## Softwarové vybavení

* + Licence na min. 32 jader VMware vSphere Standard ( 2 x Esxi servery + vCenter Standard) Technický support a aktualizace po dobu 5 let
  + 3x Windows Server 2025 Datacenter
  + 1x Windows Server Standard 2025
  + 100 ks Microsoft Windows Server 2025 User CAL
    - 20ks RDP user CAL pro Windows Server 2025

## Hardwarové vybavení

## Páteřní přepínače LAN 24\*1Gbps, 24-port SFP+ and 4-port SFP56, 25 Gbps uplink

* + L3 switch
  + Min 24 portů 1G/10G SFP+,
  + Min. 4 porty SFP56 10Gb osazené optickými SR transceiverem
  + Možnost konfigurace switche bez nutnosti připojení do sítě přes vyhrazený konzolový port
  + Plně spravovatelný switch pomocí CLI příkazové řádky
  + Konfigurace zařízení v člověku čitelné textové formě
  + USB port pro diagnostiku, přenos konfigurace a firmware
  + Minimálně 512 aktivních VLAN podle IEEE 802.1Q
  + Hardware podpora IPv4 a IPv6 ACL
  + Podpora ochran ARP, DHCP a IP protokolů
  + Dvou-faktorová autentizace pro SSH a WebGUI přihlášení
  + Dualní flash image - podpora dvou nezávislých verzí operačního systému
  + Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby
  + Interní úložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení: min. 15 GB
  + Automatizace – podpora read-only a read-write REST API včetně volání CLI příkazů
  + Automatická konfigurace portu podle připojeného zařízení
  + Podpora Cloud i On-Premise management software výrobce zařízení
  + Podpora Zero Touch Provisioning (ZTP)
  + Spínací kapacita min. 128Gbps
  + Propustnost min. 95 Mpps
  + Podpora standardů:
    - IEEE 802.1D
    - IEEE 802.1p
    - IEEE 802.1Q
    - IEEE 802.1s
    - IEEE 802.1w
    - IEEE 802.1ab
    - IEEE 802.1ad
    - IEEE 802.1az
    - IEEE 802.1x
    - SSHv1/SSHv2
  + Jednotné konfigurační rozhraní pro všechny AP i switche s možností správy připojených zařízení bez nutnosti instalace a nákupu dalšího software
  + Záruka minimálně 5 let servis u kupujícího, záruka musí být poskytnuta výrobcem zařízení a být ověřitelná na veřejně dostupném webu.
  + Záruka na zařízení minimálně 5 let zahájení opravy nebo výměny (případně odeslání zařízení) následující pracovní den

1. Specifikace LAN Infrastruktura – firewall (2 ks)
   * UTM (unified threat management) řešení – Antivirus, Anti-malware, Firewall, Prevence průniku, VPN, Filtrování webu
     + Funkce detekce aplikací
       - detekce známých aplikací na základě signatur
       - signature database automaticky aktualizované výrobcem
       - detekované aplikace je možné: povolit, monitorovat, blokovat
     + Funkce detekce a potlačení narušení (IPS/IDS)
       - minimální propustnost IPS inspekce 2,6 Gbps
       - signatury automaticky aktualizované výrobcem
       - funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům
       - funkce tzv. fail-open - při přetížení IPS je možné definovat, zda dojde k blokaci nebo propuštění provozu
     + Funkce antivirové kontroly
       - ochrana před škodlivým kódem (malware, trojské koně apod.), včetně ochrany před polymorfním kódem
       - signatury automaticky aktualizované výrobcem
       - deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 1 Gbps
       - funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
       - Funkce odstranění škodlivého aktivního obsahu z dokumentů kancelářských aplikací.
     + Funkce kategorizace webových stránek
       - založená na centrálně spravované databázi výrobce
       - možnost definice vlastních kategorií
       - možnost definice vlastních seznamů zakázaných URL
     + Funkce blokování video obsahu portálu YouTube
     + Funkce DNS filtru
       - Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL
       - Možnost importu seznamu blokovaných domén do DNS filtru
       - Detekce a blokování komunikace do botnet sítí
     + Funkce ochrany před únikem citlivých informací (DLP)
       - možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum
     + Funkce blokace stahování konkrétních typů souborů
     + Emailový antispamový modul
     + Podpora SSL deskripce
     + Podpora pravidel pro obranu proti útokům typu DoS
     + Explicitní proxy

* podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)
* podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos
* funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta
* Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru
  + 480 GB SSD =úložiště
  + Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 18000 Mbps, 16000 Mbps, 9000 Mbps
  + Latence firewallu (64 B UDP paket) - max 5 mikro sec
  + Počet firewall pravidel až 10 000
  + Počet naráz otevřených spojení – min 1.3 M
  + Podpora funkce bezdrátový kontrolér - 64 AP
  + Podpora funkce integrovaný switch controller – podpora až 24 switchů
  + Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive
  + Režim fungování L2 – transparentní režim, L3 – NAT/Router
  + Podpora VLAN
  + Podopora multicast, vytváření politiky pro multicast routování
  + Podpora 802.3ad link aggregation
  + Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading
  + Podpora centrální NAT tabulky, stavová inspekce SCTP komunikace
  + Policy-based routing
  + Podpora uplatňování základních pravidel pro kontrolu na přístupové vrstvě (NAC pravidla, politiky)
  + Funkce SSL VPN
    - Nabízené řešení musí podporovat možnost připojení klientů do VPN pomocí proprietární SSL VPN. Aplikace pro do VPN musí být podporována nejběžnějšími operačními systémy, jako například: Windows, macOS, Linux, Android nebo iOS.
    - Možnost zabezpečení připojení do VPN vynucením dvou faktorového ověření. Například pomocí emailu, SMS, hardwarovou klíčenkou, nebo proprietární aplikace dostupná pro Android i iOS.
    - Podpora bez klientského připojení do VPN na úrovni webového portálu, pomocí standardního internetového prohlížeče.
    - Vynucení ověření klientského certifikátu pro zvýšení zabezpečení.
    - Minimální propustnost SSL VPN: 1Gbps
  + Funkce IPsec VPN
  + podpora site-to-site VPN
  + podpora klientských VPN
  + dostupnost VPN klienta pro koncové stanice (Windows, MacOS)
  + funkce klientských IPSec VPN nesmí být licencovaná na počet uživatel. V opačném případě požadujeme dodání neomezené licence.
  + Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 1900
  + Minimální počet klientských IPSEC VPN tunelů: 15000
  + propustnost IPSec VPN min. 11Gbps (měřeno při AES256-SHA256)
  + podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování
  + podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování
  + podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace
* Podpora VXLAN
* Podpora L2TP, PPTP, GRE
* podpora dynamických routovací protokolů OSPF, BGP ve VPN IPsec
  + Funkce firewallu
    - Možnost nastavovat firewall politiku na základě geografických údajů
    - Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem
    - Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru
    - Viditelnost do provozu na aplikační úrovni
    - Možnost dynamického stahování externích seznamů IP adres a jejich následné použití ve firewall policy
    - Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo).
    - Traffic Shaping, QoS s podporou prioritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii
    - Administrátorské účty mohou být volitelně zabezpečený pomocí dvou faktorového ověření
    - Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvou faktorovou autentizaci, podpora certifikátů pro ověření uživatelů
  + FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici
  + Hlavní parametry appliance:
  + Musí se jednat o virtuální appliance s podporou minimálně VMware, KVM a Hyper-V
  + Minimální limit pro množství přijatých logů za jeden den 5GB
  + Podpora minimálně 4 virtuálních interfaců
  + Možnost škálovatelného navýšení kapacity úložiště na základě licence
  + Možnost provozovat appliance pouze jako dočasné úložiště logů z důvodu šetření datového pásma
  + Mít možnost specifikovat typ logů, které budou na hlavní analyzační nástroj odeslány okamžitě
  + Logovací funkce
    - * + Musí se jedna o centrální logovací prvek pro všechny UTM firewally
        + Musí umět ukládat jakkoliv Syslog zprávy
        + Funkce zpětné kontroly logů o přístupu na web (až 7 dní) z důvodu „zero-day“ malicious websites
        + Vizualizace provozu nad všemi firewally
        + Možnost dostat se z vizuálního zobrazení proklikem na konkrétní logy
        + Realtime a historický náhled do logů
        + Korelace logů
  + Navržené řešení musí obsahovat bezpečnostní řešení (firewally) od výrobce, jehož produkty procházejí pravidelným testováním a kontrolou ze strany auditorské společnosti Gartner nebo obdobné.
  + Možnost konfigurace firewallu bez nutnosti připojení do sítě přes vyhrazený konzolový port
  + Podpora řízení kvality linky pomocí QOS
  + Min. 2x WAN RJ45 1Gbps port
  + Min. 2x HA port
  + Min. 1x MGMT port
  + Min. 4x SFP port
  + Min. 2x 10 GE SFP+ port
  + Min. 16x RJ45 1Gbps port
  + Redundantní napájení s možností výměny za běhu
  + Integrovaný controller bezdrátových (Wifi) sítí
  + Wifi controller integrovaný do NGFW platformy
  + Každá bezdrátová síť (SSID) bude reprezentována virtuálním síťovým rozhraním
  + podpora bezpečnostních profilů (AV, AppControl, Webfilter, DLP) přímo na wifi controlleru
  + podpora SSL dekrypce uživatelského provozu přímo na wifi controlleru
  + Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení
  + Možnost volby z různých modelů (802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor)
  + On-wire rogue AP detekce a mitigace
  + Podpora fast-roamingu (802.11 k,v,r)
  + podpora více PSK u jednoho SSID
  + podpora IPSEC tunelu pro šifrování data plane (uživatelských dat)
  + podpora WPA3 šifrování
* Je poptáván systém pro ukládání a korelaci logů v síti zadavatele. Systém musí být plně kompatibilní s dodávanými zařízeními, musí podporovat analýzu logů nad provozem. Dále musí být schopné poskytovat reporty nad logy a informovat správce systému o hrozbách, které byly v síti odhaleny.
* Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu 5 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.

## Drive tape autoloader

* 1x LTO8 mechanika, minimálně 8 slotů na pásky, všechny sloty budou osazeny ReadWrite mediem
* Připojení přes rozhraní SAS kompatibilní se serverem z bodu D.
* software pro identifikaci chyb při čtení a zápisu, monitoring provozu páskové knihovny a mechanik, sledování zátěže mechaniky a využití médií s jednoduchým grafickým rozhraním
* rackmount provedení, maximální výška 2RU
* web based rozhraní pro vzdálenou správu páskové knihovny, kontrolu osazení slotů páskami apod.
* podpora čtení čárových kódů na páskových médiích
* 16 ks LTO 8 pásek
* 1x čistící médium
* Rozšířená podpora výrobce páskové knihovny po dobu 5 let, 24x7x4h response.

## Server backup

* + - Výška max 2U, montáž do racku hloubky 1000mm
    - Server osazený 2x CPU x86 kompatibilním CPU
    - Požadavky na CPU: 8 jader (core), frekvence min. 3.2GHz (min 4.1 GHz turbo), HT je požadován
    - 32/64bit
    - L3 cache min 22,5MB
    - Podpora min. DDR5
    - Max. spotřeba 165W
    - Operační paměť osazená minimálně 128 GB DDR4 o frekvenci min 4400GHz, rozšiřitelná minimálně na 1TB bez výměny již osazených RAM
    - Min. 2x 460 GB SSD
    - Min. 10 x 8 TB disk
    - Redundantní napájecí zdroj (2x jednofázový zdroj)
    - Min 4x 1Gbit LAN porty s podporou Large Send and Receive offload capability, VLAN tagging, MSI-X, jumbo frames, IEEE 1588, VMware NetQueue a Microsoft VMQ nezabírající rozšiřující PCIe sloty
    - Min 2x 10Gbit SFP+ porty osazené optickými SR transceivery a s podporou VLANtagging, adaptive interrupt coalescing, MSI-X, NIC teaming (bonding), Tunnel offloads (NVGRE, VXLAN), TCP/Ip Stateless Offloads, Receive Side Scaling (RSS), jumbo frames a PXE boot.
    - 1x 1Gbit port pro management
    - Rozhraní SAS kompatibilní s páskovou knihovnou
    - větráky v serveru musí být vyměnitelné za provozu a redundantní
    - napájecí zdroje splňující požadavky certifikace energetické účinnosti, např. ECOS Consulting 80 Plus (min. Titanium), případně dodavatel doloží, že jejich účinnost při napájení 230V je minimálně min. 96%, výkon max. 1000W
    - Integrovaného management a HW monitoring pomocí SW dodávaného v ceně (bez následného navýšení), možnost správy napájení, performance monitoring klíčových komponent, SW pro migraci ze stávajících serverů na nové [P2P, P2V, V2V, V2P] Nezávislý management procesor umožňující přístup k serveru i ve vypnutém stavu (možnost vzdáleného vypnutí a zapnutí, převzetí obrazovky konzole atd.)
    - Plně integrovaná grafická plnohodnotná konsole s možností vzdálené správy
    - Možnost správy a monitoringu serveru bez instalace agentů v operačním systému
    - Možnost o doplnění dalším HW (SAS) řadičem pro připojení případných externích zařízení

## Přístupové přepínače 48\*1Gbps + Poe 802.3at, 10Gbps uplink

* + Min 48 portů RJ-45 10/100/1000 Mbps s podporou PoE (min. 40 802.3af/at class 4)
  + 2 porty 10GBASE-T ports
  + 2 porty SFP+ 10Gb ports
  + Podpora stohování až 4 zařízení ve stacku (stoh se chová jako jedno zařízení)
  + Možnost správy skrze mobilní aplikaci nebo cloudový portál
  + Podpora ochran ARP, DHCP a IP protokolů
  + Podpora IPv4 a IPv6 ACL
  + Podpora standardů:
    - IEEE 802.1AX
    - IEEE 802.1D
    - IEEE 802.1Q
    - IEEE 802.1ab
    - IEEE 802.1p
    - IEEE 802.1s
    - IEEE 802.1w
  + Min. 600W pro PoE
  + Podpora VLAN
  + Spínací kapacita min 175Gbps
  + Jednotné konfigurační rozhraní pro všechny AP i switche s možností správy připojených zařízení bez nutnosti instalace a nákupu dalšího software
  + Záruka minimálně 5 let servis u kupujícího, záruka musí být poskytnuta výrobcem zařízení a být ověřitelná na veřejně dostupném webu.
  + Záruka na zařízení minimálně 5 let zahájení opravy nebo výměny (případně odeslání zařízení) následující pracovní den

## Specifikace LAN Infrastruktura – WiFi Acces Point (25 ks)

* Minimálně 802.11ax 2x2 MU-MIMO
* Minimálně 3 oddělená rádia, kdy jedno může být pro diagnostické účely wifi spektra
* AP musí být vybaveno Bluetooth Low Energy modulem umožňujícím snadné vyhledání a správu AP.
* Podpora PoE+
* AP nesmí mít externí antény, musí být integrované přímo v AP aby se nedaly z bezpečnostních důvodů odpojit.
* AP musí být vybaveno dedikovaným konzolovým portem a jedním, USB portem pro případné nahrání firmwaru přímo z usb flash disku.
* AP musí být vybaveno minimálně dvěma LAN konektory o rychlosti 1gbit.
* Možnost preferovat a přepojovat z 2,4 GHz na 5 GHz - podpora Band Steering
* Počet obsloužených klientů jednoho AP alespoň 500 zařízení
* IEEE 802.1Q VLAN Tagging
* Držák AP součástí balení
* Možnost skenovaní rogue AP v síti
* Analyzátor spektra
* Centralizovaná architektura správy wifi sítě (centrální řadič, centrální management, tzv. thin access pointy, popř. alespoň centrální řešení distribuce konfigurací s podporou automatického rozložení zátěže klientů, roamingu mezi spravované access pointy a automatickým laděním kanálů a síly signálu včetně detekce a reakce na non-Wi-Fi rušení).
* AP umožňují správu jak z cloudu výrobce, tak z centralizovaného nástroje, který musí být součástí firewallu stejného výrobce.
* Podpora mechanismu izolace klientů
* Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD ...)
* Podpora WPA2, podpora WPA3, PoE, multi SSID, ACL pro filtrování provozu
* U software a firmware je vyžadována dostupnost aktualizací, zejména bezpečnostního charakteru po celou dobu udržitelnosti projektu
* Podpora OFDMA.