Příloha č. 1 – Technická specifikace

Technické požadavky zadavatele

[1 L2 monitoring sítě a ověřování bezpečného přístupu do sítě (DDI / NAC / DNS / DHCP / IPAM) 2](#_Toc523925278)

[2 Obměna prvků síťové infrastruktury 5](#_Toc523925279)

[2.1 LAN páteřní přepínače 5](#_Toc523925280)

[2.2 LAN přístupové přepínače 7](#_Toc523925281)

[2.2.1 48-port s POE+ 7](#_Toc523925282)

[2.2.2 24-port s POE+ 10](#_Toc523925283)

[2.2.3 48-port nonPOE 12](#_Toc523925284)

[2.2.4 24-port nonPOE 14](#_Toc523925285)

[2.3 DC (TOR) přístupové přepínače 16](#_Toc523925286)

[2.4 Softwarový nástroj pro správu a dohled prvků síťové infrastruktury (NMS) 20](#_Toc523925287)

[2.5 WLAN (Wi-Fi) přístupové body 22](#_Toc523925288)

[3 Zavedení síťové behaviorální analýzy 24](#_Toc523925289)

[3.1 Kolektor s automatickým vyhodnocováním NetFlow/NetStream dat a detekcí anomálií 25](#_Toc523925290)

[3.1.1 Systém pro automatickou detekci anomálí 28](#_Toc523925291)

[3.2 Fyzické sondy pro sběr dat 32](#_Toc523925292)

[3.2.1 Výkonnostní parametry sondy 34](#_Toc523925293)

[3.3 Systém na monitorování výkonu aplikací 34](#_Toc523925294)

[4 Definice rozsahu nasazení 37](#_Toc523925295)

[4.1.1 L2 monitoring sítě a ověřování bezpečného přístupu do sítě (DDI / NAC / DNS / DHCP / IPAM) 37](#_Toc523925296)

[4.1.2 Obměna prvků síťové infrastruktury 38](#_Toc523925297)

[4.1.3 Systém pro monitoring a vyhodnocování toků v síti 39](#_Toc523925298)

[5 Specifikace nabízeného řešení 39](#_Toc523925299)

[5.1.1 L2 monitoring sítě a ověřování bezpečného přístupu do sítě (DDI / NAC / DNS / DHCP / IPAM) 39](#_Toc523925300)

[5.1.2 Obměna prvků síťové infrastruktury 39](#_Toc523925301)

[5.1.3 Systém pro monitoring a vyhodnocování toků v síti 40](#_Toc523925302)

# L2 monitoring sítě a ověřování bezpečného přístupu do sítě (DDI / NAC / DNS / DHCP / IPAM)

Nástroj pro zajištění centrální správy IP adresního prostoru musí obsahovat integrované nástroje základních síťových služeb DNS a DHCP, L2 monitoring sítě a být schopen spolupracovat s řízením přístupu do sítě jako jsou systémy NAC (založený na standardu RADIUS) – s jednotnou uživatelskou správou přes GUI.

Požadavky na celý systém jsou rozděleny do několika částí, ale ve výsledku tvoří jeden funkční celek s unifikovaným a jednotným GUI.

|  |  |  |
| --- | --- | --- |
| Název požadavku | Popis požadavku | Míra splnění (ANO/NE) |
| Obecné požadavky na systém | Řídící servery systému musí podporovat možnost provozu ve virtuálním prostředí (VMware) | Doplní účastník |
| Výkonné servery ve formě fyzických appliancí musí využívat zabezpečený operační systém, být schopné poskytovat požadované funkce i v případě nedostupnosti síťového připojení k centrálnímu serveru a komunikovat s centrálním serverem přes zabezpečený protokol (zabezpečení integrity přenášených dat a obsahu přenášených dat před odposloucháváním na síti) | Doplní účastník |
| Systém appliancí musí podporovat možnost nasazení v on-line clusteru a podporovat redundanci i přes různé lokality | Doplní účastník |
| Řešení musí obsahovat systém pro centrální správu a nastavení appliancí | Doplní účastník |
| Systém musí být schopen integrace se systémy síťové analýzy, vulnerability scannerů nebo SIEM | Doplní účastník |
| GUI systému musí být k dispozici v českém nebo anglickém jazyce | Doplní účastník |
| Systém musí podporovat v sítích možnost definice bloků adres, výběry dle bloků adres | Doplní účastník |
| Systém pro adresní plánování | Je nástrojem pro návrh a definici IP adresního plánu s možností definice sítí, výběr konkrétní sítě a práce s ní | Doplní účastník |
| Systém musí podporovat  import/export záznamů do/z adresního plánování v XML nebo CSV formátu | Doplní účastník |
| Systém musí podporovat automatické rozpoznávání zařízení na základě DHCP dotazu. | Doplní účastník |
| Systém musí podporovat automatické vytváření DNS záznamů z adresního plánu | Doplní účastník |
| Systém musí být schopen automatické přidělení zařízení do správné sítě na základě definovaného profilu. | Doplní účastník |
| Systém musí podporovat práci s migrujícími zařízeními a uživateli mezi sítěmi. | Doplní účastník |
| Systém musí podporovat monitoring na L2 vrstvě - MAC a IP adres v reálném čase, včetně toho, na kterém fyzickém portu switche se dané zařízení nachází, pokud switch tuto možnost poskytuje (na kterém portu kterého switche je připojené zařízení s danou MAC adresou), včetně podpory historie | Doplní účastník |
| Systém musí podporovat dostupnost monitoringu i v lokalitách, kde je přístup přes třetí vrstvu (routované lokality), data musí být online k dispozici přes uživatelské rozhraní na centrální lokalitě | Doplní účastník |
| Systém musí podporovat online sledování a vyhodnocení monitoringu a automatické schopnosti detekce konfliktu a schopnost konflikt řešit. | Doplní účastník |
| Systém pro monitoring sítě | Systém musí podporovat vyhledávání zařízení pomocí různých parametrů. | Doplní účastník |
| Systém musí podporovat export záznamů do XML nebo CSV | Doplní účastník |
| Musí se jednat o distribuovaný DHCP systém s možností existence více DHCP serverů na stejné síti (redundance) | Doplní účastník |
| Systém musí podporovat centrální řízení a zakládání pravidel | Doplní účastník |
| Systém musí podporovat redundanci řídícího serveru, nezávislé na lokalitě | Doplní účastník |
| Integrovaný DHCP server | Systém musí podporovat uživatelsky definované DHCP volby | Doplní účastník |
| Systém musí podporovat definice adresních skupin, k nim vázané DHCP volby | Doplní účastník |
| Systém musí podporovat možnost definice i statického záznamu (pro danou MAC není přidělovaná adresa DHCP serverem, pouze existuje záznam) | Doplní účastník |
| Systém musí podporovat možnost existence DHCP záznamů jedné MAC adresy ve více různých sítích - v každé síti obdrží daná MAC adresa přesně svou IP adresu z rozsahu dané sítě - cestující uživatelé | Doplní účastník |
| Systém musí podporovat automatické vytvoření/změna/smazání DHCP záznamu při operacích v adresním plánování | Doplní účastník |
| Systém musí podporovat centrální řízení a zakládání pravidel | Doplní účastník |
| Systém musí podporovat automatické vytváření všech potřebných DNS záznamů z adresního plánování | Doplní účastník |
| Centrální řídící server musí mít redundanci nezávislou na lokalitě | Doplní účastník |
| Integrovaný DNS server | Systém musí podporovat možnost rozdělení zón na vnitřní a vnější pro stejnou zónu, definice vazby na vnitřní nebo vnější zónu dle IP adres (sítí) DNS klientů (klienti ve vnější sítí dostávají odpovědi pouze pro DNS záznamy z vnější zóny, klienti z vnitřní zóny dostávají DNS odpovědi pro vnitřní i vnější zónu) | Doplní účastník |
| Systém musí podporovat replikaci zvolených zónových souborů na podřízený DNS server | Doplní účastník |
| Systém musí podporovat automatického vytváření PTR reverzních záznamů při zakládání “A” záznamů | Doplní účastník |
| Systém musí zobrazovat online stav záznamů DNS a adresního plánování. Včetně schopnosti automatické detekce nežádoucích záznamů a jejich odstranění. | Doplní účastník |
| Systém musí podporovat základní možnost filtrace dotazů na nežádoucí domény (blacklisting) | Doplní účastník |
| Systém musí poskytovat detailní informace o vytížení DNS serveru a počtu dotazů za vteřinu. | Doplní účastník |
| Systém musí podporovat zálohování konfigurací aktivních prvků | Doplní účastník |
| Systém musí podporovat sledování výskytu MAC adres na portech s historií pro účely určení, kde se v daném čase vyskytuje nebo vyskytovala MAC adresa | Doplní účastník |
| Systém musí podporovat řízení přístupu do sítě s využitím 802.1x/MAC autentizace a následné Autorizace (dynamické přidělení VLAN) | Doplní účastník |
| Bezpečnostní část/NAC | Systém musí podporovat automatické vytváření záznamů pro 802.1x a jejich automatická propagace do příslušných AAA zařízení z IPAMu | Doplní účastník |
| Systém musí podporovat možnost definice politik přístupů pro neznámé zařízení | Doplní účastník |
| Systém musí podporovat schopnost definovat komplexní síťové politiky, kdy podle výsledku procesu autentizace je aplikována vybraná síťová politika – definované IP a DHCP parametry | Doplní účastník |
| Systém musí podporovat uživatelské rozhraní s možností přidělování různých stupňů oprávnění. Audit musí být schopen zaznamenat minimálně kdo, kdy a jaké typy operací v systému prováděl | Doplní účastník |
| Systém musí podporovat sledování incidentů na síti s možností generování bezpečnostních reportů | Doplní účastník |
| Systém musí podporovat automatické repository - informace o verzi firmware, typu zařízení, S/N apod. | Doplní účastník |
| Spolupráce s aktivními síťovými prvky, které jsou předmětem nabídky | Systém musí podporovat sledování využití portů síťových prvků v čase - detekce nepoužívaných | Doplní účastník |
| podporovaná veškerá funkcionalita rovněž pro mobilní zařízení s přístupem přes WLAN (WiFi) | Doplní účastník |
| podpora samoobslužného rozhraní pro automatizovanou IP správu nových zařízení v síti | Doplní účastník |
| možnost vytváření recepčních zón pro zajištění přístupů návštěv (Guest zóna) | Doplní účastník |
| BYOD – spolupráce s WLAN řešením, které je předmětem nabídky |  |  |
|  |  |
|  | Doplní účastník |

# Obměna prvků síťové infrastruktury

## LAN páteřní přepínače

|  |  |  |
| --- | --- | --- |
| Název požadavku | Popis požadavku | Míra splnění (ANO/NE) |
| Umístění | Dvě fyzická chassis umístěná ve dvou DC tvářící se jako jeden celek (jedno virtuální chassis / stoh) z pohledu L2, L3 protokolů a managementu | Doplní účastník |
| Stohování | Ano, propustnost stohovacího propojení minimálně 80 Gbit/s (realizováno propoji minimálně 2x 40G).  Součástí dodávky každého přepínače musí být vždy stackovací transceiver o rychlosti minimálně 40Gbps schopný provozu na minimálně 500m po single mode vláknech.  Pokud jsou pro stohování použity standardní servisní porty na linkové kartě, musí být tyto přičteny k požadovaným portům níže.  Zároveň veškeré stohovací porty nesmí být umístěny na jedné kartě z důvodu SPOF. | Doplní účastník |
| Požadavek na funkcionalitu každého kusu | Popis požadavku | Míra splnění (ANO/NE) |
| Modulární architektura | Ano | Doplní účastník |
| Redundantní napájecí (AC) zdroje | minimálně osazené 2 kusy s dostatečnou kapacitou pro provoz v požadované konfiguraci | Doplní účastník |
| Maximální velikost | Hloubka: max. 600 mm  Výška: max. 10U | Doplní účastník |
| Sloty pro linkové karty se servisními porty | Minimálně 4 sloty vyhrazené pro linkové karty se servisními porty | Doplní účastník |
| Z toho volné sloty pro linkové karty se servisními porty určené pro budoucí rozšíření | Minimálně 2 volné sloty musí zůstat zachovány nevyužity pro budoucí rozšiřitelnost | Doplní účastník |
| Oddělené směrovací matice (forwarding plane) – zařízení bude osazeno minimálně dvěma směrovacími kartami, fabric musí mít minimálně 512MB RAM paměti | Ano | Doplní účastník |
| Oddělené řídící matice (control plane), musí mít minimálně 4 GB RAM paměti | Ano | Doplní účastník |
| Řídící matice a směrovací matice musí být přístupné z přední části přepínače | Ano | Doplní účastník |
| Minimální požadovaná propustnost na jeden slot je 160 Gbit/s (tedy 16x 10G portů na wire speed) | Ano | Doplní účastník |
| Směrovací kapacita | minimálně 750 Mpps | Doplní účastník |
| Minimální propustnost systému | 4,5 Tbit/s | Doplní účastník |
| Počet portů: | Min. 48x 10G SFP+  Min. 16x 1G SFP  Ke každému přepínači budou dodány:  36ks 10G SFP+ LR modulů  12ks 10G SFP+ SR modulů  8ks 1G SFP SR modulů  8ks 1G SFP T (RJ45) modulů | Doplní účastník |
| WLAN kontroler | Ano, systém musí umožnit funkci pro správu a konfiguraci dodaných WiFi AP včetně potřebných licencí | Doplní účastník |
| USB port pro nahrávání konfigurace a zálohy | minimálně 1x USB port | Doplní účastník |
| Dedikovaný management (out of band) nebo console port | miniUSB nebo RJ45 na přední straně přepínače | Doplní účastník |
| Záznamů ve směrovací tabulce IPv4 | Minimálně 1 milion | Doplní účastník |
| Záznamů ve směrovací tabulce IPv6 | Minimálně 0,5 milionu | Doplní účastník |
| MAC adresy | Minimálně 128.000 | Doplní účastník |
| VLAN | Minimálně 4.000 aktivních VLAN | Doplní účastník |
| VLAN L3 rozhraní | Minimálně 4.000 aktivních L3 rozhraní | Doplní účastník |
| LACP | Ano, Minimálně 128 LACP skupin | Doplní účastník |
| Multi-chassis link aggregation (MC-LAG) | Ano | Doplní účastník |
| Směrovací protokoly | Ano, RIP, RIPng, OSPF, OSPFv3, IS‑IS, IS‑ISv6, BGP a BGP4+ | Doplní účastník |
| Podpora technologie VRRP a VRRPv6 | Ano | Doplní účastník |
| Podpora multicastových směrovacích protokolů PIM-SM, PIM-SSM pro IPv4 a IPv6 | Ano | Doplní účastník |
| Podpora IGMPv1,v2,v3 a technologie IGMP snooping | Ano | Doplní účastník |
| Podpora technologie multicast VPN | Ano | Doplní účastník |
| Podpora BFD v hardware, nikoliv v CPU (BFD interval odesílání paketů 4ms a méně, detekční interval 10ms) | Ano | Doplní účastník |
| Podpora BFD pro IS-IS, OSPF, BGP, VRRP a PIM | Ano | Doplní účastník |
| STP, RSTP, MSTP nebo jiný „per VLAN“ kompatibilní protokol | Ano, např. PVST+ | Doplní účastník |
| Virtuální směrovací instance (VRF) | Ano, minimálně 2000 | Doplní účastník |
| Podpora technologie ISSU | Ano | Doplní účastník |
| Podpora H-QoS | minimálně 5 úrovní | Doplní účastník |
| Technologie Y. 1731, 802.3ah, 802.1ag, | Ano | Doplní účastník |
| ACL na IPv6, IPv4 a L2 hlavičku | Ano | Doplní účastník |
| Podpora vertikálního stohování – možnost připojit přístupové přepínače, které se chovají jako vzdálené linkové karty (z pohledu správy se jedná o jedno zařízení jako celek), podpora minimálně 100 virtualizovaných přístupových přepínačů | Ano, možnost budoucího nasazení | Doplní účastník |
| Podpora technologie RSPAN a lokálního zrcadlení provozu | Ano | Doplní účastník |
| Podpora technologie Netflow v hardware (možnost sbírat nevzorkovaná data) | Ano | Doplní účastník |
| Podpora konfigurace přes CLI - SSH, Telnet a lokální konzole | Ano | Doplní účastník |
| Podpora technologie SNMPv1, v2c a v3 | Ano | Doplní účastník |

## LAN přístupové přepínače

### 48-port s POE+

|  |  |  |
| --- | --- | --- |
| Název požadavku | Popis požadavku | Míra splnění (ANO/NE) |
| Stohování | Sestohovat musí být možné minimálně 8 přepínačů do kruhu.  Stohování musí být možné buď přes dva 10G linkové porty nebo přes specializovanou stacking card.  V případě stohování přes specializovanou stacking card, musí být tato součástí dodávky každého přepínače vč. příslušných licencí a příslušenství, a musí zajistit minimálně stejnou propustnost jako dva 10G porty.  Součástí dodávky každého přepínače musí být vždy propojovací/stackovací kabel o délce 1 metr včetně případných optických modulů.  V rámci stohu musí být možné provozovat všechny typy LAN přístupových přepínačů, tj. musí být možná kombinace „48-port s POE+“ + „24-port s POE+“ + „48-port NonPOE“ + „24-port NonPOE“ | Doplní účastník |
| Požadavek na funkcionalitu každého kusu | Popis požadavku | Míra splnění (ANO/NE) |
| Počet portů 10/100/1000 Base-T | Minimálně 48x | Doplní účastník |
| Počet portů SFP+ 10G | Minimálně 4x kompatibilní s 10G SFP+ transceivery a kompatibilní zpětně s 1G SFP transceivery.  V případě stohování přes speciální stacking card pak postačí jen 2 porty pro uplink.  Ke každému přepínači budou dodány 2ks 10G SFP+ LR modulů | Doplní účastník |
| Umístění portů | Všechny porty musí být na přední straně přepínače | Doplní účastník |
| Maximální velikost | Hloubka: max. 445 mm  Výška: max. 1U | Doplní účastník |
| USB port pro nahrávání konfigurace a zálohy | minimálně 1x USB port | Doplní účastník |
| Dedikovaný management (out of band) nebo console port | miniUSB nebo RJ45 na přední straně přepínače | Doplní účastník |
| Všechny porty neblokované | ano | Doplní účastník |
| Přepínací výkon | minimálně 330 Gbps | Doplní účastník |
| Přepínací kapacita | minimálně 130 Mpps | Doplní účastník |
| Redundantní napájecí (AC) zdroje | osazeno 2 kusy s dostatečnou kapacitou pro výkon PoE/PoE+ napájení koncových stanic v maximálním zatížení | Doplní účastník |
| Možnost osadit interním DC zdrojem s podporou PoE/PoE+ | DC zdroj musí být dostupný v době objednání přepínače  Kombinace AC + DC musí být podporována | Doplní účastník |
| Napájení koncových stanic PoE /PoE+ | Dle standardu  IEEE 802.3af (PoE) na všech 48 portech současně;  IEEE 802.3at (PoE+) minimálně na 24 portech současně | Doplní účastník |
| MAC adresy | minimálně 16000 | Doplní účastník |
| VLAN | minimálně 4000 aktivních VLAN | Doplní účastník |
| Voice VLAN a guest VLAN pro 802.1x | Ano | Doplní účastník |
| Mapování VLAN | Ano | Doplní účastník |
| Protokol na registraci VLAN | Ano, například GVRP nebo VTP nebo obdobný | Doplní účastník |
| Podpora Jumbo Frame | minimálně 10 kB | Doplní účastník |
| STP, RSTP, MSTP nebo jiný „per VLAN“ kompatibilní protokol | Ano, např. PVST+ | Doplní účastník |
| VLAN L3 rozhraní | minimálně 1000 | Doplní účastník |
| Směrovací tabulky pro IPv4 | minimálně 3000 statických záznamů;  8000 dynamických záznamů | Doplní účastník |
| L3 funkce | minimálně RIP, RIPng, OSPF a OSPFv3a IS-IS, IS-SIv6 a BGP | Doplní účastník |
| Technologie VRRP a VRRPv6 | Ano | Doplní účastník |
| Multicast směrovací protokoly | minimálně PIM-SM, PIM-SSM pro IPv4 | Doplní účastník |
| IGMPv1,v2,v3 a technologie IGMP snooping | Ano | Doplní účastník |
| Ověřování uživatelů | Ano  pomocí 802.1x a pomocí MAC adres, podpora funkcí guest VLAN | Doplní účastník |
| LACP | minimálně 120 skupin | Doplní účastník |
| Podpora BFD | minimálně pro protokoly OSPF, BGP, IS-IS, PIM, VRRP a statické záznamy ve směrovací tabulce | Doplní účastník |
| ACL na IPv6, IPv4 a L2 hlavičku | Ano | Doplní účastník |
| Technologie RSPAN a lokálního zrcadlení provozu | Ano | Doplní účastník |
| Podpora technologie sFlow v hardware | Ano | Doplní účastník |
| Konfigurace přes CLI - SSH, Telnet a lokální konzole | Ano | Doplní účastník |
| Technologie SNMPv1, v2c a v3 | Ano | Doplní účastník |

### 24-port s POE+

|  |  |  |
| --- | --- | --- |
| Název požadavku | Popis požadavku | Míra splnění (ANO/NE) |
| Stohování | Sestohovat musí být možné minimálně 8 přepínačů do kruhu.  Stohování musí být možné buď přes dva 10G linkové porty nebo přes specializovanou stacking card.  V případě stohování přes specializovanou stacking card, musí být tato součástí dodávky každého přepínače vč. příslušných licencí a příslušenství, a musí zajistit minimálně stejnou propustnost jako dva 10G porty.  Součástí dodávky každého přepínače musí být vždy propojovací/stackovací kabel o délce 1 metr včetně případných optických modulů.  V rámci stohu musí být možné provozovat všechny typy LAN přístupových přepínačů, tj. musí být možná kombinace „48-port s POE+“ + „24-port s POE+“ + „48-port NonPOE“ + „24-port NonPOE“ | Doplní účastník |
| Požadavek na funkcionalitu každého kusu | Popis požadavku | Míra splnění (ANO/NE) |
| Počet portů 10/100/1000 Base-T | Minimálně 24x | Doplní účastník |
| Počet portů SFP+ 10G | Minimálně 4x kompatibilní s 10G SFP+ transceivery a kompatibilní zpětně s 1G SFP transceivery  V případě stohování přes speciální stacking card pak postačí jen 2 porty pro uplink  Ke každému přepínači budou dodány 2ks 10G SFP+ LR modulů | Doplní účastník |
| Umístění portů | Všechny porty musí být na přední straně přepínače | Doplní účastník |
| Maximální velikost | Hloubka: max. 445 mm  Výška: max. 1U | Doplní účastník |
| USB port pro nahrávání konfigurace a zálohy | minimálně 1x USB port | Doplní účastník |
| Dedikovaný management (out of band) nebo console port | miniUSB nebo RJ45 na přední straně přepínače | Doplní účastník |
| Všechny porty neblokované | ano | Doplní účastník |
| Přepínací výkon | minimálně 330 Gbps | Doplní účastník |
| Přepínací kapacita | minimálně 90 Mpps | Doplní účastník |
| Redundantní napájecí (AC) zdroje | osazeno 2 kusy s dostatečnou kapacitou pro výkon PoE/PoE+ napájení koncových stanic v maximálním zatížení | Doplní účastník |
| Možnost osadit interním DC zdrojem s podporou PoE | DC zdroj musí být dostupný v době objednání přepínače  Kombinace AC + DC musí být podporována | Doplní účastník |
| Napájení koncových stanic PoE | Dle standardu  IEEE 802.3af (PoE) na všech 24 portech současně;  IEEE 802.3at (PoE+) minimálně na 12 portech současně | Doplní účastník |
| MAC adresy | minimálně 16000 | Doplní účastník |
| VLAN | minimálně 4000 aktivních VLAN | Doplní účastník |
| Voice VLAN a guest VLAN pro 802.1x | Ano | Doplní účastník |
| Mapování VLAN | Ano | Doplní účastník |
| Protokol na registraci VLAN | Ano, například GVRP nebo VTP nebo obdobný | Doplní účastník |
| Podpora Jumbo Frame | minimálně 10 kB | Doplní účastník |
| STP, RSTP, MSTP nebo jiný „per VLAN“ kompatibilní protokol | Ano, např. PVST+ | Doplní účastník |
| VLAN L3 rozhraní | minimálně 1000 | Doplní účastník |
| Směrovací tabulky pro IPv4 | minimálně 3000 statických záznamů;  8000 dynamických záznamů | Doplní účastník |
| L3 funkce | minimálně RIP, RIPng, OSPF a OSPFv3a IS-IS, IS-SIv6 a BGP | Doplní účastník |
| Technologie VRRP a VRRPv6 | Ano | Doplní účastník |
| Multicast směrovací protokoly | minimálně PIM-SM, PIM-SSM pro IPv4 | Doplní účastník |
| IGMPv1,v2,v3 a technologie IGMP snooping | Ano | Doplní účastník |
| Ověřování uživatelů | Ano  pomocí 802.1x a pomocí MAC adres, podpora funkcí guest VLAN | Doplní účastník |
| LACP | minimálně 120 skupin | Doplní účastník |
| Podpora BFD | minimálně pro protokoly OSPF, BGP, IS-IS, PIM, VRRP a statické záznamy ve směrovací tabulce | Doplní účastník |
| ACL na IPv6, IPv4 a L2 hlavičku | Ano | Doplní účastník |
| Technologie RSPAN a lokálního zrcadlení provozu | Ano | Doplní účastník |
| Podpora technologie sFlow v hardware | Ano | Doplní účastník |
| Konfigurace přes CLI - SSH, Telnet a lokální konzole | Ano | Doplní účastník |
| Technologie SNMPv1, v2c a v3 | Ano | Doplní účastník |

### 48-port nonPOE

|  |  |  |
| --- | --- | --- |
| Název požadavku | Popis požadavku | Míra splnění (ANO/NE) |
| Stohování | Sestohovat musí být možné minimálně 8 přepínačů do kruhu.  Stohování musí být možné buď přes dva 10G linkové porty nebo přes specializovanou stacking card.  V případě stohování přes specializovanou stacking card, musí být tato součástí dodávky každého přepínače vč. příslušných licencí a příslušenství, a musí zajistit minimálně stejnou propustnost jako dva 10G porty.  Součástí dodávky každého přepínače musí být vždy propojovací/stackovací kabel o délce 1 metr včetně případných optických modulů.  V rámci stohu musí být možné provozovat všechny typy LAN přístupových přepínačů, tj. musí být možná kombinace „48-port s POE+“ + „24-port s POE+“ + „48-port NonPOE“ + „24-port NonPOE“ | Doplní účastník |
| Požadavek na funkcionalitu každého kusu | Popis požadavku | Míra splnění (ANO/NE) |
| Počet portů 10/100/1000 Base-T | Minimálně 48x | Doplní účastník |
| Počet portů SFP+ 10G | Minimálně 4x kompatibilní s 10G SFP+ transceivery a kompatibilní zpětně s 1G SFP transceivery  V případě stohování přes speciální stacking card pak postačí jen 2 porty pro uplink  Ke každému přepínači budou dodány 2ks 10G SFP+ LR modulů | Doplní účastník |
| Umístění portů | Všechny porty musí být na přední straně přepínače | Doplní účastník |
| Maximální velikost | Hloubka: max. 445 mm  Výška: max. 1U | Doplní účastník |
| USB port pro nahrávání konfigurace a zálohy | minimálně 1x USB port | Doplní účastník |
| Dedikovaný management (out of band) nebo console port | miniUSB nebo RJ45 na přední straně přepínače | Doplní účastník |
| Všechny porty neblokované | ano | Doplní účastník |
| Přepínací výkon | minimálně 330 Gbps | Doplní účastník |
| Přepínací kapacita | minimálně 130 Mpps | Doplní účastník |
| Redundantní napájecí (AC) zdroje | osazeno 2 kusy s dostatečnou kapacitou | Doplní účastník |
| Možnost osadit interním DC zdrojem s podporou PoE | DC zdroj musí být dostupný v době objednání přepínače  Kombinace AC + DC musí být podporována | Doplní účastník |
| MAC adresy | minimálně 16000 | Doplní účastník |
| VLAN | minimálně 4000 aktivních VLAN | Doplní účastník |
| Voice VLAN a guest VLAN pro 802.1x | Ano | Doplní účastník |
| Mapování VLAN | Ano | Doplní účastník |
| Protokol na registraci VLAN | Ano, například GVRP nebo VTP nebo obdobný | Doplní účastník |
| Podpora Jumbo Frame | minimálně 10 kB | Doplní účastník |
| STP, RSTP, MSTP nebo jiný „per VLAN“ kompatibilní protokol | Ano, např. PVST+ | Doplní účastník |
| VLAN L3 rozhraní | minimálně 1000 | Doplní účastník |
| Směrovací tabulky pro IPv4 | minimálně 3000 statických záznamů;  8000 dynamických záznamů | Doplní účastník |
| L3 funkce | minimálně RIP, RIPng, OSPF a OSPFv3a IS-IS, IS-SIv6 a BGP | Doplní účastník |
| Technologie VRRP a VRRPv6 | Ano | Doplní účastník |
| Multicast směrovací protokoly | minimálně PIM-SM, PIM-SSM pro IPv4 | Doplní účastník |
| IGMPv1,v2,v3 a technologie IGMP snooping | Ano | Doplní účastník |
| Ověřování uživatelů | Ano  pomocí 802.1x a pomocí MAC adres, podpora funkcí guest VLAN | Doplní účastník |
| LACP | minimálně 120 skupin | Doplní účastník |
| Podpora BFD | minimálně pro protokoly OSPF, BGP, IS-IS, PIM, VRRP a statické záznamy ve směrovací tabulce | Doplní účastník |
| ACL na IPv6, IPv4 a L2 hlavičku | Ano | Doplní účastník |
| Technologie RSPAN a lokálního zrcadlení provozu | Ano | Doplní účastník |
| Podpora technologie sFlow v hardware | Ano | Doplní účastník |
| Konfigurace přes CLI - SSH, Telnet a lokální konzole | Ano | Doplní účastník |
| Technologie SNMPv1, v2c a v3 | Ano |  |

### 24-port nonPOE

|  |  |  |
| --- | --- | --- |
| Název požadavku | Popis požadavku | Míra splnění (ANO/NE) |
| Stohování | Sestohovat musí být možné minimálně 8 přepínačů do kruhu.  Stohování musí být možné buď přes dva 10G linkové porty nebo přes specializovanou stacking card.  V případě stohování přes specializovanou stacking card, musí být tato součástí dodávky každého přepínače vč. příslušných licencí a příslušenství, a musí zajistit minimálně stejnou propustnost jako dva 10G porty.  Součástí dodávky každého přepínače musí být vždy propojovací/stackovací kabel o délce 1 metr včetně případných optických modulů.  V rámci stohu musí být možné provozovat všechny typy LAN přístupových přepínačů, tj. musí být možná kombinace „48-port s POE+“ + „24-port s POE+“ + „48-port NonPOE“ + „24-port NonPOE“ | Doplní účastník |
| Požadavek na funkcionalitu každého kusu | Popis požadavku | Míra splnění (ANO/NE) |
| Počet portů 10/100/1000 Base-T | Minimálně 24x | Doplní účastník |
| Počet portů SFP+ 10G | Minimálně 4x kompatibilní s 10G SFP+ transceivery a kompatibilní zpětně s 1G SFP transceivery  V případě stohování přes speciální stacking card pak postačí jen 2 porty pro uplink  Ke každému přepínači budou dodány 2ks 10G SFP+ LR modulů | Doplní účastník |
| Umístění portů | Všechny porty musí být na přední straně přepínače | Doplní účastník |
| Maximální velikost | Hloubka: max. 445 mm  Výška: max. 1U | Doplní účastník |
| USB port pro nahrávání konfigurace a zálohy | minimálně 1x USB port | Doplní účastník |
| Dedikovaný management (out of band) nebo console port | miniUSB nebo RJ45 na přední straně přepínače | Doplní účastník |
| Všechny porty neblokované | ano | Doplní účastník |
| Přepínací výkon | minimálně 330 Gbps | Doplní účastník |
| Přepínací kapacita | minimálně 90 Mpps | Doplní účastník |
| Redundantní napájecí (AC) zdroje | osazeno 2 kusy s dostatečnou kapacitou | Doplní účastník |
| Možnost osadit interním DC zdrojem s podporou PoE | DC zdroj musí být dostupný v době objednání přepínače  Kombinace AC + DC musí být podporována | Doplní účastník |
| MAC adresy | minimálně 16000 | Doplní účastník |
| VLAN | minimálně 4000 aktivních VLAN | Doplní účastník |
| Voice VLAN a guest VLAN pro 802.1x | Ano | Doplní účastník |
| Mapování VLAN | Ano | Doplní účastník |
| Protokol na registraci VLAN | Ano, například GVRP nebo VTP nebo obdobný | Doplní účastník |
| Podpora Jumbo Frame | minimálně 10 kB | Doplní účastník |
| STP, RSTP, MSTP nebo jiný „per VLAN“ kompatibilní protokol | Ano, např. PVST+ | Doplní účastník |
| VLAN L3 rozhraní | minimálně 1000 | Doplní účastník |
| Směrovací tabulky pro IPv4 | minimálně 3000 statických záznamů;  8000 dynamických záznamů | Doplní účastník |
| L3 funkce | minimálně RIP, RIPng, OSPF a OSPFv3a IS-IS, IS-SIv6 a BGP | Doplní účastník |
| Technologie VRRP a VRRPv6 | Ano | Doplní účastník |
| Multicast směrovací protokoly | minimálně PIM-SM, PIM-SSM pro IPv4 | Doplní účastník |
| IGMPv1,v2,v3 a technologie IGMP snooping | Ano | Doplní účastník |
| Ověřování uživatelů | Ano  pomocí 802.1x a pomocí MAC adres, podpora funkcí guest VLAN | Doplní účastník |
| LACP | minimálně 120 skupin | Doplní účastník |
| Podpora BFD | minimálně pro protokoly OSPF, BGP, IS-IS, PIM, VRRP a statické záznamy ve směrovací tabulce | Doplní účastník |
| ACL na IPv6, IPv4 a L2 hlavičku | Ano | Doplní účastník |
| Technologie RSPAN a lokálního zrcadlení provozu | Ano | Doplní účastník |
| Podpora technologie sFlow v hardware | Ano | Doplní účastník |
| Konfigurace přes CLI - SSH, Telnet a lokální konzole | Ano | Doplní účastník |
| Technologie SNMPv1, v2c a v3 | Ano | Doplní účastník |

## DC (TOR) přístupové přepínače

|  |  |  |
| --- | --- | --- |
| Název požadavku | Popis požadavku | Míra splnění (ANO/NE) |
| Stohování | Sestohovat musí být možné minimálně 8 přepínačů do kruhu.  Stohování buď přes dva 40G linkové porty nebo přes specializovanou stacking card .  V případě stohování přes specializovanou stacking card, musí být tato součástí dodávky každého boxu vč. příslušných licencí a příslušenství, a musí zajistit minimálně stejnou propustnost jako dva 40G porty.  Součástí dodávky každého přepínače musí být vždy propojovací/stackovací kabel o délce 1 metr včetně případných optických modulů. | Doplní účastník |
| Požadavek na funkcionalitu každého kusu | Popis požadavku | Míra splnění (ANO/NE) |
| Základní vlastnosti |  |  |
| Počet portů | Minimálně  2x 10G SFP+ pro uplink  30x 1/10G RJ45 pro připojení serverů  15x 1/10G SFP+ pro připojení serverů  2x 40G QSFP+ pro budoucí rozšíření v oblasti uplinku  Ke každému přepínači budou dodány  2ks 10G SFP+ LR modulů  10ks 10SFP+ SR modulů | Doplní účastník |
| Umístění portů | Všechny porty musí být na přední straně přepínače, včetně stohovacích | Doplní účastník |
| Maximální velikost | Hloubka: max. 600 mm  Výška: max. 1U | Doplní účastník |
| Podpora rozpadu 40G portu na 4\*10G port | ano | Doplní účastník |
| Redundantní interní napájecí zdroje, vyměnitelné za chodu | ano,  dva AC zdroje součástí nabídky | Doplní účastník |
| Možnost kombinace AC a DC zdroje v jednom zařízení | ano | Doplní účastník |
| Redundantní ventilátory, vyměnitelné za chodu | Ano | Doplní účastník |
| Způsob chlazení | Předo-zadní (vyfukování přes porty, switch bude instalován porty dozadu) | Doplní účastník |
| Podpora směrovacích protokolů | Ano | Doplní účastník |
| Výkonnostní parametry |  |  |
| Minimální propustnost přepínacího subsystému | min. 1,25 Tbps a 950 Mpps | Doplní účastník |
| Minimální propustnost přepínacího subsystému ve stohu | min. 160 Gbit/s | Doplní účastník |
| Podpora MAC adres | min. 120 000 | Doplní účastník |
| Všechny porty neblokované (wirespeed) | ano | Doplní účastník |
| Vlastnosti stohování |  |  |
| Minimální počet přepínačů ve stohu (VSS, IRF, stack) | 8 | Doplní účastník |
| Automatická kontrola a sjednocení verze software přepínačů ve stohu | ano | Doplní účastník |
| Povýšení software jednotlivých přepínačů stohu bez výpadku konektivity celého stohu | ano | Doplní účastník |
| Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením | ano | Doplní účastník |
| Seskupení portů (IEEE 802.3ad) mezi různými prvky stohu | ano | Doplní účastník |
| Kterýkoli prvek ve stohu může být řídícím prvkem stohu (1:N redundance) | ano | Doplní účastník |
| Protokoly fyzické vrstvy |  |  |
| IEEE 802.3-2005 | ano | Doplní účastník |
| IEEE 802.3ad | ano | Doplní účastník |
| Podpora "jumbo rámců" min. 9000 bytes | ano | Doplní účastník |
| Protokoly 2. vrstvy |  |  |
| IEEE 802.1D | ano | Doplní účastník |
| IEEE 802.1Q | ano | Doplní účastník |
| Minimální počet aktivních VLAN | 4000 | Doplní účastník |
| Tunelování 802.1Q v 802.1Q | ano | Doplní účastník |
| IEEE 802.1X - Port Based Network Access Control | ano | Doplní účastník |
| IEEE 802.1s - multiple spanning trees | ano | Doplní účastník |
| IEEE 802.1w - Rapid Tree Spanning Protocol | ano | Doplní účastník |
| IEEE 802.1p - Minimální počet vnitřních front | 8 | Doplní účastník |
| Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní | ano | Doplní účastník |
| Detekce protilehlého zařízení (např. CDP, LLDP) | ano | Doplní účastník |
| Detekce parametrů protilehlého zařízení (např. LLDP-MED) | ano | Doplní účastník |
| Protokol pro definici šířených VLAN (např. VTP nebo GVRP) | ano | Doplní účastník |
| Detekce jednosměrnosti optické linky (např. UDLD) | ano | Doplní účastník |
| STP root guard | ano | Doplní účastník |
| STP loop guard | ano | Doplní účastník |
| Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard) | ano | Doplní účastník |
| Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech | ano | Doplní účastník |
| Protokol IP |  |  |
| IP alias (více IP sítí na jednom rozhraní) | ano | Doplní účastník |
| QoS | ano | Doplní účastník |
| QoS i na stohovacím propoji | ano | Doplní účastník |
| možnost konfigurovat QoS na stohovacím propoji | ano | Doplní účastník |
| DHCP relay | ano | Doplní účastník |
| Směrovací protokoly |  | Doplní účastník |
| OSPFv2 | ano | Doplní účastník |
| RIPv2 | ano | Doplní účastník |
| Statické směrování | ano | Doplní účastník |
| Směrovací tabulka pro IPv4 | min. 1000 záznamů | Doplní účastník |
| Podpora VRRP | ano | Doplní účastník |
| Směrování multicastu |  | Doplní účastník |
| PIM (dense i sparse mód) pro IPv4 | ano | Doplní účastník |
| IGMPv2 snooping | ano | Doplní účastník |
| IGMPv3 snooping | ano | Doplní účastník |
| Bezpečnost |  | Doplní účastník |
| Podpora reverse path check (uRPF) | ano | Doplní účastník |
| ACL na rozhraní IN/OUT (včetně virtuálních - VLAN, loopback, 802.1ad) | ano | Doplní účastník |
| ACL pro IP | ano | Doplní účastník |
| ACL pro ethernetové rámce | ano | Doplní účastník |
| IPv6 ACL | ano | Doplní účastník |
| Možnost definovat povolené MAC adresy na portu | ano | Doplní účastník |
| Možnost definovat maximální počet MAC adres na portu | ano | Doplní účastník |
| Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy) | ano | Doplní účastník |
| DHCP snooping | ano | Doplní účastník |
| Kontrola ARP protokolu (např. Dynamic ARP inspection (DAI)) | ano | Doplní účastník |
| Verifikace mapování IP-MAC (např. IP source guard) | ano | Doplní účastník |
| IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu | ano | Doplní účastník |
| Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x) | ano | Doplní účastník |
| Podpora USB portu pro nahrávání konfigurace a zálohy (minimálně 1\*USB port) | ano | Doplní účastník |
| Management |  |  |
| CLI rozhraní | ano | Doplní účastník |
| SSHv2 | ano | Doplní účastník |
| SSHv2 over IPv6 | ano | Doplní účastník |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ano | Doplní účastník |
| SNMPv2 | ano | Doplní účastník |
| SNMPv3 | ano | Doplní účastník |
| Sériová konzolová linka | ano | Doplní účastník |
| 10/100/1000 management out-of-band port | ano | Doplní účastník |
| DNS klient | ano | Doplní účastník |
| NTP klient s MD5 autentizací | ano | Doplní účastník |
| RADIUS klient pro AAA (autentizace, autorizace, accounting) | ano | Doplní účastník |
| TACACS+ klient | ano | Doplní účastník |
| Port mirroring (SPAN) | ano | Doplní účastník |
| Port mirroring 1 -> 1 | ano | Doplní účastník |
| Port mirroring N -> 1 | ano | Doplní účastník |
| Port mirroring ACL (mirroruje pouze definované toky) | ano | Doplní účastník |
| Vzdálený port mirroring (RSPAN) | ano | Doplní účastník |
| Syslog | ano | Doplní účastník |
| Podpora uživatelsky modifikovatelné automatické reakce/obsluhy událostí při provozu přepínače (pomocí skriptů) | ano | Doplní účastník |
| Přepínač obsahuje traceroute utilitu operující na linkové vrstvě (Layer 2 traceroute) | ano | Doplní účastník |
| Podpora technologie Netflow v hardware | ano | Doplní účastník |
| Ostatní požadavky |  |  |
| NTP server | ano | Doplní účastník |
| DHCP server | ano | Doplní účastník |

## Softwarový nástroj pro správu a dohled prvků síťové infrastruktury (NMS)

|  |  |  |
| --- | --- | --- |
| Název požadavku | Popis požadavku | Míra splnění (ANO/NE) |
| Běh ve virtuálním prostředí | Servery systému musí podporovat možnost provozu ve virtuálním prostředí (VMware) | Doplní účastník |
| Běh nad OS | Minimálně Microsoft Windows Server | Doplní účastník |
| Běh nad DB | Minimálně MS SQL, MySQL | Doplní účastník |
| Správa a konfigurace síťových zařízení | Minimálně v rozsahu nabízeného řešení, tedy všech páteřních a přístupových přepínačů a dále s rezervou minimálně 50 licencí pro další síťová zařízení | Doplní účastník |
| Možnost správy zařízení třetích stran a přidávání vlastních zařízení | Ano, s využitím výše požadované licence pro 50 zařízení dle nabízeného řešení | Doplní účastník |
| Přístup do GUI pomocí protokolu HTTP/HTTPS bez nutnosti instalace klientského software na terminál | Ano | Doplní účastník |
| Možnost úpravy úvodní stránky (po přihlášení do systému) pro každého daného uživatele | Ano | Doplní účastník |
| Podporované southbound protokoly | Minimálně SNMP, Telnet/STelnet, FTP/SFTP/FTPS | Doplní účastník |
| Automatické hledání zařízení přidaných do sítě | Ano | Doplní účastník |
| Možnost notifikace pomocí emailu | Ano | Doplní účastník |
| Možnosti konsolidace a analýzy chybových hlášení pro maskování opakovaných událostí | Ano | Doplní účastník |
| Lokalizace chybových hlášení na topologické mapě | Ano | Doplní účastník |
| Analýza alarmů a zobrazení souvislosti mezi jednotlivými alarmy | Ano | Doplní účastník |
| Monitorování výkonosti zařízení včetně množnosti tvorby vlastních indikátorů pro zařízení třetích stran | Ano | Doplní účastník |
| Již zabudovaná podpora pro zařízení hlavních výrobců síťových technologií | Ano, minimálně Cisco, HPE, Huawei, Juniper a případně další | Doplní účastník |
| Možnost přidání zařízení dalších výrobců | Ano | Doplní účastník |
| Zobrazení topologie sítě | L2 i L3 | Doplní účastník |
| Hromadná konfigurace zařízení různých typů | Ano | Doplní účastník |
| Podpora analýzy SLA parametrů datových linek | Ano, možnost budoucího nasazení na bázi IP SLA, NQA nebo obdobné technologie | Doplní účastník |
| Možnost tvorby konfiguračních vzorů | Ano | Doplní účastník |
| Zobrazení stavu síťových zařízení | Ano | Doplní účastník |
| Zobrazení předního panelu zařízení. | Minimálně využité porty, stavy diod, stav zdrojů, ventilátorů | Doplní účastník |
| Hromadné aktualizace zařízení | Ano | Doplní účastník |
| Automatického zálohování konfigurace, porovnání konfigurace | Ano | Doplní účastník |
| Podpora automatické konfigurace nově přidaných zařízení | Ano | Doplní účastník |

## WLAN (Wi-Fi) přístupové body

|  |  |  |
| --- | --- | --- |
| Název požadavku | Popis požadavku | Míra splnění (ANO/NE) |
| Montáž | Zavěšení na strop  Součástí dodávky musí být montážní kit pro instalaci na strop | Doplní účastník |
| Kompatibilita | Kompatibilita s WLAN kontrolerem integrovaným v páteřních přepínačích | Doplní účastník |

Požadavek na funkcionalitu každého kusu

| Definice požadavku | Míra splnění (ANO/NE) |
| --- | --- |
| Podpora technologie IEEE 802.11a/b/g/n/ac | Doplní účastník |
| Implementace čipu 802.11ac Wave 2 | Doplní účastník |
| Podpora rychlosti až 2,53 Gbit/s na fyzické vrstvě Wi-Fi | Doplní účastník |
| Podpora kanálů o šířce pásma 20 MHz, 40 MHz, 80 MHz a 160 MHz | Doplní účastník |
| Interní všesměrová anténa pro 2,4 GHz a 5 GHz – provoz v obou pásmech současně | Doplní účastník |
| Zisk antény pro 2,4 GHz minimálně 6 dBi | Doplní účastník |
| Zisk antény pro 5 GHz minimálně 6 dBi | Doplní účastník |
| Napájení pomocí PoE+ – maximální spotřeba 25 W | Doplní účastník |
| Minimálně 256MB RAM a 32MB FLASH paměti pro vlastní SW image | Doplní účastník |
| Podpora krytí minimálně IP41 | Doplní účastník |
| Provozní tepoty od – 10 °C do +50 °C | Doplní účastník |
| Minimálně 2x 10/100/1000 Base-T rozhraní | Doplní účastník |
| Podpora technologie 4X4 MU MIMO | Doplní účastník |
| Podpora technologie 4X4 SU MIMO | Doplní účastník |
| Podpora technologie MRC, STBC, LDPC a MLD | Doplní účastník |
| Podpora technologie Beamforming | Doplní účastník |
| Podpora technologie 802.11k, 802.11r a 802.11v | Doplní účastník |
| Podpora technologie WMM (Wi-Fi Multimedia) | Doplní účastník |
| Podpora automatického přeladění kanálů | Doplní účastník |
| Podpora technologie MESH a WDS | Doplní účastník |
| Podpora oddělených sítí (SSID), minimálně 16 | Doplní účastník |
| AP bude Fungovat jako tenké AP, řízené centrálním přepínačem | Doplní účastník |
| Komunikace s centrálním řídícím prvek přes CAPWAP tunel | Doplní účastník |
| Možnost přepnout AP do tzv. FAT módu | Doplní účastník |
| Podpora technologie WEP, WPA, WPA2 | Doplní účastník |
| Podpora Wireless IPS a IDS systému | Doplní účastník |
| Podpora 802.1X, MAC autentizace a ověření pomocí portálu | Doplní účastník |
| Podpora DAI (Dynamic ARP inspecition), DHCP snooping, IP source guard | Doplní účastník |
| Podpora NAT a DHCP ve FAT režimu | Doplní účastník |
| Kompletní správa pomocí centrálního řídícího prvku – kompatibilní s AC WiFi kontrolerém v centrálním modulárním chassis | Doplní účastník |
| Podpora propojení s centrálním řídícím prvek přes L2 i L3 infrastrukturu | Doplní účastník |
| Podpora spektrální analýzy | Doplní účastník |
| Podpora lokalizace Wi-Fi zařízení | Doplní účastník |
| Podpora konfigurace přes CLI – SSH, Telnet a lokální konzole | Doplní účastník |
| Podpora technologie SNMPv1, v2c a v3 | Doplní účastník |
| Podpora technologie Dying Gasp | Doplní účastník |

# Zavedení síťové behaviorální analýzy

Monitorovací systém musí umožňovat dlouhodobé detailní monitorování veškerého provozu na počítačové síti. Získané statistiky o provozu datové sítě musí umožnit v reálném čase sledovat a vyhodnocovat objemy a strukturu provozu, analyzovat příčiny provozních nebo výkonnostních problémů a odhalovat bezpečnostní hrozby. Je nezbytné, aby monitorovací systém byl zcela nezávislý na použité síťové infrastruktuře a svou funkcí monitorovanou síť neovlivňoval. Ze strany sledované sítě nesmí být monitorovací systém detekovatelný.

Uložení a zpracování statistik musí být redundantní na k tomu určených specializovaných zařízeních – kolektorech. Ty musí být vybaveny SW či HW RAIDem. Kolektory musí poskytovat grafické uživatelské rozhraní a analytické nástroje pro práci se síťovými statistikami bez nutnosti instalovat jakýkoliv software na klientské stanice a dále pak poskytovat automatizované reporty i notifikace na nestandardní situace. Ukládání dat musí probíhat kontinuálně s dostupností bez jakékoliv ztrátové agregace po dobu několika měsíců. Samozřejmostí bude plná customizace způsobu prezentace dat a reportů na základě cílového prostředí.

Systém musí pracovat s technologií datových toků (NetFlow ve verzi 9/IPFIX/jFlow/NetStream/cflow). Tato technologie představuje nejmodernějším prostředek pro monitorování sítě při zpracování všech paketů bez vzorkování, imunitu vůči šifrovanému provozu, škálovatelnost i pro vysokorychlostní sítě.

Systém pro monitoring a vyhodnocování toků v síti se bude skládat z následujících částí:

* Kolektor s automatickým vyhodnocováním NetFlow/NetStream dat a detekcí anomálií;
* Dvě fyzické sondy pro sběr dat z prvků nepodporující export flow záznamů
* Systém na monitorování výkonu aplikací

## Kolektor s automatickým vyhodnocováním NetFlow/NetStream dat a detekcí anomálií

Kolektor bude splňovat minimálně následující parametry:

| Název požadavku | Popis požadavku | Míra splnění (ANO/NE) |
| --- | --- | --- |
| Ukládání flow statistik | Zabezpečené kolektory flow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce. | Doplní účastník |
| Granularita vizualizace | Kolektor umožní zpracování a vizualizaci flow záznamů volitelně v 5-minutových nebo 30-sekundových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu toků. | Doplní účastník |
| Podpora standardů datových toků | Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. | Doplní účastník |
| Hlavní funkcionalita | 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. | Doplní účastník |
| Instalace | Snadná instalace do stávající síťové infrastruktury – racková montáž, maximálně 2U | Doplní účastník |
| Management rozhraní | Dva plnohodnotné management (administrativní) porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat. | Doplní účastník |
| Zabezpečená vzdálená správa | Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. | Doplní účastník |
| Správa uživatelů a přístupových práv | Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele. | Doplní účastník |
| LDAP autentizace | Podpora autentizace vůči LDAP (Active Directory). | Doplní účastník |
| TACACS+ autentizace | Podpora autentizace vůči TACACS+. | Doplní účastník |
| Podpora HOT SWAP a RAID | Hardwarové kolektory jsou vybavené HOT SWAP disky a podporují RAID včetně SMART detekce. | Doplní účastník |
| Dohled | Kolektor je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP. | Doplní účastník |
| Časová synchronizace | Časová synchronizace zařízení proti centrálnímu zdroji času na síti. | Doplní účastník |
| Podpora příkazové řádky | Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky. | Doplní účastník |
| Sériová linka pro konfiguraci zařízení | Možnost přístupu a konfigurace hardwarových zařízení prostřednictvím sériové linky (RS-232). | Doplní účastník |
| DNS cache | Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. | Doplní účastník |
| Podpora Cisco AVC | Podpora standardu Cisco AVC vč. položek HTTP hostname a URL. | Doplní účastník |
| Podpora dalších flow standardů | Podpora pro Cisco NEL, Cisco NSEL, Cisco AVC, Cisco NBAR2. | Doplní účastník |
| Podpora položek proměnlivé délky | Podpora IPFIX položek proměnlivé délky. | Doplní účastník |
| Monitoring výkonu sítě | Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety. | Doplní účastník |
| Monitoring informací z aplikační vrstvy | Podpora pro protokoly HTTP, VoIP SIP, DNS, Samba/CIFS, DHCP | Doplní účastník |
| Monitorování rozšířených L3/L4 informací | Podpora pro monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících identifikaci NATů. | Doplní účastník |
| řeposílání flow vč. možnosti samplingu | Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti samplování na úrovni datových toků. | Doplní účastník |
| Spolehlivý a šifrovaný přenos IPFIX dat | Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS). | Doplní účastník |
| Automatická identifikace zdroje flow statistik | 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. | Doplní účastník |
| Zálohování a obnova flow statistik | Flow statistiky je možné automaticky zálohovat na externí síťové úložiště z důvodu dlouhodobé archivace. Zálohované statistiky lze v případě potřeby přímo obnovit uživatelem do kolektoru, kde je možné tyto statistiky analyzovat standardními prostředky. | Doplní účastník |
| Podpora pro uživatelské identity | 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. Řešení je otevřené a schopné podporovat libovolný zdroj uživatelských identit (hlášení o úspěšné autentizaci uživatele). | Doplní účastník |
| Uživatelské rozhraní | Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard (konfigurace per uživatel). | Doplní účastník |
| Vizualizace statistických dat | 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. | Doplní účastník |
| Analýza dat a ad hoc výstupy | Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV. | Doplní účastník |
| Reporting | 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. | Doplní účastník |
| Řízení uživatelského přístupu | Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem). | Doplní účastník |
| Top N statistiky | Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bytů, paketů, toků, nejvyšší hodnoty RTT, průmětné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu. | Doplní účastník |
| Filtrování a přizpůsobení výstupů | 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 zahrnovat do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace). | Doplní účastník |
| Uživatelsky definovatelné alerty | 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. | Doplní účastník |
| Uživatelsky definované pohledy na datový provoz | 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.). | Doplní účastník |
| Drill-down | Možnost dohledat každý jednotlivý datový tok (flow záznam). | Doplní účastník |
| Monitoring aktivních zařízení na sítí | Monitorování zařízení připojených k datové síti, dlouhodobá historie aktivních zařízení, identifikace na základě IP adresy, MAC adresy, sledování VLAN, operačního systému, přihlášeného uživatele na daném zařízení. | Doplní účastník |
| Automatická podpora geolokace | Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země). | Doplní účastník |
| Otevřené rozhraní | Kolektor poskytuje dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.). | Doplní účastník |
| Aplikace pro mobilní zařízení | Aplikace pro mobilní zařízení platformy Android a iOS, pro zobrazování základních informací v podobě grafů a statistik per jednotlivý uživatel. | Doplní účastník |
| Monitorování dostupnosti zdroje flow dat | Monitorování dostupnosti zdroje flow dat pomocí SNMP. | Doplní účastník |
| Minimální velikost interního datového úložiště | 12 TB čisté kapacity na HW RAID6 | Doplní účastník |
| Minimální velikost RAM paměti kolektoru | 128GB RAM | Doplní účastník |
| Minimální počet toků/s který je kolektor schopen zpracovat | 250.000 toků/s | Doplní účastník |

### Systém pro automatickou detekci anomálí

Systém pro automatické vyhodnocování a monitoring IP toků musí umožnit automatickou detekci bezpečnostních nebo provozních anomálií datové sítě a jejich hlášení formou událostí. Systém musí být založen na pokročilých metodách tzv. behaviorální analýzy a umožňovat tak odhalování hrozeb a incidentů, které překonají zabezpečení na perimetru nebo bezpečnostních ochranu koncových stanic, a pro které dosud není dostupná signatura. Jedná se tak o systém včasné detekce a reakce na bezpečností incidenty, který vhodným způsobem doplní stávající nástroje pro předcházení kybernetickým bezpečnostním incidentům. Detekované události bude možné dále analyzovat, vizualizovat nebo automaticky reportovat, případně integrovat s dohledovými systémy, incident handling systémy a systémy typu SIEM. Automatická detekce bezpečnostních incidentů, anomálií provozu sítě a konfiguračních problémů výrazně přispěje ke zjednodušení správy datové sítě, zvýšení její bezpečnosti a umožní proaktivní identifikaci příčin problémů.

Systém pro automatickou detekci musí být plně integrovatelný do prostředí kolektoru, tak aby mohl uživatel pracovat pouze s jedním GUI.

| Název požadavku | Popis požadavku | Míra splnění (ANO/NE) |
| --- | --- | --- |
| Podpora flow standardů | Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream. | Doplní účastník |
| Deduplikace | Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou. | Doplní účastník |
| Korelace před a za proxy | Systém umožňuje provést korelaci flow statistik před a za proxy serverem před jejich vlastní analýzou s cílem identifikovat provoz procházející proxy serverem a tento provoz přiřadit koncovému uživateli. | Doplní účastník |
| Vzorkování na úrovni toků | Systém podporuje vzorkování na úrovní toků před jejich vlastním zpracováním. | Doplní účastník |
| Identita uživatelů | Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události. | Doplní účastník |
| Persistence doménových jmen | Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události. | Doplní účastník |
| Detekční pravidla a algoritmy | Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií. | Doplní účastník |
| Detekce síťových útoků | Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby. | Doplní účastník |
| Detekce anomálií v síťovém provozu | Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace. | Doplní účastník |
| Detekce nežádoucích aplikací | Detekce P2P sítí, a anonymizačních služeb (např. TOR) | Doplní účastník |
| Detekce událostí na základě „Threat intelligence“ dat | Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery, apod.) využíváním zdrojů IP a host reputačních databází poskytovaných výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci. | Doplní účastník |
| Detekce provozních problémů | Detekce nadměrné zátěže sítě, výpadků služeb, chybějících reverzních DNS záznamů, nových a cizích zařízení připojených k síti. | Doplní účastník |
| Detekce síťových anomálií | Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace. | Doplní účastník |
| Konfigurační průvodce | Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen. | Doplní účastník |
| Konfigurace detekčních schopností | Jednotlivé detekční schopnosti je možné konfigurovat a parametrizovat tak, aby bylo dosaženo maximální efektivity a minimálního počtu falešných poplachů. Detekční mechanismy je možné konfigurovat různým způsobem (např. s různou citlivostí) pro statistiky z různých segmentů sítě (např. LAN nebo DMZ). | Doplní účastník |
| Detekce NATů | Detekce NATů v síti s využitím rozšířených informací z L3/L4. | Doplní účastník |
| Správa filtrů | Systém umožňuje definovat filtry vč. komplexních filtrů složených z dílčích filtrů. Pro zjednodušení definice filtrů je možné používat operace jako inverze nebo rozdíl filtrů. Filtry je možné exportovat do formátu CSV nebo z tohoto formátu importovat. | Doplní účastník |
| Správa falešných poplachů | Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní. | Doplní účastník |
| Definice závažnosti událostí | Předdefinované priority událostí s možností uživatelského nastavení závažnosti událostí na základě IP adresních rozsahů, typů událostí, míst výskytu nebo detailů události. Jedna událost může mít v závislosti na konfiguraci přiřazeno více priorit. | Doplní účastník |
| Agregace událostí | Detekované události je možné automaticky agregovat tak, aby související události byly prezentovány v rámci pojmenované hrozby (např. infikované zařízení v síti, chybně nakonfigurované zařízení, používání nevhodných aplikací nebo služeb apod.). | Doplní účastník |
| Správa uživatelů a přístupových práv | Správa uživatelů a přístupových práv k událostem prostřednictvím uživatelských rolí. Separace událostí s omezením přístupu pro jednotlivé role/uživatele. | Doplní účastník |
| CEF export | Události je možné automaticky exportovat ve formátu CEF protokolem Syslog. Předpokládané využití této funkcionality je integrace se systémy typu SIEM nebo log management. | Doplní účastník |
| SNMP Trap | Události je možné reportovat do dohledových systémů prostřednictvím funkcionality SNMP trap. | Doplní účastník |
| E-mailové notifikace | Notifikace o detekovaných událostech prostřednictvím e-mailu s podporou různých formátů (HTML, incident handling systém, úsporný textový formát). Možnost připojit vzorek flow dat, na základě kterých byla událost detekována k emailovému reportu. | Doplní účastník |
| Záchyt provozu v plném rozsahu | Na výskytu události je možné automaticky reagovat spuštěním záchytu provozu v plném rozsahu. | Doplní účastník |
| Spuštění skriptu | Na výskytu události je možné automaticky reagovat spuštěním uživatelsky definovaných skriptů. | Doplní účastník |
| Uživatelské rozhraní | Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard (konfigurace per uživatel). Vizualizace průběhu provozu s vyznačením detekovaných událostí v závislosti na nastavené závažnosti událostí. | Doplní účastník |
| Integrace informací z jiných služeb | Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. Uživatelsky definované externí služby fungující na protokolu HTTP. | Doplní účastník |
| Kategorie a komentáře | Události je možné přiřazovat do uživatelsky definovaných kategorií (např. vyřešeno, důležité, apod.). Událostem je možné přímo v systému pořizovat poznámky a komentáře. | Doplní účastník |
| Vyhledávání událostí | Systém nabízí flexibilní uživatelské rozhraní pro vyhledávání událostí dle různých parametrů (typ události, IP adrese původce události, filtr, přiřazení události do kategorie, ID události apod.). Události je možné prezentovat různým způsobem (prostý seznam, agregace dle zdrojů, dle cílů apod.). | Doplní účastník |
| Interaktivní vizualizace událostí | Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých byla událost rozpoznána. | Doplní účastník |
| Reporting | Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF. Automatická distribuce reportů e-mailem. | Doplní účastník |
| CSV export | Události je možné exportovat do formátu CSV pro další zpracování. | Doplní účastník |
| Otevřené rozhraní | Systém detekce anomálií poskytuje dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.). | Doplní účastník |
| Sledování změn konfigurace | Systém loguje veškeré změny konfigurace s cílem zajistit auditovatelnost činnosti uživatelů a provedené změny s dopadem detekci událostí. Změny konfigurace je možné rovněž odesílat protokolem syslog pro auditování formou externího systému typu SIEM nebo log management. | Doplní účastník |
| Formát systémů | Systém musí běžet na HW zařízení kolektoru, musí být dostupný přes jednotné WEB GUI kolektoru | Doplní účastník |
| Výkon systému | Systém musí být schopen vyhodnotit minimálně 2 tisíce toků za vteřinu | Doplní účastník |
| Počet zdrojů | Systém musí umět pracovat minimálně se dvěma nezávislými zdroji dat (Flow instance) | Doplní účastník |
| GUI systému | GUI musí být k dispozici v českém a anglickém jazyce | Doplní účastník |

## Fyzické sondy pro sběr dat

Dvě fyzické sondy budou splňovat minimálně následující parametry:

Zdroje NetFlow/IPFIX dat (sondy) jsou výkonná autonomní zařízení, která monitorují síťový provoz, vytváří o něm statistiky v podobě IP toků (NetFlow/IPFIX data) a zasílají tyto statistiky na kolektor pro uložení a další zpracování. NetFlow/IPFIX data obsahují informace o tom, kdo komunikoval s kým, jak dlouho, jakým protokolem, kolik přenesl dat a další informace ze síťové (L3) a transportní (L4) vrstvy OSI modelu. Sondy rovněž umožňují analýzu aplikační vrstvy (L7), identifikaci aplikací (NBAR2) a podrobný monitoring hlavních aplikačních protokolů (např. HTTP, DNS, DHCP). Mimo objemových charakteristik provozu poskytují sondy rovněž výkonové parametry datové sítě (např. RTT, SRT, jitter) pro analýzu zpoždění na síti. Díky tomu přináší sonda komplexní přehled a detailní informace o dění v síti a usnadňuje tak řešení síťových problémů, správu a optimalizaci sítě a zvyšuje její bezpečnost.

Sondy musí být nezávislé na použité síťové infrastruktuře a svou funkcí nijak neovlivňují sledovanou síť. K síti musí být připojeny pasivně prostřednictvím SPAN/mirroring portu. Ze strany monitorovacích rozhraní připojených do sledované sítě nesmí být zařízení detekovatelné.

Obecné požadavky na sondy:

| Název požadavku | Popis požadavku | Míra splnění (ANO/NE) |
| --- | --- | --- |
| Pasivní zapojení | Pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, případně v kombinaci se SPAN/mirror porty). | Doplní účastník |
| Instalace | Snadná instalace do stávající síťové infrastruktury – hardwarové zařízení, maximální velikost 1U | Doplní účastník |
| Zabezpečená vzdálená správa | Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS. | Doplní účastník |
| Správa uživatelů a přístupových práv | Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. | Doplní účastník |
| Dohled | Sondu je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP. | Doplní účastník |
| Časová synchronizace | Časová synchronizace zařízení proti centrálnímu zdroji času na síti. | Doplní účastník |
| Podpora příkazové řádky | Jednoduchá instalace a nastavení zařízení prostřednictvím GUI. Základní správa prostřednictvím příkazové řádky a GUI. | Doplní účastník |
| DNS cache | Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména. | Doplní účastník |
| LDAP autentizace | Podpora autentizace vůči LDAP (Active Directory). | Doplní účastník |
| Podpora protokolů pro výměnu dat | Programové vybavení sondy musí umožnit vytváření NetFlow dat ve formátech verzi 5 a 9, IPFIX. | Doplní účastník |
| Zpracování datového provozu | Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor. | Doplní účastník |
| Analýza tunelovaného provozu | Monitorování provozu v tunelu GRE. | Doplní účastník |
| Uživatelsky definované šablony | Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX. | Doplní účastník |
| Monitorování MAC adres | Monitorování a reportování MAC adres ve flow statistikách. Možnost použít MAC adresu jako položku klíče flow záznamu. | Doplní účastník |
| Detekce aplikací | Detekce aplikací dle standardu NBAR2. | Doplní účastník |
| Analýza zpoždění na síti | Reportování RTT, SRT, delay, jitter, retransmise, out-of-order pakety jako součást flow statistik. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | Doplní účastník |
| Monitorování a analýza HTTP provozu | Monitorování a analýza HTTP provozu - včetně položek typu URL, hostname. Pro HTTPS reportování hostname jako SNI. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | Doplní účastník |
| Profilování zařízení v síti | Identifikace operačního systému vč. jeho verze. Identifikace internetového prohlížeče vč. jeho verze. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | Doplní účastník |
| Monitorování VoIP | Monitorování VoIP statistik, protokol SIP – položky typu SIP URI, jitter, latence, ztrátovost paketů. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | Doplní účastník |
| Monitorování DNS provozu | Monitorování a analýza DNS provozu - položky jako typ dotazu, dotazovaná doména, návratová hodnota, odpověď. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | Doplní účastník |
| Monitorování Samba/CIFS provozu | Monitorování a analýza Samba/CISF provozu – položky typu síťová cesta, název souboru, typ operace. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | Doplní účastník |
| Monitorování DHCP provozu | Monitorování DHCP provozu – položky jako typ DHCP požadavku, originální MAC adresa. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX). | Doplní účastník |
| Nastavení času pro expiraci toků | Podpora pro nastavení časů u aktivní a neaktivní expirace toků. | Doplní účastník |
| Vzorkování | Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků. | Doplní účastník |
| Simultánní export NetFlow statistik | Podpora simultánního exportu flow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na sondě). Pro různé cíle exportu lze použít různé flow standardy (NetFlow v5, NetFlow v9, IPFIX). | Doplní účastník |
| Export na základě filtrování dat na sondě | Podpora filtrování dat na sondě na základě IP prefixů, VLAN, AS (pro různé cíle exportu různé statistiky). | Doplní účastník |
| Vyplňování identifikace AS | Podpora vyplňování AS na základě vestavěného či dodaného seznamu. | Doplní účastník |
| Vyplňování čísla interface | Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port. | Doplní účastník |
| Záchyt provozu v plném rozsahu | Sonda umožňuje rozšíření o funkcionalitu záznamu provozu v plném rozsahu na základě uživatelem definovaného pravidla záchytu. Rozšíření je řešeno formou licence/instalace SW bez nutnosti změny HW konfigurace. | Doplní účastník |
| Monitorování rozšířených L3/L4 informací | Monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů. | Doplní účastník |
| TACACS+ autentizace | Podpora autentizace vůči TACACS+. | Doplní účastník |
| GUI systému | GUI musí být k dispozici v českém a anglickém jazyce | Doplní účastník |

### Výkonnostní parametry sondy

| Název požadavku | Popis požadavku | Míra splnění (ANO/NE) |
| --- | --- | --- |
| Kapacita paměti současných toků | Minimální kapacita paměti současných toků na sondě 4 miliony toků na každý monitorovací port. | Doplní účastník |
| Monitorovací porty sond | Sonda obsahuje minimálně 1x 10GbE monitorovací porty - rozhraní SFP+  Součástí dodávky budou 1ks SFP+ T (RJ45) nebo 1ks SFP+ SR modulů | Doplní účastník |
| Výkon sondy na monitorovacích portech | Sonda je schopna zpracovávat více než 1,4Mp/s (pakety za sekundu) na každém portu | Doplní účastník |

## Systém na monitorování výkonu aplikací

Systém na monitorování výkonu aplikací (APM – aplication performace monitoring) poskytuje informace o skutečné odezvě aplikace z pohledu uživatele (tzv. user experience) a to pro všechny uživatele a všechny jejich uživatelské transakce v reálném čase. Systém umožňuje transparentně (bez vlivu na aplikaci a infrastrukturu) a bez instalace softwarových agentů monitorovat provoz aplikace, vyhodnocovat její výkon a reportovat/notifikovat o stavu aplikace. Monitoring probíhá na úrovni uživatel – aplikační server a aplikační server – databázový server. Hlavní metriky jsou doba odezvy a čas na transportní vrstvě, což umožňuje odlišit zpoždění dané zpracováním požadavku od zpoždění přenos dat na síti. Výkon aplikace je možné vyjádřit prostřednictvím ukazatele na bázi tzv. appdexu, vypočteného na základě uživatelsky definovaného SLA. Díky tomu je možné přesně identifikovat místa a příčiny problému a tím výrazně zrychlit čas potřebný k jejich nápravě a snížit náklady na správu aplikací.

|  |  |  |
| --- | --- | --- |
| Název požadavku | Popis požadavku | Míra splnění (ANO/NE) |
| Uživatelské rozhraní | Webové uživatelské rozhraní v českém jazyce. Vizualizuje stav aplikace pomocí indexu výkonu aplikace, počtu transakcí a dalších informací ve formě grafů a tabulek. Umožnuje analyzovat stav jednotlivých částí aplikace a transakcí. | Doplní účastník |
| Uživatelsky definovatelný dashboard | Uživatelsky definovatelný dashboard pro okamžitou vizualizaci stavu aplikace pomocí widgetů. Možnost přizpůsobení a vkládání vybraných widgetů uživatelem, např. index výkonu aplikace, 5 nejpomalejších transakcí, souhrnné informace a další statistiky vztažené k definovatelnému časovému intervalu (předcházejících x hodin/dnů). | Doplní účastník |
| Reporting odezvy aplikace | Systém reportuje pro definované aplikace a každou uživatelskou transakci realizovanou nad aplikací dobu odezvy aplikace a čas na transportní vrstvě. Díky tomu je možné odlišit zpoždění sítě od zpoždění aplikace. | Doplní účastník |
| Bez-agentní monitoring | Systém monitoruje aplikace bez nutnosti instalovat jakýkoliv SW na servery nebo klientské stanice. | Doplní účastník |
| Transparentní monitoring | Systém monitoruje aplikace bez jakéhokoliv vlivu na aplikaci nebo síťovou infrastrukturu. | Doplní účastník |
| Architektura systému | Systém je možné nasadit samostatně na jedné sondě, nebo na více sondách s centrální správou a webovým uživatelským rozhraním na kolektoru. | Doplní účastník |
| Monitoring na úrovni uživatel – aplikační server | Systém umožňuje monitorovat komunikaci mezi klienty aplikace a aplikační serverem na bázi protokolu HTTP a HTTPS. V případě použití protokolu HTTPS podporuje automatické dešifrování komunikace se znalostí privátního klíče pro šifrovací protokoly, které toto umožňují. | Doplní účastník |
| Monitoring na úrovni databází | Systém umožňuje monitorovat komunikaci mezi http serverem a databázovým serverem alespoň pro následující databáze – MSSQL, Oracel, PostgreSQL, MySQL/MariaDB | Doplní účastník |
| Definice SLA a index výkonu aplikace | Systém umožňuje pro každou aplikaci, resp. i její část definovat SLA pro dobu odezvy. Systém kontinuálně vyhodnocuje všechny transakce a stanovuje celkový index výkonu aplikace na základě plnění SLA. | Doplní účastník |
| Konfigurace aplikací | Systém nabízí flexibilní možnosti definice aplikace pro monitoring. Minimálně v rozsahu IP adresy, porty, host, URL vč. regulárních výrazů pro jejich definici. | Doplní účastník |
| Skupiny | Systém umožňuje definovat skupiny pro sledování metrik pouze pro zvolenou podmnožinu transakcí (např. skupina pro PHP soubory, multimediální soubory, část klientů a uživatelů). | Doplní účastník |
| Reporting | Systém umožňuje vytvářet reporty dostupné prostřednictvím webového GUI, ve formátu PDF. Reporty je možné automaticky odesílat e-mailem. | Doplní účastník |
| Notifikace | Jako reakci na snížení indexu výkonu aplikace, případně další metriky umožňuje systém odeslat e-mail, syslog zprávu, SNMP trap, nebo spustit skript. | Doplní účastník |
| Detaily HTTP transakcí | Pro každou transakci jsou dostupné detaily minimálně v rozsahu URL, parametry, user agenty, objem přenesených dat, návratová hodnota, cookie. | Doplní účastník |
| Filtrace agregovaných transakcí | Systém umožňuje filtrovat nad seznamem agregovaných transakcí pomocí kritérií (např. APM, index, počet chyb, celkový objem přenesených dat a další). Díky tomu lze získat informace o tom, jaké části aplikace jsou nejpomalejší, vykazují nejvíce chyb, atd. | Doplní účastník |
| Filtrace jednotlivých transakcí | Systém umožňuje filtrovat nad seznamem jednotlivých transakcí pomocí různých kritérií (např. IP adresa uživatele, doba odezvy, SLA, uživatelské jméno, začátek a konec transakce a další). Díky tomu lze získat informace o tom, jaká skupina uživatelů komunikovala s aplikací, jaká byla odezva aplikace, pro jaké uživatele a transakce byla aplikace nedostupná, atd. | Doplní účastník |
| CSV export | Systém umožňuje exportovat informace o transakcích ve formátu CSV. | Doplní účastník |
| Odvozené metriky | Systém sleduje další odvozené metriky jako je průměr, medián, 99‑percentil a 95-percentil doby odezvy aplikace, zobrazuje přehled nejpomalejších transakcí, počet uživatelů souběžně pracujících s aplikací, počet transakcí dle splnění SLA, struktura chybových kódů. | Doplní účastník |
| Výkonnost systému | Systém musí umět zpracovat minimálně 5000 transakcí za minutu | Doplní účastník |
| Zdroje dat | Systém musí umět pracovat z daty z minimálně čtyř nezávislých zdrojů (sond) | Doplní účastník |
| GUI systému | GUI musí být k dispozici v českém a anglickém jazyce | Doplní účastník |

# Definice rozsahu nasazení

Systém, jako funkční celek, bude nasazen v následujícím rozsahu:

### L2 monitoring sítě a ověřování bezpečného přístupu do sítě (DDI / NAC / DNS / DHCP / IPAM)

Systém podporující redundanci a distribuovanost služeb L2 monitoringu sítě a ověřování bezpečného přístupu do sítě (DDI / NAC / DNS / DHCP / IPAM) pro centrální lokalitu Výrobní závod I a vzdálené lokality Výrobní závod II a Výrobní závod III. Systém bude celkem obsluhovat 1 000 IP adres.

Detailní počty jsou uvedeny v následující tabulce:

|  |  |
| --- | --- |
| Počet centrálních lokalit | 1 |
| Počet vzdálených lokalit | 2 |
| Celkový počet IP adres na síti | 1 000 |

### Obměna prvků síťové infrastruktury

Nabízené řešení musí reflektovat požadavky na instalaci a implementaci v prostředí sítě zadavatele, které vyplývají z následujícího blokového schématu:



Obrázek 1: Schéma síťové infrastruktury

Součástí musí být:

* Softwarový nástroj pro správu a dohled prvků síťové infrastruktury (NMS);
* WLAN (Wi-Fi) přístupové body;
* Všechny potřebné propojovací/patch a napájecí kabely, minimálně dle následující tabulky.

Detailní počty jsou uvedeny v následující tabulce:

|  |  |
| --- | --- |
| Počet páteřních přepínačů | 2 ks |
| Počet přepínačů 48-port s POE+ | 21 ks |
| Počet přepínačů 24-port s POE+ | 19 ks |
| Počet přepínačů 48-port nonPOE | 5 ks |
| Počet přepínačů 24-port nonPOE | 9 ks |
| Počet DC (TOR) přístupových přepínačů | 4 ks |
| Softwarový nástroj pro správu a dohled prvků síťové infrastruktury (NMS) | 1 ks |
| Počet WLAN (Wi-Fi) přístupových bodů | 30 ks |
| Optický patch kabel LC-SC Singlemode 9/125 2m duplex | 80 ks |
| Optický patch kabel LC-SC Singlemode 9/125 5m duplex | 80 ks |
| Optický patch kabel LC-SC Multimode 50/125 OM4 2m duplex | 40 ks |
| Optický patch kabel LC-SC Multimode 50/125 OM4 5m duplex | 40 ks |

### Systém pro monitoring a vyhodnocování toků v síti

Systém (kolektor a sondy) bude nasazen centrálně na úrovni dvou datových center v rámci objektu VZI.

Detailní počty jsou uvedeny v následující tabulce:

|  |  |
| --- | --- |
| Kolektor s automatickým vyhodnocováním NetFlow/NetStream dat a detekcí anomálií | 1 ks |
| Fyzická sonda pro sběr dat z prvků nepodporující export flow záznamů | 2 ks |
| Systém na monitorování výkonu aplikací | 1 ks |

# Specifikace nabízeného řešení

### L2 monitoring sítě a ověřování bezpečného přístupu do sítě (DDI / NAC / DNS / DHCP / IPAM)

|  |
| --- |
| Specifikace nabízeného řešení L2 monitoringu sítě a ověřování bezpečného přístupu do sítě  (výrobce, model, typ, PN) |
| Doplní účastník |

### Obměna prvků síťové infrastruktury

|  |
| --- |
| Specifikace páteřních přepínačů (výrobce, model, typ, PN) |
| Doplní účastník |
| Specifikace přepínačů 48-port s POE+ (výrobce, model, typ, PN) |
| Doplní účastník |
| Specifikace přepínačů 24-port s POE+ (výrobce, model, typ, PN) |
| Doplní účastník |
| Specifikace přepínačů 48-port nonPOE (výrobce, model, typ, PN) |
| Doplní účastník |
| Specifikace přepínačů 24-port nonPOE (výrobce, model, typ, PN) |
| Doplní účastník |
| Specifikace DC (TOR) přístupových přepínačů (výrobce, model, typ, PN) |
| Doplní účastník |
| Softwarový nástroj pro správu a dohled prvků síťové infrastruktury (NMS) (výrobce, model, typ, PN) |
| Doplní účastník |
| Specifikace WLAN (Wi-Fi) přístupových bodů (výrobce, model, typ, PN) |
| Doplní účastník |

### Systém pro monitoring a vyhodnocování toků v síti

|  |
| --- |
| Kolektor s automatickým vyhodnocováním NetFlow/NetStream dat a detekcí anomálií (výrobce, model, typ, PN) |
| Doplní účastník |
| Fyzická sonda pro sběr dat z prvků nepodporující export flow záznamů (výrobce, model, typ, PN) |
| Doplní účastník |
| Systém na monitorování výkonu aplikací (výrobce, model, typ, PN) |
| Doplní účastník |