*Příloha č. 5 – Popis předmětu plnění*

|  |
| --- |
| **POPIS PŘEDMĚTU PLNĚNÍ** |

**Tabulky mandatorních požadavků pro přepínače a bezdrátové přístupové body:**

|  |  |  |
| --- | --- | --- |
| **Bezdrátový přístupový bod typ 1a** | | |
| Výrobce zařízení | Uvedení výrobce |  |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla |  |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | Uvedení požadovaného odkazu |  |
| **Požadavek na funkcionalitu** | **Min. požadavky** | **Splňuje**  **ANO/NE** |
| ***Základní vlastnosti:*** | | |
| Access Point určený pro instalaci na strop/podhled | Podporuje |  |
| Typ antén | Integrované pro všechna pásma |  |
| Tři rádia pracující v režimu 2.4 + 5 + 6 GHz pro standardní prostředí nebo dvě rádia v režimu 5 Ghz + 2.4 GHz pro specifická nasazení, možnost statické i dynamické volby režimu | Podporuje |  |
| Samostatné rádio pro monitorování 2.4, 5 a 6 GHz RF spektra – detailní spektrální analýza s hardwarovou podporou, detekce útoků na bezdrátovou sít, detekce zdroje rušivého signálu, lokalizace klientů | Podporuje |  |
| Podpora standardů 802.11a/b/g/n/ac/ax/be | Podporuje |  |
| Podpora minimálně 2x2 pro 2.4, 5 a 6 GHz | Podporuje |  |
| Podpora MIMO, MU-MIMO, UL/DL OFDMA, TWT, BSS Coloring, MLO, Preamble puncturing, 4096 QAM a až 320 MHz kanál pro 802.11be | Podporuje |  |
| Minimální počet inzerovaných SSID (BSSID) per radio | 8 |  |
| Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 n/ac/ax klientům (Tx Beam Forming) | Podporuje |  |
| Podpora mechanismu pro přepojení klientů z 2.4GHz do 5GHz pásma | Podporuje |  |
| Podpora mechanismu pro přepojení klientů z 2.4GHz a 5GHz do 6GHz pásma | Podporuje |  |
| Access Pointy obsahují X.509 certifikát s lokální platností pro nasazeni PKI | Podporuje |  |
| Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x supplikant | Podporuje |  |
| Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark) | Podporuje |  |
| Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí Telnet a SSH | Podporuje |  |
| Podpora rozpoznání zdroje rušivého signálu podle signatur 2.4, 5 a 6 GHz | Podporuje |  |
| AP uzavřené konstrukce bez větracích otvorů a ventilátoru | Podporuje |  |
| Součástí AP je plechový úchyt pro instalaci na strop nebo stěnu | Podporuje |  |
| AP je fyzicky zabezpečitelné/zamknutelné k okolním pevným částem. | Podporuje |  |
| Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanismy pro ochranu SW a HW proti útokům | Podporuje |  |

|  |  |  |
| --- | --- | --- |
| **Bezdrátový přístupový bod typ 1b** | | |
| Výrobce zařízení | Uvedení výrobce |  |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla |  |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | Uvedení požadovaného odkazu |  |
| **Požadavek na funkcionalitu** | **Min. požadavky** | **Splňuje**  **ANO/NE** |
| ***Základní vlastnosti:*** | | |
| Access Point určený pro instalaci na strop/podhled | Podporuje |  |
| Typ antén | Integrované pro všechna pásma |  |
| Tři rádia pracující v režimu 2.4 + 5 + 6 GHz pro standardní prostředí nebo dvě rádia v režimu 6 Ghz + duální 5 GHz pro HD nasazení, možnost statické i dynamické volby režimu | Podporuje |  |
| Samostatné rádio pro monitorování 2.4, 5 a 6 GHz RF spektra – detailní spektrální analýza s hardwarovou podporou, detekce útoků na bezdrátovou sít, detekce zdroje rušivého signálu, lokalizace klientů | Podporuje |  |
| Podpora standardů 802.11a/b/g/n/ac/ax/be | Podporuje |  |
| Podpora minimálně 4x4 pro 2.4, 5 a 6 GHz | Podporuje |  |
| Podpora MIMO, MU-MIMO, UL/DL OFDMA, TWT, BSS Coloring, MLO, Preamble puncturing, 4096 QAM a až 320 MHz kanál pro 802.11be | Podporuje |  |
| Minimální počet inzerovaných SSID (BSSID) per radio | 8 |  |
| Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 n/ac/ax klientům (Tx Beam Forming) | Podporuje |  |
| Podpora mechanismu pro přepojení klientů z 2.4GHz do 5GHz pásma | Podporuje |  |
| Podpora mechanismu pro přepojení klientů z 2.4GHz a 5GHz do 6GHz pásma | Podporuje |  |
| Access Pointy obsahují X.509 certifikát s lokální platností pro nasazeni PKI | Podporuje |  |
| Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x supplikant | Podporuje |  |
| Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark) | Podporuje |  |
| Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí Telnet a SSH | Podporuje |  |
| Podpora rozpoznání zdroje rušivého signálu podle signatur 2.4, 5 a 6 GHz | Podporuje |  |
| Access Point obsahuje rádio podporující BLE 5.3 a USB 2.0 port s podporou napájení minimálně 9W | Podporuje |  |
| Integrovaný přijímač GNSS/GPS s možností připojení externí antény | Podporuje |  |
| Access Point podporuje kontejnerové prostředí pro běh aplikací | Podporuje |  |
| Integrované rádio pro podporu Ultra Wide Band (UWB) | Podporuje |  |
| 1 x 100/1000/2500/5000/10000 Mbit/s RJ45 ethernet rozhraní kompatibilní s 802.3bz | Podporuje |  |
| Možnost 802.3af/at/bt PoE napájení AP z přepínače nebo injectoru. Plná funkce všech rádií AP při použití 802.3bt, tj. 4x4 + 4x4 + 4x4 MIMO bez sníženého vysílacího výkonu libovolného rádia | Podporuje |  |
| Podpora úsporného režimu AP | Podporuje |  |
| AP uzavřené konstrukce bez větracích otvorů a ventilátoru | Podporuje |  |
| Součástí AP je plechový úchyt pro instalaci na strop nebo stěnu | Podporuje |  |
| AP je fyzicky zabezpečitelné/zamknutelné k okolním pevným částem. | Podporuje |  |
| Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanismy pro ochranu SW a HW proti útokům | Podporuje |  |

|  |  |  |
| --- | --- | --- |
| **Bezdrátový přístupový bod typ 1c** | | |
| Výrobce zařízení | Uvedení výrobce |  |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla |  |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | Uvedení požadovaného odkazu |  |
| **Požadavek na funkcionalitu** | **Min. požadavky** | **Splňuje**  **ANO/NE** |
| ***Základní vlastnosti:*** | | |
| Access Point určený pro instalaci na strop/podhled | Podporuje |  |
| Typ antén | Integrované pro všechna pásma |  |
| Tři rádia pracující v režimu 2.4 + 5 + 6 GHz pro standardní prostředí nebo dvě rádia v režimu 5 Ghz + 2.4 GHz pro specifická nasazení, možnost statické i dynamické volby režimu | Podporuje |  |
| Samostatné rádio pro monitorování 2.4, 5 a 6 GHz RF spektra – detailní spektrální analýza, detekce útoků na bezdrátovou sít, lokalizace klientů | Podporuje |  |
| Podpora standardů 802.11a/b/g/n/ac/ax a Wi-Fi6E | Podporuje |  |
| Podpora minimálně 4x4 pro 2.4, 5 a 6 GHz | Podporuje |  |
| Podpora MIMO, MU-MIMO, UL/DL OFDMA, TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax | Podporuje |  |
| Minimální počet inzerovaných SSID (BSSID) per radio | 16 |  |
| Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11 n/ac/ax klientům (Tx Beam Forming) | Podporuje |  |
| Podpora mechanismu pro přepojení klientů z 2.4GHz do 5GHz pásma | Podporuje |  |
| Podpora mechanismu pro přepojení klientů z 2.4GHz a 5GHz do 6GHz pásma | Podporuje |  |
| Access Pointy obsahují X.509 certifikát s lokální platností pro nasazeni PKI | Podporuje |  |
| Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x supplikant | Podporuje |  |
| Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark) | Podporuje |  |
| Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí Telnet a SSH | Podporuje |  |
| Hardwarová podpora spektrální analýzy s podporou 160 MHz kanálů (detekce zdroje rušivého signálu – interference) pro 2.4, 5 a 6 GHz | Podporuje |  |
| Podpora rozpoznání zdroje rušivého signálu podle signatur 2.4, 5 a 6 GHz | Podporuje |  |
| Access Point obsahuje radio podporující BLE 5.1 a USB 2.0 port s podporou napájení minimálně 4.5W | Podporuje |  |
| Access Point podporuje kontejnerové prostředí pro běh aplikací | Podporuje |  |
| Integrované senzory pro měření teploty, vlhkosti a kvality vzduchu | Podporuje |  |
| 1 x 100/1000/2500/5000 Mbit/s RJ45 ethernet rozhraní kompatibilní s 802.3bz | Podporuje |  |
| Možnost 802.3af/at/bt PoE napájení AP z přepínače nebo injectoru. Plná funkce třech rádií AP i při použití 802.3at, tj. 4x4 + 4x4 + 4x4 MIMO bez sníženého vysílacího výkonu | Podporuje |  |
| Možnost napájení z DC zdroje | Podporuje |  |
| AP uzavřené konstrukce bez větracích otvorů a ventilátoru | Podporuje |  |
| Součástí AP je plechový úchyt pro instalaci na strop nebo stěnu | Podporuje |  |
| AP je fyzicky zabezpečitelné/zamknutelné k okolním pevným částem. | Podporuje |  |
| Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanismy pro ochranu SW a HW proti útokům | Podporuje |  |

|  |  |  |
| --- | --- | --- |
| **Přepínač typ 2a** |  |  |
| Výrobce zařízení | Uvedení výrobce |  |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla |  |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | Uvedení požadovaného odkazu |  |
| **Požadavek na funkcionalitu** | **Min. požadavky** | **Splňuje ANO/NE** |
| ***Základní vlastnosti:*** | | |
| Typ přepínače | L2/L3 přepínač |  |
| Formát přepínače | Stohovatelný, 1RU |  |
| Počet dedikovaných stohovacích portů volitelného stohovacího modulu | 2 |  |
| Minimální počet zařízení ve stohu | 8 |  |
| Minimální kapacita sběrnice stohu | 80 Gb/s |  |
| Stateful Switch Over v rámci stohu | Podporuje |  |
| Možnost instalovat interní redundantní napájecí zdroj | Podporuje |  |
| Redundantní ventilátory | Podporuje |  |
| Interní redundantní napájecí zdroj požadován | Podporuje |  |
| Min. PoE budget | 700 W |  |
| Datový stohovací kabel požadován 1m | Podporuje |  |
| Počet portů mGig až 10G s 802.3at PoE napájením | 8 |  |
| Počet portů 10/100/1000 Base-TX s 802.3at PoE napájením | 40 |  |
| Uplink porty | 2x25GE SFP28 |  |
| Min. velikost sdíleného systémového bufferu | 6MB |  |
| Velikost MAC address tabulky | 16000 |  |
| Min. počet IPv4 routes | 600 |  |
| Min. počet IPv6 routes | 300 |  |
| Min. počet konfigurovatelných security ACL | 1000 |  |
| IEEE 802.3ad (Link Aggregation) | Podporuje |  |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | Podporuje |  |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | Podporuje |  |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 48 |  |
| IEEE 802.1q | Podporuje |  |
| Minimální počet aktivních VLAN | 1000 |  |
| IEEE 802.1x – Port Based Network Access Control | Podporuje |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | Podporuje |  |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | Podporuje |  |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | Podporuje |  |
| RADIUS CoA | Podporuje |  |
| Per VLAN Rapid Spanning Tree (PVRST+) nebo ekvivalentní | Podporuje |  |
| IEEE 802.1w - Rapid Spanning Tree Protocol | Podporuje |  |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | Podporuje |  |
| Podpora jumbo rámců (min. 9198 bytes) | Podporuje |  |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | Podporuje |  |
| Směrování protokolů IPv4 a IPv6 v hardware | Podporuje |  |
| OSPFv2 | Podporuje |  |
| OSPFv3 | Podporuje |  |
| Flexible network segmentation (VRF, BGP-EVPN s VXLAN) | Podporuje, povýšením firmware |  |
| ISIS | Podporuje, povýšením firmware |  |
| IP Multicast (PIM SSM, PIM SM) | Podporuje, povýšením firmware |  |
| Reverse path check (uRPF) pro IPv4 i IPv6 | Podporuje |  |
| IGMPv2, IGMPv3 | Podporuje |  |
| IGMP snooping | Podporuje |  |
| MLD snooping | Podporuje |  |
| DHCP relay | Podporuje |  |
| Minimální počet HW QoS front | 8 |  |
| QoS classification – ACL, DSCP, CoS based | Podporuje |  |
| QoS marking - DSCP, CoS | Podporuje |  |
| QoS - Strict Priority Queue | Podporuje |  |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | Podporuje |  |
| QoS Policing | Podporuje |  |
| QoS-Hierarchical QoS | Podporuje, min. 2 úrovně |  |
| First Hop Redundancy Protokol pro IPv4 i IPv6 (HSRP nebo VRRP) | Podporuje |  |
| IPv6 services (Telnet, SSH, Syslog, DHCP) | Podporuje |  |
| IPv6 QoS | Podporuje |  |
| ***Bezpečnost:*** | | |
| IPv6 Port ACL, VLAN ACL | Podporuje |  |
| IPv6 First Hop Security (RA guard, DHCPv6 Snooping, IPv6 Source Guard) | Podporuje |  |
| Možnost definovat povolené MAC adresy na portu | Podporuje |  |
| PACL, VACL | Podporuje |  |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | Podporuje, povýšením firmware |  |
| IEEE 802.1ae na uplink portech | Podporuje |  |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | Podporuje |  |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | Podporuje |  |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | Podporuje |  |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot | Podporuje |  |
| HW trusted modul pro bezpečné uložení hesel a šifrovacích klíčů | Podporuje |  |
| Podpora SUDI (IEEE 802.1ar) autentizace | Podporuje |  |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | Podporuje |  |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | Podporuje |  |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type | Podporuje |  |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | Podporuje |  |
| ***Management:*** | | |
| SSHv2 | Podporuje |  |
| CLI rozhraní | Podporuje |  |
| Vzdálená identifikace zařízení pomocí dálkově řízené LED | Podporuje |  |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | Podporuje |  |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | Podporuje |  |
| Streaming telemetrie prostřednictvím NETCONF/XML | Podporuje |  |
| SNMPv2/v3 | Podporuje |  |
| Podpora network boot (iPXE) přes IPv4 i IPv6 | Podporuje |  |
| Integrovaná RFID identifikace | Podporuje |  |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | Podporuje |  |
| NTPv3 server | Podporuje |  |

|  |  |  |
| --- | --- | --- |
| **Přepínač typ 2b** |  |  |
| Výrobce zařízení | Uvedení výrobce |  |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla |  |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | Uvedení požadovaného odkazu |  |
| **Požadavek na funkcionalitu** | **Min. požadavky** | **Splňuje ANO/NE** |
| ***Základní vlastnosti:*** | | |
| Typ přepínače | L2/L3 přepínač |  |
| Formát přepínače | Stohovatelný, 1RU |  |
| Počet dedikovaných stohovacích portů volitelného stohovacího modulu | 2 |  |
| Minimální počet zařízení ve stohu | 8 |  |
| Minimální kapacita sběrnice stohu | 80 Gb/s |  |
| Stateful Switch Over v rámci stohu | Podporuje |  |
| Možnost instalovat interní redundantní napájecí zdroj | Podporuje |  |
| Redundantní ventilátory | Podporuje |  |
| Interní redundantní napájecí zdroj požadován | Podporuje |  |
| Min. PoE budget | 700 W |  |
| Datový stohovací kabel požadován 1m | Podporuje |  |
| Počet portů 10/100/1000 Base-TX s 802.3at PoE napájením | 48 |  |
| Uplink porty | 4x10GE SFP+ |  |
| Min. velikost sdíleného systémového bufferu | 6MB |  |
| Velikost MAC address tabulky | 16000 |  |
| Min. počet IPv4 routes | 600 |  |
| Min. počet IPv6 routes | 300 |  |
| Min. počet konfigurovatelných security ACL | 1000 |  |
| IEEE 802.3ad (Link Aggregation) | Podporuje |  |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | Podporuje |  |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | Podporuje |  |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 48 |  |
| IEEE 802.1q | Podporuje |  |
| Minimální počet aktivních VLAN | 1000 |  |
| IEEE 802.1x – Port Based Network Access Control | Podporuje |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | Podporuje |  |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | Podporuje |  |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | Podporuje |  |
| RADIUS CoA | Podporuje |  |
| Per VLAN Rapid Spanning Tree (PVRST+) nebo ekvivalentní | Podporuje |  |
| IEEE 802.1w - Rapid Spanning Tree Protocol | Podporuje |  |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | Podporuje |  |
| Podpora jumbo rámců (min. 9198 bytes) | Podporuje |  |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | Podporuje |  |
| Směrování protokolů IPv4 a IPv6 v hardware | Podporuje |  |
| OSPFv2 | Podporuje |  |
| OSPFv3 | Podporuje |  |
| Flexible network segmentation (VRF, BGP-EVPN s VXLAN) | Podporuje, povýšením firmware |  |
| ISIS | Podporuje, povýšením firmware |  |
| IP Multicast (PIM SSM, PIM SM) | Podporuje, povýšením firmware |  |
| Reverse path check (uRPF) pro IPv4 i IPv6 | Podporuje |  |
| IGMPv2, IGMPv3 | Podporuje |  |
| IGMP snooping | Podporuje |  |
| MLD snooping | Podporuje |  |
| DHCP relay | Podporuje |  |
| Minimální počet HW QoS front | 8 |  |
| QoS classification – ACL, DSCP, CoS based | Podporuje |  |
| QoS marking - DSCP, CoS | Podporuje |  |
| QoS - Strict Priority Queue | Podporuje |  |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | Podporuje |  |
| QoS Policing | Podporuje |  |
| QoS-Hierarchical QoS | Podporuje, min. 2 úrovně |  |
| First Hop Redundancy Protokol pro IPv4 i IPv6 (HSRP nebo VRRP) | Podporuje |  |
| IPv6 services (Telnet, SSH, Syslog, DHCP) | Podporuje |  |
| IPv6 QoS | Podporuje |  |
| ***Bezpečnost:*** | | |
| IPv6 Port ACL, VLAN ACL | Podporuje |  |
| IPv6 First Hop Security (RA guard, DHCPv6 Snooping, IPv6 Source Guard) | Podporuje |  |
| Možnost definovat povolené MAC adresy na portu | Podporuje |  |
| PACL, VACL | Podporuje |  |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | Podporuje, povýšením firmware |  |
| IEEE 802.1ae na uplink portech | Podporuje |  |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | Podporuje |  |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | Podporuje |  |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | Podporuje |  |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot | Podporuje |  |
| HW trusted modul pro bezpečné uložení hesel a šifrovacích klíčů | Podporuje |  |
| Podpora SUDI (IEEE 802.1ar) autentizace | Podporuje |  |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | Podporuje |  |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | Podporuje |  |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type | Podporuje |  |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | Podporuje |  |
| ***Management:*** | | |
| SSHv2 | Podporuje |  |
| CLI rozhraní | Podporuje |  |
| Vzdálená identifikace zařízení pomocí dálkově řízené LED | Podporuje |  |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | Podporuje |  |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | Podporuje |  |
| Streaming telemetrie prostřednictvím NETCONF/XML | Podporuje |  |
| SNMPv3 | Podporuje |  |
| Podpora network boot (iPXE) přes IPv4 i IPv6 | Podporuje |  |
| Integrovaná RFID identifikace | Podporuje |  |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | Podporuje |  |
| NTPv3 server | Podporuje |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Přepínač typ 2c** |  | |  |
| Výrobce zařízení | Uvedení výrobce | |  |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla | |  |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | Uvedení požadovaného odkazu | |  |
| **Požadavek na funkcionalitu** | **Min. požadavky** | | **Splňuje ANO/NE** |
| ***Základní vlastnosti:*** | | | |
| Typ přepínače | L2/L3 přepínač | |  |
| Formát přepínače | Stohovatelný, 1RU | |  |
| Počet dedikovaných stohovacích portů volitelného stohovacího modulu | 2 | |  |
| Minimální počet zařízení ve stohu | 8 | |  |
| Minimální kapacita sběrnice stohu | 80 Gb/s | |  |
| Stateful Switch Over v rámci stohu | Podporuje | |  |
| Možnost instalovat interní redundantní napájecí zdroj | Podporuje | |  |
| Redundantní ventilátory | Podporuje | |  |
| Datový stohovací kabel požadován 1m | Podporuje | |  |
| Počet portů 10/100/1000 Base-TX | 48 | |  |
| Uplink porty | 4x1GE SFP | |  |
| Min. velikost sdíleného systémového bufferu | 6MB | |  |
| Velikost MAC address tabulky | 16000 | |  |
| Min. počet IPv4 routes | 2000 | |  |
| Min. počet IPv6 routes | 1000 | |  |
| Min. počet konfigurovatelných security ACL | 1000 | |  |
| IEEE 802.3ad (Link Aggregation) | Podporuje | |  |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | Podporuje | |  |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | Podporuje | |  |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 48 | |  |
| IEEE 802.1q | Podporuje | |  |
| Minimální počet aktivních VLAN | 1000 | |  |
| IEEE 802.1x – Port Based Network Access Control | Podporuje | |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | Podporuje | |  |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | Podporuje | |  |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | Podporuje | |  |
| RADIUS CoA | Podporuje | |  |
| Per VLAN Rapid Spanning Tree (PVRST+) nebo ekvivalentní | Podporuje | |  |
| IEEE 802.1w - Rapid Spanning Tree Protocol | Podporuje | |  |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | Podporuje | |  |
| Podpora jumbo rámců (min. 9198 bytes) | Podporuje | |  |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | Podporuje | |  |
| Směrování protokolů IPv4 a IPv6 v hardware | Podporuje | |  |
| OSPFv2 | Podporuje | |  |
| OSPFv3 | Podporuje | |  |
| Flexible network segmentation (VRF, BGP-EVPN s VXLAN) | Podporuje, povýšením firmware | |  |
| ISIS | Podporuje, povýšením firmware | |  |
| IP Multicast (PIM SSM, PIM SM) | Podporuje, povýšením firmware | |  |
| Reverse path check (uRPF) pro IPv4 i IPv6 | Podporuje | |  |
| IGMPv2, IGMPv3 | Podporuje | |  |
| IGMP snooping | Podporuje | |  |
| MLD snooping | Podporuje | |  |
| DHCP relay | Podporuje | |  |
| Minimální počet HW QoS front | 8 | |  |
| QoS classification – ACL, DSCP, CoS based | Podporuje | |  |
| QoS marking - DSCP, CoS | Podporuje | |  |
| QoS - Strict Priority Queue | Podporuje | |  |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | Podporuje | |  |
| QoS Policing | Podporuje | |  |
| QoS-Hierarchical QoS | Podporuje, min. 2 úrovně | |  |
| First Hop Redundancy Protokol pro IPv4 i IPv6 (HSRP nebo VRRP) | Podporuje | |  |
| IPv6 services (Telnet, SSH, Syslog, DHCP) | Podporuje | |  |
| IPv6 QoS | Podporuje | |  |
| ***Bezpečnost:*** | | | |
| IPv6 Port ACL, VLAN ACL | Podporuje | |  |
| IPv6 First Hop Security (RA guard, DHCPv6 Snooping, IPv6 Source Guard) | Podporuje | |  |
| Možnost definovat povolené MAC adresy na portu | Podporuje | |  |
| PACL, VACL | Podporuje | |  |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | Podporuje, povýšením firmware | |  |
| IEEE 802.1ae na uplink portech | Podporuje | |  |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | Podporuje |  | |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | Podporuje |  | |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | Podporuje |  | |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot | Podporuje |  | |
| HW trusted modul pro bezpečné uložení hesel a šifrovacích klíčů | Podporuje |  | |
| Podpora SUDI (IEEE 802.1ar) autentizace | Podporuje |  | |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | Podporuje |  | |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | Podporuje |  | |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type | Podporuje |  | |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | Podporuje |  | |
| ***Management:*** | | | |
| SSHv2 | Podporuje |  | |
| CLI rozhraní | Podporuje |  | |
| Vzdálená identifikace zařízení pomocí dálkově řízené LED | Podporuje |  | |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | Podporuje |  | |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | Podporuje |  | |
| Streaming telemetrie prostřednictvím NETCONF/XML | Podporuje |  | |
| SNMPv3 | Podporuje |  | |
| Podpora network boot (iPXE) přes IPv4 i IPv6 | Podporuje |  | |
| Integrovaná RFID identifikace | Podporuje |  | |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | Podporuje |  | |
| NTPv3 server | Podporuje |  | |

|  |  |  |
| --- | --- | --- |
| **Přepínač typ 2d** |  |  |
| Výrobce zařízení | Uvedení výrobce |  |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla |  |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | Uvedení požadovaného odkazu |  |
| **Požadavek na funkcionalitu** | **Min. požadavky** | **Splňuje ANO/NE** |
| ***Základní vlastnosti:*** | | |
| Typ přepínače | L2/L3 přepínač |  |
| Formát přepínače | Stohovatelný, 1RU |  |
| Počet dedikovaných stohovacích portů volitelného stohovacího modulu | 2 |  |
| Minimální počet zařízení ve stohu | 8 |  |
| Minimální kapacita sběrnice stohu | 1600 Gb/s |  |
| Sdílení výkonu napájecích zdrojů napříč celým stohem | Podporuje |  |
| Stateful Switch Over v rámci stohu | Podporuje |  |
| Non-stop Forwarding | Podporuje |  |
| Možnost instalovat interní redundantní napájecí zdroj | Podporuje |  |
| Možnost povyšovat uplink modul | Podporuje |  |
| Redundantní ventilátory | Podporuje |  |
| Redundantní ventilátory vyměnitelné za chodu zařízení | Podporuje |  |
| Interní redundantní napájecí zdroj požadován | Podporuje |  |
| Volný slot pro redundantní zdroj požadován | Podporuje |  |
| Min. PoE budget | 2700 W |  |
| Datový stohovací kabel požadován 1m | Podporuje |  |
| Počet portů 100M/1/2,5/5/10Gbps s 90W PoE napájením | 48 |  |
| Uplink porty | 4x40/100GE QSFP28 |  |
| Min. velikost sdíleného systémového bufferu | 32MB |  |
| Velikost MAC address tabulky | 60000 |  |
| Min. počet IPv4 routes | 50000 |  |
| Min. počet IPv6 routes | 90000 |  |
| Min. počet konfigurovatelných security ACL | 5000 |  |
| IEEE 802.3ad (Link Aggregation) | Podporuje |  |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | Podporuje |  |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | Podporuje |  |
| Minimální počet konfigurovatelných Link Aggregation Group trunků | 128 |  |
| IEEE 802.1q | Podporuje |  |
| Minimální počet aktivních VLAN | 1000 |  |
| IEEE 802.1x – Port Based Network Access Control | Podporuje |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | Podporuje |  |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | Podporuje |  |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | Podporuje |  |
| RADIUS CoA | Podporuje |  |
| Per VLAN Rapid Spanning Tree (PVRST+) nebo ekvivalentní | Podporuje |  |
| IEEE 802.1w - Rapid Spanning Tree Protocol | Podporuje |  |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | Podporuje |  |
| Podpora jumbo rámců (min. 9198 bytes) | Podporuje |  |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | Podporuje |  |
| Směrování protokolů IPv4 a IPv6 v hardware | Podporuje |  |
| OSPFv2 | Podporuje |  |
| OSPFv3 | Podporuje |  |
| ISIS | Podporuje |  |
| LISP dle RFC 6830 nebo ekvivalentní | Podporuje |  |
| BGPv4 | Podporuje |  |
| VXLAN s BGP EVPN | Podporuje |  |
| Policy based routing uvnitř VRF | Podporuje |  |
| Graceful Insertion and Removal | Podporuje |  |
| IP Multicast (PIM SSM, PIM SM) | Podporuje |  |
| Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF) | Podporuje |  |
| MPLS VPN | Podporuje |  |
| MPLS VPN přes GRE tunely | Podporuje |  |
| MPLS VPN - 6VPE | Podporuje |  |
| VXLAN enkapsulace | Podporuje |  |
| Reverse path check (uRPF) pro IPv4 i IPv6 | Podporuje |  |
| IGMPv2, IGMPv3 | Podporuje |  |
| IGMP snooping | Podporuje |  |
| MLD snooping | Podporuje |  |
| DHCP relay | Podporuje |  |
| Minimální počet HW QoS front | 8 |  |
| QoS classification – ACL, DSCP, CoS based | Podporuje |  |
| QoS marking - DSCP, CoS | Podporuje |  |
| QoS - Strict Priority Queue | Podporuje |  |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | Podporuje |  |
| QoS Policing | Podporuje |  |
| QoS-Hierarchical QoS | Podporuje, min. 2 úrovně |  |
| First Hop Redundancy Protokol pro IPv4 i IPv6 (HSRP nebo VRRP) | Podporuje |  |
| IPv6 services (Telnet, SSH, Syslog, DHCP) | Podporuje |  |
| IPv6 QoS | Podporuje |  |
| ***Bezpečnost:*** | | |
| IPv6 Port ACL, VLAN ACL | Podporuje |  |
| IPv6 First Hop Security (RA guard, DHCPv6 Snooping, IPv6 Source Guard) | Podporuje |  |
| Možnost definovat povolené MAC adresy na portu | Podporuje |  |
| PACL, VACL | Podporuje |  |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | Podporuje |  |
| IEEE 802.1ae na všech portech | Podporuje |  |
| IEEE 802.1ae (AES-GCM-256) na všech portech | Podporuje |  |
| IPSec enkrypce v hardware | Podporuje, min. 100 Gbps |  |
| IKEv2 | Podporuje |  |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | Podporuje |  |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | Podporuje |  |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | Podporuje |  |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot | Podporuje |  |
| HW trusted modul pro bezpečné uložení hesel a šifrovacích klíčů | Podporuje |  |
| Podpora SUDI (IEEE 802.1ar) autentizace | Podporuje |  |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | Podporuje |  |
| Multicast DNS (mDNS) gateway | Podporuje |  |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | Podporuje |  |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type | Podporuje |  |
| Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS | Podporuje |  |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | Podporuje |  |
| ***Management:*** | | |
| SSHv2 | Podporuje |  |
| CLI rozhraní | Podporuje |  |
| Vzdálená identifikace zařízení pomocí dálkově řízené LED | Podporuje |  |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | Podporuje |  |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | Podporuje |  |
| Application hosting | Podporuje |  |
| Aplikace softwarových záplat, nikoli povyšování celého firmware | Podporuje |  |
| Streaming telemetrie prostřednictvím NETCONF/XML | Podporuje |  |
| SNMPv3 | Podporuje |  |
| Podpora network boot (iPXE) přes IPv4 i IPv6 | Podporuje |  |
| Integrovaná RFID identifikace | Podporuje |  |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | Podporuje |  |
| NTPv3 server | Podporuje |  |

|  |  |  |
| --- | --- | --- |
| **Datacentrový přepínač typ 2e** |  |  |
| Výrobce zařízení | Uvedení výrobce |  |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla |  |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | Uvedení požadovaného odkazu |  |
| **Požadavek na funkcionalitu** | **Min. požadavky** | **Splňuje ANO/NE** |
| ***Základní vlastnosti:*** | | |
| Typ přepínače | L2 nebo L3 přepínač |  |
| Formát přepínače | Fixní, 1RU |  |
| Redundantní AC zdroj, výdech teplého vzduchu na straně portů, napájecí kabely min. délky 2m s koncovkou IEC 60320 C14 | ANO |  |
| Celková propustnost přepínače | 3,6 Tbps |  |
| Minimální velikost operační paměti | 32 GB |  |
| Minimální počet aktivních neblokovaných portů typu 1/10/25GE s volitelným fyzickým rozhraním | 48 |  |
| Minimální počet aktivních neblokovaných uplink portů 40/100GE s volitelným fyzickým rozhraním typu QSFP28 | 6 |  |
| Podpora dual-rate 40/100GE QSFP rozhraní | Podporuje |  |
| Možnost rozšířit funkcionalitu přepínače o VXLAN routing, např. formou licence | Podporuje |  |
| Možnost rozšířit funkcionalitu přepínače o VXLAN with MP-BGP EVPN control plane, podporu EVPN Route Type 2 (MAC/IP Advertisement Route), Route Type 3 (Inclusive Multicast Ethernet Tag Route), Route Type 4 (Ethernet Segment Route) a Route Type 5 (IP Prefix Route), např. formou licence | Podporuje |  |
| Možnost rozšířit funkcionalitu přepínače o IP multicast routing ve VXLAN infrastruktuře, např. formou licence | Podporuje |  |
| IEEE 802.3ad (Link Aggregation) | Podporuje |  |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | Podporuje |  |
| Minimálně 32 linek jako součást Link Aggregation Group | Podporuje |  |
| Minimální počet konfigurovatelných Link Aggregation Groups | 80 |  |
| Podpora jumbo rámců (min. 9198 bytes) | Podporuje |  |
| IEEE 802.1Q | Podporuje |  |
| Minimální počet aktivních VLAN | 3900 |  |
| Podpora instance spanning-tree protokolu per VLAN | Podporuje |  |
| IEEE 802.1w - Rapid Spanning Tree Protocol | Podporuje |  |
| Detekce protilehlého zařízení (např. LLDP) | Podporuje |  |
| Minimální počet MAC záznamů | 200000 |  |
| QoS classification – ACL, DSCP, CoS based | Podporuje |  |
| QoS marking - DSCP, CoS | Podporuje |  |
| QoS - Priority Based Flow Control (IEEE 802.1Qbb) | Podporuje |  |
| QoS - Flow aware congestion management | Podporuje |  |
| QoS - Flow aware packet prioritization | Podporuje |  |
| Min. velikost sdíleného systémového bufferu | 40 MB |  |
| Možnost zobrazit využití bufferů per port a per queue v reálném čase | Podporuje |  |
| RoCEv2 (RDMA over Converged Ethernet) | Podporuje |  |
| Podpora technologie IEEE 802.1AE (AES-GCM-XPN-­256) na všech SFP a QSFP portech | Podporuje |  |
| Možnost rozšířit funkcionalitu přepínače o PTP (IEEE 1588) včetně PTP Telecom profile (G.8275.1) a Synchronous Ethernet (SyncE), např. formou licence | Podporuje |  |
| Možnost rozšířit funkcionalitu přepínače o IPv4 routing např. formou licence – minimální počet host IPv4 routes | 1M |  |
| Možnost rozšířit funkcionalitu přepínače o IPv6 routing např. formou licence – minimální počet host IPv6 routes | 500000 |  |
| First Hop Redundancy Protokol (např. VRRP, HSRP) pro IP4 i IPv6 | Podporuje |  |
| Možnost rozšířit funkcionalitu přepínače o IPv4 multicast routing s podporou IGMPv2, IGMPv3, např. formou licence | Podporuje |  |
| Možnost rozšířit funkcionalitu přepínače o IPv6 mutlicast routing s podporou MLDv2, např. formou licence | Podporuje |  |
| IGMP snooping | Podporuje |  |
| Port ACL, VLAN ACL | Podporuje |  |
| IPv6 First Hop Security (Binding guard, RA guard, DHCPv6 snooping) | Podporuje |  |
| Možnost rozšířit funkcionalitu přepínače o line rate flow telemetrii (schopnost monitorovat každý paket, každý datový tok procházející přepínačem), např. formou licence | Podporuje |  |
| Možnost rozšířit funkcionalitu přepínače o export line rate flow telemetrie ve formátu NetFlow v9 nebo IPFIX, např. formou licence | Podporuje |  |
| Control Plane Policing | Podporuje |  |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu a to prostřednictvím nemodifikovatelných interních HW prostředků | Podporuje |  |
| Podpora funkce umožňující administrátorovi ověřit, že zařízení skutečně nabootovalo důvěryhodný operační systém | Podporuje |  |
| Operační systém zařízení využívá nástroje, které znemožňují injektovat škodlivý kód do běžícího systému | Podporuje |  |
| Ochrana proti modifikaci HW prostředků zařízení využívající X.509 PKI pro ověření autentičnosti HW prostředků zařízení | Podporuje |  |
| Model-driven programovatelnost prostřednictvím NETCONF/YANG a RESTConf | Podporuje |  |
| Python scripting | Podporuje |  |
| Ansible programming | Podporuje |  |
| Možnost rozšířit funkcionalitu přepínače o streaming telemetrii umožňující kolekci a posílání stavových a statistických informací přímo z HW přepínače, např. formou licence | Podporuje |  |
| Možnost bezobslužného provisioningu nekonfigurovaného zařízení | Podporuje |  |
| CLI rozhraní | Podporuje |  |
| SSHv2 | Podporuje |  |
| SNMPv3 | Podporuje |  |
| NTP server | Podporuje |  |
| RADIUS klient pro AAA (autentizace, autorizace, accounting) | Podporuje |  |
| TACACS+ klient | Podporuje |  |
| Možnost rozšířit funkcionalitu přepínače o vzdálený port mirroring přes L3 směrovanou síť, např. formou licence | Podporuje |  |
| Syslog | Podporuje |  |
| Role Based Access Control | Podporuje |  |

|  |  |  |
| --- | --- | --- |
| **HW appliance nástroje správy sítě typ 3** |  |  |
| Výrobce zařízení | Uvedení výrobce |  |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla |  |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | Uvedení požadovaného odkazu |  |
| **Požadavek na funkcionalitu** | **Min. požadavky** | **Splňuje ANO/NE** |
| ***Základní vlastnosti:*** | | |
| Centralizovaný síťový kontrolér a management systém pro drátovou a bezdrátovou (LAN i WLAN) infrastrukturu | Podporuje |  |
| Formát | Hardware |  |
| Platforma nesmí být v cestě datovému toku sítě. To znamená, že veškerý datový provoz koncových bodů nebude muset procházet platformou pro jakoukoli komunikaci s jinými koncovými body / externí sítí | Podporuje |  |
| Platforma musí poskytovat webové rozhraní pro jednotnou správu drátové a bezdrátové sítě poskytující integrovaný pohled na drátovou i bezdrátovou síť. Poskytuje správci rychlý a snadný pohled na stav sítě, umožňující snadnou identifikaci výpadků, izolaci problémů v síti a obsahující doporučení pro identifikaci nápravy hlavních příčin | Podporuje |  |
| Platforma poskytuje grafické zobrazení topologie sítě s možností vyhledávání a exportu. Vytvoření mapy fyzické topologie sítě lokality na základě rolí jednotlivých síťových prvků softwarově definované sítě. Možnost umístění lokality do mapy na základě adresy lokality nebo GPS souřadnice. Možnost organizovat síťovou hierarchii organizace do oblastí, budov a pateř | Podporuje |  |
| Automatizace poskytovaná platformou je založená na politikách. Zjednodušuje a abstrahuje od složitosti správy sítě při nasazování a vynucování politiky v celé síti | Podporuje |  |
| Platforma umožňuje automatizaci nastavení standardních síťových služeb (DNS, DHCP, AAA, přístupová oprávnění, monitoring) pro síťová zařízení podle lokality | Podporuje |  |
| Platforma podporuje centralizovanou správu standardních konfigurací s využitím konfiguračních šablon | Podporuje |  |
| Platforma umožňuje automatizaci provozních změn – modifikaci chování síťového zařízení aplikací konfigurační šablony | Podporuje |  |
| Platforma musí umožnit kontrolu (náhled) plánované konfigurační změny před její aktivací na síťovém zařízení | Podporuje |  |
| Platforma musí poskytnout detailní informace o výsledku požadavku na provedení konfigurační změny | Podporuje |  |
| Platforma musí zobrazit informace o provedených konfiguračních změnách síťového zařízení včetně změn nerealizovaných centralizovaným síťovým kontrolérem – tzv. out-of-band změny | Podporuje |  |
| Platforma musí poskytovat podrobný soupis a inventář zařízení uspořádaný podle typu zařízení, jména, IP adresy, MAC adresy, firmware, sériového čísla a konfigurace. Tento inventář musí být možno automaticky aktualizovat minimálně po každých 30 minutách | Podporuje |  |
| Platforma musí poskytovat informace o stavu životního cyklu spravovaných síťových zařízení pro snadnou identifikaci zařízení se známým datem blížícího se konce podpory výrobce apod. | Podporuje |  |
| Platforma podporuje automatické zprovoznění nových zařízení – jejich nalezení, zajištění bezpečné komunikace s kontrolérem, zavedení do inventáře a pod správu, upgrade na požadovanou verzi programového vybavení a konfiguraci s využitím základní konfigurační šablony | Podporuje |  |
| Platforma podporuje tvorbu konfiguračních šablon v Apache Velocity Language a Jinja a jejich skládání do kompozitních šablon | Podporuje |  |
| Konfigurační šablony musí podporovat definici proměnných různých, definici jejich implicitních hodnot a vazbu na databázi platformy (např. seznam rozhraní konkrétního zařízení) | Podporuje |  |
| Aplikace šablon na zařízení musí být možná okamžitě nebo později v definovaném časovém okamžiku nebo pouze vygenerovat náhled konfigurace | Podporuje |  |
| Platforma musí poskytovat nástroj pro simulaci konfiguračních šablon | Podporuje |  |
| Šablony mohou být přiřazeny k zařízení na základě lokality, modelu a značky | Podporuje |  |
| Platforma umožňuje mít integrovaný modul síťové analýzy a také funkce kognitivní analýzy prostřednictvím Machine Learning pro řešení problémů se sítí | Podporuje, formou povýšení licence |  |
| Přístup ke kontrolérům musí být možný na základě rolí (pouze čtení, povolené změny a administrátor) | Podporuje |  |
| Platforma musí poskytovat informace o provedených změnách (kdo, co, kdy) – auditní logy | Podporuje |  |
| Platforma musí podporovat následující standardní protokoly, které jí umožňují komunikovat se síťovými zařízeními: NETCONF, SSH, SNMP, HTTP(S) | Podporuje |  |
| Platforma musí podporovat autentizaci pomocí TACACS a RADIUS | Podporuje |  |
| Platforma musí poskytovat otevřená rozhraní API pro vytváření inteligentní, otevřené a programovatelné sítě/fabriky pro konfiguraci pokročilých automatizačních služeb | Podporuje |  |
| Platforma musí poskytovat otevřená rozhraní API pro zasílání událostí z monitoringu | Podporuje |  |
| Platforma musí podporovat rozhraní API REST (Representational State Transfer) | Podporuje |  |
| Platforma musí podporovat automatické aktualizování software kontroléru z cloudu přes cloud tethering | Podporuje |  |
| Platforma musí podporovat automatické aktualizace aplikací kontroléru prostřednictvím cloudového tetheringu | Podporuje |  |
| Platforma musí podporovat režim redundance s plnou perzistencí dat pro vysokou dostupnost | Podporuje |  |
| Platforma poskytuje centrální správu bezdrátových sítí (SSID) pro jednotlivé lokality | Podporuje |  |
| latforma poskytuje mapy síly signálu bezdrátové sítě včetně „heatmap“ síly signálu a jeho kvality | Podporuje |  |
| Platforma umožňuje 3D vizualizaci bezdrátového signálu včetně možnosti simulace změn a automatické detekce problémů | Podporuje, formou povýšení licence |  |
| Platforma umožňuje lokalizování polohy klientů po integraci s volitelným lokalizačním serverem | Podporuje, formou povýšení licence |  |
| Platforma musí umožňovat jednoduchou a centralizovanou definici síťových a bezpečnostních politik | Podporuje |  |
| Platforma musí podporovat dvouúrovňovou segmentaci sítě založenou na politikách pro uživatele, zařízení a IoT pomocí automatizovaného nasazení síťové infrastruktury jako fabriky | Podporuje, formou povýšení licence |  |
| Platforma musí podporovat integraci s dalšími bezpečnostními zařízeními prostřednictvím Platform Exchange GRID (pxGrid), který využívá mnoho dodavatelů zabezpečení, jako jsou Checkpoint, LogRhythm, Splunk, Huntsman, Infoblox, Ping Identity, Cisco ISE a mnoho dalších | Podporuje, formou povýšení licence |  |
| Možnost registrace a správy příslušných licencí připojených síťových prvků | Podporuje |  |
| Podpora simulace a konfigurace vysílacích parametrů bezdrátové sítě na základě algoritmů strojového učení | Podporuje, formou povýšení licence |  |
| Podpora integrace s nástroji pro plánování rozmístění jednotlivých AP (např. Ekahau) v rámci importu mapových podkladů | Podporuje |  |
| Poskytuje informace o spravované síti a jejím stavu ve formě reportů | Podporuje |  |
| Kontrolér musí podporovat správu obrazů softwaru aktivních prvků, udržovat centrální úložiště obrazů programového vybavení zařízení a aplikovat je jednotlivě i najednou na více zařízení (například ve stohu) | Podporuje |  |
| Kontrolér musí podporovat správu obrazů softwarových oprav (patch) a aplikovat je jednotlivě i najednou na více zařízení (například ve stohu) | Podporuje, formou povýšení licence |  |
| Kontrolér musí umožnit definovat softwarovou politiku, jaký konkrétní obraz softwaru aktivního prvku je v síti a / nebo v lokalitě standardem pro rodinu zařízení a / nebo roli zařízení (přístup, distribuce, jádro sítě) | Podporuje |  |
| Kontrolér musí umožnit operátorovi jednoduchou identifikaci aktivních prvků, které vyžadují změnu obrazu software z důvodu změny v softwarové politice nebo protože stávající obraz aktivního prvku není v souladu se platnou politikou | Podporuje |  |
| Funkce správy obrazu softwaru musí podporovat provádění předběžných kontrol inventáře zařízení ohledně dostupnosti doporučeného prostoru ve flash paměti. Po nasazení (aktualizaci softwarového obrazu) musí zkontrolovat úspěšnou aktivaci nainstalovaného obrazu | Podporuje |  |
| Platforma musí podporovat HTTPS, SFTP a SCP pro distribuci softwarových obrazů | Podporuje |  |
| Kontrolér musí podporovat plánování distribuce a aktivace obrazů softwaru na jednotlivá síťová zařízení ve fabrice i mimo fabriku. Distribuci a aktivaci musí být možno provést v rozdílný čas | Podporuje |  |
| Kontrolér musí být schopen indikovat, že softwarový obraz (verze programového vybavení) je zasažen bezpečnostní zranitelností | Podporuje |  |
| Kontrolér musí být schopen indikovat, že software provozovaný na síťovém zařízení je zasažen známou významnou chybou relevantní k provozovaným funkcionalitám a umožnit tento incident řešit | Podporuje, formou povýšení licence |  |
| Kontrolér musí podporovat sladění charakteristik softwarového obrazu se softwarovou politikou u nově zprovozňovaných zařízení | Podporuje |  |
| Zobrazení informace o monitorované síti / vybrané části sítě | Podporuje |  |
| Zobrazení informace o monitorovaných aktivních prvcích | Podporuje |  |
| Zobrazení informace o připojených drátových a bezdrátových koncových stanicích a uživatelích | Podporuje |  |
| Zobrazení informace o využívaných aplikacích | Podporuje |  |
| Zobrazení informace o aplikacích používaných jednotlivými drátovými i bezdrátovými klienty | Podporuje |  |
| Zobrazení informace o využití napájení v rámci sítě (PoE) | Podporuje |  |
| Schopnost zobrazení cizích AP (Rogue AP) a klientů (Rogue Client), možnost vynuceného odpojení klientů prostřednictvím infrastruktury | Podporuje |  |
| Možnost detekce rušivých signálů (interference) a identifikace zdrojů interference na základě signatur včetně automatického záchytu detekovaného provozu a lokalizace | Podporuje, formou povýšení licence |  |
| Detekce problémů s klientem / koncovým bodem | Podporuje, formou povýšení licence |  |
| Detekce problémů se síťovými zařízeními | Podporuje, formou povýšení licence |  |
| Uvedení doporučených nápravných kroků pro každý zjištěný výpadek nebo problém | Podporuje, formou povýšení licence |  |
| Uchování 24 hodin provozní historie sítě umožňující analýzu stavu sítě stejnými postupy jako u právě probíhajících výpadků | Podporuje |  |
| Uchování minimálně 14 denní provozní historie sítě umožňující analýzu i řešení výpadků a problémů, ke kterým došlo v minulosti, stejnými postupy jako u právě probíhajících výpadků | Podporuje, formou povýšení licence |  |
| Detailní zobrazení stavu a provozní historie síťového zařízení, souvisejících událostí, problémů a topologie připojení sousedních aktivních prvků v analyzovaném čase | Podporuje, formou povýšení licence |  |
| Detailní zobrazení stavu a provozní historie klienta / koncového bodu, souvisejících událostí, problémů, detail síťového připojení v analyzovaném čase a přehled využívaných aplikací včetně výkonnostních parametrů (jitter, loss, latency, throughput) | Podporuje, formou povýšení licence |  |
| Využití metod strojového učení (Machine Learning) lokálně nebo v cloudu výrobce | Podporuje, formou povýšení licence |  |
| Využití metod automatického uvažování (Machine Reasoning) v rámci postupů pro řešení vybraných typů problémů. | Podporuje |  |
| Možnost spektrální analýzy a záchytu bezdrátové komunikace s automatickým vyhodnocením anomálií | Podporuje, formou povýšení licence |  |
| Automatické vytváření vzoru chování sítě pro identifikaci anomálií | Podporuje, formou povýšení licence |  |
| Automatická klasifikace koncových zařízení a vyhodnocování anomálií na základě DPI (Deep Packet Inspection) a telemetrických dat | Podporuje, formou povýšení licence |  |
| Platforma poskytuje funkce pro automatizaci výměny vadného zařízení novým zařízením při zachování konfigurace a monitoring historie | Podporuje |  |
| Postup pro výměnu stávajícího AP – jeho nahrazení novým (typicky modernizace) | Podporuje |  |
| Možnost změnit stav identifikační led (beacon) u zařízení, kde je identifikační led podporována, z centralizovaného management a monitoring systému pro snadnou identifikaci zařízení vyžadujícího zásah lokálním správcem | Podporuje |  |
| Min. počet man-day podpory při nasazení | 5 |  |

|  |  |  |
| --- | --- | --- |
| **Pár HW Nex-Gen Firewall typ 4** |  |  |
| Výrobce zařízení | Uvedení výrobce |  |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Uchazeč hlavní produktové číslo nabízeného zařízení) | Uvedení produktového čísla |  |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | Uvedení požadovaného odkazu |  |
| **Požadavek na funkcionalitu** | **Min. požadavky** | **Splňuje ANO/NE** |
| Typ zařízení | Next-Gen Firewall |  |
| Formát zařízení | 2 kusy HW appliance, max 1 RU/kus |  |
| Dedikovaný 1GB ethernet port pro management | Podporuje |  |
| Minimální počet 1GE portů s fyzickým rozhraním typu RJ45 (10M/100M/1G) Gbps) | 8 |  |
| Minimální počet 10GE portů s fyzickým rozhraním typu SFP+ (1/10 Gbps) | 4 |  |
| Podporovaný počet současně otevřených spojení aplikačního FW | 400 K |  |
| Rychlost vytváření nových spojení přes aplikační FW | 50 K/sec |  |
| Propustnost aplikačního FW (top parametry) | 13 Gbps |  |
| Propustnost aplikačního FW + IPS (top parametry) | 11 Gbps |  |
| Propustnost IPsec VPN (top parametry) | 13 Gbps |  |
| Propustnost TLS – HW decryption (top parametry) | 2,5 Gbps |  |
| Podpora L2 (transparentního) módu s podporou NAT a PAT | Podporuje |  |
| Podpora L3 (routovaného) módu s podporou NAT a PAT | Podporuje |  |
| Podpora transparentního inline IPS módu | Podporuje |  |
| Pro inline IPS režim jsou k dispozici karty/rozhraní s HW bypass (Fail-to-Wire) | Podporuje |  |
| Minimální počet VLAN | 1024 |  |
| Podpora stateful failover v režimu active/standby | Podporuje |  |
| Podpora stateful failover v režimu active/active | Podporuje |  |
| Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru | Podporuje |  |
| Cluster firewallů se musí vzhledem k další infrastruktuře tvářit jako jeden prvek s podporou LACP | Podporuje |  |
| Cluster podporuje stavovou inspekci nesymetrického provozu vstupující do různých firewallů clusteru | Podporuje |  |
| Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podorou LACP | Podporuje |  |
| OSPF, BGP | Podporuje |  |
| Podpora IPv6 dynamického směrování – OSPFv3, BGP | Podporuje |  |
| Policy based Routing | Podporuje |  |
| Kontrola paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod. | Podporuje |  |
| Filtrace IPv4, IPv6 | Podporuje |  |
| Možnost filtrace podle identity uživatele nebo jeho skupiny definované v AD | Podporuje |  |
| Možnost filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích | Podporuje |  |
| Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu | Podporuje |  |
| NAT64 a DNS64 | Podporuje |  |
| Možnost řízení rychlosti datových toků na úrovni pravidel FW | Podporuje |  |
| Funkce IPS | Podporuje |  |
| Možnost rozšíření o funkce URL filtrace | Podporuje, formou povýšení licence |  |
| Možnost rozšíření o funkce antimalware filtrace | Podporuje, formou povýšení licence |  |
| Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele | Podporuje |  |
| Podpora FQDN v přístupových pravidlech | Podporuje |  |
| Podpora časových informací v přístupových filtrech | Podporuje |  |
| Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech | Podporuje |  |
| API rozhraní pro sdílení kontextových informací s dalšími systémy | Podporuje |  |
| Možnost definovat typ provozu předávaný k inspekci do IPS | Podporuje |  |
| Podpora také IDS režimu – pasivního monitorování (TAP režim) | Podporuje |  |
| Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close) | Podporuje |  |
| Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti | Podporuje |  |
| Podpora 802.1Q tagovaných rámců | Podporuje |  |
| Podpora různých IPS politik pro různé typy provozu | Podporuje |  |
| Inspekce pro IPv4 i IPv6 | Podporuje |  |
| Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému | Podporuje |  |
| IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií | Podporuje |  |
| Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací | Podporuje |  |
| Podpora aplikace pro psaní zákaznických filtrů | Podporuje |  |
| Podpora importu komunitních filtrů/signatur Snort | Podporuje |  |
| IPS musí umět detekovat a blokovat útoky průzkumných aktivit | Podporuje |  |
| IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS | Podporuje |  |
| IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C | Podporuje |  |
| IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii | Podporuje |  |
| Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události | Podporuje |  |
| Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku | Podporuje |  |
| Funkce pro kontrolu DLP (např. pomocí IPS signatur) | Podporuje |  |
| Podpora vrstvev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive | Podporuje |  |
| Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí | Podporuje |  |
| Možnost definice uživatelské vrstvy politik | Podporuje |  |
| Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik | Podporuje |  |
| Různé politiky lze sdílet a aplikovat na různé senzory | Podporuje |  |
| Možnost integrace s platformou řízení přístupu do sítě (AAA) a řízení karantény/segmentace koncových stanic na základě firewallem detekovaných incidentů | Podporuje |  |
| Možnost automatické aktualizace IPS signatur podle zranitelností stanic v síti při integraci s detektory zranitelností | Podporuje |  |
| Propagace detekovaných zranitelnosti CVE do aktivních IPS signatur | Podporuje |  |
| Možnost integrace s XDR a externími systémy analýzy | Podporuje |  |
| Analytické a detekční nástroje pro práci se šifrovaným provozem i bez jeho dekrypce | Podporuje |  |
| Aplikační signatury i pro SSL encrypted provoz | Podporuje |  |
| Podpora SSL dekrypce i pro TLS 1.3 | Podporuje |  |
| Možnost definovat pravidla SSL dekrypce i pro provoz TLS 1.3 | Podporuje |  |
| Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod. | Podporuje |  |
| Podpora pasivního monitorování (TAP režim) | Podporuje |  |
| Podpora 802.1Q tagovaných rámců | Podporuje |  |
| SSL/TLS inspekce (dekrypce/enkrypce) | Podporuje |  |
| Security Inteligence database – známé uzly botnet sítí C&C | Podporuje |  |
| Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, apod. | Podporuje |  |
| Security Inteligence database – známé nebezpečné URL adresy a jmenné domény | Podporuje |  |
| Možnost integrovat vlastní reputační databáze | Podporuje |  |
| Podpora komunitních, otevřených standardů popisu apliací (OpenAppID) | Podporuje |  |
| Filtry mohou zohlednit roli a identitu uživatele | Podporuje |  |
| Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow) | Podporuje |  |
| Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě | Podporuje |  |
| Řešení musí být schopné pasivního sběru informací o síťových zařízení a zobrazení:  • Typ zařízení  • Operační systém  • Dodavatel OS  • Použité síť. protokoly  • Použité síť. služby  • Otevřené porty síť. služeb  • Potenciální zranitelnosti | Podporuje |  |
| Přehled o síťových spojení má poskytovat minimálně tyto informace:  • Čas startu a konce flow  • Akce (allow, deny,..)  • Důvod případného blokování  • Zdroj. a cíl. adresa  • Vstupní a výstupní zóna  • Vstupní a výstupní rozhraní  • Zdroj. a cíl. port  • Aplikační protokol  • IPS událost, pokud vznikne  • Riziková úroveň IPS události  • Použitá síťová aplikace  • Rizikovost aplikace  • „Business impact“ aplikace  • Množství přenesených dat | Podporuje |  |
| Vzdálené správa přes grafické rozhraní bez nutnosti instalace zvláštního SW | Podporuje |  |
| Přístup ke GUI http/https protokolem | Podporuje |  |
| Možnost vzdáleného přístupu protokolem SSH přímo do FW | Podporuje |  |
| RBAC pro administrátory | Podporuje |  |
| Možnost oddělení práv správy pro různé FW podle rolí správců | Podporuje |  |
| Možnost oddělení práv správy bezpečnostních pravidel podle rolí správců | Podporuje |  |
| Možnost správy pravidel, objektů i přes API | Podporuje |  |
| Možnost přístupu k textovým logům (syslog) přímo ve FW | Podporuje |  |
| Možnost centrální správy při nasazení více firewallů | Podporuje |  |
| Při centrální správě: možnost sdílených bezpečnostních politik | Podporuje |  |
| Při použití clusteru se spravuje pouze jeden logický prvek | Podporuje |  |
| Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu | Podporuje |  |
| Zobrazení logů a událostí v grafickém rozhraní správy | Podporuje |  |
| Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování | Podporuje |  |
| Funkce IPS a Next-Gen FW vyžadující dlohodobější ukládání dat, korelace, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního sytému (centrální dohledové konzole) | Podporuje |  |
| Centrální dohledová konzole musí být schopna dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod. | Podporuje |  |
| Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu | Podporuje |  |
| Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole | Podporuje |  |
| Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic | Podporuje |  |
| Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu | Podporuje |  |
| Pro reporty lze definovat template definující formát a obsah reportu | Podporuje |  |
| Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu | Podporuje |  |
| V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N | Podporuje |  |
| Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů | Podporuje |  |
| Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod. | Podporuje |  |
| Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů. | Podporuje |  |
| Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod. | Podporuje |  |
| Podpora posílání událostí formou syslog, email, SNMP na externí platformy | Podporuje |  |
| Podpora Event Streamer API (eStreamer) pro sdílení informací se externími systémy. Minimálně pro tyto SIEM:  • ArcSight  • BMC Remedy  • Q1Labs-QRadar  • Splunk | Podporuje |  |
| Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay | Podporuje |  |
| Podpora API pro přístup z externích systémů k databázím centralizovaného managementu | Podporuje |  |
| Podpora řízeného přístupu podle rolí administrátorů | Podporuje |  |
| Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora | Podporuje |  |
| Možnost založit pro daný incident „ticket“ přímo v prostředí GUI managementu | Podporuje |  |
| Workflow pro předávání „ticketů“ mezi administrátory | Podporuje |  |
| Konkrétní bezpečnostní incident až na úrovni paketu lze přiložit k danému „tiketu“ pro další analýzu | Podporuje |  |
| Možnost definice politik pro sledování odpovídajících parametrů „zdraví“ na senzorech a centralizované konzoli (zařížení CPU, obsazení paměti, komunikace s cloudovými službami, apod.) | Podporuje |  |
| Zákaznicky definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví“ | Podporuje |  |
| Různé politiky pro sledování „zdraví“ lze aplikovat na různé senzory nebo centralizovanou konzoli | Podporuje |  |
| Nativní integrovatelnost do platformy centrální správy incidentů, korelaci a automatizaci | Podporuje |  |