
3. Obsahovat popis implementovaných bezpečnostních opatření
4. Poskytovat podklady pro zajištění akceptace plnění dle požadavků Výzvy č. 40
5. Být dostatečně podrobná pro administrativní správu systému IT pracovníky zadavatele
6. Být v českém jazyce, z čehož se připouští následující výjimky:

* V případě technických manuálů výrobců k dodávaným komponentám, kde není oficiální česká verze k dispozici, zadavatel připustí originální manuály v anglickém jazyce.
* V případě specifických technických popisů, diagramů nebo schémat s technickou terminologií, kde by překlad mohl vést k významovým posunům nebo nepřesnostem, je možné tyto části ponechat v anglickém jazyce s doplněním českého vysvětlujícího popisu.
* V případě exportů konfiguračních souborů, logů nebo výstupů z analytických nástrojů, které jsou standardně generovány v anglickém jazyce, není překlad vyžadován.

1. Obsahovat veškeré náležitosti pro splnění projektových indikátorů a prokázání účelu projektu

Dodavatel je povinen v rámci akceptace plnění napravit nalezené chyby vysoké závažnosti v implementaci technických opatření a poskytovat součinnost při auditu implementovaných bezpečnostních opatření.

Nástroje pro ochranu integrity komunikačních sítí

### FIREWALL – 2 KS

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje požadavky (ANO/NE) |
| Provedení a funkcionalita | * Do racku 1U, včetně montážního kitu * Front to back airflow * Standardní rozměry do racku velikosti 19” * 2x redundantní zdroj napájení typu AC * Výrobce musí umožňovat správu firewallu na mezi-platformově jednotném operačním systému – usnadnění administrativní zátěže * Ověření zařízení na úrovni certifikátů založených na metodě TPM * Funkce DHCP serveru * Možnost redundance internetového připojení * Funkcionalita NAT (IPv4 a IPv6 NAT) * Funkčnost protokolu LLDP * Podpora sZTP (Secure Zero Touch Provisioning) * Možnost připojení USB flash disku * Zařízení umožňuje prohlížení a změny konfigurace bez vlivu na aktivně běžící konfiguraci (administrátor může aktivovat dle uvážení) * Možnost uložení více než 40 starších verzí konfigurací s možností jejich opětovného použití * Validace konfigurace před aktivací administrátorem * Možnost nastavení specifického času pro aktivaci předem připravené konfigurace |  |
| Porty | * Min. 16x GE RJ45 a zároveň min. 4x SFP+ port * Min. 2x SFP28 port * Dedikovaný konzolový port – min. 1x * Dedikované out-of-band MGMT rozhraní 1GbE RJ45 * Kompatibilita pro 1G transceivery * Dva fyzicky oddělené porty pro HA (High Availability):   + Alespoň jeden pro systémová data, synchronizaci konfigurace a heartbeats   + Alespoň jeden pro synchronizaci stavových toků a průtok datového provozu mezi nody v případě active/active HA * Konfigurace L2 a L3 interface * Telemetrický interface (gRPC nebo alternativní) * LACP bonding * MACsec na portech zařízení * Možnost přepnutí datových portů do L2 switching módu (kromě dedikovaných OOB mgmt interface a HA portů) |  |
| NGFW | * Funkcionality NG Firewall:   + IPS (Intrusion Prevention System)   + Aplikační firewall   + URL filtering   + Antimalware a botnet ochrana * Podpora zero-day ochrany, inspekce SSL provozu, sandbox emulace provozu * Plná integrace IPS a firewallu * Předdefinované a použitelné šablony IPS politik * Definice IPS pravidel pomocí kombinace src, dst, služba, IPS kontrola * Možnost nastavit IPS v režimech:   + Detect and log   + Detect and block   + Detect and log and block * NG funkcionality konfigurovatelné na úrovni bezpečnostních politik * Možnost SSL/TLS inspekce * Podpora TLS 1.2 a TLS 1.3 * Min. 4500 předdefinovaných aplikačních signatur * Min. 16 000 předdefinovaných IPS signatur |  |
| Funkcionalita FW a OS | * Blokování spojení na úrovni DNS názvu (zabránění komunikace na konkrétní DNS záznamy) * Možnost konfigurace na sobě nezávislých routovacích tabulek * Možnost konfigurace logických bezpečnostních zón * Min. 400 logických bezpečnostních zón, mezi kterými lze konfigurovat bezpečnostní politiky * Možnost konfigurace bezpečnostních politik * Min. 14 000 konfigurovatelných bezpečnostních politik * Velikost RIB – min. 1,5 milionu záznamů * Velikost FIB – min. 1 milion záznamů (pro možnost nasazení Full BGP) * Možnost přidat komentář ke každému pravidlu * Možnost časově omezit platnost pravidel * Možnost paralelní práce více administrátorů * Detekce kolizí a duplicit v politikách * Možnost definice skupin oprávnění ke změnám konfigurace pro administrátory * Konfigurace politik a nastavení prostřednictvím GUI * Možnost připojení skrze REST API * NETCONF připojení na firewall s možností uživatelsky definovaného čísla portu * Výrobce musí poskytovat sadu automatizačních nástrojů (operační a jiné skripty) * Robustnost OS: * Výpadek management procesu nemá vliv na ostatní procesy zařízení * Není dopad na koncové uživatele komunikující skrze firewall * Podpora firewallové inspekce EVPN-VXLAN provozu (L4 a L7) * Layer 2 forwarding pomocí ASIC čipu * N+1 redundance – zachování propustnosti i při výpadku jednoho prvku HA * OS musí splňovat robustnost HW oddělením Control a Forwarding plane * Více než 2500 VLAN, možnost konfigurace VLAN L3 interface ve všech definovaných VLAN * Protokoly pro dynamické směrování:   + OSPFv2, OSPFv3 a BGP * BFD (Bidirectional Forwarding Detection) pro:   + Static   + OSPF   + BGP * Alespoň 200 OSPF navázaných sousedství * Alespoň 1500 BGP peerů |  |
| Interní úložiště | min. 100GB SSD |  |
| Počet současných spojení | min. 1,8M |  |
| Počet nových spojení za sekundu | 150tis. |  |
| Počet IPsec VPN tunellů | Alespoň 1,5tis. |  |
| Propustnosti | min. 7 Gbps (imix) |  |
| Propustnost L4 stavového firewallu min 10 Gbps (Enterprise mix). |  |
| Propustnost NGFW (L4 firewall + IPS + aplikační kontrola min 17Gbps na průměrných HTTP stavových spojeních). |  |
| Propustnost aplikační kontroly + IDP + URL filtering + feedy bezpečnostní inteligence + sandbox min 2 Gbps na HTTP stavových spojeních s krátkou životností |  |
| IPsec VPN min. 7 Gbps (imix) |  |
| Logování | * Možnost logování na úrovni bezpečnostních politik s možností odesílat tyto logy na externí kolektor logů a s možností určení zda bude logováno při inicializaci nebo ukončení stavového spojení tekoucího touto politikou * Umožňuje lokální uchovávání logů po dobu definovanou velikostí úložiště, typicky několik dní až týdnů, s možností rotace a archivace dle nastavení. |  |
| Zabezpečení VPN | Umožňuje dvoufaktorové ověřování pomocí mobilní aplikace |  |
| Vysoká dostupnost | Redundantní HA konfigurace řešení složená min ze dvou fyzických prvků.  HA redundance active-active i active-standby, umožňující stavovou synchronizaci |  |
| Dualstack | podpora současného běhu IPv4 a IPv6 |  |
| Aplikační kontrola | Umožňuje detekovat, monitorovat a řídit přístup k síťovým aplikacím na základě jejich signatur, nikoli pouze podle portů. Tato funkce zahrnuje také kontrolu komunikace v šifrovaných protokolech, jako jsou HTTPS, IMAPS nebo POP3S. |  |
| Antivirus | Cloudový antivirový systém. Podporuje archivaci škodlivého obsahu. Chrání proti virům, červům, trojským koním, spyware a dalším typům malwaru. |  |
| URL filtering | Omezuje přístup na webové stránky podle kategorií (např. sociální sítě, hazard). Může být implementováno lokálně nebo prostřednictvím cloudového serveru. |  |
| Kategorizace a blokace provozu | Umožňuje kategorizaci webového obsahu s možností monitorování navštívených kategorií na úrovni uživatele nebo skupiny. Dále nabízí možnost nastavení kvót, které omezují dobu přístupu uživatele k určitým kategoriím během dne. |  |
| Antispam | Poskytuje antispamovou a antivirovou inspekci elektronické pošty. |  |
| Sandbox | Nabízí možnost integrování sandboxu s firewallem pro ověřování škodlivosti kódu jeho spuštěním v reálném operačním systému. Poskytuje ochranu proti známým i neznámým hrozbám, včetně zero-day útoků. Technologie sandboxingu umožňuje izolovanou analýzu podezřelých souborů a kódu v bezpečném prostředí, čímž zajišťuje maximální ochranu produkční sítě. (tato služba však nemusí být součástí základní dodávky). |  |
| Aktualizace | Automatické aktualizace bezpečnostních funkcí poskytované výrobcem zařízení zajišťují aktuálnost ochrany. |  |
| Ověřování uživatelů | Integrace s AD s možností RADIUS nebo TACACS+  Funkcionalita 802.1X  Podpora definice bezpečnostních politik na základě ověřování uživatelů vůči AD/LDAP |  |
| Management a monitoring | HTTP/S, SSH, SNMP, syslog |  |
| Transceivery | Dodání 4 ks Single-mode transceiverů pro HA porty, tak aby byla zajištěna plná funkčnost HA |  |
| Modul SFP28-25G-SR 4ks - od stejného výrobce pro datové porty |  |
| Modul SFP+ -10G-SR 8ks - od stejného výrobce |  |
| Modul SFP-1G-LX 2ks - od stejného výrobce pro datové porty |  |
| Transceivery musí být kompatibilní s dodaným řešením |  |
| Záruka | min. 36 měsíců v režimu 24x7 poskytovaná výrobcem zařízení nebo jeho partnerem. Doručení náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a zalicencovaných funkcí. |  |

### FIREWALL – 4 KS

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje požadavky (ANO/NE) |
| Provedení a funkcionalita | * Do racku 1U, včetně montážního kitu * Front to back airflow * Standardní rozměry do racku velikosti 19“ * 2x redundantní zdroj napájení typu AC * Výrobce musí umožňovat správu firewallu na mezi-platformově jednotném operačním systému, cílem je usnadnění administrativní zátěže * Funkce DHCP serveru * Možnost redundance internetového připojení * Funkcionalita NAT (IPv4 a IPv6 NAT) * Funkčnost protokolu LLDP * Podpora sZTP (Secure Zero Touch Provisioning) * Možnost připojení USB flash disku * Zařízení umožňuje prohlížení a změny konfigurace bez vlivu na aktivně běžící konfiguraci. Administrátor může tuto konfiguraci převést na aktivní dle svého uvážení * Zařízení umožňuje uložení více než 40 starších verzí konfigurací s možností jejich použití jako aktivní konfigurace * Zařízení umožňuje validaci konfigurace před tím, než administrátor provede její aktivaci * Administrátor může nastavit specifický čas, kdy dojde k aktivování předem připravené konfigurace |  |
| Porty | * Min. 8x GE RJ45 a zároveň zařízení musí disponovat **minimálně:**   **8× SFP/SFP+ porty s podporou rychlostí 1GbE i 10GbE**.   * Do těchto portů požadujeme dodat optické transceivery s následujícími parametry:   + 4× SFP transceiver (1GbE) pro připojení stávající infrastruktury   + 2× SFP+ transceiver (10GbE) pro připojení páteřní sítě a serverových systémů * Dedikovaný konzolový port – min. 1x * Rozhraní pro konzolový přístup * Dedikované out-of-band MGMT rozhraní 1GbE RJ45 * Kompatibilita pro 1G transceivery * Konfigurace L2 a L3 interface * Telemetrický interface (gRPC nebo alternativní) * LACP bonding * MACsec na portech zařízení * Možnost přepnutí datových portů do L2 switching módu (kromě dedikovaných OOB mgmt interface a HA portů) |  |
| NGFW | * Funkcionality NG Firewall – IPS, aplikační firewall a URL filtering, antimalware a botnet ochrana * Podpora zero-day ochrany, inspekce SSL provozu, sandbox emulace provozu * Plná integrace IPS a firewallu * Předdefinované a použitelné šablony IPS politik * Definice IPS pravidel pomocí kombinace src, dst, služba, IPS kontrola * Možnost nastavit IPS v režimech detect and log, detect and block, detect and log and block * NG funkcionality konfigurovatelné na úrovni bezpečnostních politik * Možnost SSL/TLS inspekce, možnost pracovat s TLS1.2 a TLS1.3 * Min. 3000 předdefinovaných aplikačních signatur * Min. 16 000 předdefinovaných IPS signatur |  |
| Funkcionalita FW a OS | * Operační systém výrobce musí splňovat požadavek na robustnost HW oddělením Control a Forwarding plane * Blokování spojení na úrovni DNS názvu, cílem tohoto požadavku je zabránit komunikaci na konkrétní DNS záznamy * Možnost konfigurace na sobě nezávislých routovacích tabulek * Možnost konfigurace logických bezpečnostních zón * Min. 400 logických bezpečnostních zón, napříč kterými lze konfigurovat bezpečnostní politiky * Možnost konfigurace bezpečnostních politik * Min. 3000 konfigurovatelných bezpečnostních politik * Možnost přidat komentář ke každému pravidlu * Možnost časově omezit platnost pravidel * Možnost práce a změn více administrátorů paralelně * Detekce kolizí a duplicit v politikách * Možnost definice skupin oprávnění ke změnám konfigurace pro administrátory * Konfigurace politik a nastavení prostřednictvím GUI * Možnost připojení skrze REST API * NETCONF připojení na firewall s možností uživatelsky definovaného čísla portu * Výrobce musí poskytovat sadu automatizačních nástrojů (operační a jiné skripty) * Operační systém výrobce poskytuje robustnost na úrovni výpadku procesu, který nutně nemusí ovlivnit chod celého zařízení (např. výpadek management procesu nemá vliv na ostatní procesy zařízení a tím pádem není dopad na koncové uživatele komunikující skrze firewall) * Layer 2 forwarding * Více než 2500 VLAN, možnost konfigurace VLAN L3 interface ve všech definovaných VLAN * Protokoly pro dynamické směrování OSPFv2, OSPFv3 a BGP * BFD (static, OSPF, BGP) |  |
| Interní úložiště | min. 5GB SSD |  |
| Počet současných spojení | min. 350 tisíc |  |
| Počet nových spojení za sekundu | min 15 tisíc |  |
| Počet IPsec VPN tunellů | min. 1,5 tisíce |  |
| Propustnosti | Propustnost L4 stavového firewallu min 1,5 Gbps (Enterprise mix). |  |
| Propustnost NGFW (L4 firewall + IPS + aplikační kontrola min 400Mbps na 64kb transakcích). |  |
| Propustnost L4 Firewall + aplikační kontroly + IDP + URL filtering + feedy bezpečnostní inteligence min 250Mbps |  |
| IPsec VPN min. 300 Mbps (imix) |  |
| Logování | Možnost logování na úrovni bezpečnostních politik s možností odesílat tyto logy na externí kolektor logů a s možností určení zda bude logováno při inicializaci nebo ukončení stavového spojení tekoucího touto politikou.  Logy ukládané do souborů. |  |
| Zabezpečení VPN | Umožňuje dvoufaktorové ověřování pomocí mobilní aplikace |  |
| Vysoká dostupnost | Redundantní HA konfigurace řešení složená min ze dvou fyzických prvků.  HA redundance active-active i active-standby, umožňující stavovou synchronizaci |  |
| Dualstack | podpora současného běhu IPv4 a IPv6 |  |
| Aplikační kontrola | Umožňuje detekovat, monitorovat a řídit přístup k síťovým aplikacím na základě jejich signatur, nikoli pouze podle portů. Tato funkce zahrnuje také kontrolu komunikace v šifrovaných protokolech, jako jsou HTTPS, IMAPS nebo POP3S. |  |
| Antivir | Integrovaný antivirus, možnost volby různých databází signatur, podpora archivace škodlivého obsahu, podpora protokolu ICAP pro offload AV detekce, možnost detekce tzv. Grayware (rootkit, malware, spywave, keylogger, atd) |  |
| URL filtering | Omezuje přístup na webové stránky podle kategorií (např. sociální sítě, hazard). Může být implementováno lokálně nebo prostřednictvím cloudového serveru. |  |
| Kategorizace a blokace provozu | založená na kategorizaci webového obsahu, možnost monitorování navštívených kategorii na uživatele či skupinu, možnost kvóty – uživatel může navštěvovat určitou kategorii jen po určitou dobu během dne (služba není součástí dodávky). |  |
| Antispam | Antispamová a antivirová inspekce elektronické pošty |  |
| Sandbox | Možnost integrovaného sandbox (ověření škodlivosti kódu spuštěním v reálných operačních systémech) v zařízení nebo integrované rozhraní pro napojení na externí službu výrobce zařízení (služba není součástí dodávky). |  |
| Aktualizace | automatická aktualizace bezpečnostních funkcí poskytovaná výrobcem zařízení |  |
| Ověřování uživatelů | Integrace s AD s možností RADIUS nebo TACACS+  Funkcionalita 802.1X  Podpora definice bezpečnostních politik na základě ověřování uživatelů vůči AD/LDAP |  |
| Management a monitoring | HTTP/S, SSH, SNMP, syslog |  |
| Transceivery | * Celkový počet potřebných transceiverů je minimálně 6 ks (4× SFP 1GbE a 2× SFP+ 10GbE). * Pokud konkrétní návrh řešení dodavatele vyžaduje pro splnění všech požadavků technické specifikace větší počet transceiverů, je dodavatel povinen navrhnout a dodat odpovídající počet. * Přesný typ a počet osazených portů tedy může záviset na konkrétním návrhu řešení, které dodavatel předloží, vždy však musí být splněny minimální požadavky uvedené výše. |  |
| Transceivery musí být kompatibilní s dodaným řešením |  |
| Záruka | Podpora a záruka min. 36 měsíců v režimu 24x7 poskytovaná výrobcem zařízení nebo jeho partnerem. Doručení náhradního zařízení max. následující den po nahlášení závady, včetně nároku na bezpečnostní aktualizace firmware a zalicencovaných funkcí. |  |

### Nástroje pro ochranu integrity komunikačních sítí

INFRASTRUKTURA – core SWITCH – 2 ks

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje požadavky (ANO/NE) |
| Základní vlastnosti | * Core přepínač pro montáž do 19" rozvadeče, včetně montážní sady * Maximální výška přepínače 1U * Všechny přístupové a uplink porty umístěné na přední straně přepínače * Všechny porty a rozhraní pro správu umístěné na přední straně přepínače * Stohovatelný, plně řiditelný L2/L3 přepínač podnikové třídy s podporou cloudové správy |  |
| Porty a rozhraní pro správu | * Minimálně 48x SFP28 s rychlostí 1/10/25Gb * Minimálně 8x QSFP28 s rychlostí 40/100Gb * 1x RJ45 konzolový port nebo USB konzolový port pro lokální konfiguraci * 1x RJ45 s rychlostí 10/100/1000BASE-T pro out-of-band management * 1x USB pro přenos souborů do a z přepínače (firmware, konfigurace apod.) |  |
| Vlastnosti stohování | * Možnost stohovat až 8 zařízení * Podpora technologií FPS (Front Plane Stacking) anebo BPS (Back Plane Stacking) v topologii kruh * Při použití FPS (Front Plane Stacking) musí na přepínači zůstat min. 6x QSFP28 s rychlostí 40/100 Gb * Při nevyužití stohování musí být možné použít všechny QSFP28 porty jako datové 40/100 Gb porty * Minimální propustnost stohování v topologii kruh 400 Gbps |  |
| Vlastnosti napájení | * Minimálně 2x napájecí zdroj 230V * Výměna vadného zdroje za provozu |  |
| Ventilátory | * Modulární ventilátory * Přepínač plně osazen ventilátory * Výměna vadného ventilátoru za provozu * Možnost volby proudění vzduchu chlazení ze předu dozadu a zezadu dopředu |  |
| Kapacitní a výkonové vlastnosti přepínače | * Minimální neblokovaná přepínací kapacita: 4 Tbps * Minimální přepínací rychlost: 1000 Mpps * Minimální počet podporovaných VLAN: 4000 * Minimální kapacita tabulky MAC adres: 280000 * Minimální kapacita tabulky směrovacích záznamů pro IPv4: 250000 * Minimální kapacita tabulky směrovacích záznamů pro IPv6: 130000 * Minimální velikost Jumbo Frame: 9200B * Minimální kapacita směrovací tabulky pro multicast implementované v hardware: 100000 |  |
| Další požadované funkce a vlastnosti | * Podpora virtuálních LAN dle IEEE 802.1Q+B45:B61 * Podpora agregace více portů s využitím protokolu LACP (Link Aggregation Control Protocol) dle IEEE 802.3ad * Podpora technologie MLAG, MC-LAG apod. pro „Dual Homing“ připojení zařízení do sítě, např. pro servery, firewally, přepínače třetích stran apod. * Podpora objevení zařízení s využitím protokolu LLDP (Link Layer Discovery Protocol) dle IEEE 802.1ab včetně jeho rozšíření LLDP-MED (Media Endpoint Discovery) * Podpora statických směrovacích záznamů pro IPv4 i IPv6 * Podpora funkcí DHCP client, DHCP relay a DHCP server pro IPv4 * Podpora funkcí DHCP client, DHCP relay IPv6 * Podpora funkce DHCP snooping * Podpora funkce IPSG (IP Source Guard) * Podpora funkcí IGMP (Internet Group Management Protocol) a IGMP snooping pro IPv4 ve verzích 1,2 a 3 * Podpora funkcí MLD (Multicast Listener Discovery) a MLD snooping pro IPv6 ve verzích 1 a 2 * Podpora funkce ND (Neighbor Discovery) pro IPv6 * Podpora IPFIX technologie implementované v HW * Podpora ověřeného přístupu do sítě prostřednictvím protokolu IEEE 802.1x * Podpora současné konfigurace ověřeného přístupu IEEE 802.1x a MAB (Mac Authentication Bypass) s možností volby jejich pořadí * Podpora změny autorizace ověřeného přístupu IEEE 802.1x s využitím CoA (Change of Authorization) * Podpora přiřazení politiky, role nebo dynamického ACL (Access Control List) na základě autorizace * Podpora současného ověření několika zařízení/uživatelů na jediném přístupovém portu s možnožností přídělení různé politiky, role nebo dynamického ACL (Access Control List) * Podpora zabezpečení RADIUS protokolu pro ověřování pomocí RADIUS security (RADSec, RADIUS over TLS) * Podpora omezení provozu prostřednictvím ACL (Access Control List) s definicí atributů na vrstvách L2/L3/L4, implementované v hardware pro IPv4 i IPv6 * Podpora zabezpečeného vzdáleného přístupu a správy pomocí protokolů SSHv2, SCP a SFTP * Podpora zabezpečeného monitorování pomocí protokolu SNMPv3 (Simple Network Management Protocol) * Podpora centrální zabezpečené správy prostřednictvím cloudového managementu * Podpora protokolu MSTP (Multiple Spanning Tree Protocol) dle IEEE 802.1s * Podpora protokolu PVST+ (Per-VLAN Spanning Tree) * Podpora ZTP (Zero Touch Provisioning) prostřednictvím cloudového managementu * Podpora VXLAN a VXLAN gateway pro propojení VXLAN * Podpora skriptování přímo na zařízení (např. Python) * Podpora dynamického směrovacího protokolu OSPF a OSPFv3 * Podpora dynamického směrovacího protokolu BGP a BGP+ * Podpora PIM-SM/SSM * Podpora IGMP v2/v3 * Podpora VRF * Podpora VRRP / VRRPv3 * Podpora ECMP * Podpora statického směrování |  |
|  | * Škálovatelná cloudová SaaS (Software as a Service) služba postavená na mikroslužbách * Služba provozovaná v datových centrech v rámci EU na platformách AWS/Google Cloud/Microsoft Azure, případně v privátním datovém centru výrobce s garantovanou dostupností * Garantovaná dostupnost služby minimálně 99,99% * Podpora multitenantního přístupu a možností delegování přístupu k samostatným tentantům * Podpora API pro integraci s aplikacemi třetích stran pro účely ověřování, automatizace, monitorování apod. * Podporuje centrální správu přepínačů a jejich ZTP (Zero Touch Provisioning) s přidělením politiky a konfiguračních šablon * Podporuje definice konfiguračních šablon pro přepínače v rámci politiky * Podporuje definice konfiguračních šablon pro přístupové porty přepínače v rámci politiky * Podporuje lokální změn konfigurace přepínače nebo přístupového portu, lokální změny mají přednost před šablonou * Podporuje definice šablon pro sestavení stohu přepínačů * Podporuje zabezpečené přihlašování administrátorů ke službě s využitím MFA (Multi-Factor Authentication) * Podporuje přihlašování administrátorů ke službě s využitím SSO (Single Sign On) s využitím protokolu SAMLv2 (např. Entra ID, Ping Identity, Okta a další) * Podporuje aktualizaci firmware přepínačů s bezpečným přenosem a kontrolou přenosu, zdrojem firmware je přímo služba samotná |  |
| Transceiver a kabeláž | * Modul SFP28-25G-SR 1ks - od stejného výrobce * Modul SFP+-10G-SR 30ks * Originální DAC kabely pro stohování Core přepínačů, delka 1m: 2ks |  |
| Záruky | * Doživotní limitovaná záruka výrobce na hardware, řešení opravy formou dopředné výměny přepínače s odesláním následující pracovní den po identifikaci a uznání závady * Doživotní limitovaná záruka výrobce na software, řešení formou vydávání aktualizací a záplat pro firmware přepínačů |  |
| Licence | * Licence pro centrální správu přepínačů prostřednictvím služby cloudového managementu na dobu minimálně 5 let |  |

## Aktivní prvky – PoE 48port – 7 ks

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje požadavky (ANO/NE) |
| Základní vlastnosti | * Stohovatelný, plně řiditelný L2/L3 přepínač podnikové třídy s podporou cloudové správy * Přístupový přepínač pro montáž do 19" rozvadeče, včetně montážní sady * Maximální výška přepínače 1U * Maximální hloubka 40 cm * Všechny přístupové a uplink porty umístěné na přední straně přepínače * Všechny porty a rozhraní pro správu umístěné na přední straně přepínače |  |
| Porty a rozhraní pro správu | * Minimálně 48x RJ45 s rychlostí 10/100/1000 Base-T s podporou PoE dle IEEE 802.3at třídy 4 (30W) * Minimálně 4x SFP+ s rychlostí 1/10Gb * 1x RJ45 konzolový port nebo USB konzolový port pro lokální konfiguraci * 1x RJ45 s rychlostí 10/100/1000BASE-T pro out-of-band management   1x USB pro přenos souborů do a z přepínače (firmware, konfigurace apod.) |  |
| Vlastnosti stohování | * Možnost stohovat až 8 zařízení * Podpora technologií FPS (Front Plane Stacking) anebo BPS (Back Plane Stacking) v topologii kruh * Při použití FPS (Front Plane Stacking) musí na přepínači zůstat min. 2x SFP+ s rychlostí 1/10 Gb * Při nevyužití stohování musí být možné použít všechny SFP+ porty jako datové 10 Gb porty * Minimální propustnost stohování v topologii kruh 40 Gbps |  |
| Vlastnosti napájení | * Minimálně 1x napájecí zdroj 230V * Vlastnosti PoE napájení * Podpora napájení připojených zařízení dle standardů IEEE 802.3at * Celkový výkon dostupný pro napajení zažízení prostřednictvím PoE minimálně 370W * Podpora funkce Perpetual PoE pro napájení připojených zařízení i při restartu nebo aktualizaci přepínače * Podpora funkce Fast PoE pro rychlé obnovení napájení připojených zařízení |  |
| Kapacitní a výkonové vlastnosti přepínače | * Minimální neblokovaná přepínací kapacita: 176 Gbps * Minimální přepínací rychlost: 130 Mpps * Minimální počet podporovaných VLAN: 4000 * Minimální kapacita tabulky MAC adres: 32000 * Minimální kapacita tabulky směrovacích záznamů: 1000 * Minimální velikost Jumbo Frame: 9200B |  |
| Další požadované funkce a vlastnosti | * Podpora virtuálních LAN dle IEEE 802.1Q+B43:B63 * Podpora agregace více portů s využitím protokolu LACP (Link Aggregation Control Protocol) dle IEEE 802.3ad * Podpora objevení zařízení s využitím protokolu LLDP (Link Layer Discovery Protocol) dle IEEE 802.1ab včetně jeho rozšíření LLDP-MED (Media Endpoint Discovery) * Podpora statických směrovacích záznamů pro IPv4 i IPv6 * Podpora funkcí DHCP client, DHCP relay a DHCP server pro IPv4 * Podpora funkcí DHCP client, DHCP relay IPv6 * Podpora funkce DHCP snooping * Podpora funkce IPSG (IP Source Guard) * Podpora funkcí IGMP (Internet Group Management Protocol) a IGMP snooping pro IPv4 ve verzích 1,2 a 3 * Podpora funkcí MLD (Multicast Listener Discovery) a MLD snooping pro IPv6 ve verzích 1 a 2 * Podpora funkce ND (Neighbor Discovery) pro IPv6 * Podpora analýzy provozu minimálně prostřednictvím sFlow verze 5 * Podpora ověřeného přístupu do sítě prostřednictvím protokolu IEEE 802.1x * Podpora současné konfigurace ověřeného přístupu IEEE 802.1x a MAB (Mac Authentication Bypass) s možností volby jejich pořadí * Podpora změny autorizace ověřeného přístupu IEEE 802.1x s využitím CoA (Change of Authorization) * Podpora přiřazení politiky, role nebo dynamického ACL (Access Control List) na základě autorizace * Podpora současného ověření několika zařízení/uživatelů na jediném přístupovém portu s možnožností přídělení různé politiky, role nebo dynamického ACL (Access Control List) * Podpora zabezpečení RADIUS protokolu pro ověřování pomocí RADIUS security (RADSec, RADIUS over TLS) * Podpora omezení provozu prostřednictvím ACL (Access Control List) s definicí atributů na vrstvách L2/L3/L4, implementované v hardware pro IPv4 i IPv6 * Podpora zabezpečeného vzdáleného přístupu a správy pomocí protokolů SSHv2, SCP a SFTP * Podpora zabezpečeného monitorování pomocí protokolu SNMPv3 (Simple Network Management Protocol) * Podpora centrální zabezpečené správy prostřednictvím cloudového managementu * Podpora protokolu MSTP (Multiple Spanning Tree Protocol) dle IEEE 802.1s * Podpora protokolu PVST+ (Per-VLAN Spanning Tree) * Podpora ZTP (Zero Touch Provisioning) prostřednictvím cloudového managementu |  |
| Požadované vlastnosti a funkce služby cloudového managementu | * Škálovatelná cloudová SaaS (Software as a Service) služba postavená na mikroslužbách * Služba provozovaná v datových centrech v rámci EU na platformách AWS/Google Cloud/Microsoft Azure, případně v privátním datovém centru výrobce s garantovanou dostupností * Garantovaná dostupnost služby minimálně 99,99% * Podpora multitenantního přístupu a možností delegování přístupu k samostatným tentantům * Podpora API pro integraci s aplikacemi třetích stran pro účely ověřování, automatizace, monitorování apod. * Podporuje centrální správu přepínačů a jejich ZTP (Zero Touch Provisioning) s přidělením politiky a konfiguračních šablon * Podporuje definice konfiguračních šablon pro přepínače v rámci politiky * Podporuje definice konfiguračních šablon pro přístupové porty přepínače v rámci politiky * Podporuje lokální změn konfigurace přepínače nebo přístupového portu, lokální změny mají přednost před šablonou * Podporuje definice šablon pro sestavení stohu přepínačů * Podporuje zabezpečené přihlašování administrátorů ke službě s využitím MFA (Multi-Factor Authentication) * Podporuje přihlašování administrátorů ke službě s využitím SSO (Single Sign On) s využitím protokolu SAMLv2 (např. Entra ID, Ping Identity, Okta a další) * Podporuje aktualizaci firmware přepínačů s bezpečným přenosem a kontrolou přenosu, zdrojem firmware je přímo služba samotná |  |
| Transceiver a kabeláž | * Originální DAC kabely pro stohování ACCESS přepínačů, délka 1m: 6ks * Modul SFP+ -10G-SR 15ks |  |
| Licence | * Licence pro centrální správu přepínačů prostřednictvím služby cloudového managementu na dobu minimálně 5 let |  |
| Záruky | * Doživotní limitovaná záruka výrobce na hardware, řešení opravy formou dopředné výměny přepínače s odesláním následující pracovní den po identifikaci a uznání závady * Doživotní limitovaná záruka výrobce na software, řešení formou vydávání aktualizací a záplat pro firmware přepínačů |  |

## Aktivní prvky – PoE 24port – 5 ks

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje požadavky (ANO/NE) |
| Základní vlastnosti | * Stohovatelný, plně řiditelný L2/L3 přepínač podnikové třídy s podporou cloudové správy * Přístupový přepínač pro montáž do 19" rozvadeče, včetně montážní sady * Maximální výška přepínače 1U * Maximální hloubka 40 cm * Všechny přístupové a uplink porty umístěné na přední straně přepínače * Všechny porty a rozhraní pro správu umístěné na přední straně přepínače |  |
| Porty a rozhraní pro správu | * Minimálně 24x RJ45 s rychlostí 10/100/1000 Base-T s podporou PoE dle IEEE 802.3at třídy 4 (30W) * Minimálně 4x SFP+ s rychlostí 1/10Gb * 1x RJ45 konzolový port nebo USB konzolový port pro lokální konfiguraci * 1x RJ45 s rychlostí 10/100/1000BASE-T pro out-of-band management   1x USB pro přenos souborů do a z přepínače (firmware, konfigurace apod.) |  |
| Vlastnosti stohování | * Možnost stohovat až 8 zařízení * Podpora technologií FPS (Front Plane Stacking) anebo BPS (Back Plane Stacking) v topologii kruh * Při použití FPS (Front Plane Stacking) musí na přepínači zůstat min. 2x SFP+ s rychlostí 1/10 Gb * Při nevyužití stohování musí být možné použít všechny SFP+ porty jako datové 10 Gb porty * Minimální propustnost stohování v topologii kruh 40 Gbps |  |
| Vlastnosti napájení | * Minimálně 1x napájecí zdroj 230V |  |
| Vlastnosti PoE napájení | * Podpora napájení připojených zařízení dle standardů IEEE 802.3at * Celkový výkon dostupný pro napajení zažízení prostřednictvím PoE minimálně 195W * Podpora funkce Perpetual PoE pro napájení připojených zařízení i při restartu nebo aktualizaci přepínače * Podpora funkce Fast PoE pro rychlé obnovení napájení připojených zařízení |  |
| Kapacitní a výkonové vlastnosti přepínače | * Minimální neblokovaná přepínací kapacita: 128 Gbps * Minimální přepínací rychlost: 95 Mpps * Minimální počet podporovaných VLAN: 4000 * Minimální kapacita tabulky MAC adres: 32000 * Minimální kapacita tabulky směrovacích záznamů: 1000 * Minimální velikost Jumbo Frame: 9200B |  |
| Další požadované funkce a vlastnosti | * Podpora virtuálních LAN dle IEEE 802.1Q * Podpora agregace více portů s využitím protokolu LACP (Link Aggregation Control Protocol) dle IEEE 802.3ad * Podpora objevení zařízení s využitím protokolu LLDP (Link Layer Discovery Protocol) dle IEEE 802.1ab včetně jeho rozšíření LLDP-MED (Media Endpoint Discovery) * Podpora statických směrovacích záznamů pro IPv4 i IPv6 * Podpora funkcí DHCP client, DHCP relay a DHCP server pro IPv4 * Podpora funkcí DHCP client, DHCP relay IPv6 * Podpora funkce DHCP snooping * Podpora funkce IPSG (IP Source Guard) * Podpora funkcí IGMP (Internet Group Management Protocol) a IGMP snooping pro IPv4 ve verzích 1,2 a 3 * Podpora funkcí MLD (Multicast Listener Discovery) a MLD snooping pro IPv6 ve verzích 1 a 2 * Podpora funkce ND (Neighbor Discovery) pro IPv6 * Podpora analýzy provozu minimálně prostřednictvím sFlow verze 5 * Podpora ověřeného přístupu do sítě prostřednictvím protokolu IEEE 802.1x * Podpora současné konfigurace ověřeného přístupu IEEE 802.1x a MAB (Mac Authentication Bypass) s možností volby jejich pořadí * Podpora změny autorizace ověřeného přístupu IEEE 802.1x s využitím CoA (Change of Authorization) * Podpora přiřazení politiky, role nebo dynamického ACL (Access Control List) na základě autorizace * Podpora současného ověření několika zařízení/uživatelů na jediném přístupovém portu s možnožností přídělení různé politiky, role nebo dynamického ACL (Access Control List) * Podpora zabezpečení RADIUS protokolu při ověřování pomocí RADIUS security (RADSec, RADIUS over TLS) * Podpora omezení provozu prostřednictvím ACL (Access Control List) s definicí atributů na vrstvách L2/L3/L4, implementované v hardware pro IPv4 i IPv6 * Podpora zabezpečeného vzdáleného přístupu a správy pomocí protokolů SSHv2, SCP a SFTP * Podpora zabezpečeného monitorování pomocí protokolu SNMPv3 (Simple Network Management Protocol) * Podpora centrální zabezpečené správy prostřednictvím cloudového managementu * Podpora protokolu MSTP (Multiple Spanning Tree Protocol) dle IEEE 802.1s * Podpora protokolu PVST+ (Per-VLAN Spanning Tree) * Podpora ZTP (Zero Touch Provisioning) prostřednictvím cloudového managementu |  |
| Požadované vlastnosti a funkce služby cloudového managementu | * Škálovatelná cloudová SaaS (Software as a Service) služba postavená na mikroslužbách * Služba provozovaná v datových centrech v rámci EU na platformách AWS/Google Cloud/Microsoft Azure, případně v privátním datovém centru výrobce s garantovanou dostupností * Garantovaná dostupnost služby minimálně 99,99% * Podpora multitenantního přístupu a možností delegování přístupu k samostatným tentantům * Podpora API pro integraci s aplikacemi třetích stran pro účely ověřování, automatizace, monitorování apod. * Podporuje centrální správu přepínačů a jejich ZTP (Zero Touch Provisioning) s přidělením politiky a konfiguračních šablon * Podporuje definice konfiguračních šablon pro přepínače v rámci politiky * Podporuje definice konfiguračních šablon pro přístupové porty přepínače v rámci politiky * Podporuje lokální změn konfigurace přepínače nebo přístupového portu, lokální změny mají přednost před šablonou * Podporuje definice šablon pro sestavení stohu přepínačů * Podporuje zabezpečené přihlašování administrátorů ke službě s využitím MFA (Multi-Factor Authentication) * Podporuje přihlašování administrátorů ke službě s využitím SSO (Single Sign On) s využitím protokolu SAMLv2 (např. Entra ID, Ping Identity, Okta a další) * Podporuje aktualizaci firmware přepínačů s bezpečným přenosem a kontrolou přenosu, zdrojem firmware je přímo služba samotná |  |
| Transceiver | * Modul SFP+ -10G-SR 15ks |  |
| Licence | * Licence pro centrální správu přepínačů prostřednictvím služby cloudového managementu na dobu minimálně 5 let * Licence pro síťový operační systém nezbytné pro právo a využití požadovaných vlastností a funkcí přepínače |  |
| Záruky | * Doživotní limitovaná záruka výrobce na hardware, řešení opravy formou dopředné výměny přepínače s odesláním následující pracovní den po identifikaci a uznání závady * Doživotní limitovaná záruka výrobce na software, řešení formou vydávání aktualizací a záplat pro firmware přepínačů |  |

## Aktivní prvky – PoE 12port – 1 ks

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje požadavky (ANO/NE) |
| Základní vlastnosti | * Stohovatelný, plně řiditelný L2/L3 přepínač podnikové třídy s podporou cloudové správy * Přístupový přepínač pro montáž do 19" rozvadeče, včetně montážní sady * Maximální výška přepínače 1U * Maximální hloubka 40 cm * Všechny přístupové a uplink porty umístěné na přední straně přepínače * Všechny porty a rozhraní pro správu umístěné na přední straně přepínače |  |
| Porty a rozhraní pro správu | * Minimálně 12x RJ45 s rychlostí 10/100/1000 Base-T s podporou PoE dle IEEE 802.3at třídy 4 (30W) * Minimálně 4x SFP+ s rychlostí 1/10Gb * 1x RJ45 konzolový port nebo USB konzolový port pro lokální konfiguraci * 1x RJ45 s rychlostí 10/100/1000BASE-T pro out-of-band management * 1x USB pro přenos souborů do a z přepínače (firmware, konfigurace apod.) |  |
| Vlastnosti stohování | * Možnost stohovat až 8 zařízení * Podpora technologií FPS (Front Plane Stacking) anebo BPS (Back Plane Stacking) v topologii kruh * Při použití FPS (Front Plane Stacking) musí na přepínači zůstat min. 2x SFP+ s rychlostí 1/10 Gb * Při nevyužití stohování musí být možné použít všechny SFP+ porty jako datové 10 Gb porty * Minimální propustnost stohování v topologii kruh 40 Gbps |  |
| Vlastnosti napájení | * Minimálně 1x napájecí zdroj 230V |  |
| Vlastnosti PoE napájení | * Podpora napájení připojených zařízení dle standardů IEEE 802.3at * Celkový výkon dostupný pro napajení zažízení prostřednictvím PoE minimálně 124W * Podpora funkce Perpetual PoE pro napájení připojených zařízení i při restartu nebo aktualizaci přepínače * Podpora funkce Fast PoE pro rychlé obnovení napájení připojených zařízení |  |
| Kapacitní a výkonové vlastnosti přepínače | * Minimální neblokovaná přepínací kapacita: 104 Gbps * Minimální přepínací rychlost: 77 Mpps * Minimální počet podporovaných VLAN: 4000 * Minimální kapacita tabulky MAC adres: 32000 * Minimální kapacita tabulky směrovacích záznamů: 1000 * Minimální velikost Jumbo Frame: 9200B |  |
| Další požadované funkce a vlastnosti | * Podpora virtuálních LAN dle IEEE 802.1Q * Podpora agregace více portů s využitím protokolu LACP (Link Aggregation Control Protocol) dle IEEE 802.3ad * Podpora objevení zařízení s využitím protokolu LLDP (Link Layer Discovery Protocol) dle IEEE 802.1ab včetně jeho rozšíření LLDP-MED (Media Endpoint Discovery) * Podpora statických směrovacích záznamů pro IPv4 i IPv6 * Podpora funkcí DHCP client, DHCP relay a DHCP server pro IPv4 * Podpora funkcí DHCP client, DHCP relay IPv6 * Podpora funkce DHCP snooping * Podpora funkce IPSG (IP Source Guard) * Podpora funkcí IGMP (Internet Group Management Protocol) a IGMP snooping pro IPv4 ve verzích 1,2 a 3 * Podpora funkcí MLD (Multicast Listener Discovery) a MLD snooping pro IPv6 ve verzích 1 a 2 * Podpora funkce ND (Neighbor Discovery) pro IPv6 * Podpora analýzy provozu minimálně prostřednictvím sFlow verze 5 * Podpora ověřeného přístupu do sítě prostřednictvím protokolu IEEE 802.1x * Podpora současné konfigurace ověřeného přístupu IEEE 802.1x a MAB (Mac Authentication Bypass) s možností volby jejich pořadí * Podpora změny autorizace ověřeného přístupu IEEE 802.1x s využitím CoA (Change of Authorization) * Podpora přiřazení politiky, role nebo dynamického ACL (Access Control List) na základě autorizace * Podpora současného ověření několika zařízení/uživatelů na jediném přístupovém portu s možnožností přídělení různé politiky, role nebo dynamického ACL (Access Control List) * Podpora zabezpečení RADIUS protokolu při ověřování pomocí RADIUS security (RADSec, RADIUS over TLS) * Podpora omezení provozu prostřednictvím ACL (Access Control List) s definicí atributů na vrstvách L2/L3/L4, implementované v hardware pro IPv4 i IPv6 * Podpora zabezpečeného vzdáleného přístupu a správy pomocí protokolů SSHv2, SCP a SFTP * Podpora zabezpečeného monitorování pomocí protokolu SNMPv3 (Simple Network Management Protocol) * Podpora centrální zabezpečené správy prostřednictvím cloudového managementu * Podpora protokolu MSTP (Multiple Spanning Tree Protocol) dle IEEE 802.1s * Podpora protokolu PVST+ (Per-VLAN Spanning Tree) * Podpora ZTP (Zero Touch Provisioning) prostřednictvím cloudového managementu |  |
| Požadované vlastnosti a funkce služby cloudového managementu | * Škálovatelná cloudová SaaS (Software as a Service) služba postavená na mikroslužbách * Služba provozovaná v datových centrech v rámci EU na platformách AWS/Google Cloud/Microsoft Azure, případně v privátním datovém centru výrobce s garantovanou dostupností * Garantovaná dostupnost služby minimálně 99,99% * Podpora multitenantního přístupu a možností delegování přístupu k samostatným tentantům * Podpora API pro integraci s aplikacemi třetích stran pro účely ověřování, automatizace, monitorování apod. * Podporuje centrální správu přepínačů a jejich ZTP (Zero Touch Provisioning) s přidělením politiky a konfiguračních šablon * Podporuje definice konfiguračních šablon pro přepínače v rámci politiky * Podporuje definice konfiguračních šablon pro přístupové porty přepínače v rámci politiky * Podporuje lokální změn konfigurace přepínače nebo přístupového portu, lokální změny mají přednost před šablonou * Podporuje definice šablon pro sestavení stohu přepínačů * Podporuje zabezpečené přihlašování administrátorů ke službě s využitím MFA (Multi-Factor Authentication) * Podporuje přihlašování administrátorů ke službě s využitím SSO (Single Sign On) s využitím protokolu SAMLv2 (např. Entra ID, Ping Identity, Okta a další) * Podporuje aktualizaci firmware přepínačů s bezpečným přenosem a kontrolou přenosu, zdrojem firmware je přímo služba samotná |  |
| Licence | * Licence pro centrální správu přepínačů prostřednictvím služby cloudového managementu na dobu minimálně 5 let * Licence pro síťový operační systém nezbytné pro právo a využití požadovaných vlastností a funkcí přepínače |  |
| Záruky | * Doživotní limitovaná záruka výrobce na hardware, řešení opravy formou dopředné výměny přepínače s odesláním následující pracovní den po identifikaci a uznání závady * Doživotní limitovaná záruka výrobce na software, řešení formou vydávání aktualizací a záplat pro firmware přepínačů |  |

## Aktivní prvky –48port – 8 ks

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje požadavky (ANO/NE) |
| Základní vlastnosti | * Stohovatelný, plně řiditelný L2/L3 přepínač podnikové třídy s podporou cloudové správy * Přístupový přepínač pro montáž do 19" rozvadeče, včetně montážní sady * Maximální výška přepínače 1U * Maximální hloubka 40 cm * Všechny přístupové a uplink porty umístěné na přední straně přepínače * Všechny porty a rozhraní pro správu umístěné na přední straně přepínače |  |
| Porty a rozhraní pro správu | * Minimálně 48x RJ45 s rychlostí 10/100/1000 Base-T s podporou PoE dle IEEE 802.3at třídy 4 (30W) * Minimálně 4x SFP+ s rychlostí 1/10Gb * 1x RJ45 konzolový port nebo USB konzolový port pro lokální konfiguraci * 1x RJ45 s rychlostí 10/100/1000BASE-T pro out-of-band management   1x USB pro přenos souborů do a z přepínače (firmware, konfigurace apod.) |  |
| Vlastnosti stohování | * Možnost stohovat až 8 zařízení * Podpora technologií FPS (Front Plane Stacking) anebo BPS (Back Plane Stacking) v topologii kruh * Při použití FPS (Front Plane Stacking) musí na přepínači zůstat min. 2x SFP+ s rychlostí 1/10 Gb * Při nevyužití stohování musí být možné použít všechny SFP+ porty jako datové 10 Gb porty * Minimální propustnost stohování v topologii kruh 40 Gbps |  |
| Vlastnosti napájení | * Minimálně 1x napájecí zdroj 230V |  |
| Kapacitní a výkonové vlastnosti přepínače | * Minimální neblokovaná přepínací kapacita: 176 Gbps * Minimální přepínací rychlost: 130 Mpps * Minimální počet podporovaných VLAN: 4000 * Minimální kapacita tabulky MAC adres: 32000 * Minimální kapacita tabulky směrovacích záznamů: 1000 * Minimální velikost Jumbo Frame: 9200B |  |
| Další požadované funkce a vlastnosti | * Podpora virtuálních LAN dle IEEE 802.1Q * Podpora agregace více portů s využitím protokolu LACP (Link Aggregation Control Protocol) dle IEEE 802.3ad * Podpora objevení zařízení s využitím protokolu LLDP (Link Layer Discovery Protocol) dle IEEE 802.1ab včetně jeho rozšíření LLDP-MED (Media Endpoint Discovery) * Podpora statických směrovacích záznamů pro IPv4 i IPv6 * Podpora funkcí DHCP client, DHCP relay a DHCP server pro IPv4 * Podpora funkcí DHCP client, DHCP relay IPv6 * Podpora funkce DHCP snooping * Podpora funkce IPSG (IP Source Guard) * Podpora funkcí IGMP (Internet Group Management Protocol) a IGMP snooping pro IPv4 ve verzích 1,2 a 3 * Podpora funkcí MLD (Multicast Listener Discovery) a MLD snooping pro IPv6 ve verzích 1 a 2 * Podpora funkce ND (Neighbor Discovery) pro IPv6 * Podpora analýzy provozu minimálně prostřednictvím sFlow verze 5 * Podpora ověřeného přístupu do sítě prostřednictvím protokolu IEEE 802.1x * Podpora současné konfigurace ověřeného přístupu IEEE 802.1x a MAB (Mac Authentication Bypass) s možností volby jejich pořadí * Podpora změny autorizace ověřeného přístupu IEEE 802.1x s využitím CoA (Change of Authorization) * Podpora přiřazení politiky, role nebo dynamického ACL (Access Control List) na základě autorizace * Podpora současného ověření několika zařízení/uživatelů na jediném přístupovém portu s možnožností přídělení různé politiky, role nebo dynamického ACL (Access Control List) * Podpora zabezpečení RADIUS protokolu pro ověřování pomocí RADIUS security (RADSec, RADIUS over TLS) * Podpora omezení provozu prostřednictvím ACL (Access Control List) s definicí atributů na vrstvách L2/L3/L4, implementované v hardware pro IPv4 i IPv6 * Podpora zabezpečeného vzdáleného přístupu a správy pomocí protokolů SSHv2, SCP a SFTP * Podpora zabezpečeného monitorování pomocí protokolu SNMPv3 (Simple Network Management Protocol) * Podpora centrální zabezpečené správy prostřednictvím cloudového managementu * Podpora protokolu MSTP (Multiple Spanning Tree Protocol) dle IEEE 802.1s * Podpora protokolu PVST+ (Per-VLAN Spanning Tree) * Podpora ZTP (Zero Touch Provisioning) prostřednictvím cloudového managementu |  |
| Požadované vlastnosti a funkce služby cloudového managementu | * Škálovatelná cloudová SaaS (Software as a Service) služba postavená na mikroslužbách * Služba provozovaná v datových centrech v rámci EU na platformách AWS/Google Cloud/Microsoft Azure, případně v privátním datovém centru výrobce s garantovanou dostupností * Garantovaná dostupnost služby minimálně 99,99% * Podpora multitenantního přístupu a možností delegování přístupu k samostatným tentantům * Podpora API pro integraci s aplikacemi třetích stran pro účely ověřování, automatizace, monitorování apod. * Podporuje centrální správu přepínačů a jejich ZTP (Zero Touch Provisioning) s přidělením politiky a konfiguračních šablon * Podporuje definice konfiguračních šablon pro přepínače v rámci politiky * Podporuje definice konfiguračních šablon pro přístupové porty přepínače v rámci politiky * Podporuje lokální změn konfigurace přepínače nebo přístupového portu, lokální změny mají přednost před šablonou * Podporuje definice šablon pro sestavení stohu přepínačů * Podporuje zabezpečené přihlašování administrátorů ke službě s využitím MFA (Multi-Factor Authentication) * Podporuje přihlašování administrátorů ke službě s využitím SSO (Single Sign On) s využitím protokolu SAMLv2 (např. Entra ID, Ping Identity, Okta a další) * Podporuje aktualizaci firmware přepínačů s bezpečným přenosem a kontrolou přenosu, zdrojem firmware je přímo služba samotná |  |
| Transcievery a kabeláž | * Modul SFP+ -10G-SR 15ks |  |
| Záruky | * Doživotní limitovaná záruka výrobce na hardware, řešení opravy formou dopředné výměny přepínače s odesláním následující pracovní den po identifikaci a uznání závady * Doživotní limitovaná záruka výrobce na software, řešení formou vydávání aktualizací a záplat pro firmware přepínačů |  |
| Licence | * Licence pro centrální správu přepínačů prostřednictvím služby cloudového managementu na dobu minimálně 5 let |  |

## aktivní prvky –24port – 16 ks

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje požadavky (ANO/NE) |
| Základní vlastnosti | * Stohovatelný, plně řiditelný L2/L3 přepínač podnikové třídy s podporou cloudové správy * Přístupový přepínač pro montáž do 19" rozvadeče, včetně montážní sady * Maximální výška přepínače 1U * Maximální hloubka 40 cm * Všechny přístupové a uplink porty umístěné na přední straně přepínače * Všechny porty a rozhraní pro správu umístěné na přední straně přepínače |  |
| Porty a rozhraní pro správu | * Minimálně 24x RJ45 s rychlostí 10/100/1000 Base-T * Minimálně 4x SFP+ s rychlostí 1/10Gb * 1x RJ45 konzolový port nebo USB konzolový port pro lokální konfiguraci * 1x RJ45 s rychlostí 10/100/1000BASE-T pro out-of-band management * 1x USB pro přenos souborů do a z přepínače (firmware, konfigurace apod.) |  |
| Vlastnosti stohování | * Možnost stohovat až 8 zařízení * Podpora technologií FPS (Front Plane Stacking) anebo BPS (Back Plane Stacking) v topologii kruh * Při použití FPS (Front Plane Stacking) musí na přepínači zůstat min. 2x SFP+ s rychlostí 1/10 Gb * Při nevyužití stohování musí být možné použít všechny SFP+ porty jako datové 10 Gb porty * Minimální propustnost stohování v topologii kruh 40 Gbps |  |
| Vlastnosti napájení | * Minimálně 1x napájecí zdroj 230V |  |
| Kapacitní a výkonové vlastnosti přepínače | * Minimální neblokovaná přepínací kapacita: 128 Gbps * Minimální přepínací rychlost: 95 Mpps * Minimální počet podporovaných VLAN: 4000 * Minimální kapacita tabulky MAC adres: 32000 * Minimální kapacita tabulky směrovacích záznamů: 1000 * Minimální velikost Jumbo Frame: 9200B |  |
| Další požadované funkce a vlastnosti | * Podpora virtuálních LAN dle IEEE 802.1Q * Podpora agregace více portů s využitím protokolu LACP (Link Aggregation Control Protocol) dle IEEE 802.3ad * Podpora objevení zařízení s využitím protokolu LLDP (Link Layer Discovery Protocol) dle IEEE 802.1ab včetně jeho rozšíření LLDP-MED (Media Endpoint Discovery) * Podpora statických směrovacích záznamů pro IPv4 i IPv6 * Podpora funkcí DHCP client, DHCP relay a DHCP server pro IPv4 * Podpora funkcí DHCP client, DHCP relay IPv6 * Podpora funkce DHCP snooping * Podpora funkce IPSG (IP Source Guard) * Podpora funkcí IGMP (Internet Group Management Protocol) a IGMP snooping pro IPv4 ve verzích 1,2 a 3 * Podpora funkcí MLD (Multicast Listener Discovery) a MLD snooping pro IPv6 ve verzích 1 a 2 * Podpora funkce ND (Neighbor Discovery) pro IPv6 * Podpora analýzy provozu minimálně prostřednictvím sFlow verze 5 * Podpora ověřeného přístupu do sítě prostřednictvím protokolu IEEE 802.1x * Podpora současné konfigurace ověřeného přístupu IEEE 802.1x a MAB (Mac Authentication Bypass) s možností volby jejich pořadí * Podpora změny autorizace ověřeného přístupu IEEE 802.1x s využitím CoA (Change of Authorization) * Podpora přiřazení politiky, role nebo dynamického ACL (Access Control List) na základě autorizace * Podpora současného ověření několika zařízení/uživatelů na jediném přístupovém portu s možnožností přídělení různé politiky, role nebo dynamického ACL (Access Control List) * Podpora zabezpečení RADIUS protokolu při ověřování pomocí RADIUS security (RADSec, RADIUS over TLS) * Podpora omezení provozu prostřednictvím ACL (Access Control List) s definicí atributů na vrstvách L2/L3/L4, implementované v hardware pro IPv4 i IPv6 * Podpora zabezpečeného vzdáleného přístupu a správy pomocí protokolů SSHv2, SCP a SFTP * Podpora zabezpečeného monitorování pomocí protokolu SNMPv3 (Simple Network Management Protocol) * Podpora centrální zabezpečené správy prostřednictvím cloudového managementu * Podpora protokolu MSTP (Multiple Spanning Tree Protocol) dle IEEE 802.1s * Podpora protokolu PVST+ (Per-VLAN Spanning Tree) * Podpora ZTP (Zero Touch Provisioning) prostřednictvím cloudového managementu |  |
| Požadované vlastnosti a funkce služby cloudového managementu | * Škálovatelná cloudová SaaS (Software as a Service) služba postavená na mikroslužbách * Služba provozovaná v datových centrech v rámci EU na platformách AWS/Google Cloud/Microsoft Azure, případně v privátním datovém centru výrobce s garantovanou dostupností * Garantovaná dostupnost služby minimálně 99,99% * Podpora multitenantního přístupu a možností delegování přístupu k samostatným tentantům * Podpora API pro integraci s aplikacemi třetích stran pro účely ověřování, automatizace, monitorování apod. * Podporuje centrální správu přepínačů a jejich ZTP (Zero Touch Provisioning) s přidělením politiky a konfiguračních šablon * Podporuje definice konfiguračních šablon pro přepínače v rámci politiky * Podporuje definice konfiguračních šablon pro přístupové porty přepínače v rámci politiky * Podporuje lokální změn konfigurace přepínače nebo přístupového portu, lokální změny mají přednost před šablonou * Podporuje definice šablon pro sestavení stohu přepínačů * Podporuje zabezpečené přihlašování administrátorů ke službě s využitím MFA (Multi-Factor Authentication) * Podporuje přihlašování administrátorů ke službě s využitím SSO (Single Sign On) s využitím protokolu SAMLv2 (např. Entra ID, Ping Identity, Okta a další) * Podporuje aktualizaci firmware přepínačů s bezpečným přenosem a kontrolou přenosu, zdrojem firmware je přímo služba samotná |  |
| Transcievery a kabeláž | * Modul SFP+ -10G-SR 15ks |  |
| Licence | * Licence pro centrální správu přepínačů prostřednictvím služby cloudového managementu na dobu minimálně 5 let * Licence pro síťový operační systém nezbytné pro právo a využití požadovaných vlastností a funkcí přepínače |  |
| Záruky | * Doživotní limitovaná záruka výrobce na hardware, řešení opravy formou dopředné výměny přepínače s odesláním následující pracovní den po identifikaci a uznání závady * Doživotní limitovaná záruka výrobce na software, řešení formou vydávání aktualizací a záplat pro firmware přepínačů |  |

## aktivní prvky –12port – 4 ks

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje požadavky (ANO/NE) |
| Základní vlastnosti | * Stohovatelný, plně řiditelný L2/L3 přepínač podnikové třídy s podporou cloudové správy * Přístupový přepínač pro montáž do 19" rozvadeče, včetně montážní sady * Maximální výška přepínače 1U * Maximální hloubka 40 cm * Všechny přístupové a uplink porty umístěné na přední straně přepínače * Všechny porty a rozhraní pro správu umístěné na přední straně přepínače |  |
| Porty a rozhraní pro správu | * Minimálně 12x RJ45 s rychlostí 10/100/1000 Base-T * Minimálně 4x SFP+ s rychlostí 1/10Gb * 1x RJ45 konzolový port nebo USB konzolový port pro lokální konfiguraci * 1x RJ45 s rychlostí 10/100/1000BASE-T pro out-of-band management   1x USB pro přenos souborů do a z přepínače (firmware, konfigurace apod.) |  |
| Vlastnosti stohování | * Možnost stohovat až 8 zařízení * Podpora technologií FPS (Front Plane Stacking) anebo BPS (Back Plane Stacking) v topologii kruh * Při použití FPS (Front Plane Stacking) musí na přepínači zůstat min. 2x SFP+ s rychlostí 1/10 Gb * Při nevyužití stohování musí být možné použít všechny SFP+ porty jako datové 10 Gb porty * Minimální propustnost stohování v topologii kruh 40 Gbps |  |
| Vlastnosti napájení | * Minimálně 1x napájecí zdroj 230V |  |
| Kapacitní a výkonové vlastnosti přepínače | * Minimální neblokovaná přepínací kapacita: 104 Gbps * Minimální přepínací rychlost: 77 Mpps * Minimální počet podporovaných VLAN: 4000 * Minimální kapacita tabulky MAC adres: 32000 * Minimální kapacita tabulky směrovacích záznamů: 1000 * Minimální velikost Jumbo Frame: 9200B |  |
| Další požadované funkce a vlastnosti | * Podpora virtuálních LAN dle IEEE 802.1Q * Podpora agregace více portů s využitím protokolu LACP (Link Aggregation Control Protocol) dle IEEE 802.3ad * Podpora objevení zařízení s využitím protokolu LLDP (Link Layer Discovery Protocol) dle IEEE 802.1ab včetně jeho rozšíření LLDP-MED (Media Endpoint Discovery) * Podpora statických směrovacích záznamů pro IPv4 i IPv6 * Podpora funkcí DHCP client, DHCP relay a DHCP server pro IPv4 * Podpora funkcí DHCP client, DHCP relay IPv6 * Podpora funkce DHCP snooping * Podpora funkce IPSG (IP Source Guard) * Podpora funkcí IGMP (Internet Group Management Protocol) a IGMP snooping pro IPv4 ve verzích 1,2 a 3 * Podpora funkcí MLD (Multicast Listener Discovery) a MLD snooping pro IPv6 ve verzích 1 a 2 * Podpora funkce ND (Neighbor Discovery) pro IPv6 * Podpora analýzy provozu minimálně prostřednictvím sFlow verze 5 * Podpora ověřeného přístupu do sítě prostřednictvím protokolu IEEE 802.1x * Podpora současné konfigurace ověřeného přístupu IEEE 802.1x a MAB (Mac Authentication Bypass) s možností volby jejich pořadí * Podpora změny autorizace ověřeného přístupu IEEE 802.1x s využitím CoA (Change of Authorization) * Podpora přiřazení politiky, role nebo dynamického ACL (Access Control List) na základě autorizace * Podpora současného ověření několika zařízení/uživatelů na jediném přístupovém portu s možnožností přídělení různé politiky, role nebo dynamického ACL (Access Control List) * Podpora zabezpečení RADIUS protokolu při ověřování pomocí RADIUS security (RADSec, RADIUS over TLS) * Podpora omezení provozu prostřednictvím ACL (Access Control List) s definicí atributů na vrstvách L2/L3/L4, implementované v hardware pro IPv4 i IPv6 * Podpora zabezpečeného vzdáleného přístupu a správy pomocí protokolů SSHv2, SCP a SFTP * Podpora zabezpečeného monitorování pomocí protokolu SNMPv3 (Simple Network Management Protocol) * Podpora centrální zabezpečené správy prostřednictvím cloudového managementu * Podpora protokolu MSTP (Multiple Spanning Tree Protocol) dle IEEE 802.1s * Podpora protokolu PVST+ (Per-VLAN Spanning Tree) * Podpora ZTP (Zero Touch Provisioning) prostřednictvím cloudového managementu |  |
| Požadované vlastnosti a funkce služby cloudového managementu | * Škálovatelná cloudová SaaS (Software as a Service) služba postavená na mikroslužbách * Služba provozovaná v datových centrech v rámci EU na platformách AWS/Google Cloud/Microsoft Azure, případně v privátním datovém centru výrobce s garantovanou dostupností * Garantovaná dostupnost služby minimálně 99,99% * Podpora multitenantního přístupu a možností delegování přístupu k samostatným tentantům * Podpora API pro integraci s aplikacemi třetích stran pro účely ověřování, automatizace, monitorování apod. * Podporuje centrální správu přepínačů a jejich ZTP (Zero Touch Provisioning) s přidělením politiky a konfiguračních šablon * Podporuje definice konfiguračních šablon pro přepínače v rámci politiky * Podporuje definice konfiguračních šablon pro přístupové porty přepínače v rámci politiky * Podporuje lokální změn konfigurace přepínače nebo přístupového portu, lokální změny mají přednost před šablonou * Podporuje definice šablon pro sestavení stohu přepínačů * Podporuje zabezpečené přihlašování administrátorů ke službě s využitím MFA (Multi-Factor Authentication) * Podporuje přihlašování administrátorů ke službě s využitím SSO (Single Sign On) s využitím protokolu SAMLv2 (např. Entra ID, Ping Identity, Okta a další) * Podporuje aktualizaci firmware přepínačů s bezpečným přenosem a kontrolou přenosu, zdrojem firmware je přímo služba samotná |  |
| Záruky | * Doživotní limitovaná záruka výrobce na hardware, řešení opravy formou dopředné výměny přepínače s odesláním následující pracovní den po identifikaci a uznání závady * Doživotní limitovaná záruka výrobce na software, řešení formou vydávání aktualizací a záplat pro firmware přepínačů |  |
| Licence | * Licence pro centrální správu přepínačů prostřednictvím služby cloudového managementu na dobu minimálně 5 let * Licence pro síťový operační systém nezbytné pro právo a využití požadovaných vlastností a funkcí přepínače |  |

WIFI – 80KS

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje požadavky (ANO/NE) |
| Architektura a základní vlastnosti platformy cloudového managementu Wi-Fi | * Škálovatelná cloudová SaaS (Software as a Service) služba postavená na mikroslužbách+B10:B31 * Služba SaaS provozovaná v datových centrech v rámci EU na platformách AWS/Google Cloud/Microsoft Azure s garantovanou dostupností * Garantovaná dostupnost SaaS služby minimálně 99,99% * Služba je v souladu s mezinárodními bezpečnostními standardy ISO/IEC 27001, 27017, 27701 a CSA-STAR * Služba provozována v datových centrech v souladu s SOC Type 1, 2 a 3 * Služba obsahuje podpůrné nástroje pro zajištění souladu s GDPR (dohledávání informací, audit log, apod.) * Otevřené a dokumentované API pro integraci s aplikacemi třetích stran pro účely ověřování, automatizace, monitorování apod. * Centrální správa bezdrátových přístupových bodů a jejich ZTP (Zero Touch Provisioning) s přidělením politiky a konfiguračních šablon * Možnost definice konfiguračních šablon pro bezdrátové přístupové body v rámci politiky * Možnost definice konfiguračních šablon pro bezdrátové sítě v rámci politiky * Možnost flexibilního přiřazení konfiguračních politik a šablon na základě lokality, skupin apod. * Možnost lokálních změn konfigurace bezdrátového přístupového bodu, lokální změny mají přednost před šablonou * Šifrování CAPWAP management provozu bezdrátových přístupových bodů pomocí HTTPS a DTLS * Možnost vzdáleného přístupu z platformy do plnohodnotné CLI zařízení prostřednictvím šifrovaného management tunelu pro potřeby pokročilé diagnostiky v reálném čase * Podpora pro bezpečné přihlašování administrátorů ke službě s využitím MFA (Multi-Factor Authentication) * Podpora pro bezpečné přihlašování administrátorů ke službě s využitím SSO (Single Sign On) s využitím protokolu SAMLv2 (např. Entra ID, Ping Identity, Okta a další) * Podpora multitenantního přístupu řízení přístupových práv administrátorů RBAC (Role Based Access Control) s možností delegování přístupu k samostatným subjektům a lokalitám. * Podpora WIPS (Wireless Intrusion Prevention System) pro detekci a potlačení bezdrátových útoků * Podpora sběru lokalizačních analytických údajů (tzv. Location Based Analytics) * Podpora technologie dynamických/privátních sdílených klíčů pro bezpečné přidělení unikátního hesla (pro IoT, Guest apod.) s možností jejich distribuce prostřednictvím emailu, SMS nebo aplikace třetí strany s využitím API * Podpora responzivního captive portálu s možností přizpůsobení registrace dle lokalit, skupin apod. a s možností zaslání registračních údajů přes email a SMS |  |
| Typ a počet zařízení | * Enterprise AP pro vnitřní použití, pracující v obou Wi-Fi pásmech současně s možností volby režimu, tvz. SSR (Software Selectable Radio), celkový počet zařízení: 80 |  |
| Architektura a základní vlastnosti AP | * Integrované IoT rádio BLE 5 (Bluetooth Low Energy) * Integrovaný sensor v pásmu 2.4Ghz a 5Ghz (tzv. 3-radio design AP) * Variabilita správy, nasazení a managementu AP (fyzický kontrolér, virtuální kontrolér, public-cloud management) * Integrovaná DPI (Deep Packet Inspection) pro aplikační vizibilitu a řízení bez vlivu na výkonnost Wi-Fi sítě * Certifikace Wi-FI CERTIFIED 6 od Wi-Fi aliance * Minimální počet SSID na každé rádio: 8 * Podpora standardu Wi-Fi6 |  |
| Rádiová specifikace a vlastnosti | * Podpora 2x2:2 MIMO (Multiple-In, Multiple-Out) pro pásmo 2.4 GHz * Podpora 4x4:4 MIMO (Multiple-In, Multiple-Out) pro pásmo 5 GHz * Možnost volby rádiového módu v rámci SSR - 2.4GHz/5GHz, dual 5GHz * Podpora WIPS * Podpora standardů 802.11a/b/g/n/ac/ax * Podpora OFDMA v obou pásmech * Podpora 802.1ax s modulací 1024-QAM * Podpora TxBF (Transmit Beamforming) * Podpora HE20/HE40 pro pásmo 2,4 GHz * Podpora HE20/HE40/HE80 pro pásmo 5 GHz * Podpora automatické správy kanálů a vysílacích výkonů * Podpora WPA3 * BLE rádio v souladu s IEEE 802.15.4 |  |
| Antenní systém | * Integrovaný všesměrový anténní systém pro pásmo 2.4 GHz * Minimální zisk antény v 2.4 Ghz pásmu 4 dBi * Integrovaný všesměrový anténní systém pro pásmo 5 GHz * Minimální zisk antény v 5 Ghz pásmu 4.5 dBi * Integrovaný všesměrový anténní systém v obou pásmech pro sensor rádio * Minimální zisk sensor antény pro 2.4 / 5 GHz pásmo 3.5 / 4.5 dBi * Integrovaný všesměrový anténní systém pro BLE * Minimální zisk IoT antény 3 dBi * Vyzařovací diagramy AP v obou pásmech a polarizacích součástí technické specifikace |  |
| Fyzická rozhraní a vlastnosti | * 1x 100/1000/2500 Mbps Ethernet port (RJ45) * 1x 10/100/1000 Mbps Ethernet port (RJ45) * Konzolový port Micro USB * Minimálně 1x USB 2.0 port |  |
| Fyzické provedení, napájení a další vlastnosti | * Možnost napájení AP přes PoE IEEE 802.3at při zachování plné funkcionality * Univerzální držák pro montáž na strop či stěnu součástí dodávky AP |  |
| Licence | * Licence pro centrální správu přepínačů prostřednictvím cloudového managementu na dobu minimálně 5 let |  |
| Záruky | * Záruka na hardware minimálně 5 let, řešení opravy formou dopředné výměny s odesláním následující pracovní den po identifikaci a uznání závady výrobcem |  |

Další systémové požadavky:

|  |
| --- |
| Požadujeme jednotnou správu všech síťových prvků (Wi-Fi přístupové body, switche a NAC) prostřednictvím cloudové platformy od jednoho výrobce. |
| Platforma musí umožňovat konfiguraci, monitoring a správu všech zařízení z jednoho centrálního rozhraní. |
| Řešení musí být škálovatelné od malých instalací po rozsáhlé podnikové sítě s tisíci zařízeními. |
| Platforma musí splňovat nejvyšší standardy zabezpečení dat, včetně šifrování dat v klidu i během přenosu (TLS/SSL). |
| Soulad s GDPR a dalšími relevantními předpisy o ochraně dat. |
| Možnost řízení přístupu na základě rolí (Role-Based Access Control – RBAC) pro administrátory. |
| Real-time monitoring všech síťových prvků a připojených zařízení. |
| Přehledné reporty o výkonu sítě, bezpečnostních incidentech a souladu se směrnicemi. |
| Historie připojení a auditní logy dostupné přímo v cloudové platformě. |
| Podpora automatického nasazení nových zařízení bez nutnosti manuální konfigurace (zero-touch provisioning). |
| Zajištění SLA na úrovni 99,9 % dostupnosti cloudové platformy. |
| Zálohování konfigurací systému v cloudu s možností rychlé obnovy v případě havárie. |
| Automatické aktualizace softwaru všech spravovaných zařízení prostřednictvím cloudové platformy bez nutnosti manuálního zásahu. |
| Upozornění na bezpečnostní incidenty prostřednictvím e-mailu nebo SMS. |
| Intuitivní webové rozhraní pro správu systému dostupné z jakéhokoliv zařízení s internetovým připojením. |

### Nástroj pro ochranu koncových stanic

### Ochrana koncových stanic a SVR

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje  požadavky  (ANO/NE) |
| Základní vlastnosti | * Bezagentová ochrana VM v prostředí VMware (vShield, NSX-V, NSX-T). * Podpora bezenginového skenování s lehkým klientem na VM, přičemž skenovací úlohy provádí externí zařízení bez omezení počtu těchto zařízení licencí. * Automatické skenování dat při přístupu (otevření, kopírování, přenosy). * Reálné časové skenování specifických typů souborů s možností omezení velikosti. * Deduplikace skenovacích procesů (stejný soubor nebude skenován vícekrát). * Automatické skenování paměti procesů v reálném čase. * Aktualizace bezpečnostního obsahu alespoň jednou za hodinu. |  |
| Detekce a prevence hrozeb | * Detekce na základě virových definic (signatur) a strojového učení (cloud/lokálně). * Ochrana proti 0-day útokům, včetně bezsouborových útoků a anomálního chování. * Analýza spouštěných procesů před spuštěním a jejich blokace při detekci škodlivého chování. * Možnost automatické detonace podezřelých souborů v Sandboxu s podrobným reportem. * Izolace infikovaných stanic od sítě s komunikací pouze s centrální správou. * Ochrana proti phishingovým webům a podvodným stránkám. * Zaznamenávání uživatelských akcí s detailními logy. |  |
| Monitoring a logování incidentů | * Logování systémové, procesové a síťové aktivity během incidentů. * Generování modelu „execution tree“ a časové osy útoku. |  |
| Síťová ochrana a firewall | * Prověřování HTTP, RDP, FTP, SSH/SCP provozu a šifrovaného SSL provozu. * Firewall s IDS/IPS funkcemi a možností vypnutí IDS. * Blokace Network Discovery nebo její omezení na LAN/internet. |  |
| Behaviorální analýza a hodnocení rizik | * Varování před rizikovým chováním uživatelů (např. slabá hesla). * Hodnocení rizik pomocí „Risk score“ pro uživatele i stanice. * Automatická náprava rizik nebo doporučení kroků k jejich odstranění. |  |
| Správa a administrace | * Multi-tenantní správa s granularitou nastavení pro skupiny i jednotlivé stanice. * Možnost vzdálené instalace/odinstalace klienta a správy aktualizací mezi klienty. * Integrace s Active Directory pro správu zařízení. |  |

### NAC

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje  požadavky  (ANO/NE) |
| Architektura a základní vlastnosti platformy cloudového managementu SD-WAN | * Škálovatelná cloudová SaaS (Software as a Service) služba postavená na mikroslužbách * Služba SaaS provozovaná v datových centrech v rámci EU na platformách AWS/Google Cloud/Microsoft Azure s garantovanou dostupností * Garantovaná dostupnost SaaS služby minimálně 99,99% * Služba je v souladu s mezinárodními bezpečnostními standardy ISO/IEC 27001, 27017, 27701 a CSA-STAR * Služba provozována v datových centrech v souladu s SOC Type 1, 2 a 3 * Otevřené a dokumentované API pro integraci s aplikacemi třetích stran pro účely ověřování, automatizace, monitorování apod. * Možnost definice konfiguračních šablon, politik a bezpečnostních profilů pro SD-WAN zařízení v rámci politiky * Podpora pro bezpečné přihlašování administrátorů ke službě s využitím MFA (Multi-Factor Authentication) * Podpora pro bezpečné přihlašování administrátorů ke službě s využitím SSO (Single Sign On) s využitím protokolu SAMLv2 (např. Entra ID, Ping Identity, Okta a další) * Podpora multitenantního přístupu řízení přístupových práv administrátorů RBAC (Role Based Access Control) s možností delegování přístupu k samostatným subjektům a lokalitám. |  |
| Typ a počet zařízení | * Cloud NAC (Cloud Network Access Control) minimálně pro 1000 uživatelů na dobu 5 let |  |
| Požadované vlastnosti a funkce služby cloudového NAC | * RADIUS jako cloudová služba * Plná kompabilita s dodanými přístupovými přepínači a přístupovými body * Zajištění flrexibilního přístupu k síťi na základě ověření uživatele pomocí protokolu 802.1x nebo MAC * Možnost definovat skupiny zařízení a uživatelů, která mohou přistupovat do sítě * Možnost dynamicky přidělit VLAN a ACL pro jednotlivá koncová zařízení * Autentizace vůči Microsoft Entra ID. Šifrovaná komunikace prostřednictvím protokolu SAML. * Možnost integrace s Microsoft Ingune a on-premise Active Directory * Nativní podpora RadSec komunikace mezi Cloud NAC a přístupovými přepínači a přístupovými body * Centralizaovaný monitoring a management. |  |

### Nástroj pro ochranu integrity komunikačních sítí

Analýza síťového provozu – 1ks

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje požadavky (ANO/NE) |
| Základní vlastnosti | * Možnost snadné instalace do síťové infrastruktury, možnost neinvazního zapojení monitoringu * Jednoduchá konfigurace pomocí dostupných konfiguračních šablon, které umožňují výběr z dostupných “Presets” a jejich aplikací vytvářet profily, kapitoly, reporty, alerty, widgety a dashboardy bez nutnosti manuální konfigurace. * Časová synchronizace zařízení proti centrálnímu zdroji času na síti. * Základní správa prostřednictvím GUI, případně příkazové řádky. * Možnost dohledat informace o datových tocích * Samostatná HW appliance pro sondu (je-li vyžadována, monitoring nejméně 3 linek optika 10G) a pro kolektor, nemůže jít o virtualizované řešení * Podpora provádění forenzních analýz * Dostupnost historie informací o datových tocích po dobu 12 měsíců * Budou-li využity transceivery, tak výhradně podporované výrobcem dodaného řešení * Monitorování dostupnosti zdroje flow dat pomocí SNMP. * Možnost porovnávat aktuální data s historickými hodnotami. * Podpora distribuované architektury. * Automatické vyhodnocování informací o flow pro automatickou detekci bezpečnostních nebo provozních anomálií a jejich hlášení formou událostí. * Podpora pokročilých metod detekce bezpečnostních událostí založených na behavoriální analýze. * Detekce, vizualizace a další analýza bezpečnostních událostí, a to napříč spektrem možných typů bezpečnostních událostí - v rozsahu nejméně desítek detekčních metod. * Možnost přizpůsobení míry detekce pomocí snadné správy false positive událostí * Možnost využití priorit v rámci bezpečnostních událostí, podpora více perspektiv * Detekce potenciálních hrozeb i na základě nepatrných anomálií v síťovém provozu. * Možnost definovat vlastní pravidla pro detekční metody (přizpůsobení metod) * Možnost zasílání informací do SIEM/LM * Možnost spolupráce s MISP, podpora uživatelských skriptů a automatizace |  |
| Požadavky na architekturu nasazení | * Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. Podpora VPC flow logů z AWS, Azure a GCP. * Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. * Podpora standardu Cisco AVC vč. položek HTTP hostname a URL. * Podpora pro Cisco NEL, Cisco NSEL, Cisco NBAR2. * Podpora rozšíření VMware NSX, Gigamon a Ixia IPFIX Extensions. * Systém podporuje rozdílné samplovací (vzorkovací) poměry pro každé rozhraní u jednotlivých zdrojů flow dat. * Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory * Možnost převodu formátu (NetFlow v5/v9, IPFIX) přeposílaných flow statistik. * Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS) dle standardu RFC 7011. * Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování. O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu. * Kolektor automaticky detekuje výpadky nebo výrazné poklesy v příjmu dat od jednotlivých zdrojů flow dat. * Flow statistiky je možné automaticky zálohovat na externí síťové úložiště z důvodu dlouhodobé archivace. * Kolektor umožňuje zobrazení přihlášeného uživatele u daného zařízení (IP adresy) včetně historie. Flow statistiky je možné filtrovat na základě loginu uživatele. Uživatelské identity jsou získávány ze systémů řízení přístupu do sítě (např. Cisco ISE) nebo Active Directory. * Monitorování zařízení připojených k datové síti, dlouhodobá historie aktivních zařízení, identifikace na základě IP adresy, MAC adresy, sledování VLAN, operačního systému * Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země). |  |
| Správa | * Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS, soulad s FIPS 140-2. * Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele. * Podpora autentizace vůči LDAP (Active Directory). * Podpora autentizace vůči TACACS+. * Kolektor poskytuje veřejně dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.). |  |
| Sběr dat a vizualizace | * Zabezpečené kolektory flow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách. * Kolektor umožňující zpracování a vizualizaci flow záznamů, a to s výběrem zdrojů dat a období * Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení. * Kolektor je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP, podpora provozního monitorovacího řešení Zabbix. * Podpora IPFIX položek proměnlivé délky. * Sběr a analýza metrik jako RTT, SRT, delay, jitter, retransmise, out-of-order pakety. * Podpora pro protokoly HTTP, VoIP SIP, DNS, SMB/CIFS, DHCP, SMTP, POP3, IMAP a MS SQL (TDS). * Podpora pro monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících identifikaci NATů. * Časové známky je možné přidat do flow záznamů, které tuto informaci nemají od zdroje flow záznamů. * Systém bude schopen sbírat a ukládat dlouhodobě data z tisíců zdrojů flow dat. Disková kapacita datového úložiště musí umožnit uložit záznamy statistik po dobu minimálně 12 měsíců. * Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel). * Uživatel může sdílet dashboard s dalšími uživateli nebo uživatelskými rolemi, kteří si mohou sdílený dashboard zobrazit (případně i editovat). * Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH), včetně plné konfigurace grafů a pohledů uživatelem. * Vizualizace výkonnostních metrik sítě v grafech provozu společně s volumetrickými statistikami. * Zařízení vizualizuje výkonnostní metriky sítě (např. doba zpoždění sítě RTT, doba zpoždění serveru SRT) vykreslováním křivek do průběhového grafu síťového provozu. Při označení časového intervalu jsou zobrazeny průměrné hodnoty výkonnostních metrik bez potřeby spuštění dotazu nad uloženými flow statistikami v kolektoru. * Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV. * Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště. * Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem). * Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bajtů, paketů, toků, nejvyšší hodnoty RTT, průměrné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu. * Systém umožňuje filtrovat s využitím libovolných atributů flow statistik vč. L7 rozšíření nebo výkonnostních parametrů sítě. Filtry je možné kombinovat prostřednictvím logických spojek AND, OR, NOT. Výstupy je možné formátovat, zejména zahrnout do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace). * Automatická notifikace v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, překročení definované relativní nebo absolutní prahové hodnoty, atd.) prostřednictví emailu, SNMP trapu a syslogu, možnost automatického spuštění uživatelem definovaného skriptu. * Uživateli je umožněno definovat si vlastní perzistentní pohledy na data, které budou systémem kontinuálně aktualizovány. K definici pohledu je možné použít libovolný filtr (komunikace daného síťového segmentu, download a upload na server podnikové aplikace, protokol HTTP, apod.). * Systém umožňuje vizualizovat využití sítě v geografickém nebo logickém kontextu pomocí síťové topologie. |  |
| Záruka | * Podpora a záruka výrobce 8x5 NBD v pracovních dnech vzdáleně/HW s reakcí následující pracovní den v místě instalace na 5 let. |  |

## Nástroj pro zajišťování úrovně dostupnosti informací

### Server 2 ks

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje požadavky (ANO/NE) |
| Provedení, příslušenství | * Rackové provedení, min. 1U, max. 2U, šířka 19“ * Montáž do racku výsuvné lyžiny včetně ramene pro kabely * Barevně značené hot-plug vnitřní komponenty a místa pro uchopení. |  |
| CPU | * Dvousocketový systém založený na Intel platformě (z důvodu kompatibility se současným clusterem). * 2x CPU s přesně 8 fyzickými jádry (z licenčních důvodů na serverech provozovaných sysrémů) o základní frekvenci min. 2.8 GHz. Výkon CPU Throughput SPECrate® 2017 Integer minimálně 130 Base pro 2 socket sestavu. Tento výsledek testu musí být dostupný přímo pro nabízený konkrétní model konkrétního výrobce serveru. |  |
| RAM + HDD | * Požadovaná kapacita RAM minimálně 256 GB typu DDR4 2666 složená z 16 DIMM modulů. * Musí umožnovat přidat min. dalších 256 GB paměti ve stejných modulech a kapacitě, bez nutnosti výměny původních modulů. * Bez interních disků pro úložiště dat * Samostatný diskový prostor pro boot operačního systému osazený NVMe hot-plug disky o kapacitě: min. kapacitě 480GB NVMe v RAID 1 |  |
| LAN | * min. 2x 25GbE SFP28 * min. 2x 10GbE SFP+ * 1x Dual port 1GbE karta rozhraní RJ45 * 1x nezávislý management port s rozhraním RJ45 |  |
| SAN | * min. 2x Fibre Channel min. 16Gb včetně optických transceiverů a příslušných optických patchcordů |  |
| Rozhraní | * 3 x USB (1 vpředu, 2 vzadu) * min. 1x USB 3.0 |  |
| TPM | Integrovaný TPM čip verze min. 2.0 |  |
| Napájecí zdroje a ventilátory | * 2 plně redundantní napájecí zdroje třídy Titanium |  |
| Podpora operačních systémů | * VMware vSphere™ 7.0 a novější * Microsoft® Windows Server® 2019/2022, x64 * SUSE® Linux® Enterprise Server * Ubuntu Server LTS * Red Hat® Enterprise Linux |  |
| Management a vzdálená správa | Grafická konzole pro správu a monitorování serverů s možností integrace do proaktivního monitoringu s prediktivní analýzou prostřednictvím cloudového portálu výrobce. Tento portál je přístupný také přes mobilní aplikace dostupné pro iOS a Android. Pokud jsou vyžadovány licence, musí být součástí řešení po celou dobu platnosti podpory  Samostatný management port s podporou failoveru na jinou síťovou kartu v serveru musí podporovat VLAN, LLDP Discovery síťové infrastruktury a protokoly IPv4 i IPv6 |  |
| Přehled o stavu a zabezpečení | Na čelní straně serveru umístěný displej, který zobrazuje základní údaje o serveru (min. IP adresu serveru a chybové stavy)  Management musí být schopen poskytovat ovladače pro instalované operační systémy bez nutnosti speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS). Dále musí umožňovat aktualizaci firmware hardwaru s možností ověření a stažení aktuálních verzí z online repozitáře výrobce nebo z bezpečného lokálního repozitáře spravovaného administrátorem. |  |
| Kompatibilita s centrálním managementem | Schopnost integrace do prostředí VMware vCenter a následná správa z tohoto prostředí, včetně diskového subsystému, bez nutnosti přihlašování se na rozhraní OOB. Management umožňuje monitorování spotřeby elektrické energie na úrovni serveru, hosta a virtuálního serveru (VMware)  Vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, včetně vzdálené konzole KVM over IP, který zároveň umožňuje průběžné vyhodnocování průměrného vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů |  |
| Certifikáty, monitoring | * Automatická instalace a obnova SSL certifikátu vestavěného serveru * Přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE * Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů, včetně událostí o přihlášení a změnách konfigurace * Možnost streamování údajů ze senzorů serveru, telemetrie a provozních reportů pro účely prediktivního vyhodnocování a zabezpečení, s podporou pro Splunk nebo ELK stack |  |
| Zámek konfigurace | Možnost vrácení firmware na předchozí verzi. Automatické obnovení zabezpečeného operačního systému včetně BIOSu serveru a firmware BMC. Podpora uzamčení serveru pro zvýšení bezpečnosti (System Lock Down). |  |
| Ukončování systému | Možnost přístupu přes dedikovaný USB port s emulací síťového připojení  Vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle) |  |
| Záruka a technická podpora výrobce | Podpora na 5 roků typu 24x7x365 s reakční dobou opravy následující pracovní den, oprava v místě instalace, 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 přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory |  |
| Kompatibilita | Všechny servery budou od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu |  |

### Server BACK UP - 1 ks

### Backup server

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje požadavky (ANO/NE) |
| Provedení | * Rackové provedení, min. 1U, max. 2U, šířka 19“ * Montáž do racku výsuvné lyžiny včetně ramene pro kabely * Barevně značené hot-plug vnitřní komponenty a místa pro uchopení. |  |
| CPU | * Dvousocketový systém založený na Intel platformě (z důvodu kompatibility se současným clusterem). * Osazený 2x CPU s přesně 8 fyzickými jádry (z licenčních důvodů na serverech provozovaných sysrémů) o základní frekvenci min. 2.8 GHz. Výkon CPU Throughput SPECrate® 2017 Integer minimálně 130 Base pro 2 socket sestavu. Tento výsledek testu musí být dostupný přímo pro nabízený konkrétní model konkrétního výrobce serveru. |  |
| RAM | * Požadovaná kapacita RAM minimálně 256 GB typu DDR4 2666 složená z 16 DIMM modulů. Musí umožnovat přidat min. dalších 256 GB paměti ve stejných modulech a kapacitě, bez nutnosti výměny původních modulů. |  |
| Diskový subsystém | * Interní diskové úložiště z nejméně 6 NL-SAS disků v RAID 6 o efektivní kapacitě min. 20TB * Samostatný diskový prostor pro boot operačního systému osazený NVMe hot-plug disky o kapacitě: min. kapacitě 480GB NVMe v RAID 1 |  |
| LAN | * min. 2x 25GbE SFP28 * min. 2x 10GbE SFP+ * 1x Dual port 1GbE karta rozhraní RJ45 * 1x nezávislý management port s rozhraním RJ45 |  |
| SAN | * min. 2x Fibre Channel min. 16Gb včetně optických transceiverů a příslušných optických patchcordů |  |
| Rozhraní | * 3 x USB (1 vpředu, 2 vzadu), min. 1x USB 3.0 * 2 x VGA (1 vpředu, 1 vzadu) |  |
| TPM | Integrovaný TPM čip verze min. 2.0 |  |
| Napájecí zdroje a ventilátory | * 2 plně redundantní napájecí zdroje třídy Titanium |  |
| Podpora operačních systémů | VMware vSphere™ 7.0 a novější  Microsoft® Windows Server® 2019/2022, x64  SUSE® Linux® Enterprise Server  Ubuntu Server LTS  Red Hat® Enterprise Linux |  |
| Management a vzdálená správa | Grafická konzole pro správu a monitorování serverů s možností integrace do proaktivního monitoringu s prediktivní analýzou prostřednictvím cloudového portálu výrobce. Tento portál je přístupný také přes mobilní aplikace dostupné pro iOS a Android. Pokud jsou vyžadovány licence, musí být součástí řešení po celou dobu platnosti podpory  Samostatný management port s podporou failoveru na jinou síťovou kartu v serveru musí podporovat VLAN, LLDP Discovery síťové infrastruktury a protokoly IPv4 i IPv6 |  |
| Přehled o stavu a zabezpečení | Na čelní straně serveru umístěný displej, který zobrazuje základní údaje o serveru (min. IP adresu serveru a chybové stavy)  Management musí být schopen poskytovat ovladače pro instalované operační systémy bez nutnosti speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS). Dále musí umožňovat aktualizaci firmware hardwaru s možností ověření a stažení aktuálních verzí z online repozitáře výrobce nebo z bezpečného lokálního repozitáře spravovaného administrátorem. |  |
| Kompatibilita s centrálním managementem | Schopnost integrace do prostředí VMware vCenter a následná správa z tohoto prostředí, včetně diskového subsystému, bez nutnosti přihlašování se na rozhraní OOB. Management umožňuje monitorování spotřeby elektrické energie na úrovni serveru, hosta a virtuálního serveru (VMware)  Vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, včetně vzdálené konzole KVM over IP, který zároveň umožňuje průběžné vyhodnocování průměrného vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů |  |
| Certifikáty, monitoring | * Automatická instalace a obnova SSL certifikátu vestavěného serveru * Přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE * Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů, včetně událostí o přihlášení a změnách konfigurace * Možnost streamování údajů ze senzorů serveru, telemetrie a provozních reportů pro účely prediktivního vyhodnocování a zabezpečení, s podporou pro Splunk nebo ELK stack |  |
| Zámek konfigurace | Možnost vrácení firmware na předchozí verzi. Automatické obnovení zabezpečeného operačního systému včetně BIOSu serveru a firmware BMC. Podpora uzamčení serveru pro zvýšení bezpečnosti (System Lock Down) |  |
| Ukončování systému | Možnost přístupu přes dedikovaný USB port s emulací síťového připojení  Vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle) |  |
| Záruka a technická podpora výrobce | Podpora na 5 roků typu 24x7x365 s reakční dobou opravy následující pracovní den, oprava v místě instalace, 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 přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory |  |
| Kompatibilita | Všechny servery budou od jednoho výrobce z důvodu zajištění maximální kompatibility a jednotného servisního místa a managementu |  |

### Diskové pole

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Minimální požadavek** |  |
| Výrobce a model | (doplnit výrobce a model) | Řešení splňuje požadavky (ANO/NE) |
| Parametry | * Výška max. 2U, šířka 19“, montáž do racku * Hybridní dvouřadičové (dual-active) diskové pole od stejného výrobce jako servery o velikosti max. 2U, rozšiřitelné (pomocí expanzních jednotek) na min. 276 disků, pole musí umožňovat mix různých typů disků min. NL-SAS, SAS, SSD * Front End konektivita min. 4x FC porty na řadič (tj. 8 portů na diskové pole) * Pole musí být osazeno min. 17 ks SSD SAS o kapacitě disku min. 1,92TB SSD SAS * Pole musí podporovat následující typy RAID 1, 5, 6, 10 a distribuovaný RAID přes všechny disky stejného typu (např. DDP, Adapt RAID apod.) |  |
| Záruka, servis | * Podpora na 5 roků typu 24x7x365 s dobou opravy následující pracovní den, oprava v místě instalace, servis je poskytován výrobcem diskového pole. 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 přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory |  |

### 

Společné požadavky pro kapitoly 1 – 4

## Implementace

Implementace analýzy síťového provozu:

* Instalace a konfigurace sondy a agentů pro dohled nad celý prostředím
* Instalace a konfigurace systému pro sběr dat a vyhodnocení
* Konfigurace monitorovacích politik na základě doporučení dané technologie a schválené projektové dokumentace
* Ověření monitorovacích pravidel, testovací provoz

Implementace serverového HW:

* Fyzická instalace serverového HW, aktualizace firmware, zahoření, provedení HW testů
* Konfigurace konzole pro vzdálenou správu a management
* Nasazení a konfigurace virtualizace
* Nasazení a konfigurace SW pro replikaci datového úložiště
* Instalace a konfigurace UPS
* Instalace prostředí a virtuálních systémů
* Migrace stávajícího prostředí virtuálních serverů na nový HW

Implementace síťových prvků a FW

* Instalace a fyzické rozmístění switchů a FW v definovaných lokalitách
* Konfigurace bezpečnostních politik na FW
* Konfigurace sítě a jednotlivých segmentů
* Fyzické propojení síťových prvků včetně přepojení celé sítě a klientských zařízení do nové sítě
* Kompletní konfigurace a nastavení NAC

Implementace zálohování a archivace:

* Instalace a konfigurace zálohovacího serveru
* Konfigurace zálohovacích politik pro zálohování serverové infrastruktury
* Konfigurace a implementace HARDENED REPOSITORY dle BP
* Ověření zálohovacích pravidel

Provedení závěrečných akceptačních testů, zpracování dokumentace a zaškolení

* Provedení testu výpadku jednoho fyzického nodu
* Provedení testu výpadku napájení
* Provedení testu obnovy libovolného serveru či dat ze zálohy
* Zpracování komplexní dokumentace popisující konfiguraci celého prostředí
* Zpracování komplexní bezpečnostní dokumentace dle požadavků bezpečnostních norem
* Zaškolení interní obsluhy správy sítě, zaškolení obsluhy dohledového centra podpory pro vyhodnocení bezpečnostních událostí.

# Společné požadavky

|  |
| --- |
| **Požadavek** |
| Dodavatel bere na vědomí, že součástí akceptace plnění jsou výsledky auditu, který bude prověřovat, zda jím implementovaná bezpečnostní opatření jsou funkční. Dodavatel pak poskytne součinnost nebo napraví nalezené chyby vysoké závažnosti v implementaci technických opatření. |
| Součástí je zajištění instalace a konfigurace veškerých komponent v návaznosti na stávající infrastrukturu školy (tj. včetně dopravy, montáže, instalace a implementace do stávající IT infrastruktury) v sídle zadavatele. |
| Součástí instalace musí být i zaškolení IT administrátorů minimálně v rozsahu nutném pro samostatnou administraci všech komponent zakázky. Administrací se rozumí zejména: konfigurace, monitoring činnosti, aktualizace, řešení problémů, zálohování konfigurace. |
| Zákaznická dokumentace bude zahrnovat:   * popis všech prvků/zařízení, * popis způsobu zálohy a obnovy konfigurace všech prvků/zařízení * veškeré požadavky na zachování záruky/podpory (např. environmentální, kompatibilita, …) * informaci o způsobu řešení servisních požadavků |
| Dodavatel do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou k plnohodnotnému zprovoznění dodané technologie jako logického a funkčního celku. |
| Dodavatel zajistí instalaci a konfiguraci dodaných HW a SW komponent v návaznosti na stávající infrastrukturu organizace, a to včetně instalace a implementace do stávající IT infrastruktury v sídle zadavatele:   * 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 * konfiguraci datových prostor polí, integrace s hypervizorem, nastavení dohledu a instalace SW pro monitoring výkonu * zapojení do stávající LAN |

# Maintenance

MAINTENANCE - (software maintenance) je proces pravidelného udržování, vylepšování a opravování softwarových aplikací po jejich prvotním vývoji a nasazení. Zadavatel v rámci stanovení nabídkové ceny nacení veškerou potřebnou maintenance k řádnému provozovaní dodaného řešení. Potřebnou maintenence dodavatel nacení po dobu udržitelnosti projektu 5let. Maintenance bude dle povahy dodaného řešení pokrývat níže uvedené scénáře:

**Korekční údržba:** Oprava chyb a problémů, které se objeví po nasazení softwaru. To může zahrnovat opravy bezpečnostních zranitelností, chyb v kódu nebo jiné problémy, které ovlivňují funkčnost softwaru.

**Adaptivní údržba:** Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti.

**Perfekcionistická údržba:** Vylepšení softwaru za účelem zvýšení jeho výkonu nebo použitelnosti. To může zahrnovat optimalizaci kódu, zlepšení uživatelského rozhraní nebo zavádění nových funkcí.

Údržba softwaru je klíčová pro zajištění, že software zůstane funkční, bezpečný a relevantní i po dlouhou dobu po jeho původním nasazení.

# Provozní podpora

|  |
| --- |
| **Požadavek** |
| Podpora a servis pro dodaný HW a SW budou poskytovány po dobu udržitelnosti projektu (tj. 60 měsíců od předání díla), nebude-li dohodnuto smluvními stranami jinak – dodavatel bude kalkulovat pro základní technickou podporu **2 hodiny/měsíc.** |
| Bude zajištěna udržitelnost HW a SW včetně třetích stran, dodaných v rámci veřejné zakázky. |
| Technická podpora a servis zařízení HW a SW budou realizovány dodavatelem, případně prostřednictvím odpovídajícího servisního kanálu výrobce. |
| Technická podpora a servis budou realizovány v místě zadavatele. Výjimku tvoří činnosti realizovatelné vzdáleným připojením. |
| Technická podpora bude zajišťována těmito způsoby:   * Telefonicky prostřednictvím přiděleného tel. kontaktu. * Prostřednictvím servisního e-mailu. * Prostřednictvím elektronické oznamovací služby (tzv. helpdesku). * Prostřednictvím vzdáleného připojení na PC uživatele / server. |
| Telefonická, e-mailová podpora a podpora prostřednictvím vzdáleného připojení bude k dispozici minimálně v pracovních dnech od 7 do 16 hod. |
| Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24 hod (s výjimkou předem nahlášených servisních zásahů při správě systému HelpDesk). |
| **Postup při řešení incidentů – SLA**  Zadavatel bude incident oznamovat dodavateli bez zbytečného odkladu jedním ze způsobů a na kontaktních místech, kam budou mít zajištěny přístup pověřené osoby Zadavatele (HelpDesk).  Součástí nahlášení požadavku Zadavatelem musí být:   * popis Incidentu nebo Požadavku, * jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh nezbytných pro replikaci incidentu, * kontaktní osoba.   Dodavatelem používaný systém pro HelpDesk musí pokrýt uvedené informace pro nahlášení požadavku.  **Dodavatel zahájí řešení kritického incidentu ohrožující provoz organizace do 4 pracovních hodin od nahlášení, za pracovní hodiny se považuje období mezi 7:00 a 16:00 v pracovní dny.**  **Dodavatel zahájí řešení nekritického incidentu NBD od nahlášení.**  Dodavatel neprodleně potvrdí obdržení požadavku v systému HelpDesk a poskytne Zadavateli informace o předpokládaném způsobu řešení požadavku, požadavcích na součinnost Zadavatele a předpokládaný termín vyřešení požadavku.  Dodavatel v průběhu řešení požadavku, pokud mu to charakter požadavku a způsob řešení umožňuje, průběžně informuje Zadavatele o aktuálním stavu a případných změnách v předpokládaném způsobu, požadované součinnosti a termínů vyřešení. V případě že dodavatel v průběhu řešení požadavku zjistí, že se jedná o Incident, jehož zdroj je prvek třetích stran, informuje Zadavatele o této skutečnosti, předpokládaném způsobu, požadované součinnosti a termínů vyřešení a pokračuje v řešení v režimu BE (Best Effort) tzn. dodavatel vyvine maximální možné úsilí na provedení požadavku a zejména na zajištění požadovaných parametrů předmětu plnění v nejkratší možné době.  Zjistí-li dodavatel v průběhu řešení Incidentu, že Incident je neodstranitelný, je v rámci Běžné pracovní doby povinen nepřetržitě pracovat na náhradním řešení a informovat o tomto stavu Zadavatele.  Zjistí-li dodavatel v průběhu řešení Incidentu, že Incident má přímou souvislost s neodborným či neoprávněným jednáním osob Zadavatele případně byl Incident vyvolán produkty či službami třetí osoby, je dodavatel povinen bezodkladně informovat o tomto stavu Zadavatele. Zadavatel se zavazuje bezodkladně uhradit v plné výši náklady nad rámec této smlouvy dodavatelem prokazatelně vynaložené k řešení Incidentu, přičemž samotná identifikace Incidentu je součástí plnění této smlouvy.  Zadavatel je oprávněn dořešení Incidentu kdykoliv zastavit či pozastavit, přičemž nárok dodavatele na úhradu již vynaložených prostředků zůstává nedotčen. Incident je v tomto případě považován za vyřešený.  V případě úspěšného vyřešení požadavku, je řešitel před ukončením požadavku povinen provést ověření funkčnosti služby (pokud je to možné). Iniciátora Incidentu informuje o:   * v případě Incidentu specifikuje příčinu (pokud je známa), * vyzve iniciátora k ověření funkčnosti služby.   Po ověření funkčnosti ze strany Zadavatele se Požadavek považuje za vyřešený.  Po vyřešení požadavku dodavatel požadavek uzavře v systému HelpDesk a informuje Zadavatele.  Zadavatel má právo ve lhůtě 10 dnů od uzavření požadavku vznést výhrady nebo připomínky ke způsobu řešení nebo k výslednému stavu; v takovém případě se požadavek nepovažuje za uzavřený a Strany se zavazují zahájit společné jednání za účelem odstranění veškerých vzájemných rozporů a nalezení shody nad způsobem řešení nebo výsledném stavu, a to nejpozději do pěti (5) pracovních dnů od výzvy kterékoliv Strany. Záruky na servisní služby Zadavatel požaduje záruku na veškeré servisní služby provedené v rámci podpory provozu v délce trvání minimálně 3 měsíců (není-li u konkrétní služby uvedeno jinak) od okamžiku realizace. Veškeré HW opravy po dobu záruky budou bez dalších nákladů pro provozovatele. |