1.02.Aktivní prvky

## Společné požadavky pro všechny aktivní prvky

* Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství), a musí být určen pro trh v rámci EU.
* Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností   
  a parametrů.
* Je požadována servisní podpora na software a hardware s odesláním náhradních dílů NBD (následující pracovní den) po oznámení poruchy v minimální délce 60 měsíců od předání. Tato servisní podpora musí být garantovaná výrobcem zařízení, včetně registrace servisní podpory   
  u výrobce. Prodávající za tímto účelem předloží kupujícímu před zahájením plnění certifikát   
  či prohlášení výrobce (v listinném či elektronickém originálu či z těchto originálů úředně zkonvertováno) a provede registraci servisní podpory u výrobce s tím, že kupující bude mít možnost si provedení této registrace a její délku ověřit.
* Je požadována dostupnost softwarových aktualizací (nové verze programového vybavení) po dobu minimálně 60 měsíců od předání.
* Je požadován jednotný cloud management nástroj pro správu přepínačů i přístupových bodů bezdrátové sítě (AP).
* Součástí dodávky bude veškeré příslušenství a propojovací prvky dle standardu zařízení a zákazníka.

## Typ 1 + Typ 9 – 4 kusy

|  |  |
| --- | --- |
| **Konkrétní specifikace nabízeného zboží** | |
| Model – typové/výrobní označení |  |
| Výrobce: |  |

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje**  **[Ano/Ne]** |
| **Základní vlastnosti** |  |  |
| Třída zařízení: přepínač | Ano |  |
| Formát zařízení do racku | Ano |  |
| Velikost zařízení: 1U | Ano |  |
| Provedení bez ventilátoru | Ano |  |
| Počet 1Gbit/s metalických portů | 24× RJ45 |  |
| Počet 10Gbit/s SFP+ nezávislých optických portů | 4× SFP+ |  |
| 10GE interface zpětně kompatibilní s 1Gbit/s transceivery | ano |  |
| Všechny ethernet porty jsou dostupné zepředu | ano |  |
| Interní napájecí zdroj | Ano |  |
| Podpora PoE+ dle standardu 802.3at | Min. 20 portů |  |
| Podpora PoE++ (60W) dle standardu 802.3bt | Min. 4 porty |  |
| Dostupný výkon pro PoE+/PoE++ napájení | 240W |  |
| Celková propustnost přepínače | 128 Gb/s |  |
| Celkový paketový výkon přepínače | 95 Mpps |  |
| **Základní funkce a protokoly** |  |  |
| Podpora "jumbo rámců" včetně velikosti 9198 Byte | Ano |  |
| Počet LACP skupin/linek ve skupině: 8/8 | Ano |  |
| Minimální počet záznamů v tabulce MAC adres: 8 000 | Ano |  |
| Minimální počet záznamů v tabulce ARP: 700 | Ano |  |
| Protokol pro definici šířených VLAN: MVRP | Ano |  |
| Podpora VLAN podle IEEE 802.1Q, minimálně 500 aktivních VLAN | Ano |  |
| IEEE 802.1s - Multiple Spanning Tree | Ano |  |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) | Ano |  |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED | Ano |  |
| Detekce jednosměrnosti optické linky (např. UDLD) | Ano |  |
| Podpora NTP | Ano |  |
| Statické směrování IPv4 a IPv6 | Ano |  |
| Minimální počet IPv4 záznamů ve směrovací tabulce: 500 | Ano |  |
| Minimální počet IPv6 záznamů ve směrovací tabulce: 500 | Ano |  |
| IGMP v2 a v3 | Ano |  |
| IGMP snooping | Ano |  |
| MLD v1 a v2 | Ano |  |
| MLD snooping | Ano |  |
| Hardware podpora IPv4 a IPv6 ACL | Ano |  |
| ACL definice na základě skupiny fyzických portů | Ano |  |
| ACL aplikovatelný na interface a VLAN | Ano |  |
| BPDU a Root guard | Ano |  |
| DHCP snooping | Ano |  |
| HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps | Ano |  |
| 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port | Ano |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) | Ano |  |
| Podpora Critical VLAN | Ano |  |
| Podpora Dynamic ARP protection | Ano |  |
| Port security | Ano |  |
| Podpora IPv4 a IPv6 QoS | Ano |  |
| IEEE 802.1p - minimální počet front: 8 | Ano |  |
| **Analytické a automatizační nástroje** | Ano |  |
| Podpora REST API pro automatizaci nastavení sítě. | Ano |  |
| Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači | Ano |  |
| Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní) | Ano |  |
| Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události | Ano |  |
| Grafické rozhraní pro zobrazení výsledků monitorování a analytických skriptů. Možnost zobrazení stavu monitorovaných metrik do grafů atp. | Ano |  |
| Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase. | Ano |  |
| Interní uložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení | Ano |  |
| **Management** | Ano |  |
| Konzolový port | Ano |  |
| 1xRJ45 OoB management port s podporou ethernetu | Ano |  |
| Konfigurace zařízení v člověku čitelné textové formě | Ano |  |
| Podpora automatických i manuálních snapshotů konfigurace systému | Ano |  |
| USB port pro diagnostiku, přenos konfigurace a firmware | Ano |  |
| Podpora managementu přes IPv4 i IPv6 | Ano |  |
| SSHv2 a HTTPS pro IPv4 a IPv6 | Ano |  |
| Podpora SNMPv2c a SNMPv3 | Ano |  |
| RMON | Ano |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | Ano |  |
| Lokálně vynucené RBAC na úrovni přepínače | Ano |  |
| Dualní flash image | Ano |  |
| Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů | Ano |  |
| Podpora RADIUS včetně RADIUS CoA (RFC3576) | Ano |  |
| Podpora TACACS+ | Ano |  |
| Analýza síťového provozu sFlow podle RFC 3176 | Ano |  |
| Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM chipu | Ano |  |
| Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN | Ano |  |
| Podpora Zero Touch Provisioning (ZTP) | Ano |  |
| Součástí každého přepínače musí být licence pro jeho centrální správu a monitoring pomocí cloud management nástroje od výrobce přepínače | Ano |  |
| Je-li součástí přepínače časově omezená licence (subscription), musí být tato minimálně na 5 let | Ano |  |

## Typ 2 – 2 kusy

|  |  |  |
| --- | --- | --- |
| **Požadavky na funkcionalitu** | **Minimální požadavky** | **Splňuje**  **[Ano/Ne]** |
| **Základní vlastnosti** |  |  |
| Typ zařízení: L3 přepínač | Ano |  |
| Velikost zařízení: 1U | Ano |  |
| Počet 1/10/25 Gbps portů s volitelným fyzickým rozhraním | 44x SFP28 |  |
| Počet 10/25 Gbps portů s volitelným fyzickým rozhraním s podporou MACSec | 4x SFP28 |  |
| Počet 40/100 Gbps portů s volitelným fyzickým rozhraním | 6x QSFP28 |  |
| Podpora rozdělení 40 GE portů na 4x10 GE a 100GE portů na 4x25 GE | Ano |  |
| Podpora originálních transceiverů výrobce: 10GBASE-T SFP+ | Ano |  |
| 2x interní hot-swap AC napájecí zdroj | Ano |  |
| Redundantní hot-swap ventilátory | Ano |  |
| Směr proudění vzduchu zařízením: předo-zadní | Ano |  |
| Minimální přepínací výkon | 4,8 Tbps |  |
| Minimální paketový výkon | 2600 Mpps |  |
| Minimální paketový buffer | 32 MB |  |
| Hloubka přepínače | Max. 56 cm |  |
| **Vlastnosti stohování** |  |  |
| Podporovaný počet přepínačů ve stohu | 2 |  |
| Kapacita stohovacího propojení | 600 Gbps |  |
| Stoh podporuje distribuované přepínání paketů | Ano |  |
| Libovolný prvek stohu může být řídícím prvkem (1:1 redundance) | Ano |  |
| Seskupení portů IEEE 802.3ad mezi různými prvky stohu (MC-LAG) | Ano |  |
| Podpora upgrade OS ve stohu bez narušení provozu (ISSU) | Ano |  |
| Podpora automatizace upgrade OS ve stohu bez narušení provozu přes REST API | Ano |  |
| **Funkce a protokoly** |  |  |
| Podpora jumbo rámců včetně velikosti 9198 Byte | Ano |  |
| Podpora linkové agregace IEEE 802.1AX | Ano |  |
| Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4 | Ano |  |
| Minimální počet LACP skupin/linek ve skupině | 52/16 |  |
| Podpora LACP Fallback (např. pro PXE boot) | Ano |  |
| Minimální počet záznamů v tabulce MAC adres | 210 000 |  |
| Minimální počet záznamů v tabulce ARP | 140 000 |  |
| Protokol pro definici šířených VLAN | MVRP |  |
| Počet aktivních VLAN podle IEEE 802.1Q | 4000 |  |
| Tunelování 802.1Q v 802.1Q | Ano |  |
| VLAN translace – swap 802.1Q tagů na trunk portu | Ano |  |
| Podpora zařazování do VLAN podle standardu 802.1v | Ano |  |
| Private VLAN včetně primary, secondary a community VLAN | Ano |  |
| IEEE 802.1s – Multiple Spanning Tree a IEEE 802.1w | Ano |  |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) | Ano |  |
| Podpora ERPS (ITU G.8032) pro rychlou konvergenci do 100ms v kruhových sítích | Ano |  |
| Detekce protilehlého zařízení pomocí LLDP, včetně LLDP over OoB management port | Ano |  |
| Detekce jednosměrnosti optické linky (např. UDLD nebo ekvivalentní) | Ano |  |
| DHCP server a relay pro IPv4 a IPv6 včetně podpory VRF | Ano |  |
| Podpora zapouzdření: GRE over IPv4 | Ano |  |
| Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace | Ano |  |
| Podpora NTP server | Ano |  |
| Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subnety | Ano |  |
| Podpora L3 routed port včetně L3 sub-interface – nadřazené L3 rozhraní lze rozdělit | Ano |  |
| Statické směrování IPv4 a IPv6 | Ano |  |
| Počet IPv4 záznamů ve směrovací tabulce | 600 000 |  |
| Počet IPv6 záznamů ve směrovací tabulce | 600 000 |  |
| Dynamické směrování: RIP, RIPng, OSPFv2 včetně HMAC-SHA-384, OSPFv3, BGP, MP-BGP | Ano |  |
| Funkce BGP konfederace a route reflector pro IPv4 a IPv6 | Ano |  |
| Podpora BGP MD5 autentizace a BGP TTL security | Ano |  |
| Podpora policy based routing | Ano |  |
| Podpora VRRPv2 a VRRPv3 | Ano |  |
| Podpora route map | Ano |  |
| ECMP včetně možnosti konfigurace rozkládání zátěže podle L3 a L4 | Ano |  |
| Podpora minimálně 256 virtuálních směrovacích instancí (VRF) | Ano |  |
| IGMP v2 a v3, IGMP snooping | Ano |  |
| MLD v1 a v2, MLD snooping | Ano |  |
| Směrování multicast: PIM-DM, PIM-SM, IPv6 PIM-SM, PIM-SSM, IPv6 PIM-SSM, MSDP | Ano |  |
| Hardware podpora IPv4 a IPv6 ACL | Ano |  |
| DHCP snooping pro IPv4 a IPv6 | Ano |  |
| ACL klasifikace na úrovni zdrojová/cílová MAC adresa, zdrojová/cílová IPv4/IPv6 adresa, číslo zdrojového/cílového portu, protokol, TTL hodnota, číslo VLAN, | Ano |  |
| HW ochrana proti zahlcení portu (broadcast/multicast/unicast) nastavitelná na kbps a pps | Ano |  |
| IEEE 802.1p – Minimálně 8 front | Ano |  |
| 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port | Ano |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) | Ano |  |
| Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675 | Ano |  |
| 802.1X s podporou odlišných Preauth VLAN, Fail VLAN, Critical VLAN a Critical voice VLAN | Ano |  |
| Uživatelské role definované lokálně v přepínači, jejich aplikace dle výsledku autorizace | Ano |  |
| Uživatelské role dynamicky stahovatelné z RADIUS, jejich aplikace dle výsledku autorizace | Ano |  |
| Port security – omezení počtu MAC adres na port, statické MAC, sticky MAC | Ano |  |
| Podpora IPv6 RA Guard, DHCPv6 Guard a IPv6 Destination Guard | Ano |  |
| BPDU guard a Root guard | Ano |  |
| Podpora service insertion včetně technologie VXLAN | Ano |  |
| Podpora static a dynamic VXLAN s využítím BGP-EVPN | Ano |  |
| Podpora PBR VXLAN | Ano |  |
| Podpora Group based policy pro VXLAN (VXLAN GBP) | Ano |  |
| Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU | Ano |  |
| Vynucení zadat heslo administrátora a nastavitelná politika komplexity hesla přímo na přepínači | Ano |  |
| Možnost instalace vlastního certifikátu včetně podpory Enrollment over Secure Transport (EST) | Ano |  |
| TACACS+ a RADIUS klient pro AAA (autentizace, autorizace, accounting) | Ano |  |
| Aktivní monitoring dostupnosti RADIUS a TACACS+ přednastaveným jménem a heslem | Ano |  |
| Podpora Radius over TLS (RadSec) | Ano |  |
| Podpora RADIUS CoA (RFC3576) | Ano |  |
| 802.1x autentizace přepínače vůči nadřazenému přepínači s podporou EAP-TLS a EAP-MD5 | Ano |  |
| QoS ochrana před zahlcením WRED | Ano |  |
| Podpora Data Center Bridging (PFC 802.1Qbb, ETS 802.1Qaz) | Ano |  |
| IP Explicit Congestion Notification (ECN) | Ano |  |
| Podpora RoCEv2 | Ano |  |
| Podpora MPLS L3 VPN | Ano |  |
| **Management** |  |  |
| CLI formou 1x USB-C console port | Ano |  |
| Bezdrátová sériová konzole pomocí Bluetooth | Ano |  |
| Konfigurace zařízení v člověku čitelné textové formě | Ano |  |
| OoB management formou portu RJ45 s podporou ethernetu | Ano |  |
| USB port pro přenos konfigurace a firmware | Ano |  |
| Podpora IPv4 a IPv6 management: SSHv2 server, HTTPS server, SFTP a SCP klient | Ano |  |
| Podpora RSA s délkou klíče minimálně 4096 bitů | Ano |  |
| Podpora SNMPv2c a SNMPv3 | Ano |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | Ano |  |
| Lokálně vynucené RBAC na úrovni přepínače | Ano |  |
| Duální flash image – podpora dvou nezávislých verzí operačního systému | Ano |  |
| Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler) | Ano |  |
| TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více SYSLOG serverů | Ano |  |
| Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby | Ano |  |
| Podpora standardního Linux Shellu (BASH) pro debugging a skriptování | Ano |  |
| Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači | Ano |  |
| Možnost vytváření vlastních diagnostických a korelačních skriptů a jejich grafických interpretací v jazyce Python (korelace libovolných událostí a hodnot v podobě grafů) | Ano |  |
| Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů – možnost vynášení stavu monitorovaných metrik do grafů atp. | Ano |  |
| Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase | Ano |  |
| Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní) | Ano |  |
| Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události | Ano |  |
| Interní úložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení: min. 30 GB | Ano |  |
| Analýza síťového provozu sFlow podle RFC 3176 pro oba směry ingress a egress | Ano |  |
| Analýza síťového provozu IPFIX | Ano |  |
| Ochrana proti nahrání modifikovaného SW prostřednictvím image signing a secure boot, ověřující autentičnost a integritu OS prostřednictvím TPM chipu | Ano |  |
| SPAN a ERSPAN port mirroring, alespoň 4 různé obousměrné session | Ano |  |
| IP SLA pro měření dostupnosti a zpoždění provozu VoIP – režim responder i probe | Ano |  |
| Podpora integrace s automatizačními nástroji (Ansible, NAPALM) | Ano |  |
| Automatizace – podpora read-only a read-write REST API včetně volání CLI příkazů | Ano |  |
| Podpora Cloud i On-Premise management software výrobce zařízení | Ano |  |
| Podpora Zero Touch Provisioning (ZTP) | Ano |  |
| Součástí každého přepínače musí být licence pro jeho centrální správu a monitoring pomocí cloud management nástroje od výrobce přepínače | Ano |  |
| Je-li součástí přepínače časově omezená licence (subscription), musí být tato minimálně na 5 let | Ano |  |

## Typ 3 – 15 kusů

|  |  |
| --- | --- |
| **Konkrétní specifikace nabízeného zboží** | |
| Model – typové/výrobní označení |  |
| Výrobce: |  |

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje**  **[Ano/Ne]** |
| **Základní vlastnosti** |  |  |
| Třída zařízení: L3 switch | Ano |  |
| Formát zařízení do racku | Ano |  |
| Velikost zařízení: 1U | Ano |  |
| Počet MultiGigabit 100Mbit/1Gbit/2,5Gbit/5Gbit/10Gbit/s metalických portů | 24x RJ45 |  |
| Počet 10/25/50Gbit/s nezávislých opt. portů s volitelným fyzickým rozhraním | 2x SFP56 |  |
| Počet 10/25Gbit/s nezávislých opt. portů s volitelným fyzickým rozhraním | 2x SFP28 |  |
| Všechny ethernet porty jsou dostupné zepředu | Ano |  |
| Interní AC hot-swap napájecí zdroje 230 V | Ano |  |
| Vyměnitelné ventilátory – hot swap | Ano |  |
| Podpora PoE dle standardu 802.3bt | Ano |  |
| Dostupný výkon pro PoE napájení | 1440W |  |
| Celková propustnost přepínače | 780 Gbit/s |  |
| Celkový paketový výkon přepínače | 580 Mpps |  |
| Paketový buffer | 16MB |  |
| Maximální hloubka přepínače | max. 39cm |  |
| **Vlastnosti stohování** |  |  |
| Podporovaný počet přepínačů ve stohu | 10 |  |
| Kapacita stohovacího propojení | 200 Gbps |  |
| Stoh podporuje distribuované přepínaní paketů | Ano |  |
| Kterýkoli prvek ve stohu může být řídícím prvkem (1:N redundance) | Ano |  |
| Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor) | Ano |  |
| Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG) | Ano |  |
| Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF | Ano |  |
| Součástí dodávky přepínače je stohovací kabel 50Gbit/s | Ano |  |
| **Základní funkce a protokoly** | Ano |  |
| Podpora "jumbo rámců" včetně velikosti 9198 Byte | Ano |  |
| Podpora linkové agregace IEEE 802.1AX | Ano |  |
| Konfigurovatelné rozkládání LACP zátěže podle L2,L3 | Ano |  |
| Počet LACP skupin/linek ve skupině | 256/16 |  |
| Počet záznamů v tabulce MAC adres | 32 000 |  |
| Počet záznamů v tabulce ARP | 49 000 |  |
| Protokol pro definici šířených VLAN | MVRP |  |
| Podpora VLAN podle IEEE 802.1Q, minimálně 4000 aktivních VLAN | Ano |  |
| VLAN translace - swap 802.1Q tagů na trunk portu | Ano |  |
| Podpora zařazování do VLAN podle standardu 802.1v | Ano |  |
| IEEE 802.1s - Multiple Spanning Tree | Ano |  |
| STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+) | Ano |  |
| Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED | Ano |  |
| Detekce jednosměrnosti optické linky (např. UDLD) | Ano |  |
| DHCP server | Ano |  |
| DHCP relay pro IPv4 a IPv6 | Ano |  |
| Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace | Ano |  |
| Statické směrování IPv4 a IPv6 | Ano |  |
| Počet záznamů ve směrovací tabulce | 61 000 |  |
| Dynamické směrování OSPFv2, OSPFv3 a BGP včetně podpory BFD | Ano |  |
| Podpora BGP a MP-BGP včetně podpory BFD | Ano |  |
| Podpora Layer-3 routed port | Ano |  |
| IGMP v2 a v3 | Ano |  |
| MLD v1 a v2 | Ano |  |
| Hardware podpora IPv4 a IPv6 ACL | Ano |  |
| ACL definice na základě skupiny fyzických portů | Ano |  |
| ACL aplikovatelný na interface, LAG, VLAN | Ano |  |
| BPDU a Root guard | Ano |  |
| DHCP snooping pro IPv4 a IPv6 | Ano |  |
| HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps | Ano |  |
| 802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port | Ano |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) | Ano |  |
| Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675 | Ano |  |
| Podpora Critical VLAN | Ano |  |
| Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely. | Ano |  |
| Uživatelské role mohou být lokálně definované v přepínači nebo mohou být dynamicky stáhnuty z RADIUS serveru na základě výsledku autorizace. | Ano |  |
| Podpora IPv6 RA Guard | Ano |  |
| IP source guard / dynamic IP lockdown | Ano |  |
| Podpora Dynamic ARP protection | Ano |  |
| Port security | Ano |  |
| Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU | Ano |  |
| Podpora IPv4 a IPv6 QoS | Ano |  |
| IEEE 802.1p - minimální počet front | 8 |  |
| **SDN funkce** |  |  |
| Podpora service insertion včetně technologie VXLAN | Ano |  |
| Podpora BGP EVPN s využítím VXLAN | Ano |  |
| Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izololovat více koncových zařízení na jednom portu do unikátních tunelů | Ano |  |
| Přiřazení koncového zařízení do tunelu na základě výsledku autorizace | Ano |  |
| **Analytické a automatizační nástroje** |  |  |
| Podpora REST API pro automatizaci nastavení sítě. | Ano |  |
| Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači | Ano |  |
| Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní) | Ano |  |
| Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události | Ano |  |
| Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů. Možnost vynášení stavu monitorovaných metrik do grafů atp. | Ano |  |
| Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase. | Ano |  |
| Interní uložistě dat pro sběr provozních dat a pokročilou dignostiku zařízení | Ano |  |
| Kapacita interního úložiště dat pro analytické účely: 30 GB | 30 GB |  |
| **Management** |  |  |
| USB-C konzolový port | Ano |  |
| 1xRJ45 OoB management port s podporou ethernetu | Ano |  |
| Podpora minimálně 64 virtuálních směrovacích instancí (VRF) | Ano |  |
| Minimální počet VRF instancí | 64 |  |
| Konfigurace zařízení v člověku čitelné textové formě | Ano |  |
| Podpora automatických i manuálních snapshotů konfigurace systému | Ano |  |
| USB port pro diagnostiku, přenos konfigurace a firmware | Ano |  |
| Přímé bezdrátové připojení ke konzoli zařízení skrze bluetooth | Ano |  |
| Podpora managementu přes IPv4 i IPv6 | Ano |  |
| SSHv2 a HTTPS pro IPv4 a IPv6 | Ano |  |
| Podpora SNMPv2c a SNMPv3 | Ano |  |
| RMON | Ano |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | Ano |  |
| Lokálně vynucené RBAC na úrovni přepínače | Ano |  |
| Dualní flash image | Ano |  |
| Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů | Ano |  |
| Podpora RADIUS včetně RADIUS CoA (RFC3576) | Ano |  |
| Podpora TACACS+ | Ano |  |
| Analýza síťového provozu sFlow podle RFC 3176 | Ano |  |
| Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN | Ano |  |
| Podpora IP SLA pro měření zpoždění provozu VoIP | Ano |  |
| Podpora Zero Touch Provisioning (ZTP) | Ano |  |
| Součástí každého přepínače musí být licence pro jeho centrální správu a monitoring pomocí pomocí cloud management nástroje od výrobce přepínače | Ano |  |
| Je-li součástí přepínače časově omezená licence (subscription), musí být tato minimálně na 5 let | Ano |  |

## Typ 4 – 28 kusů

|  |  |
| --- | --- |
| **Konkrétní specifikace nabízeného zboží** | |
| Model – typové/výrobní označení: |  |
| Výrobce: |  |

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje**  **[Ano/Ne]** |
| **Základní vlastnosti** |  |  |
| Třída zařízení: přepínač | Ano |  |
| Formát zařízení do racku | Ano |  |
| Velikost zařízení: 1U | Ano |  |
| Stohovatelný | Ano |  |
| Počet 10/100/1000 Mbit/s metalických portů | 36 x RJ45 |  |
| Počet MultiGigabit 1Gbit/2,5Gbit/5Gbit/s metalických portů | 12x RJ45 |  |
| Počet portů 10 Gbit/s a jejich typ | 4x SFP+ |  |
| Všechny produkční ethernet porty jsou dostupné zepředu | Ano |  |
| Podpora PoE++ (60W) dle standardu 802.3bt | 48 portů |  |
| Dostupný výkon pro PoE+ napájení | 740 W |  |
| **Výkonnostní parametry** |  |  |
| Minimální paketový výkon přepínače v paketech/vteřinu | 130 milionu |  |
| Rychlost stohovacího propojení | alespoň 40 Gbit/s |  |
| **Vlastnosti stohování** |  |  |
| Minimální počet přepínačů ve stohu | 8 |  |
| Automatická kontrola a sjednocení verze software přepínačů ve stohu | Ano |  |
| Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením | Ano |  |
| Seskupení portů (IEEE 802.3ad) mezi různými prvky stohu | Ano |  |
| Redundance řídícího prvku v rámci stohu | Ano |  |
| IEEE 802.1ae na min. 2 uplink portech | Ano |  |
| Minimální počet MAC adres | 32 000 |  |
| **Protokoly fyzické vrstvy** |  |  |
| IEEE 802.3-2005 | Ano |  |
| IEEE 802.3ad | Ano |  |
| Podpora "jumbo rámců" | Ano |  |
| **Protokoly 2. vrstvy** |  |  |
| IEEE 802.1D | Ano |  |
| IEEE 802.1Q | Ano |  |
| Minimální počet aktivních VLAN | 2000 |  |
| IEEE 802.1X - Port Based Network Access Control | Ano |  |
| IEEE 802.1s - multiple spanning trees | Ano |  |
| IEEE 802.1w - Rapid Tree Spanning Protocol | Ano |  |
| IEEE 802.1p - Minimální počet vnitřních front | 8 |  |
| Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní | Ano |  |
| Detekce protilehlého zařízení (např. CDP, LLDP) | Ano |  |
| Detekce parametrů protilehlého zařízení (např. LLDP-MED) | Ano |  |
| Protokol pro definici šířených VLAN (MVRP nebo VTP) | Ano |  |
| Detekce jednosměrnosti optické linky (např. UDLD) | Ano |  |
| STP root guard | Ano |  |
| STP loop guard | Ano |  |
| Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard) | Ano |  |
| Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech | Ano |  |
| **Protokol IP** |  |  |
| IP alias (více IP sítí na jednom rozhraní) | Ano |  |
| QoS | Ano |  |
| DHCP relay | Ano |  |
| **Protokol IPv6** |  |  |
| IPv6 ACL | Ano |  |
| IPv6 QoS | Ano |  |
| IPv6 services ( DNS, SSH, Syslog, ICMP) | Ano |  |
| HTTP, SNMP over IPv6 | Ano |  |
| RADIUS, TACACS+ over IPv6 | Ano |  |
| IPv6 MLDv2 snooping | Ano |  |
| IPv6 Port ACL | Ano |  |
| IPv6 First Hop Security RA guard | Ano |  |
| IPv6 First Hop Security DHCPv6 guard | Ano |  |
| IPv6 First Hop Security IPv6 Binding Integrity Guard | Ano |  |
| **Směrovací protokoly** |  |  |
| Statické směrování | Ano |  |
| OSPF s podporou minimálně 2000 směrovacích informací | Ano |  |
| **Směrování multicastu** |  |  |
| IGMPv2 snooping | Ano |  |
| IGMPv3 snooping | Ano |  |
| IPv6 MLDv1 & v2 snooping | Ano |  |
| Multicast ( PIM SSM, PIM SM) | Ano |  |
| **Bezpečnost** |  |  |
| ACL na rozhraní IN/OUT | Ano |  |
| ACL pro IP | Ano |  |
| ACL pro ethernetové rámce | Ano |  |
| IPv6 ACL | Ano |  |
| Možnost definovat povolené MAC adresy na portu | Ano |  |
| Možnost definovat maximální počet MAC adres na portu | Ano |  |
| Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy) | Ano |  |
| DHCP snooping | Ano |  |
| Dynamic ARP inspection (DAI) | Ano |  |
| Verifikace mapování IP-MAC (např. IP source guard) | Ano |  |
| Ochrana centrálního procesoru (control plane) před útoky typu DoS | Ano |  |
| IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu | Ano |  |
| IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači | Ano |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) | Ano |  |
| Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x) | Ano |  |
| **Podpora koncových zařízení** |  |  |
| EEE (IEEE 802.3az) | Ano |  |
| **Management** |  |  |
| CLI rozhraní | Ano |  |
| SSHv2 | Ano |  |
| SSHv2 over IPv6 | Ano |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | Ano |  |
| SNMPv2 a v3 | Ano |  |
| USB anebo sériová konzolová linka | Ano |  |
| 10/100 management out-of-band port | Ano |  |
| DNS klient | Ano |  |
| NTP klient s MD5 autentizací | Ano |  |
| RADIUS klient pro AAA (autentizace, autorizace, accounting) | Ano |  |
| TACACS+ klient | Ano |  |
| Port mirroring (SPAN) | Ano |  |
| Port mirroring 1 -> 1 | Ano |  |
| Port mirroring N -> 1 | Ano |  |
| Port mirroring ACL (mirroruje pouze definované toky) | Ano |  |
| Vzdálený port mirroring ERSPAN | Ano |  |
| Syslog | Ano |  |
| Měření zakončení a délky metalického kabelu (TDR) | Ano |  |
| Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů) | Ano |  |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | Ano |  |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů | Ano |  |
| Součástí každého přepínače musí být licence pro jeho centrální správu a monitoring pomocí cloud management nástroje od výrobce přepínače | Ano |  |
| Application Visibility - Monitorování aplikačních toků prostřednictvím technologie NetFlow nebo IPFIX | Ano |  |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | Ano |  |
| Podpora skripování v jazyce Python – lokální interpret jazyka v přepínači | Ano |  |
| Interní úložiště dat pro sběr provozních dat a pokročilou dignostiku zařízení: min. 4 GB | Ano |  |
| Podpora L3 routed port | Ano |  |
| Podpora Radius over TLS (RadSec) | Ano |  |
| Podpora TPM nebo HW trusted modulů | Ano |  |
| LACP Fallback (např. pro PXE boot) | Ano |  |
| Min. velikost sdíleného systémového bufferu: 6 MB | Ano |  |
| Multicast DNS (mDNS) gateway | Ano |  |
| Je-li součástí přepínače časově omezená licence (subscription), musí být tato minimálně na 5 let | Ano |  |

## Typ 5 + Typ 7 – 6 kusů

|  |  |
| --- | --- |
| **Konkrétní specifikace nabízeného zboží** | |
| Model – typové/výrobní označení: |  |
| Výrobce: |  |

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje**  **[Ano/Ne]** |
| **Základní vlastnosti** |  |  |
| Třída zařízení: přepínač | Ano |  |
| Formát zařízení do racku | Ano |  |
| Velikost zařízení: 1U | Ano |  |
| Stohovatelný | Ano |  |
| Počet 10/100/1000 Mbit/s metalických portů | 24 x RJ45 |  |
| Počet portů 10 Gbit/s a jejich typ | 4x SFP+ |  |
| Všechny produkční ethernet porty jsou dostupné zepředu | Ano |  |
| Podpora PoE+ dle standardu 802.3at | 24 portů |  |
| Dostupný výkon pro PoE+ napájení | 740 W |  |
| **Výkonnostní parametry** |  |  |
| Minimální paketový výkon přepínače v paketech/vteřinu | 90 milionu |  |
| Rychlost stohovacího propojení | alespoň 40 Gbit/s |  |
| **Vlastnosti stohování** |  |  |
| Minimální počet přepínačů ve stohu | 8 |  |
| Automatická kontrola a sjednocení verze software přepínačů ve stohu | Ano |  |
| Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením | Ano |  |
| Seskupení portů (IEEE 802.3ad) mezi různými prvky stohu | Ano |  |
| Redundance řídícího prvku v rámci stohu | Ano |  |
| Minimální počet MAC adres | 32 000 |  |
| **Protokoly fyzické vrstvy** |  |  |
| IEEE 802.3-2005 | Ano |  |
| IEEE 802.3ad | Ano |  |
| Podpora "jumbo rámců" | Ano |  |
| **Protokoly 2. vrstvy** |  |  |
| IEEE 802.1D | Ano |  |
| IEEE 802.1Q | Ano |  |
| Minimální počet aktivních VLAN | 2000 |  |
| IEEE 802.1X - Port Based Network Access Control | Ano |  |
| IEEE 802.1s - multiple spanning trees | Ano |  |
| IEEE 802.1w - Rapid Tree Spanning Protocol | Ano |  |
| IEEE 802.1p - Minimální počet vnitřních front | 8 |  |
| Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní | Ano |  |
| Detekce protilehlého zařízení (např. CDP, LLDP) | Ano |  |
| Detekce parametrů protilehlého zařízení (např. LLDP-MED) | Ano |  |
| Protokol pro definici šířených VLAN (MVRP nebo VTP) | Ano |  |
| Detekce jednosměrnosti optické linky (např. UDLD) | Ano |  |
| STP root guard | Ano |  |
| STP loop guard | Ano |  |
| Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard) | Ano |  |
| Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech | Ano |  |
| **Protokol IP** |  |  |
| IP alias (více IP sítí na jednom rozhraní) | Ano |  |
| QoS | Ano |  |
| DHCP relay | Ano |  |
| **Protokol IPv6** |  |  |
| IPv6 ACL | Ano |  |
| IPv6 QoS | Ano |  |
| IPv6 services ( DNS, SSH, Syslog, ICMP) | Ano |  |
| HTTP, SNMP over IPv6 | Ano |  |
| RADIUS, TACACS+ over IPv6 | Ano |  |
| IPv6 MLDv2 snooping | Ano |  |
| IPv6 Port ACL | Ano |  |
| IPv6 First Hop Security RA guard | Ano |  |
| IPv6 First Hop Security DHCPv6 guard | Ano |  |
| IPv6 First Hop Security IPv6 Binding Integrity Guard | Ano |  |
| **Směrovací protokoly** |  |  |
| Statické směrování | Ano |  |
| OSPF s podporou minimálně 2000 směrovacích informací | Ano |  |
| **Směrování multicastu** |  |  |
| IGMPv2 snooping | Ano |  |
| IGMPv3 snooping | Ano |  |
| IPv6 MLDv1 & v2 snooping | Ano |  |
| Multicast ( PIM SSM, PIM SM) | Ano |  |
| **Bezpečnost** |  |  |
| ACL na rozhraní IN/OUT | Ano |  |
| ACL pro IP | Ano |  |
| ACL pro ethernetové rámce | Ano |  |
| IPv6 ACL | Ano |  |
| Možnost definovat povolené MAC adresy na portu | Ano |  |
| Možnost definovat maximální počet MAC adres na portu | Ano |  |
| Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy) | Ano |  |
| DHCP snooping | Ano |  |
| Dynamic ARP inspection (DAI) | Ano |  |
| Verifikace mapování IP-MAC (např. IP source guard) | Ano |  |
| Ochrana centrálního procesoru (control plane) před útoky typu DoS | Ano |  |
| IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu | Ano |  |
| IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači | Ano |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) | Ano |  |
| Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x) | Ano |  |
| **Podpora koncových zařízení** |  |  |
| EEE (IEEE 802.3az) | Ano |  |
| **Management** |  |  |
| CLI rozhraní | Ano |  |
| SSHv2 | Ano |  |
| SSHv2 over IPv6 | Ano |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | Ano |  |
| SNMPv2 a v3 | Ano |  |
| USB anebo sériová konzolová linka | Ano |  |
| 10/100 management out-of-band port | Ano |  |
| DNS klient | Ano |  |
| NTP klient s MD5 autentizací | Ano |  |
| RADIUS klient pro AAA (autentizace, autorizace, accounting) | Ano |  |
| TACACS+ klient | Ano |  |
| Port mirroring (SPAN) | Ano |  |
| Port mirroring 1 -> 1 | Ano |  |
| Port mirroring N -> 1 | Ano |  |
| Port mirroring ACL (mirroruje pouze definované toky) | Ano |  |
| Vzdálený port mirroring ERSPAN | Ano |  |
| Syslog | Ano |  |
| Měření zakončení a délky metalického kabelu (TDR) | Ano |  |
| Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů) | Ano |  |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | Ano |  |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů | Ano |  |
| Součástí každého přepínače musí být licence pro jeho centrální správu a monitoring pomocí cloud management nástroje od výrobce přepínače | Ano |  |
| Application Visibility - Monitorování aplikačních toků prostřednictvím technologie NetFlow nebo IPFIX | Ano |  |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | Ano |  |
| Podpora skripování v jazyce Python – lokální interpret jazyka v přepínači | Ano |  |
| Interní úložiště dat pro sběr provozních dat a pokročilou dignostiku zařízení: min. 4 GB | Ano |  |
| Podpora L3 routed port | Ano |  |
| Podpora Radius over TLS (RadSec) | Ano |  |
| Podpora TPM nebo HW trusted modulů | Ano |  |
| LACP Fallback (např. pro PXE boot) | Ano |  |
| Min. velikost sdíleného systémového bufferu: 6 MB | Ano |  |
| Multicast DNS (mDNS) gateway | Ano |  |
| Je-li součástí přepínače časově omezená licence (subscription), musí být tato minimálně na 5 let | Ano |  |

## Typ 6 – 6 kusů

|  |  |
| --- | --- |
| **Konkrétní specifikace nabízeného zboží** | |
| Model – typové/výrobní označení: |  |
| Výrobce: |  |

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje**  **[Ano/Ne]** |
| **Základní vlastnosti** |  |  |
| Třída zařízení: přepínač | Ano |  |
| Formát zařízení do racku | Ano |  |
| Velikost zařízení: 1U | Ano |  |
| Stohovatelný | Ano |  |
| Počet 10/100/1000 Mbit/s metalických portů | 48 x RJ45 |  |
| Počet portů 10 Gbit/s a jejich typ | 4x SFP+ |  |
| Všechny produkční ethernet porty jsou dostupné zepředu | Ano |  |
| **Výkonnostní parametry** |  |  |
| Minimální paketový výkon přepínače v paketech/vteřinu | 130 milionu |  |
| Rychlost stohovacího propojení | alespoň 40 Gbit/s |  |
| **Vlastnosti stohování** |  |  |
| Minimální počet přepínačů ve stohu | 8 |  |
| Automatická kontrola a sjednocení verze software přepínačů ve stohu | Ano |  |
| Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením | Ano |  |
| Seskupení portů (IEEE 802.3ad) mezi různými prvky stohu | Ano |  |
| Redundance řídícího prvku v rámci stohu | Ano |  |
| IEEE 802.1ae na min. 2 uplink portech | Ano |  |
| Minimální počet MAC adres | 32 000 |  |
| **Protokoly fyzické vrstvy** |  |  |
| IEEE 802.3-2005 | Ano |  |
| IEEE 802.3ad | Ano |  |
| Podpora "jumbo rámců" | Ano |  |
| **Protokoly 2. vrstvy** |  |  |
| IEEE 802.1D | Ano |  |
| IEEE 802.1Q | Ano |  |
| Minimální počet aktivních VLAN | 2000 |  |
| IEEE 802.1X - Port Based Network Access Control | Ano |  |
| IEEE 802.1s - multiple spanning trees | Ano |  |
| IEEE 802.1w - Rapid Tree Spanning Protocol | Ano |  |
| IEEE 802.1p - Minimální počet vnitřních front | 8 |  |
| Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní | Ano |  |
| Detekce protilehlého zařízení (např. CDP, LLDP) | Ano |  |
| Detekce parametrů protilehlého zařízení (např. LLDP-MED) | Ano |  |
| Protokol pro definici šířených VLAN (MVRP nebo VTP) | Ano |  |
| Detekce jednosměrnosti optické linky (např. UDLD) | Ano |  |
| STP root guard | Ano |  |
| STP loop guard | Ano |  |
| Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard) | Ano |  |
| Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech | Ano |  |
| **Protokol IP** |  |  |
| IP alias (více IP sítí na jednom rozhraní) | Ano |  |
| QoS | Ano |  |
| DHCP relay | Ano |  |
| **Protokol IPv6** |  |  |
| IPv6 ACL | Ano |  |
| IPv6 QoS | Ano |  |
| IPv6 services ( DNS, SSH, Syslog, ICMP) | Ano |  |
| HTTP, SNMP over IPv6 | Ano |  |
| RADIUS, TACACS+ over IPv6 | Ano |  |
| IPv6 MLDv2 snooping | Ano |  |
| IPv6 Port ACL | Ano |  |
| IPv6 First Hop Security RA guard | Ano |  |
| IPv6 First Hop Security DHCPv6 guard | Ano |  |
| IPv6 First Hop Security IPv6 Binding Integrity Guard | Ano |  |
| **Směrovací protokoly** |  |  |
| Statické směrování | Ano |  |
| OSPF s podporou minimálně 2000 směrovacích informací | Ano |  |
| **Směrování multicastu** |  |  |
| IGMPv2 snooping | Ano |  |
| IGMPv3 snooping | Ano |  |
| IPv6 MLDv1 & v2 snooping | Ano |  |
| Multicast ( PIM SSM, PIM SM) | Ano |  |
| **Bezpečnost** |  |  |
| ACL na rozhraní IN/OUT | Ano |  |
| ACL pro IP | Ano |  |
| ACL pro ethernetové rámce | Ano |  |
| IPv6 ACL | Ano |  |
| Možnost definovat povolené MAC adresy na portu | Ano |  |
| Možnost definovat maximální počet MAC adres na portu | Ano |  |
| Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy) | Ano |  |
| DHCP snooping | Ano |  |
| Dynamic ARP inspection (DAI) | Ano |  |
| Verifikace mapování IP-MAC (např. IP source guard) | Ano |  |
| Ochrana centrálního procesoru (control plane) před útoky typu DoS | Ano |  |
| IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu | Ano |  |
| IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači | Ano |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) | Ano |  |
| Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x) | Ano |  |
| **Podpora koncových zařízení** |  |  |
| EEE (IEEE 802.3az) | Ano |  |
| **Management** |  |  |
| CLI rozhraní | Ano |  |
| SSHv2 | Ano |  |
| SSHv2 over IPv6 | Ano |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | Ano |  |
| SNMPv2 a v3 | Ano |  |
| USB anebo sériová konzolová linka | Ano |  |
| 10/100 management out-of-band port | Ano |  |
| DNS klient | Ano |  |
| NTP klient s MD5 autentizací | Ano |  |
| RADIUS klient pro AAA (autentizace, autorizace, accounting) | Ano |  |
| TACACS+ klient | Ano |  |
| Port mirroring (SPAN) | Ano |  |
| Port mirroring 1 -> 1 | Ano |  |
| Port mirroring N -> 1 | Ano |  |
| Port mirroring ACL (mirroruje pouze definované toky) | Ano |  |
| Vzdálený port mirroring ERSPAN | Ano |  |
| Syslog | Ano |  |
| Měření zakončení a délky metalického kabelu (TDR) | Ano |  |
| Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů) | Ano |  |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | Ano |  |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů | Ano |  |
| Součástí každého přepínače musí být licence pro jeho centrální správu a monitoring pomocí cloud management nástroje od výrobce přepínače | Ano |  |
| Application Visibility - Monitorování aplikačních toků prostřednictvím technologie NetFlow nebo IPFIX | Ano |  |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | Ano |  |
| Podpora skripování v jazyce Python – lokální interpret jazyka v přepínači | Ano |  |
| Interní úložiště dat pro sběr provozních dat a pokročilou dignostiku zařízení: min. 4 GB | Ano |  |
| Podpora L3 routed port | Ano |  |
| Podpora Radius over TLS (RadSec) | Ano |  |
| Podpora TPM nebo HW trusted modulů | Ano |  |
| LACP Fallback (např. pro PXE boot) | Ano |  |
| Min. velikost sdíleného systémového bufferu: 6 MB | Ano |  |
| Multicast DNS (mDNS) gateway | Ano |  |
| Je-li součástí přepínače časově omezená licence (subscription), musí být tato minimálně na 5 let | Ano |  |

## Typ 8 – 2 kusy

|  |  |
| --- | --- |
| **Konkrétní specifikace nabízeného zboží** | |
| Model – typové/výrobní označení: |  |
| Výrobce: |  |

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje**  **[Ano/Ne]** |
| **Základní vlastnosti** |  |  |
| Třída zařízení: přepínač | Ano |  |
| Formát zařízení do racku | Ano |  |
| Velikost zařízení: 1U | Ano |  |
| Stohovatelný | Ano |  |
| Počet 10/100/1000 Mbit/s metalických portů | 48 x RJ45 |  |
| Počet portů 10 Gbit/s a jejich typ | 4x SFP+ |  |
| Všechny produkční ethernet porty jsou dostupné zepředu | Ano |  |
| Podpora PoE+ dle standardu 802.3at | 48 portů |  |
| Dostupný výkon pro PoE+ napájení | 740 W |  |
| **Výkonnostní parametry** |  |  |
| Minimální paketový výkon přepínače v paketech/vteřinu | 130 milionu |  |
| Rychlost stohovacího propojení | alespoň 40 Gbit/s |  |
| **Vlastnosti stohování** |  |  |
| Minimální počet přepínačů ve stohu | 8 |  |
| Automatická kontrola a sjednocení verze software přepínačů ve stohu | Ano |  |
| Možnost předkonfigurace neexistujícího přepínače ve stohu před jeho připojením | Ano |  |
| Seskupení portů (IEEE 802.3ad) mezi různými prvky stohu | Ano |  |
| Redundance řídícího prvku v rámci stohu | Ano |  |
| IEEE 802.1ae na min. 2 uplink portech | Ano |  |
| Minimální počet MAC adres | 32 000 |  |
| **Protokoly fyzické vrstvy** |  |  |
| IEEE 802.3-2005 | Ano |  |
| IEEE 802.3ad | Ano |  |
| Podpora "jumbo rámců" | Ano |  |
| **Protokoly 2. vrstvy** |  |  |
| IEEE 802.1D | Ano |  |
| IEEE 802.1Q | Ano |  |
| Minimální počet aktivních VLAN | 2000 |  |
| IEEE 802.1X - Port Based Network Access Control | Ano |  |
| IEEE 802.1s - multiple spanning trees | Ano |  |
| IEEE 802.1w - Rapid Tree Spanning Protocol | Ano |  |
| IEEE 802.1p - Minimální počet vnitřních front | 8 |  |
| Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní | Ano |  |
| Detekce protilehlého zařízení (např. CDP, LLDP) | Ano |  |
| Detekce parametrů protilehlého zařízení (např. LLDP-MED) | Ano |  |
| Protokol pro definici šířených VLAN (MVRP nebo VTP) | Ano |  |
| Detekce jednosměrnosti optické linky (např. UDLD) | Ano |  |
| STP root guard | Ano |  |
| STP loop guard | Ano |  |
| Možnost autorecovery po chybovém stavu (UDLD, root guard, loop guard) | Ano |  |
| Multicast/broadcast storm control - hardwarové omezení poměru unicast/multicast rámců na portu v procentech | Ano |  |
| **Protokol IP** |  |  |
| IP alias (více IP sítí na jednom rozhraní) | Ano |  |
| QoS | Ano |  |
| DHCP relay | Ano |  |
| **Protokol IPv6** |  |  |
| IPv6 ACL | Ano |  |
| IPv6 QoS | Ano |  |
| IPv6 services ( DNS, SSH, Syslog, ICMP) | Ano |  |
| HTTP, SNMP over IPv6 | Ano |  |
| RADIUS, TACACS+ over IPv6 | Ano |  |
| IPv6 MLDv2 snooping | Ano |  |
| IPv6 Port ACL | Ano |  |
| IPv6 First Hop Security RA guard | Ano |  |
| IPv6 First Hop Security DHCPv6 guard | Ano |  |
| IPv6 First Hop Security IPv6 Binding Integrity Guard | Ano |  |
| **Směrovací protokoly** |  |  |
| Statické směrování | Ano |  |
| OSPF s podporou minimálně 2000 směrovacích informací | Ano |  |
| **Směrování multicastu** |  |  |
| IGMPv2 snooping | Ano |  |
| IGMPv3 snooping | Ano |  |
| IPv6 MLDv1 & v2 snooping | Ano |  |
| Multicast ( PIM SSM, PIM SM) | Ano |  |
| **Bezpečnost** |  |  |
| ACL na rozhraní IN/OUT | Ano |  |
| ACL pro IP | Ano |  |
| ACL pro ethernetové rámce | Ano |  |
| IPv6 ACL | Ano |  |
| Možnost definovat povolené MAC adresy na portu | Ano |  |
| Možnost definovat maximální počet MAC adres na portu | Ano |  |
| Možnost definovat různé chování při překročení počtu MAC adres na portu (zablokování portu, blokování nové MAC adresy) | Ano |  |
| DHCP snooping | Ano |  |
| Dynamic ARP inspection (DAI) | Ano |  |
| Verifikace mapování IP-MAC (např. IP source guard) | Ano |  |
| Ochrana centrálního procesoru (control plane) před útoky typu DoS | Ano |  |
| IEEE 802.1x autentizace i autorizace více koncových zařízení na jednom portu | Ano |  |
| IEEE 802.1x autentizace přepínače vůči nadřazenému přepínači | Ano |  |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou) | Ano |  |
| Ověřování dle IEEE 802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení 802.1x) | Ano |  |
| **Podpora koncových zařízení** |  |  |
| EEE (IEEE 802.3az) | Ano |  |
| **Management** |  |  |
| CLI rozhraní | Ano |  |
| SSHv2 | Ano |  |
| SSHv2 over IPv6 | Ano |  |
| Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL | Ano |  |
| SNMPv2 a v3 | Ano |  |
| USB anebo sériová konzolová linka | Ano |  |
| 10/100 management out-of-band port | Ano |  |
| DNS klient | Ano |  |
| NTP klient s MD5 autentizací | Ano |  |
| RADIUS klient pro AAA (autentizace, autorizace, accounting) | Ano |  |
| TACACS+ klient | Ano |  |
| Port mirroring (SPAN) | Ano |  |
| Port mirroring 1 -> 1 | Ano |  |
| Port mirroring N -> 1 | Ano |  |
| Port mirroring ACL (mirroruje pouze definované toky) | Ano |  |
| Vzdálený port mirroring ERSPAN | Ano |  |
| Syslog | Ano |  |
| Měření zakončení a délky metalického kabelu (TDR) | Ano |  |
| Uživatelsky modifikovatelná automatická reakce/obsluhy událostí při provozu přepínače (pomocí skriptů) | Ano |  |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | Ano |  |
| Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů | Ano |  |
| Součástí každého přepínače musí být licence pro jeho centrální správu a monitoring pomocí cloud management nástroje od výrobce přepínače | Ano |  |
| Application Visibility - Monitorování aplikačních toků prostřednictvím technologie NetFlow nebo IPFIX | Ano |  |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | Ano |  |
| Podpora skripování v jazyce Python – lokální interpret jazyka v přepínači | Ano |  |
| Interní úložiště dat pro sběr provozních dat a pokročilou dignostiku zařízení: min. 4 GB | Ano |  |
| Podpora L3 routed port | Ano |  |
| Podpora Radius over TLS (RadSec) | Ano |  |
| Podpora TPM nebo HW trusted modulů | Ano |  |
| LACP Fallback (např. pro PXE boot) | Ano |  |
| Min. velikost sdíleného systémového bufferu: 6 MB | Ano |  |
| Multicast DNS (mDNS) gateway | Ano |  |
| Je-li součástí přepínače časově omezená licence (subscription), musí být tato minimálně na 5 let | Ano |  |

1.03.Bezdrátová infrastruktura

## Přístupové body bezdrátové sítě (AP) - 299 kusů

|  |  |
| --- | --- |
| **Konkrétní specifikace nabízeného zboží** | |
| Model – typové/výrobní označení: |  |
| Výrobce: |  |

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje**  **[Ano/Ne]** |
| **Základní vlastnosti** |  |  |
| Indoor přístupový bod | Ano |  |
| Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax, 802.11be | Ano |  |
| Certifikace Wi-Fi Aliance: Wi-Fi CERTIFIED a, b, g, n, ac, 6, 7, WPA3-Enterprise, Enhanced Open (OWE) | Ano |  |
| Pracovní režim: samostatný AP | Ano |  |
| Pracovní režim: AP řízený prostřednictvím cloudového kontroléru | Ano |  |
| Minimální počet portů ethernet LAN: 1x 100/1000/2500 Mbit/s RJ45 | Ano |  |
| Podpora napájení prostřednictvím PoE dle standardu IEEE 802.3at | Ano |  |
| Rozsah provozních teplot 0° až +40°C | Ano |  |
| Vestavěná interní anténa MIMO, omni down-tilt | Ano |  |
| Radiová část: tri-band, podpora pásem 2,4 GHz 5 GHz a 6 GHz | Ano |  |
| Minimální MIMO a počet spatial stream: 2x2:2 | Ano |  |
| Podpora TWT, BSS Coloring a až 160 MHz kanál | Ano |  |
| HW podpora OFDMA | Ano |  |
| Možnost nastavení vysílacího výkonu s krokem 0.5 dBm | Ano |  |
| Max data rate: 2400 Mbit/s pro 6GHz, 1200 Mbit/s pro 5GHz a 300 Mbit/s pro 2,4GHz | Ano |  |
| Minimálně 16 inzerovaných BSSID na rádio | Ano |  |
| Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP | Ano |  |
| Integrovaný TPM pro bezpečné uložení certifikátů | Ano |  |
| USB port | Ano |  |
| Indikační LED diody informující o stavu zařízení | Ano |  |
| Automatická detekce Rogue AP | Ano |  |
| Hardware filtry proti intermodulačnímu rušením z mobilních sítí (Advanced Cellular Coexistence nebo obdobné) | Ano |  |
| Součástí každého přístupového bodu bezdrátové sítě e musí být licence pro jeho centrální správu pomocí cloud management nástroje - včetně funkce centrálního řídícího systému Wi-Fi – kontroléru přístupových bodů | Ano |  |
| Zero touch provisioning (ZTP) pomocí management software | Ano |  |
| Integrované Bluetooth 5.4 rádio | Ano |  |
| Integrované Zigbee 802.15.4 rádio | Ano |  |
| Podpora režimu SLEEP s max. spotřebou energie do 3,5 W | Ano |  |
| Součástí AP je příslušenství pro montáž na zeď nebo strop | Ano |  |
| Je-li součástí přepínače časově omezená licence (subscription), musí být tato minimálně na 5 let | Ano |  |

1.04.Specifikace AAA server

Předmětem dodávky je software pro řízení přístupu zařízení a uživatelů do počítačové sítě nemocnice   
a to jak v části LAN, tak i WLAN, který bude splňovat minimální požadavky uvedeny níže. Software může být ve formě HW appliance anebo SW image pro virtualizaci v prostředí VMware, Hyper-V nebo KVM. Zadavatel požaduje 1 ks licence na funkce popsané níže. Funkce musí být dostupné pro všechny prvky zadavatele bez omezení.

|  |  |
| --- | --- |
| **Konkrétní specifikace nabízeného zboží** | |
| Model – typové/výrobní označení: |  |
| Výrobce: |  |

|  |  |  |
| --- | --- | --- |
| **Požadavek na funkcionalitu** | **Minimální požadavky** | **Splňuje**  **[Ano/Ne]** |
| **Třída zařízení** | **SW nebo HW appliance** |  |
| On premise řešení pro externí captive portál pro pacienty a návštěvy a jejich rozšířenou autentizaci (pro 1000 hostů) | Ano |  |
| Appliance bez nutnosti dodatečných licencí např. pro OS nebo databáze | Ano |  |
| Podpora 802.1X autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN | Ano |  |
| Podpora minimálně pro 5000 současně autentizovaných zařízení (pomocí 802.1X) s možností vytváření clusterů více virtuálních instancí. Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance. Cluster podporuje active-active režim pro ověřování. | Ano |  |
| Podpora RADIUS CoA podle RFC3576 | Ano |  |
| Platforma podporuje změnu autorizačního stavu zařízení bez nutnosti změny definice autorizační politiky, např. pro odpojení nebo karanténu koncových zařízení. | Ano |  |
| Podpora minimálně následujících metod autentizace: PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace | Ano |  |
| Podpora TACACS+ autentizace správců síťových zařízení | Ano |  |
| Využití dalších možností autentizace a autorizace. Minimálně: LDAP, MS AD, Token, MAC auth, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta) | Ano |  |
| Podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v Active Directory | Ano |  |
| Možnost autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. za účelem omezení celkového času online či objemu přenesených dat za delší časové období | Ano |  |
| Možnost integrace s MDM (Mobile Device Management) platformami třetích stran (minimálně AirWatch, Citrix, MobileIron, JAMF) | Ano |  |
| Podpora REST API pro většinu základních úkonů AAA platforma | Ano |  |
| Podpora REST volání vyvolaného autentizační či autorizační událostí (minimálně pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.) | Ano |  |
| Zpracovávání syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení ze stávajícího firewallu Checkpoint a izolace konkrétního klienta na základě tohoto hlášení. | Ano |  |
| Zpracovávání syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení. | Ano |  |
| Administrátor systému musí mít možnost vlastní tvorby parseru/integrace syslog hlášení pro možnost uživatelské integrace s libovolnými systémy třetích stran. | Ano |  |
| Sběr dodatečných informací o připojených zařízeních (“profiling”) jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě. | Ano |  |
| Platforma obsahuje funkci otestovat autentizační politiky, včetně flexibilní volby typu autentizace, atributů klienta, atd. | Ano |  |
| Možnost registrace zařízení pomocí MAC adresy pro non-IT uživatele - omezená funkce administračního rozhraní, se zařazením zařízení do skupiny s definovanou politikou přístupu. | Ano |  |
| Podpora autentizace  pomocí účtů sociálních sítí – Google, Google Plus, Facebook, Facebook WIFI, Twitter, LinkedIn, Microsoft | Ano |  |
| Podpora autentizace lokálními účty v rámci portálu, ověření pomocí jméno+heslo, autetizační kód | Ano |  |
| Možnost samoobslužné registrace hosta do sítě s SMS a email ověřením | Ano |  |
| Přístup zdarma pouze s akceptací podmínek užití | Ano |  |
| arify lze omezit časově, z hlediska rychlosti připojení či objemu přenesených dat | Ano |  |
| Vynucení odpojení zařízení ihned po naplnění jakéhokoliv z limitů | Ano |  |
| Perzistence autentizace/registrace skrze MAC caching a zobrazení už jen uvítacích stránek s osobním oslovením hosta při dalších návštěvách | Ano |  |
| Možnost vytváření účtů samoobslužnou registrací | Ano |  |
| Možnost provozovat více graficky i obsahově unikátních portálů v rámci jedné instalace | Ano |  |
| Redakční systém pro plnou grafickou a obsahovou úpravu jednotlivých captive portálů umožňuje  o   Uprava barev, fontů, pozadí a loga  o   Úprava registračních formulářů – přidávání a odebírání polí pro vstupní data formuláře včetně validace vkládaného obsahu  o   Možnost vkládání animací, videí a dalšího dynamického obsahu  o   Vytváření specifických stránek pro různé typy zařízení a operačních systémů (např. pro efektivní navedení do specifického app store) | Ano |  |

1.05.FW a vzdálený přístup (VPN)

## NGFW – 2 kusy – lokalita Kyjov

|  |  |
| --- | --- |
| **Konkrétní specifikace nabízeného zboží** | |
| Model – typové/výrobní označení: |  |
| Výrobce: |  |

**Minimální požadavky na NGFW**

* HW appliance o velikosti 1 RU
* Podpora režimu vysoké dostupnosti (active/passive, active/active)
* Správa zařízení pracujících v režimu vysoké dostupnosti musí probíhat prostřednictvím jednoho konfiguračního rozhraní
* Grafické konfigurační rozhraní a příkazový řádek
* Zařízení musí mít minimálně následující portovou kapacitu:

|  |  |  |
| --- | --- | --- |
| **Typy portů** | **Minimální požadavek** | **Splňuje**  **[Ano/Ne]** |
| 1 GbE Copper | Min. 16 |  |
| 2.5 GbE Copper | Min. 2 |  |
| 1 GbE SFP | Min. 8 |  |
| 10 GbE SFP+ | Min. 4 |  |
| USB 3.0 Type A | Min. 2 |  |

**Minimální výkonové požadavky**

* Firewall propustnost minimálně 35 Gbps
* Propustnost Threat Prevention (Enterprise Mix, Firewall, IPS/IDS, Aplikační kontrola, Antivir, Botnet), minimálně 4 Gbps
* Propustnost NGFW (Enterprise Mix, Firewall, IPS, Aplikační kontrola), minimálně 12 Gbps
* Propustnost IPS (Enterprise Mix), minimálně 17 Gbps
* Počet nových spojení za vteřinu minimálně 130 000
* Počet současných spojení, min. 4 000 000

**Funkční požadavky**

* Firewall, Antispam, AntiBot, Antivirus, Aplikační kontrola, URL filtering, Cloud Sandboxing, Zabezpečení DNS, Inspekce HTTPS, Zero-phishing ochrana
* Lokální HDD, min 1x 240 GB SSD, v případě výpadku centrálního management log serveru
* Dodávaná firewall platforma musí být ve formě samostatné hardware appliance
* Instalace do standardního 19" kabinetu s originálním rack mount kitem, velikost 1U
* Podpora redundance dvou zařízení v režimu Active-Standby se stavovou synchronizací
* Podpora agregace fyzických portů LACP
* Podpora dual stack IPv4 a IPv6
* Předefinované Threat ochrany a profily pro IPS, Antivirus, Anti-botnet a Zero-day ochranu
* Minimální počet rozpoznávaných aplikací 6 000
* Podpora URL filteringu na základě předdefinovaných URL kategorií.
* Podpora explicitní HTTP/HTTPs proxy
* Možnost získávání identit uživatelů z AD bez nutnosti instalace software na AD servery
* Sdílení identit mezi jednotlivými firewally bez nutnosti externích komponent
* Ochrana proti SNI spoofing v rámci HTTPs inspekce
* Podpora S2S VPN, min. podpora algoritmů pro šifrování: AES-128, AES-256 a integritu: SHA-256 a AES-XCBC
* RA VPN terminace pro 200 souběžných spojení
* Ochrana proti neznámým hrozbám: emulace soborů ve virtuálním sandbox prostředí, min. podporované typy souborů: PowerPoint, Word, Excel, Pdf, exe, archivy (zip, tar, 7z, rar)
* Bezpečnostní logy musí být ukládány na fyzicky oddělenou management platformu.
* Počet publikovaných zranitelností OS (na základě CVE) firewall za poslední 3 roky, max. 15
* Řešení musí být uvedeno v Gartner Magic Quadrant for Enterprise Network Firewalls za roky 2020-2022 minimálně 1x v kvadrantu Leader
* Součástí dodávky bude veškeré příslušenství a propojovací prvky dle standardu zařízení a zákazníka.

Požadované výkonové a funkční parametry a uvedené minimální požadavky na NGFW je nutné doložit oficiálním produktovým listem výrobce.

**Jeden centrální management pro obě lokality umožňující napojení všech 4 ks dodávaných NGFW**

* Management musí být fyzicky oddělený od firewall platformy
* Jednotný centrální management: správa politik a analýza logů na jedné konsolidované virtuální appliance (Hyper-V, ESXi)
* Management musí ukládat a zpracovávat logy ze všech firewallů, objem logů za den min. 15 GB/den
* Management log server musí zpracovat min. 40 000 logů/sekundu
* Dlouhodobé ukládání historických log záznamů, min. interní kapacita úložiště 8TB
* Podpora administrátorských profilů pro delegaci oprávnění (čtení, zápis)
* Kontrola politik proti chybám a duplicitám
* Práce s bezpečnostními logy – možnost prohledávání všech typů logů (fw, ips, malware) s definováním vlastních permanentních filtrů.
* Integrovaný monitoring musí poskytovat grafické rozhraní pro sledování parametrů v reálnem čase a historii alespoň 30 dní (využití paměti, CPU, počet navázaných spojení, počet nově otevřených spojení za sekundu, propustnost, atd …).
* Podpora služby vlastní certifikační autority pro vydávaní PKI certifikátů pro bezpečné přihlašovaní uživatelů a administrátorů a pro VPN klientský přístup
* Je-li management licence omezena počtem řízených objektů bezpečnostních bran, musí podporovat řízení min. 4 objektů bran
* Je-li management licence omezena diskovou kapacitou, licence pro min. 8TB musí být součástí nabídky

## NGFW – 2 kusy – lokalita Veselí nad Moravou

|  |  |
| --- | --- |
| **Konkrétní specifikace nabízeného zboží** | |
| Model – typové/výrobní označení: |  |
| Výrobce: |  |

**Minimální požadavky na NGFW**

* HW appliance o velikosti 1 RU
* Podpora režimu vysoké dostupnosti (active/passive, active/active)
* Správa zařízení pracujících v režimu vysoké dostupnosti musí probíhat prostřednictvím jednoho konfiguračního rozhraní
* Grafické konfigurační rozhraní a příkazový řádek
* Zařízení musí mít minimálně následující portovou kapacitu:

|  |  |  |
| --- | --- | --- |
| **Typy portů** | **Minimální požadavek** | **Splňuje**  **[Ano/Ne]** |
| 1 GbE Copper | Min. 8 |  |
| 1 GbE SFP | Min. 1 |  |
| 10 GbE SFP+ | Min. 2 |  |
| USB 3.0 Type A | Min. 1 |  |

**Minimální výkonové požadavky**

* Firewall propustnost minimálně 15 Gbps
* Propustnost Threat Prevention (Enterprise Mix, Firewall, IPS/IDS, Aplikační kontrola, Antivir, Botnet), minimálně 3 Gbps
* Propustnost NGFW (Enterprise Mix, Firewall, IPS, Aplikační kontrola), minimálně 7 Gbps
* Propustnost IPS (Enterprise Mix), minimálně 11 Gbps
* Počet nových spojení za vteřinu minimálně 90 000
* Počet současných spojení, min. 2 000 000

**Funkční požadavky**

* Firewall, Antispam, AntiBot, Antivirus, Aplikační kontrola, URL filtering, Cloud Sandboxing, Zabezpečení DNS, Inspekce HTTPS, Zero-phishing ochrana
* Lokální HDD, min 1x 240 GB SSD, v případě výpadku centrálního management log serveru
* Dodávaná firewall platforma musí být ve formě samostatné hardware appliance
* Podpora redundance dvou zařízení v režimu Active-Standby se stavovou synchronizací
* Podpora agregace fyzických portů LACP
* Podpora dual stack IPv4 a IPv6
* Předefinované Threat ochrany a profily pro IPS, Antivirus, Anti-botnet a Zero-day ochranu
* Minimální počet rozpoznávaných aplikací 6 000
* Podpora URL filteringu na základě předdefinovaných URL kategorií.
* Podpora explicitní HTTP/HTTPs proxy
* Možnost získávání identit uživatelů z AD bez nutnosti instalace software na AD servery
* Sdílení identit mezi jednotlivými firewally bez nutnosti externích komponent
* Ochrana proti SNI spoofing v rámci HTTPs inspekce
* Podpora S2S VPN, min. podpora algoritmů pro šifrování: AES-128, AES-256 a integritu: SHA-256 a AES-XCBC
* RA VPN terminace pro 50 souběžných spojení
* Ochrana proti neznámým hrozbám: emulace soborů ve virtuálním sandbox prostředí, min. podporované typy souborů: PowerPoint, Word, Excel, Pdf, exe, archivy (zip, tar, 7z, rar)
* Bezpečnostní logy musí být ukládány na fyzicky oddělenou management platformu.
* Počet publikovaných zranitelností OS (na základě CVE) firewall za poslední 3 roky, max. 15
* Řešení musí být uvedeno v Gartner Magic Quadrant for Enterprise Network Firewalls za roky 2020-2022 minimálně 1x v kvadrantu Leader
* Součástí dodávky bude veškeré příslušenství a propojovací prvky dle standardu zařízení a zákazníka.

Požadované výkonové a funkční parametry a uvedené minimální požadavky na NGFW je nutné doložit oficiálním produktovým listem výrobce.

**Jeden centrální management pro obě lokality umožňující napojení všech 4 ks dodávaných NGFW**

* Management musí být fyzicky oddělený od firewall platformy
* Jednotný centrální management: správa politik a analýza logů na jedné konsolidované virtuální appliance (Hyper-V, ESXi)
* Management musí ukládat a zpracovávat logy ze všech firewallů, objem logů za den min. 15 GB/den
* Management log server musí zpracovat min. 40 000 logů/sekundu
* Dlouhodobé ukládání historických log záznamů, min. interní kapacita úložiště 8TB
* Podpora administrátorských profilů pro delegaci oprávnění (čtení, zápis)
* Kontrola politik proti chybám a duplicitám
* Práce s bezpečnostními logy – možnost prohledávání všech typů logů (fw, ips, malware) s definováním vlastních permanentních filtrů.
* Integrovaný monitoring musí poskytovat grafické rozhraní pro sledování parametrů v reálnem čase a historii alespoň 30 dní (využití paměti, CPU, počet navázaných spojení, počet nově otevřených spojení za sekundu, propustnost, atd …).
* Podpora služby vlastní certifikační autority pro vydávaní PKI certifikátů pro bezpečné přihlašovaní uživatelů a administrátorů a pro VPN klientský přístup
* Je-li management licence omezena počtem řízených objektů bezpečnostních bran, musí podporovat řízení min. 4 objektů bran
* Je-li management licence omezena diskovou kapacitou, licence pro min. 8TB musí být součástí nabídky

1.06.Monitoring datových toků (NDR)

|  |  |
| --- | --- |
| **Konkrétní specifikace nabízeného zboží** | |
| Model – typové/výrobní označení: |  |
| Výrobce: |  |

**Obecné vlastnosti řešení**

* Řešení musí umět identifikovat zero-day útoky (např. na základě behaviorální analýzy).
* Zpracovává **NetFlow/IPFIX** záznamy i **plný síťový provoz (Deep Packet Inspection – DPI)**.
* Umožňuje detailní pohled na to, **kdo, kdy, kam a kolik dat** v síti přenáší.
* Umí rozpoznávat **aplikace, protokoly a služby** i bez nutnosti dešifrování dat.
* Využívá strojové učení a behaviorální analýzu pro odhalování neobvyklého chování.
* Detekuje například:

malware komunikaci (C&C),

laterální pohyb útočníka v síti,

skenování portů a zranitelností,

neobvyklé objemy přenosů nebo časy aktivit.

* Umí identifikovat i zero-day útoky díky behaviorálnímu modelování.
* Podporuje standardní protokoly (NetFlow, IPFIX, Syslog, SNMP).
* Snadno se propojuje s firewally, SIEM systémy (např. Splunk, QRadar, ArcSight), nebo monitoringovými nástroji (např. Zabbix, PRTG).
* Může pracovat pasivně (bez zásahu do sítě).
* Nabízí intuitivní webové rozhraní s přehlednými dashboardy.
* Graficky zobrazuje topology, datové toky, hrozby a události.
* Umožňuje historickou analýzu provozu (zpětné dohledávání incidentů).
* Automaticky generuje reporty o bezpečnosti, provozu i SLA.

**HW - kolektor tokových dat se sondou**

Systém pro analýzu síťového provozu a bezpečnostní monitoring, který okamžitě identifikuje bezpečnostní rizika a události a který splňuje klíčové požadavky uvedené níže.

Při definici technických požadavků jsou všechny uvedené požadavky závazné. Je-li definice požadavku „umožňuje, lze, je možné, možnost, …“ je uvedený parametr závazný a požadovaná funkcionalita musí být v rámci Systému dodána/naimplementována a případně licencována. Tyto technické požadavky jsou minimální možné, Poskytovatel (dále také „dodavatel“) může nabídnout charakteristiky (funkce) lepší.

**Implementační služby**

Všechna dodavatelem instalovaná zařízení nebo komponenty musí být dodavatelem profesionálně nainstalovány a zprovozněny a po jejich nasazení řádně dokumentovány a otestovány, vč. prokázání, že tato zařízení plní všechny požadované a výkonnostní parametry.

Všechna dodavatelem instalovaná zařízení budou zabezpečena a nebudou obsahovat zjevná rizika a zranitelnosti, a to po celou dobu provozu služby.

Dodavatel zajistí vyladění a nastavení detekce všech dodávaných systémů tak, aby nebyly detekované nežádoucí a falešně pozitivní události. Tato činnost bude provedena ve spolupráci s kompetentními osobami zadavatele. Dodavatel zajistí integraci nástroje s aktuálním log managementem zadavatele, dále pak nastavení aktivních alertů a reportů dle potřeb zadavatele.

**Produktová podpora výrobce**

Dodavatel musí zajistit:

* softwarovou produktovou podporu řešení v délce 60 měsíců od podepsání akceptačního protokolu po předáním monitorovacího systému.
* záruku na veškerá dodaná HW zařízení minimálně v rozsahu 5 let NBD ode dne akceptace (Next Business Day) On-Site.

**Administrátorské školení**

V rámci realizace je požadováno administrátorské a uživatelské školení pro zaměstnance zadavatele v rozsahu nezbytném pro kvalifikovanou obsluhu včetně videozáznamu pro zpětné použití, který bude dostupný online na zabezpečeném úložišti dodavatele.

Dále je požadováno opakované proškolení uživatelů jednou ročně v rozsahu minimálně 1MD, včetně revize analýzy bezpečnostních událostí ve všech lokalitách.

**Minimální výkonové požadavky**

|  |  |
| --- | --- |
| **Minimální požadované funkcionality/vlastnosti** | **Splňuje**  **[Ano/Ne]** |
| **Systém pro analýzu síťového provozu** |  |
| Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění. |  |
| Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti. |  |
| Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection), nikoli pouze čísla portu. |  |
| Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších. |  |
| Systém musí být plně funkční v offline prostředí objednatele bez využití cloudového prostředí pro sběr, ukládání a zpracování dat a veškeré konfigurace a reporting jsou k dispozici přímo v systému. |  |
| Aktualizace systému musí být možné provádět uživatelsky v offline režimu. |  |
| **Zpracování a ukládání síťových toků** |  |
| Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku. |  |
| Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapouzdření. |  |
| Je požadováno vysokorychlostní úložiště pro uchování historie datových toků na dobu minimálně 90 dnů složené z NVMe disků. |  |
| **Analýza aplikačních a systémových logů** |  |
| Systém musí být schopen sbírat a analyzovat aplikační a systémové logy ve formátu syslog z dohledovaných zařízení a identifikovat nebezpečné nebo potenciálně škodlivé aktivity. |  |
| **Uživatelské rozhraní** |  |
| Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů. |  |
| Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně: |  |
| * granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute), |  |
| * granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute), |  |
| * vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů, |  |
| * vytváření vlastních uživatelských pohledů, reportů, dashboardů apod. |  |
| **Automatické hlášení (alerty) a reporting** |  |
| Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu. |  |
| Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní systému. |  |
| Systém musí mít možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.). |  |
| Je požadováno vytváření automatizovaných reportů v českém jazyce. |  |
| **Integrace systému** |  |
| Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez použití API systému, a to minimálně: |  |
| * syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat) |  |
| * přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní |  |
| * export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data) včetně aplikačních metadat alespoň pro protokoly HTTP, HTTPS a SMTP |  |
| * integrace s firewally, alespoň Fortinet a Checkpoint, pro automatické a manuální reakce vyvolané systémem |  |

**Požadavky na architekturu nasazení**

|  |  |
| --- | --- |
| **Minimální požadované funkcionality/vlastnosti** | **Splňuje**  **[Ano/Ne]** |
| **Obecné požadavky pro nasazení** |  |
| Pro všechny HW komponenty senzor a kolektor je požadován formát 1U serveru pro umístění do racku velikosti 19“. |  |
| Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap. |  |
| Pro všechny HW komponenty senzor a kolektor je požadováno samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku systému typu IPMI, IDRAC, ILO apod. |  |
| **Požadavky pro pokrytí IT prostředí** |  |
| Je požadován 1x HW datový kolektor/sensor o průměrné propustnosti minimálně 2Gbps pro alespoň 1500 hostů s monitorovacím rozhraním 2x10/25GE a 4x1GE.  Na zařízení je požadována dostupná historie dat minimálně 90 dnů zpětně, uložená na rychlém úložišti typu NVMe skládající se z minimálně 2 ks disků, každý disk o kapacitě alespoň 3,8 TB. Požadován je hardwarový RAID minimálně na úrovni RAID1 a osazení disků se schopností hot-swap. Datový sensor/kolektor musí být vybaven jedním procesorem v architektuře x86 s minimálně 12 fyzickými jádry a 24 vlákny a s podporou pamětí DDR5 s rychlostí 6400 MT/s. Datový sensor/kolektor osazen minimálně 128 GB operační paměti, vybavený kolejnicemi do racku a ramenem pro organizaci kabelů a s možností osazení celkem až 8 disků. Součástí dodávky bude veškeré příslušenství a propojovací prvky dle standardu zařízení a zákazníka. |  |

**Požadavky na schopnost detekce bezpečnostních událostí**

|  |  |
| --- | --- |
| **Minimální požadované funkcionality/vlastnosti** | **Splňuje**  **[Ano/Ne]** |
| **Monitorování zařízení, segmentů sítě a využívaných síťových služeb** |  |
| Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně: |  |
| * změna IP/MAC adresy hosta, |  |
| * duplicitní IP/MAC adresa, |  |
| * změna VLAN, |  |
| * vytvoření nové podsítě, |  |
| * připojení nového zařízení, |  |
| * použití nebo vznik nové služby, |  |
| * nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení, |  |
| * přístup nového zařízení ke službě či zařízení |  |
| * ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení. |  |
| Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním. |  |
| **Samostatné učení behaviorálních aktivit a detekce anomálií** |  |
| Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace. |  |
| Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro: |  |
| * odchylku od modelu pro přenos dat, toků a paketů, |  |
| * odchylku od modelu pro počet komunikačních partnerů, |  |
| * odchylku od modelu entropie na komunikačních portech, |  |
| * odchylku od modelu pro počet síťových toků a využitých síťových služeb, |  |
| * odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy). |  |
| Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy. |  |
| **Identifikace neznámých hrozeb a podezřelých chování** |  |
| Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování: |  |
| * průzkumné aktivity v síti, |  |
| * detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě, |  |
| * detekce repetitivních vzorců chování na síti, |  |
| * detekce botnetů a ovládání kompromitované stanice, |  |
| * detekce příznaků těžení kryptoměn, |  |
| * útoky hrubou silou a enumerace dat, |  |
| * rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely. |  |
| **Detekce na základě databáze známých hrozeb** |  |
| Systém musí být schopen identifikovat hrozby a reportovat události na základě |  |
| * detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik, |  |
| * reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů. |  |
| Uživatel musí být schopen importovat vlastní záznamy. |  |
| Systém musí využívat tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace. |  |
| Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc). |  |
| Uživatel musí být schopen prostřednictvím webové aplikace přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu bez nutnosti znalosti syntaxe a sémantiky pravidel.  Příklad možné syntaxe detekčního pravidla:  *alert tcp $HOME\_NET any -> any any (msg:”Command Shell Access”; content:”C:\\Users\\Administrator\\Desktop\\hfs2.3b”;)* |  |
| **Analýza šifrované komunikace** |  |
| Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb. |  |
| **Asistované učení** |  |
| Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů: |  |
| * IP adresa, |  |
| * MAC adresa, |  |
| * hostname, |  |
| * segment sítě / podsíť, |  |
| * lokalita – ASN, země, apod. |  |
| * směr komunikace – určení klienta, nebo serveru, |  |
| * detekovaná událost – kategorie, název apod. |  |
| * použité služby, protokolu, portu, |  |
| * libovolné kombinaci výše popsaných. |  |
| Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii. |  |

**Požadavky na zajištění síťové viditelnosti**

|  |  |
| --- | --- |
| **Minimální požadované funkcionality/vlastnosti** | **Splňuje**  **[Ano/Ne]** |
| **Vyhledávání, filtrování a vizualizace dat** |  |
| Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka. |  |
| Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně: |  |
| * podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN, |  |
| * prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not. |  |
| Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů. |  |
| Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách. |  |
| Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS.  Metadata jsou v tomto případě chápána jako přenášená aplikační metadata nebo vlastní data servisních protokolů. U protokolu HTTP například http hlavička s metodou, URI, host, user-agent, cookies apod. V odpovědi pak návratový kód a další http parametry. |  |
| Systém umožnuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat. |  |
| **Kontextuální informace** | |
| Systém musí být schopen pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace: |  |
| * jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie |  |
| * hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu |  |
| * IP geolokace |  |
| * IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá |  |
| * historie použitých MAC adresa a výrobce zařízení |  |
| * operační systém a jeho historie na zařízení |  |
| * uživatelem zadané poznámky a informace k zařízení |  |
| * automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy. |  |
| * seznam provozovaných a využívaných služeb (klient a server) u daného zařízení a množství na nich přenesených dat. |  |
| * seznam detekovaných bezpečnostních a provozních událostí daného zařízení. |  |
| **Zaznamenávání, ukládání a zpětná analýza plného provozu** |  |
| Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací. |  |
| Je požadována schopnost importu vlastního PCAP souboru prostřednictvím webového rozhraní a jeho zpětná analýza všemi detekčními a analytickými prostředky kolektoru. |  |
| Je požadována schopnost zobrazení plného obsahu PCAP souboru v prostředí webového rozhraní aplikace a dále pak automatizovaná analýza surových dat za účelem identifikace provozních nedostatků zachycených pouze v datovém PCAP souboru. |  |

**Další požadované oblasti využití**

|  |  |
| --- | --- |
| **Minimální požadované funkcionality/vlastnosti** | **Splňuje**  **[Ano/Ne]** |
| **Monitorování politik kybernetické bezpečnosti** |  |
| Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, a to minimálně: |  |
| * monitorovat definovanou komunikační matici a detekovat, kdy jsou tyto matice porušeny – alespoň jaké zařízení smí komunikovat s jakým zařízením, přes jaký protokol, v jakém čase. |  |
| * detekce změn v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru. |  |
| Pro účely monitorování politik kybernetické bezpečnosti musí systém poskytovat uživatelský rámec pro definování pravidel pomocí: |  |
| * uživatelem definované podsítě na základě rozsahů IP adres |  |
| * uživatelsky libovolně definovaných skupin zařízení |  |
| * automaticky přiřazené značky/tagu zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy. |  |
| **Management bezpečnostních událostí a incidentů** |  |
| Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně: |  |
| * spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele, |  |
| * jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů, |  |
| * možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.), |  |
| * možnost exportování dat do emailu, csv, pdf, syslogu a podobně, |  |
| * možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran. |  |
| **Detekce úniku dat** |  |
| Systém musí být schopen detekovat přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo). |  |
| Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS. |  |
| V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS je požadováno ukládání informací o všech po síti přenášených souborech alespoň v rozsahu: |  |
| * název souboru, |  |
| * velikost souboru, |  |
| * HASH souboru. |  |
| **Monitoring výkonu aplikací a sítě** |  |
| Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty) model normálního chování pro výkonnostní parametry minimálně: |  |
| * přenosová rychlost sítě, |  |
| * rychlost odezvy aplikace, |  |
| * odezva systému z pohledu uživatele. |  |
| Výpočet uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování musí být prováděna pro: |  |
| * všechny porty a služby TCP, |  |
| * pro všechny kombinace služeb a zařízení. |  |
| Systém musí v celé monitorované síti, mezi všemi zařízeními a na všech službách měřit informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewally. |  |
| **Monitoring cloudových služeb** |  |
| Systém musí být schopen monitorovat přístupy zařízení a uživatelů ke cloudovým službám, a to minimálně Google Workspace a Microsoft Office 365, vč. monitoringu operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů. |  |
| Systém musí být schopen tyto informace autonomně a průběžně získávat z aplikačních rozhraní těchto cloudových služeb bez nutnosti využití řešení třetích stran. |  |
| **Inventarizace sítě a grafická vizualizace topologie** |  |
| Systém musí být schopen zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech, nebo podsítích. Včetně detailního přehledu zařízení. |  |
| Systém musí být schopen graficky vykreslit celou topologii sítě, dle zaznamenané komunikace. |  |
| Systém musí být schopen zobrazit inventář jednotlivých lokalit, přehledy zařízení, přehledy výrobců, tagy zřízení, uživatele. |  |
| Systém umožňuje všechny inventarizační informace řadit dle různých parametrů. |  |

1.07.Systém dvoufaktorové autentizace na VPN

|  |  |
| --- | --- |
| **Konkrétní specifikace nabízeného zboží** | |
| Model – typové/výrobní označení: |  |
| Výrobce: |  |

**Obecné minimální požadavky na 2FA pro Lokalitu Kyjov a Lokalitu Veselí nad Moravou**

* licence musí umožnit možnost připojení pro až 300 uživatelů
* Jedná-li se o časově omezenou licenci (subscription), musí být tato licence minimálně na 5 let

|  |  |
| --- | --- |
| **Minimální požadované funkcionality/vlastnosti** | **Splňuje**  **[Ano/Ne]** |
| RA VPN musí podporovat "Split Tunnelling" (t.j. možnost přístupu k internetovým stránkám mimo VPN, zatímco intranetová komunikace je směrována do vpn tunelu). |  |
| Podporované ověřování musí zahrnovat uživatelské jméno / heslo z Active Directory, lokální účty, klientský certifikát, SAML protokol pro ověřování uživatelů vůči Identity Providerovi, Radius, TACACS |  |
| Musí být možné používat jednorázové heslo (OTP) ve spojení se standardním uživatelským heslem (druhý faktor) ve formě SMS kódu nebo SW Tokenu (aplikace typu MS, Google Authenticator apod.) |  |
| Podpora multifaktorové autentizace pomocí kombinace ověřovacích metod uvedených výše |  |
| Interní certifikační autorita pro vydávání certifikátů PKI pro RA VPN uživatele a administrátory |  |