Technická specifikace

Next-Gen Firewall, IPS a anti-malware

Za účelem zabezpečení průmyslové sítě, interní segmentaci sítě a zabezpečení sítového perimetru je poptáváno 1 ks zařízení typu Next Generation Firewall (dále jen NGFW) ve formě hardware appliance s podporou výrobce v režimu 24x7 a aktualizací všech požadovaných bezpečnostních funkcí po dobu 5 let.

Obecné požadavky

- 1x hardware appliance o velikosti max 1U
- Podpora virtualizace uvnitř hw appliance formou vytváření virtuálních kontextů
- Grafické konfigurační rozhraní a příkazový řádek
- Minimální počty požadovaných síťových rozhraní:
    - 6x GE RJ 45
    - 2x GE SFP
    - Konzole sériové linky pro přístup k příkazovému řádku
- Zdvojený (redundantní) zdroj napájení 2x DC adaptér (100-240 V AC)
- Podpora plnohodnotné inspekce sítového provozu v režimech
    - NAT/router
    - L2 transparentní režim (dva a více sítových rozhraní)
    - L2 interface pair (dvě sítové rozhraní)

Výkonové požadavky

Požadované výkonové parametry je nutné doložit oficiálním produktovým listem výrobce. Dodavatel garantuje demonstraci dosažení minimálních výkonových parametrů propustností vybraných funkcí na vyžádání.

- Minimální požadovaná propustnost stavového firewallu pro IPv4 i IPv6 provoz 10 Gbps (UDP pakety o velikosti 512 B)
- Nízké vložené zpoždění zařízení (latence)
- Minimální počet současně navázaných spojení firewallu 1.5 M
- Minimální počet nových spojení za sekundu 45 k
- Výkon zařízení min. 10 M paketů / sekundu
- Propustnost při zapnutí bezpečnostních a inspekčních funkcí (měřeno na reálném provozu)
    - Propustnost NGFW (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, logování) min. 1 Gbps
    - Propustnost ochrany proti hrozbám a škodlivému kódu (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, ochrana proti škodlivému kódu, logování) min. 850 Mbps
    - Propustnost ochrany proti hrozbám (IPS, ochrana proti sítovým útokům, logování) min. 1.3 Gbps
    - Propustnost funkce rozpoznávání sítových aplikací na L7 min. 1.5 Gbps
- Propustnost IPSEC VPN v konfiguraci AES256/SHA256 min. 6 Gbps
- Propustnost funkce SSL inspekce provozu min. 700 Mbps
- Součástí dodávky musí být licence na min. 10 virtuálních kontextů, včetně kompletní NGFW funkcionality ve všech kontextech

Funkční požadavky

- Podpora a zabezpečení kancelářských (IT) a průmyslových řídicích systémů (ICS/OT) minimálně s ohledem na tyto bezpečnostní funkce:
    - Funkce rozpoznávání kancelářských a průmyslových aplikací na L7 – aplikační vrstvě, podpora alespoň 3000 kancelářských aplikací a 700 průmyslových aplikací, protokolů či příkazů; jednotlivé aplikace/protokoly uspořádány do kategorií; výrobce automaticky udržuje a aktualizuje databázi podporovaných aplikací
    - Funkce ochrany před sítovými útoky vycházející z výrobcem udržované a aktualizované databáze, ochrana před útoky typu DoS, verifikace protokolů, min.

10 000 signatur v databázi; podpora zabezpečení kancelářských (IT) a průmyslových řídicích systémů (ICS/OT)
    - Ochrana před výskytem škodlivého kódu v síťovém provozu (antivirus/antimalware) s podporou zabezpečení kancelářských (IT) a průmyslových řídicích systémů (ICS/OT) a škodlivého kódu pro mobilní zařízení; podpora funkce sanitarizace dokumentů (odstranění aktivního obsahu) a předení zkoumaných souborů pro analýzu v prostředí typu sandbox
    - funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze.
    - funkce SSL inspekce pro kontrolu protokolů s možností vytváření výjimek. Výjimky z SSL inspekce požadujeme minimálně:
        - na základě administrátorem definovaných adres
        - na základě kategorie URL, branné z URL filtrační databáze (např. kategorie bankovnictví, zdravotnictví atd.)
- ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign-On
- funkce dynamického routingu (min. BGP, OSPF, RIP), pokud jsou tyto funkce licencované, tak licence musí být součástí dodávky
- funkce QoS, traffic shaping
- funkce klientské VPN (přístup do VPN v tunelovém režimu s VPN klientem a přístup do VPN přes webový portál; možnost aplikace identit uživatele ve smyslu definice bezpečnostní politiky VPN uživatelů; SSL VPN nebo IPsec VPN)
- site-to-site IPsec VPN s podporou statického i dynamického routování
- Podpora OT/ICS/IoT protokolů (minimálně klasifikace provozu, identifikace zařízení, ochrana zařízení před sítovým útokem)
- Umístění výrobce v Gartner MQ for Network Firewalls v sekci „Leaders“ v posledních 3 letech.

Agregační LAN přepínač – 24 portů

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Třída zařízení: přepínač	ano
Formát zařízení do racku	ano
Velikost zařízení: 1U	ano
Počet 1Gbit/s metalických portů	24x 10/100/1000Mbps RJ45
Počet optických 10GE portů s volitelným fyzickým rozhraním (SFP+)	4x
Interní AC zdroj	ano
Maximální spotřeba přepínače při plném zatížení	66W
Celková přepínací propustnost přepínače	128Gbit/s
Celkový paketový výkon přepínače	95Mpps
Minimální paketový buffer: 8MB	ano
Maximální hloubka přepínače: 33 cm	ano
Vlastnosti stohování	
Podporovaný počet přepínačů ve stohu: 8	ano
Kapacita stohovacího propojení: 80 Gbps	ano
Stoh podporuje distribuované přepínaní paketů	ano
Stohování přes standartní uplink porty (možnost zapojení stohu na minimálně 100m)	ano
Redundance řídícího prvku v rámci stohu	ano
Podpora stohování různých typů přepínačů (PoE, Non-PoE, 24port, 48port)	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 každého přepínače je stohovací kabel minimálně 10GE s minimální délkou 1m	ano
Základní 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	ano
Počet LACP skupin/linek ve skupině: 32/8	ano
Minimální počet záznamů v tabulce MAC adres: 16 000	ano
Minimální počet záznamů v tabulce ARP: 8 000	ano
Protokol pro definici šířených VLAN: MVRP	ano
Podpora VLAN podle IEEE 802.1Q, minimálně 2000 aktivních VLAN	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
Podpora NTPv3	ano
Statické směrování IPv4 a IPv6	ano
Minimální počet IPv4 záznamů ve směrovací tabulce: 2 000	ano
Minimální počet IPv6 záznamů ve směrovací tabulce: 1 000	ano

Dynamické směrování OSPFv2, OSPFv3, RIP, RIPng	ano
Podpora Layer-3 routed port	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, LAG, VLAN	ano
BPDU a Root guard	ano
DHCP snooping pro IPv4 a IPv6	ano
IPv6 RA Guard	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
Podpora uživatelských rolí definovaných lokálně v přepínači, jejich aplikace na základě výsledku autorizace	ano
Podpora uživatelských rolí dynamicky stahovatelných z RADIUS serveru, jejich aplikace na základě výsledku autorizace	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	ano
SDN funkce	
Podpora technologie VXLAN	ano
Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izolovat 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 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
Kapacita interního úložiště dat pro analytické účely minimálně 14 GB	ano
Management	
USB-C 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
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 standardního Linux Shellu (BASH) pro debugging a skriptování	ano
Podpora TACACS+	ano
Podpora Secure RADIUS (RadSec)	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 IP SLA pro měření zpoždění provozu VoIP	ano
Podpora Zero Touch Provisioning (ZTP)	ano

Ostatní podmínky:

- Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství)
- Dodávka musí obsahovat veškeré potřebné licence bez časového omezení pro splnění požadovaných vlastností a parametrů.
- Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.
- Jsou požadovány software aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců.
- Je požadovaná technická podpora výrobce po dobu 60 měsíců.
- Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

Přístupový LAN přepínač - 48 portů

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Typ zařízení: L2 switch	ano
Formát zařízení do racku	ano
Maximální velikost zařízení: 1U	ano
Počet 1Gbit/s metalických portů	48×RJ45
Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním	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	Ne
Dostupný výkon pro PoE+ napájení	0W
Podpora Energy Efficient Ethernet (802.3az)	Ano
Minimální přepínací výkon:	176 Gb/s
Minimální paketový výkon:	98 Mpps
Minimální paketový buffer: 12MB	Ano
Maximální přípustná hloubka přepínače:	max. 25 cm
Bez ventilátoru	ne
Základní funkce a protokoly	
Podpora "jumbo rámců" včetně velikosti 9198 Byte	ano
Podpora linkové agregace IEEE 802.3ad	ano
Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4	ano
Minimální počet LACP skupin/linek ve skupině: 8/8	ano
Protokol pro definici šířených VLAN: MVRP	ano
Minimálně 512 aktivních VLAN podle IEEE 802.1Q	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
NTP pro IPv4 a IPv6 včetně MD5 autentizace	ano
Statické směrování IPv4 a IPv6	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 rozhraní IN včetně virtuálních VLAN	ano
BPDU guard a Root guard	ano
DHCP snooping pro IPv4 a IPv6	ano
HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na kbps	ano
ICMPv4 a ICMPv6 rate-limiting per port	ano
Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port	ano
Konfigurovatelná kombinace pořadí postupného ověřování na portu (IEEE 802.1x, MAC adresou)	ano
802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN a Critical voice VLAN	ano
Dynamické zařazování do VLAN	ano

802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)	ano
Ochrana ARP protokolu (Dynamic ARP protection nebo funkčně ekvivalentní)	ano
Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC	ano
Ochrana proti flapování linek s možností konfigurace citlivosti a akce při překročení	ano
Uplink failure detection – detekce výpadku uplink a automatický shutdown navázaných downlink portů	ano
Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU	ano
Podpora instalace vlastního certifikátu včetně Enrollment over Secure Transport (EST)	ano
Podpora IPv4 a IPv6 QoS	ano
Minimálně 8 front pro IEEE 802.1p	ano
802.1x autentizace přepínače vůči nadřazenému přepínači s podporou EAP-TLS a EAP-MD5	ano
Management	
CLI formou 1x USB-C console port	ano
Konfigurace zařízení v člověku čitelné textové formě	ano
USB port pro diagnostiku, přenos konfigurace a firmware	ano
Podpora managementu přes IPv4 i IPv6	ano
Podpora SSHv2 server, HTTPS server, SFTP a SCP klient	ano
Kryptografické SSH algoritmy: AES256, HMAC-SHA2-256, DHG15 nebo vyšší	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 - podpora dvou nezávislých verzí operačního systému	ano
TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logování na více serverů	ano
Podpora SYSLOG over TLS	ano
Měření zakončení a délky metalického kabelu (např. TDR nebo ekvivalentní)	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 RADIUS, RADIUS CoA (RFC3576), RADIUS IPSec	ano
Podpora TACACS+ včetně command authorization	ano
Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)	ano
Aktivní monitoring dostupnosti RADIUS a TACACS+ přednastaveným jménem a heslem	ano
Interní uložiště dat pro sběr provozních dat a pokročilou dignostiku zařízení: min. 15 GB	ano
Analýza síťového provozu sFlow podle RFC 3176	ano
Port mirroring (SPAN), alespoň 4 různé obousměrné session	ano
Podpora Zero Touch Provisioning (ZTP)	ano
Podpora REST API v režimech read-only a read-write pro automatizaci nastavení	ano
Automatická konfigurace portu podle připojeného zařízení	ano
Podpora Cloud based management	ano
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ano

Ostatní podmínky:

- Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství)
- Dodávka musí obsahovat veškeré potřebné licence bez časového omezení pro splnění požadovaných vlastností a parametrů.
- Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.
- Jsou požadovány software aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců.

- Je požadovaná technická podpora výrobce po dobu 60 měsíců.
- Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

Přístupový LAN přepínač - 24 portů

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Typ zařízení: L2 switch	ano
Formát zařízení do racku	ano
Maximální velikost zařízení: 1U	ano
Počet 1Gbit/s metalických portů	24×RJ45
Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním	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	Ne
Dostupný výkon pro PoE+ napájení	0W
Podpora Energy Efficient Ethernet (802.3az)	Ano
Minimální přepínací výkon:	128 Gb/s
Minimální paketový výkon:	95 Mpps
Minimální paketový buffer: 12MB	Ano
Maximální přípustná hloubka přepínače:	max. 25 cm
Bez ventilátoru	ne
Základní funkce a protokoly	
Podpora "jumbo rámců" včetně velikosti 9198 Byte	ano
Podpora linkové agregace IEEE 802.3ad	ano
Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4	ano
Minimální počet LACP skupin/linek ve skupině: 8/8	ano
Protokol pro definici šířených VLAN: MVRP	ano
Minimálně 512 aktivních VLAN podle IEEE 802.1Q	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
NTP pro IPv4 a IPv6 včetně MD5 autentizace	ano
Statické směrování IPv4 a IPv6	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 rozhraní IN včetně virtuálních VLAN	ano
BPDU guard a Root guard	ano
DHCP snooping pro IPv4 a IPv6	ano
HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na kbps	ano

ICMPv4 a ICMPv6 rate-limiting per port	ano
Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port	ano
Konfigurovatelná kombinace pořadí postupného ověřování na portu (IEEE 802.1x, MAC adresou)	ano
802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN a Critical voice VLAN	ano
Dynamické zařazování do VLAN	ano
802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)	ano
Ochrana ARP protokolu (Dynamic ARP protection nebo funkčně ekvivalentní)	ano
Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC	ano
Ochrana proti flapování linek s možností konfigurace citlivosti a akce při překročení	ano
Uplink failure detection – detekce výpadku uplink a automatický shutdown navázaných downlink portů	ano
Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU	ano
Podpora instalace vlastního certifikátu včetně Enrollment over Secure Transport (EST)	ano
Podpora IPv4 a IPv6 QoS	ano
Minimálně 8 front pro IEEE 802.1p	ano
802.1x autentizace přepínače vůči nadřazenému přepínači s podporou EAP-TLS a EAP-MD5	ano
Management	
CLI formou 1x USB-C console port	ano
Konfigurace zařízení v člověku čitelné textové formě	ano
USB port pro diagnostiku, přenos konfigurace a firmware	ano
Podpora managementu přes IPv4 i IPv6	ano
Podpora SSHv2 server, HTTPS server, SFTP a SCP klient	ano
Kryptografické SSH algoritmy: AES256, HMAC-SHA2-256, DHG15 nebo vyšší	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 - podpora dvou nezávislých verzí operačního systému	ano
TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logování na více serverů	ano
Podpora SYSLOG over TLS	ano
Měření zakončení a délky metalického kabelu (např. TDR nebo ekvivalentní)	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 RADIUS, RADIUS CoA (RFC3576), RADIUS IPSec	ano
Podpora TACACS+ včetně command authorization	ano
Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)	ano
Aktivní monitoring dostupnosti RADIUS a TACACS+ přednastaveným jménem a heslem	ano
Interní uložiště dat pro sběr provozních dat a pokročilou dignostiku zařízení: min. 15 GB	ano
Analýza síťového provozu sFlow podle RFC 3176	ano
Port mirroring (SPAN), alespoň 4 různé obousměrné session	ano
Podpora Zero Touch Provisioning (ZTP)	ano
Podpora REST API v režimech read-only a read-write pro automatizaci nastavení	ano
Automatická konfigurace portu podle připojeného zařízení	ano
Podpora Cloud based management	ano
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ano

Ostatní podmínky:

- Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství)
- Dodávka musí obsahovat veškeré potřebné licence bez časového omezení pro splnění požadovaných vlastností a parametrů.
- Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.
- Jsou požadovány software aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců.
- Je požadovaná technická podpora výrobce po dobu 60 měsíců.
- Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

Přístupový LAN přepínač s napájením PoE - 48 portů

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Typ zařízení: L2 switch	ano
Formát zařízení do racku	ano
Maximální velikost zařízení: 1U	ano
Počet 1Gbit/s metalických portů	48×RJ45
Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním	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	ano
Dostupný výkon pro PoE+ napájení	370W
Podpora Energy Efficient Ethernet (802.3az)	ano
Minimální přepínací výkon:	176 Gb/s
Minimální paketový výkon:	98 Mpps
Minimální paketový buffer: 12MB	ano
Maximální přípustná hloubka přepínače:	max. 31 cm
Bez ventilátoru	ne
Základní funkce a protokoly	
Podpora "jumbo rámců" včetně velikosti 9198 Byte	ano
Podpora linkové agregace IEEE 802.3ad	ano
Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4	ano
Minimální počet LACP skupin/linek ve skupině: 8/8	ano
Protokol pro definici šířených VLAN: MVRP	ano
Minimálně 512 aktivních VLAN podle IEEE 802.1Q	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
NTP pro IPv4 a IPv6 včetně MD5 autentizace	ano
Statické směrování IPv4 a IPv6	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 rozhraní IN včetně virtuálních VLAN	ano
BPDU guard a Root guard	ano
DHCP snooping pro IPv4 a IPv6	ano
HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na kbps	ano
ICMPv4 a ICMPv6 rate-limiting per port	ano
Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port	ano
Konfigurovatelná kombinace pořadí postupného ověřování na portu (IEEE 802.1x, MAC adresou)	ano
802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN a Critical voice VLAN	ano
Dynamické zařazování do VLAN	ano
802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)	ano
Ochrana ARP protokolu (Dynamic ARP protection nebo funkčně ekvivalentní)	ano
Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC	ano
Ochrana proti flapování linek s možností konfigurace citlivosti a akce při překročení	ano
Uplink failure detection – detekce výpadku uplink a automatický shutdown navázaných downlink portů	ano
Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU	ano
Podpora instalace vlastního certifikátu včetně Enrollment over Secure Transport (EST)	ano
Podpora IPv4 a IPv6 QoS	ano
Minimálně 8 front pro IEEE 802.1p	ano
802.1x autentizace přepínače vůči nadřazenému přepínači s podporou EAP-TLS a EAP-MD5	ano
Management	
CLI formou 1x USB-C console port	ano
Konfigurace zařízení v člověku čitelné textové formě	ano
USB port pro diagnostiku, přenos konfigurace a firmware	ano
Podpora managementu přes IPv4 i IPv6	ano
Podpora SSHv2 server, HTTPS server, SFTP a SCP klient	ano
Kryptografické SSH algoritmy: AES256, HMAC-SHA2-256, DHG15 nebo vyšší	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 - podpora dvou nezávislých verzí operačního systému	ano
TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logování na více serverů	ano
Podpora SYSLOG over TLS	ano
Měření zakončení a délky metalického kabelu (např. TDR nebo ekvivalentní)	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 RADIUS, RADIUS CoA (RFC3576), RADIUS IPSec	ano
Podpora TACACS+ včetně command authorization	ano
Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)	ano
Aktivní monitoring dostupnosti RADIUS a TACACS+ přednastaveným jménem a heslem	ano
Interní uložiště dat pro sběr provozních dat a pokročilou dignostiku zařízení: min. 15 GB	ano
Analýza síťového provozu sFlow podle RFC 3176	ano
Port mirroring (SPAN), alespoň 4 různé obousměrné session	ano

Podpora Zero Touch Provisioning (ZTP)	ano
Podpora REST API v režimech read-only a read-write pro automatizaci nastavení	ano
Automatická konfigurace portu podle připojeného zařízení	ano
Podpora Cloud based management	ano
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ano

Ostatní podmínky:

- Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství)
- Dodávka musí obsahovat veškeré potřebné licence bez časového omezení pro splnění požadovaných vlastností a parametrů.
- Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.
- Jsou požadovány software aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců.
- Je požadovaná technická podpora výrobce po dobu 60 měsíců.
- Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

Přístupový LAN přepínač s napájením PoE - 24 portů

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Typ zařízení: L2 switch	ano
Formát zařízení do racku	ano
Maximální velikost zařízení: 1U	ano
Počet 1Gbit/s metalických portů	24×RJ45
Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním	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	ano
Dostupný výkon pro PoE+ napájení	370W
Podpora Energy Efficient Ethernet (802.3az)	ano
Minimální přepínací výkon:	128 Gb/s
Minimální paketový výkon:	95 Mpps
Minimální paketový buffer: 12MB	ano
Maximální přípustná hloubka přepínače:	max. 31 cm
Bez ventilátoru	ne
Základní funkce a protokoly	
Podpora "jumbo rámců" včetně velikosti 9198 Byte	ano
Podpora linkové agregace IEEE 802.3ad	ano
Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4	ano
Minimální počet LACP skupin/linek ve skupině: 8/8	ano
Protokol pro definici šířených VLAN: MVRP	ano
Minimálně 512 aktivních VLAN podle IEEE 802.1Q	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
NTP pro IPv4 a IPv6 včetně MD5 autentizace	ano
Statické směrování IPv4 a IPv6	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 rozhraní IN včetně virtuálních VLAN	ano
BPDU guard a Root guard	ano
DHCP snooping pro IPv4 a IPv6	ano
HW ochrana proti zahlcení (broadcast/multicast/unicast storm) nastavitelná na kbps	ano
ICMPv4 a ICMPv6 rate-limiting per port	ano
Ověřování 802.1X včetně více uživatelů na port, minimálně 32 uživatelů/port	ano
Konfigurovatelná kombinace pořadí postupného ověřování na portu (IEEE 802.1x, MAC adresou)	ano
802.1X s podporou odlišných Preauth VLAN, Fail VLAN a Critical VLAN a Critical voice VLAN	ano
Dynamické zařazování do VLAN	ano
802.1x volitelně bez omezování přístupu (pro monitoring a snadné nasazení)	ano
Ochrana ARP protokolu (Dynamic ARP protection nebo funkčně ekvivalentní)	ano
Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC	ano
Ochrana proti flapování linek s možností konfigurace citlivosti a akce při překročení	ano
Uplink failure detection – detekce výpadku uplink a automatický shutdown navázaných downlink portů	ano
Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU	ano
Podpora instalace vlastního certifikátu včetně Enrollment over Secure Transport (EST)	ano
Podpora IPv4 a IPv6 QoS	ano
Minimálně 8 front pro IEEE 802.1p	ano
802.1x autentizace přepínače vůči nadřazenému přepínači s podporou EAP-TLS a EAP-MD5	ano
Management	
CLI formou 1x USB-C console port	ano
Konfigurace zařízení v člověku čitelné textové formě	ano
USB port pro diagnostiku, přenos konfigurace a firmware	ano
Podpora managementu přes IPv4 i IPv6	ano
Podpora SSHv2 server, HTTPS server, SFTP a SCP klient	ano
Kryptografické SSH algoritmy: AES256, HMAC-SHA2-256, DHG15 nebo vyšší	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 - podpora dvou nezávislých verzí operačního systému	ano
TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logování na více serverů	ano
Podpora SYSLOG over TLS	ano
Měření zakončení a délky metalického kabelu (např. TDR nebo ekvivalentní)	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 RADIUS, RADIUS CoA (RFC3576), RADIUS IPSec	ano

Podpora TACACS+ včetně command authorization	ano
Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)	ano
Aktivní monitoring dostupnosti RADIUS a TACACS+ přednastaveným jménem a heslem	ano
Interní uložiště dat pro sběr provozních dat a pokročilou dignostiku zařízení: min. 15 GB	ano
Analýza síťového provozu sFlow podle RFC 3176	ano
Port mirroring (SPAN), alespoň 4 různé obousměrné session	ano
Podpora Zero Touch Provisioning (ZTP)	ano
Podpora REST API v režimech read-only a read-write pro automatizaci nastavení	ano
Automatická konfigurace portu podle připojeného zařízení	ano
Podpora Cloud based management	ano
Konfigurační šablony aplikovatelné na rozhraní, spravované samotným zařízením bez dodatečných externích nástrojů	ano

Ostatní podmínky:

- Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství)
- Dodávka musí obsahovat veškeré potřebné licence bez časového omezení pro splnění požadovaných vlastností a parametrů.
- Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.
- Jsou požadovány software aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců.
- Je požadovaná technická podpora výrobce po dobu 60 měsíců.
- Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

Bezdrátový přístupový bod - wifi AP

Požadavek na funkcionalitu	Minimální požadavky
Základní vlastnosti	
Třída zařízení: indoor přístupový bod	ano
Uzavřená konstrukce bez ventilátorů	ano
Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax	ano
Plnohodnotná certifikace Wi-Fi Aliance: IEEE 802.11a/b/g/n/ac	ano
Plnohodnotná certifikace Wi-Fi Aliance: WPA3-CNSA, WPA3-SAE, WPA3-OWE	ano
Pracovní režim AP bez kontroléru (autonomní)	ano
Pracovní režim AP řízené kontrolérem (lightweight)	ano
Pracovní režim AP v roli kontroléru s možností správy až 120 AP	ano
Minimální počet portů ethernet LAN: 1x 100/1000 Mbit/s RJ45	ano
Podpora standardů IEEE 802.3af (PoE), IEEE 802.3at (PoE+)	ano
Podpora standardního PoE IEEE 802.3af 15W bez nutnosti redukce výkonu libovolného rádia	ano
Podpora napájení z AC napájecího zdroje	ano
Vestavěná interní anténa MIMO, omni down-tilt	ano
Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz	ano
MIMO a počet nezávislých streamů na 2,4GHz rádio: 2x2:2	ano
MIMO a počet nezávislých streamů na 5GHz rádio: 2x2:2	ano
Podpora šířky kanálu 80 MHz	ano
HW podpora DL-OFDMA, UL-OFDMA a DL-MU-MIMO	ano
Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP	ano
Možnost nastavení vysílacího výkonu s krokem 0.5 dBm	ano
Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 5GHz: 1200 Mbps	ano

Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 2.4GHz: 570 Mbps	ano
Integrovaný TPM pro bezpečné uložení certifikátů a klíčů	ano
Podpora 802.11ac explicitního beamformingu	ano
Podpora airtime fairness	ano
Prioritizace jednotlivých SSID na základě vysílacího času	ano
USB port s podporou 3G/4G USB modemu jako WAN uplink	ano
Vypínatelné indikační LED diody informující o stavu zařízení	ano
Band Steering či obdobné (prioritizace 5GHz pásma v případě je-li podporováno)	ano
Detekce Rogue AP	ano
Minimální počet inzerovaných SSID (BSSID) na radio: 16	ano
Nastavitelný DTIM interval pro jednotlivé SSID	ano
Mapování SSID do různých VLAN podle IEEE 802.1Q	ano
VLAN Pooling	ano
HW Podpora wireless MESH funkcionality s protokolem pro optimální výběr cesty v rámci MESH stromu	ano
Podpora Layer-2 izolace bezdrátových klientů	ano
HW Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz	ano
Hardware filtry pro filtraci intermodulačního rušením pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné)	ano
Detekce a monitorování problémů WLAN odchytáváním provozu na AP ve formátu PCAP a jeho zasíláním do Ethernetového analyzátoru, schopnost zachytávat rámce včetně 802.11 hlaviček	ano
DHCP server, směrování a NAT pro bezdrátové klienty	ano
AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN	ano
Automatická identifikace připojeného zařízení a jeho operačního systému	ano
Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming	ano
Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP	ano
Optimalizace provozu: multicast-to-unicast konverze	ano
Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace)	ano
Filtrování přístupu na web	ano
Podpora RadSec (RADIUS over TLS)	ano
802.11w ochrana management rámců	ano
Podpora Kensington lock	ano
Podpora MAC ověřování a 802.1X ověřování s využitím lokální DB v AP	ano
Podpora 802.1X suplicant, AP se ověřuje před připojením do LAN	ano
Volitelně možnost spravovat AP cloud management nástrojem	ano
CLI formou serial konsole port a serial over bluetooth	ano
SSHv2, SNMPv2c a SNMPv3	ano
AP podporuje zero touch provisioning pomocí externího management SW jehož IP adresu získá z cloud aktivační služby poskytované výrobcem	ano
Integrované Bluetooth 5.0 Low Energy (BLE) rádio	ano
Integrované Zigbee 802.15.4 rádio	ano
Podpora režimu SLEEP s max. spotřebou energie do 4W	ano
Součástí AP je příslušenství pro montáž na zeď nebo strop	ano

Ostatní podmínky:

- Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství).
- Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.

- Je požadována záruka na hardware s výměnou NBD v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.
- Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

NetFlow analyzer

Za účelem sběru provozních informací (logů) a vyhodnocování bezpečnostních a jiných incidentů je poptáván nástroj log managementu běžící v režimu VM appliance, která je rovněž určena do prostředí VMware.

Konzole musí být musí být plně integrovatelná se všemi ostatními nabízenými nástroji a její součástí musí být podpora výrobce na 5 let v režimu 24x7 a všechny potřebné aktualizace a služby.

Obecné požadavky

- Forma VM appliance pro platformu VMware ESXI
- Celkové množství přijatých logů za den min. 2 GB
- Celková alokovaná disková kapacita min. 1 TB
- Možné navýšení výše uvedených parametrů dokoupením licence (škálovatelnost)
- Obousměrné propojení s konzolí centrální správy
- Centrální logovací prvek pro všechny nabízené komponenty
- Realtime analýza provozu
- Podpora retrospektivního procházení logů za účelem odhalení dříve neznámých hrozeb
- Možnost rychlé identifikace případných problémů a hrozeb v síti dle detekce – např. IPS, AV …
- Databáze předvyplněných reportů (bezpečnostní incidenty, využití konektivity, navštěvované kategorie webů atd.)
- Možnost tvorby vlastních detailních reportů
- Možnost exportu reportů (HTML, PDF, CSV, XML)
- Podpora vyhodnocování událostí a upozornění na ně (email, SNMP trap)
- Možnost vlastní definice monitorovaných událostí
- Grafický výstup analýzy

Server do racku pro hypervizor a Active Directory

Pro zajištění provozu všech aplikací bude instalován HW server, na kterém bude spuštěn hypervisor umožňující provoz jednotlivých virtuálních serverů. Server musí splňovat následující kritéria:

- Dvousocketový server (CPU) o velikosti max 1U osazený 2x CPU
- CPU 8 jader, TDP 195W, 2.8GHz, AVX Turbo 3.9GHz, paměťová sběrnice 5200MHz, L3 cache 37MB, CPU poslední dostupné generace
    - SPECrate2017_int_base min. 339
    - SPECrate2017_fp_base min. 490
    - SPECpower_ssj2008 pro dany model serveru min. 15400
    - Vysledeky SPEC CPU2017 a SPECpower_ssj2008 pro nabízený model serveru musí byt verejne dostupne na www.spec.org
    - Passmark min. 69000
- Ram: 32 paměťovych slotů, osazeno 8x32GB DDR5 5600MHz 2Rx8 ECC RAM, možno rozšířit az na 8TB RAM
- 8x 2.5” hot-plug pozice pro disky
- Osazení disků
    - 2x 3.84TB SSD DWPD min. 3.5
    - 2x 240GB SSD DWPD min. 1.5
    - 2x 960GB SSD DWPD min. 1.5
- HW RAID řadič 12G, SAS/SATA, podpora RAID Levels 0, 1, 10, 5, 50
- 2x Redundantní hot-plug napájeci zdroj min. 900W každý, účinnost alespoň 96% (titanium)
- 1x 1Gbit LAN port na zakladni desce + 1x 1Gbit LAN port pro vzdaleny management
- 4x 1Gbit RJ45 LAN OCP karta
- 2x 10Gb SFP+ karta včetne optických Multi Mode LC modulů
- Spotřeba serveru v nabízene konfiguraci (odběr ze sítě):
    - při 100% zatížení max. 670W
    - při 50% 100% zatížení max. 350W
    - bez 100% zatížení max. 230W.
- Redundantni hotswapove ventilatory
- HW management, zapnutí, vypnutí, restart serveru, časove neomezená licence pro vzdalené KVM nezavislé na OS a vzdalené připojení médií
- interni management serveru umožňuje updatu serveru online (z OS) i offline (automaticnym updatem z interní SD karty) bez nutnosti instalace dalšího nástroje pro správu, možnost bootu z interní SD karty, časově neomezená licence
- 1x PCIe4.0 slot x16 + 3x PCIe PCIe5.0 slot x16 + 2x OCP slot pro LAN karty
- Rack Mount Kit a rameno na kabeláž
- Možnost trvalého provozu serveru (365x24) při teplotě 5°C - 40°C
- Záruka 5 let NBD fix přímo od výrobce (zaručená oprava do příštího pracovního dne)

Software pro Server pro hypervizor a Active Directory

Požadavky na operační systém pro virtualizované servery:

- Licence pro serverový operační systém pro provoz 8 virtuálních serverů na 1 fyzickém serveru, který je součástí nabídky

- Operační systém musí být plně kompatibilní s MS Windows server a provozovanými aplikacemi a Active Directory
- Součástí dodávky požadujeme 100 licencí pro klientská zařízení (počítače, notebooky, tablety) a 70 licencí pro uživatele pro přístup k Active Directory serveru
- Součástí dodávky požadujeme licence pro 70 uživatelů poštovního serveru plně kompatibilního s operačním systémem a MS Exchange
- Součástí dodávky požadujeme licence pro 70 uživatelů vzdáleného přihlášení k serveru (terminálový server) plně kompatibilního s operačním systémem serveru

Hypervizor

Požadavky na použitý hypervisor:

- Hypervizor musí podporovat provoz virtuálních serverů s OS MS Windows Server 2016 až 2022, RedHat Enterprise Linux (RHEL), Debian GNU/Linux a FreeBSD.

Záložní zdroj UPS pro server

Jako záložní zdroj napětí, pro případ výpadku elektrické energie, požadujeme UPS s následujícími vlastnostmi:

- Záložní zdroj do racku, výška max. 2U
- Smart Line interactive
- Vstupní napětí 230V, konektor C20
- Výstupní výkon min. 2200VA / 2200W, min. 8x C13
- Včetně síťové komunikační karty a managementu – licence na 5 let
- Možnost rozšíření o další bateriový modul
- Součástí dodávky min. 1x ks bateriového modulu 72V, výška max. 2U
- Čas běhu sestavy UPS a bateriových modulů při výpadku napájení při odběru 1500W minimálně 35 minut

NAS uložiště pro zálohování

Požadavky na NAS uložiště pro zálohování:

- Min. 4 diskové uložiště
- Provedení Rack
- Podpora 3,5“ SATA disků
- Osazení min. 2x10TB disky, SATA 7200rpm, 256MB cache určené pro NAS
- Podpora RAID 0,1,5,6
- Min. 2x 1Gbps LAN port + 1x 10Gb
- Min. 4GB RAM
- Podpora iSCSI

Zálohovací SW

Požadavky na software pro zálohování serveru:

- Licence na zálohovací SW, která umožní zálohování virtuálních serverů
- Zálohování pro minimálně 10 virtuální serverů ve variantě zálohování i pro poštovní server kompatibilní s MS Exchange

- Zálohování a obnova virtuálních serverů, jednotlivých souborů
- Zálohování a obnova objektů Active Directory
- Integrovaná deduplikace komprese a šifrování dat
- Podpora zálohování na externí diskové uložiště NAS
- Včetně základní podpory a ochrany upgrade min. 1 rok

Ostatní služby infrastruktury a platformy

DNSSEC resolver – zřízení DNSSEC resolveru v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

AD, LDAP - využití stávající AD s databází uživatelů a skupin uživatelů v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

SSO - předpokládáme instalaci SSO (Single Sign On) utility jako součást bezpečnostní brány do standardního serverového operačního systému.

RADIUS - předpokládáme instalaci RADIUS serveru v rámci standardního serverového operačního systému instalovaného v rámci serverové platformy.

Montážní a implementační práce - pro splnění standardu konektivity škol

Hardware

- Doprava na místo
- Fyzická montáž do datového rozvaděče
    - Prostor připraví zákazník
    - Popis jednotlivých dodaných prvků – popisky, štítky
    - Fotodokumentace
- Zapojení, oživení do sítě zákazníka
    - Konfigurace MGMT IP adres
    - Aktualizace dle doporučení výrobce na poslední verze FW, BIOS
    - Doložení dle výrobce o aktuálnosti
- Vyvázání kabeláže
    - Popis kabelů
    - Dokumentace + fotodokumentace k zapojení
- Fyzická likvidace odpadu, odvoz

Software

- Instalace virtualizační platformy
- Instalace operačních systémů
- Instalace a konfigurace Active directory
- Konfigurace všech potřebných rolí dle standartu konektivity do škol včetně RADIUS serveru
- Konfigurace operačních systémů, rolí dle doporučení výrobce
- Instalace a konfigurace poštovního serveru
- Konfigurace MGMT reportů
    - Reportování stavů HW
    - RAID, FAN, PSU, CPU, RAM, HDD
- Instalace jednotlivých serverů / zařízení dle standartu konektivity do škol
- Implementace všech žákovských PC a učitelských notebooků a PC k novému serveru
- Konfigurace aktivních prvků a bezdrátových přístupových bodů dle standardu konektivity škol

Vnitřní konektivita školy (LAN a WLAN)

Povinné parametry projektu (bez ohledu typ síťového připojení):

- Systém správy uživatelů (Identity Management), tj. centrální databáze identit (LDAP, AD apod.) a její využití pro autentizaci uživatelů (žáci i učitelé) za účelem bezpečného a auditovatelného přístupu k síti, resp. službám. Využívání jednoho účtu více uživateli není povoleno (využívání tzv. anonymních účtů).
- Logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas-počítačový systém6.
- Systémy zálohování a obnovy dat serverové infrastruktury.
- Systémy pro antivirovou ochranu počítačových systémů, antispamovou ochranu poštovních serverů.

Povinné parametry projektu v oblasti pevné LAN:

- Minimální konektivita koncových uživatelských zařízení 1000 Mbps fullduplex.
- Minimální konektivita serverů, aktivních síťových prvků, bezpečnostních zařízení (např. IPS, IDS, Next Generation Firewall aj.), datových úložišť (NAS) 1000 Mbps fullduplex.
- Síťové prvky musí splňovat následující funkcionality: centrální směrovače a centrální přepínače (L2 i L3)7 s neblokující architekturou přepínacího subsystému (wire speed), management, podpora 802.1Q VLAN (možnost tvorby virtuálních sítí - VLAN), základní bezpečnostní prvky proti zneužití přístupu k síti [např. MAC based omezení (port-sec), 802.1X autentizace aj.].
- Strukturovaná kabeláž pro připojení počítačových systémů a dalších zařízení (tiskárny, servery, AP aj.).
- Páteřní rozvody mezi budovami v areálu, kde probíhá výuka nebo příprava na ni, realizovány prostřednictvím optických vláken nebo metalických kabelů. Vztahuje se na budovu/areál, kde se projekt realizuje.

Minimální parametry projektu v případě řešení bezdrátových sítí (WLAN):

- Návrh topologie Wi-Fi sítě a analýza pokrytí signálem počítající s konzistentní Wi-Fi službou v příslušných prostorách školy a s kapacitami pro provoz mobilních zařízení pedagogického sboru i studentů.
- Zabezpečení minimálně AES šifrováním a standardem WPA2-Enterprise nebo WPA3-Enterprise, multi SSID, ACL pro filtrování provozu.
- Zajištění vzájemně oddělených sítí pro zaměstnance školy, žáky/studenty školy a externí zařízení (hosty).
- Podpora mechanismu izolace uživatelů.
- Podpora standardu IEEE 802.11ac (Wi-Fi 5) a případně novějších (Wi-Fi 6), současná funkce AP v pásmu 2,4 a 5 GHz a novějších protokolů a pásem.

Všechny body výše vychází z daného standartu, který je nutno dodržet.

- Plná integrace nového řešení do stávající infrastruktury ICT školy
- Implementace bezpečnostního softwaru

Dokumentace

- Kompletní dokumentace vč. Fotodokumentace HW zapojení
  - Zálohy konfigurací na přiloženém CD
  - Obálka vč. Uživatelských jmen a hesel
  - Seznam vytvořených uživatelů vč. Vzdálených přístupů
  - Kompletní dokumentace nastavení jednotlivých rolí dle standartu
- Výstupní protokol, který prověří fungování definovaného standartu konektivity škol
- Veškeré licence v tištěné i elektronické formě na přiloženém CD
- Předávací protokol o předání dokumentací

Předání

1. Zaškolení obsluhy, předání informací o celém řešení
2. Testovací provoz, který ověří funkčnost (cca 1 měsíc)