Technická specifikace pro veřejnou zakázku *„Kybernetická bezpečnost ZZS MSK – SW+HW vybavení“* - dodávka aktivních síťových prvků a podpůrných systémů řízení síťového provozu

**Zpracoval:** Ing. David Jedziniak

**Verze:** 1.0

**K datu:** 17.2.2025

# Modernizace infrastruktury počítačové sítě ZZS MSK

V rámci modernizace infrastruktury počítačové sítě je předmětem zakázky částečná obnova a doplnění prvků počítačové sítě ZZS MSK (dále jen Zadavatel). Pořizovaná zařízení musí být plně kompatibilní se současně provozovanou infrastrukturou, transparentně bez ztráty doposud vložených investic.

## Popis stávajícího řešení pevné infrastruktury

Pevná část počítačové sítě je tvořena přístupovými a agregačními přepínači Cisco Catalyst 2960/3560/9500/9600. Napříč celou sítí je používán protokol VTP, další parametry jsou uvedeny v tabulce požadavků. Poptávané přepínače jsou určeny k náhradě zastaralých přepínačů. V celé síti bude podporován protokol IPv6 vč. vybraných bezpečnostních mechanismů.

## Popis stávajícího řešení WiFi sítě

Pro rozšíření kapacity provozované přístupové sítě, možnosti poskytnutí nových služeb a zároveň zachování kompatibility se současným provozovaným řešením, je záměrem pořídit přístupové bezdrátové body s níže uvedenými specifikacemi.

## Požadavky na dodaná zařízení

Dodavatel poskytne Zadavateli po dobu trvání podpory všechny relevantní SW vydání a verze SW nabízené výrobcem tak, aby dodané řešení vyhovovalo zadání Zadavatele a fungovalo bez závad. Dodavatel se dále zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení.

Dodavatel je povinen řádným způsobem uzavřít dohodu o podpoře s výrobcem zařízení tak, aby v případě závady na dodaných zařízeních, kterou není dodavatel schopen sám odstranit, bylo možné tuto závadu eskalovat přímo k výrobci zařízení. Zároveň je dodavatel povinen zajistit Zadavateli přístup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.

Dodavatel je povinen zajistit dostupnost náhradních dílů od výrobce a dostupnost vlastní podpory pro dodané řešení za podmínek specifikovaných Zadavatelem.

Dodavatel je povinen s dodávkou doložit oficiální potvrzení zastoupení výrobce o určení dodávaného HW (seznamu sériových čísel dodávaných zařízení) pro evropský trh a koncového zákazníka ZZS MSK na českém trhu, pokud o to zadavatel požádá. Zadavatel požaduje originální a nové zařízení, licencované ve jménu zákazníka tak, aby bylo možné eskalovat případné závady na technickou podporu výrobce.

Zadavatel požaduje dodat taková zařízení, u kterých je výrobcem deklarovaná produktová podpora a stabilita minimálně 7 let od data dodání, a to včetně nových programových verzí, údržby a podpory programového vybavení.

## Požadavky na záruku

Běžná záruka za jakost bude zahrnovat:

* výměnu vadného dílu nebo zařízení nejpozději do 10ti pracovních dnů od nahlášení závady zástupcem Zadavatele, se zahájením řešení následující pracovní den po nahlášení Zadavatelem,
* nárok na bezplatnou instalaci nových verzí firmware v případě, kdy aktuální verze firmware obsahuje vady, které mají vliv na kvalitu poskytované služby zařízením nebo v případě, kdy v instalovaném firmware byla odhalena bezpečnostní zranitelnost, a to v rozsahu dodané licence.

Rozšířená servisní podpora (dále „RSP“) je poskytována spolu se zárukou a dále po jejím skončení (pokud je požadována delší než záruka), kdy záruku rozšiřuje o následující:

* výměnu vadného dílu nebo zařízení nad rámec záruky v místě plnění se zahájením řešení na místě nebo odesláním náhradního dílu následující pracovní den po ohlášení závady (8x5xNBD),
* nárok na bezplatnou instalaci všech nových verzí firmware v rozsahu dodané licence,
* nárok na přímou podporu výrobce v případě softwarových nebo hardwarových závad, jejichž řešení nebude v silách dodavatele.

Ve specifikaci jednotlivých komponent mohou být uvedeny další upřesnění rozsahu servisní podpory nebo záruky.

## Tabulka poptávaných prvků a komponent a typ požadované záruky/podpory

|  |  |  |
| --- | --- | --- |
| Zařízení | kusy | Typ záruky |
| Agregační přepínač – typ č.1 | 4 | 3 roky záruka, 7 let RSP |
| Stohovací kabel pro L2/L3 přepínače typ č.1 | 2 | 3 roky záruka, 7 let RSP |
| Přístupový přepínač – typ č.1 | 28 | 7 let záruka |
| Přístupový přepínač – typ č.2 | 23 | 7 let záruka |
|  |  |  |
| Bezdrátový přístupový bod | 135 | 3 roky záruka, 7 let RSP |
|  |  |  |
| Firewall – typ č.1 | 6 | 3 roky záruka, 7 let RSP |
| Firewall – typ č.2 | 14 | 3 roky záruka, 7 let RSP |
| Software pro evidenci výpočetní techniky | 1 | 3 roky záruka, 7 let RSP |
| Software k řízení síťového provozu | 1 | 3 roky záruka, 7 let RSP |

# Technické požadavky na zařízení

## Agregační přepínač – typ č.1

Za účelem připojení zařízení do síťové infrastruktury, interní segmentace sítě a zabezpečení síťového perimetru jsou poptávaný L2/L3 přepínač ve formě hardware appliance a to s následujícími vlastnostmi:

* L2/L3 přepínač
* podpora přepínání na 3. vrstvě
* v provedení pro montáž do 19“ racku
* každý přepínač bude osazen min. 48 porty podporující POE minimálně ve formátu 802.3at
* každý přepínač bude osazen min. 12 multigigabit porty (10G/5G/2,5G/1G/100M/10M)
* každý přepínač bude osazen min. 36 2,5G/1G/100M portů
* každý přepínač bude osazen modulem s min. 8 uplink 10GE porty se sloty ve formátu min. SFP+
* podporující osazení 2 ks redundantních napájecích zdrojů
* každý dodaný přepínač bude osazen 2 ks napájecími zdroji s min. příkonem 1000 W
* podpora stohovatelnosti s min. kapacitou sběrnice stohu 400 Gbps
* součástí dodávky bude u každého přepínače stohovací kit
* min. forwarding rate 400 Mpps
* min. kapacita přepínání 500 Gbps
* podpora IEEE 802.3ad (Link Aggregation – LAG)
* podpora minimální 2000 aktivních VLAN
* podpora IEEE 802.1w – Rapid Spanning Tree Protocol
* podpora instance spanning-tree protokolu per VLAN
* podpora jumbo rámců
* podpora detekce protilehlého zařízení (např. CDP nebo LLDP)
* podpora protokolů MVRP nebo VTP pro definici a správu VLAN sítí
* podpora OSPFv2, OSPFv3,(dle RFC draft-savage-eigrp-05 nebo RFC 7868), ISIS a BGPv4
* podpora IP Multicast (PIM SSM, PIM SM)
* podpora virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF)
* podpora First Hop Redundancy Protokol (např. VRRP, HSRP) pro IPv4 i IPv6
* podpora Reverse path check (uRPF)
* podpora minimálně 8 HW QoS front
* podpora QoS - Strict Priority Queue, QoS classification – ACL, DSCP, CoS based, QoS marking – DSCP, CoS, QoS Policing, QoS-Hierarchical QoS
* podpora řízení přístupu Port ACL, VLAN ACL
* osazeno HW trusted modul pro bezpečné uložení hesel a šifrovacích klíčů
* podpora IGMPv2/v3 snooping , MLD snooping
* podpora Multicast DNS (mDNS) gateway
* podpora exportu monitorovaných dat ve formátu NetFlow v9 nebo IPFIX
* podpora SSHv2, CLI rozhraní, Python scripting, , Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení
* Model-driven programovatelnost prostřednictvím RESTCONF,
* podpora SNMPv2/v3 a NTPv3 server
* podpora IEEE 802.1x, podpora TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)
* podpora vzdáleného port mirroring (ERSPAN)

Dodávaná zařízení musí být plně kompatibilní se stávajícím prostředím a umožnit napojení a výměnu dat o hierarchii sítě (VLAN, informace o redundantním propojení atd.) se stávajícími prvky popsanými v bodě “Popis stávajícího řešení pevné infrastruktury”. Požadavek je uveden z důvodu zajištění dostupnosti a kvality služeb, kdy je nutné začlenění prvků do stávající infrastruktury, která není ve správě a majetku zadavatele.

Zapojení bude provedeno v budově krajského operačního střediska, které je kritickou infrastrukturou. Pokud se ukáže, že dodané zboží nesplňuje požadavky na plnou kompatibilitu s výše uvedenými prvky, vyhrazuje si Zadavatel právo od smlouvy odstoupit.

## Stohovací kabel pro L2/L3 agregační přepínač – typ č.1

Pro HW stacking přepínačů č.1 je poptáváno dodání 2 ks kabelů o délce 0,5 m.

## Přístupový přepínač – typ č.1

Za účelem připojení zařízení do síťové infrastruktury, interní segmentace sítě a zabezpečení síťového perimetru je poptáván L2/L3 přepínač ve formě hardware appliance a to s následujícími vlastnostmi:

* L3/L2 přepínač
* podpora přepínání na 3. vrstvě
* v provedení pro montáž do 19“ racku
* každý přepínač osazen minimálně 48 POE+ porty
* každý přepínač osazen minimálně 48 1G portů (1G/100M/10M)
* každý přepínač bude osazen min. 4 uplink porty se sloty ve formátu SFP+
* každý přepínač bude mít min. napájecí příkon pro PoE+ 370 W
* podpora stohovatelnosti
* min. velikost interní paměti 1024 MB
* min. velikost FLASH paměti 512 MB
* min. kapacita přepínání 150 Gbps
* podpora IEEE 802.3ad (Link Aggregation – LAG)
* podpora minimální 2000 aktivních VLAN
* podpora IEEE 802.1w – Rapid Spanning Tree Protocol
* podpora instance spanning-tree protokolu per VLAN
* podpora jumbo rámců (minimálně 9000 bytes)
* podpora detekce protilehlého zařízení (např. CDP nebo LLDP)
* podpora protokolů MVRP nebo VTP pro definici a správu VLAN sítí
* podpora minimálně 8 HW QoS front
* podpora QoS - Strict Priority Queue
* podpora IGMPv2/v3, MLD, SSHv2, CLI rozhraní, SNMPv2/v3 a NTPv3 server
* podpora IEEE 802.1x, podpora TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)

## Přístupový přepínač – typ č.2

Za účelem připojení zařízení do síťové infrastruktury, interní segmentace sítě a zabezpečení síťového perimetru je poptáván L2/L3 přepínač ve formě hardware appliance a to s následujícími vlastnostmi:

* L3/L2 přepínač
* podpora přepínání na 3. vrstvě
* v provedení pro montáž do 19“ racku
* každý přepínač osazen minimálně 48 x POE+ porty
* každý přepínač osazen minimálně 32 x 1G portů (1G/100M/10M)
* každý přepínač osazen minimálně 16 x 2,5G portů
* každý přepínač bude osazen min. 4 uplink porty se sloty ve formátu SFP+
* každý přepínač bude mít min. napájecí příkon pro PoE+ 740 W
* podpora stohovatelnosti
* min. velikost interní paměti 1024 MB
* min. velikost FLASH paměti 512 MB
* min. kapacita přepínání 220 Gbps
* podpora IEEE 802.3ad (Link Aggregation - LAG)
* podpora minimální 2000 aktivních VLAN
* podpora IEEE 802.1w – Rapid Spanning Tree Protocol
* podpora instance spanning-tree protokolu per VLAN
* podpora jumbo rámců (minimálně 9000 bytes)
* podpora detekce protilehlého zařízení (např. CDP nebo LLDP)
* podpora protokol MVRP nebo VTP pro definici a správu VLAN sítí
* podpora minimálně 8 HW QoS front
* podpora QoS – Strict Priority Queue
* podpora IGMPv2/v3, MLD, SSHv2, CLI rozhraní, SNMPv2/v3 a NTPv3 server
* podpora IEEE 802.1x, podpora TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting)

## Bezdrátový přístupový bod

Za účelem šíření Wi-Fi signálu je poptáváno jednotné, centrálně spravované Wi-Fi 6 řešení s podporou výrobce 24x7x365 s hodinovou odezvou na kritické incidenty a odezvou následující pracovní den pro incidenty nekritické na dobu 7 let.

## Obecné požadavky

* Instalace na strop/podhled nebo stěnu
* Integrované antény pro pásma 2,4 GHz, 5 GHz
* Podpora ověřování proti Microsoft AD
* Podpora moderních protokolů pro zabezpečení min. WPA3
* Access point má integrovaný Bluetooth rádiový modul
* Podpora minimálně 500 připojených klientů na jeden přípojný bod
* Plně kompatibilní s poptávaných software pro řízení provozu
* Centrální správa všech AP (může jít o max. 6 různých management prostředí – pro každý z okresů), kdy AP budou umístěny do 32 lokalit a datově propojeny přes IPSec VPN
* Podpora zasílání logů a diagnostických dat na centrální dohledový systém pomocí Syslogu nebo SNMP. Zasílání musí být dostatečně detailní pro získání přehledu minimálně o:
  + nově připojených klientech (způsobu autentifikace, použitím SID apod.),
  + důvodu odmítnutí připojení klienta a diagnostiku dalších problémů s připojením.

## Výkonové požadavky

* Min. 1x 100/1000/2500 Base-T RJ45 LAN rozhraní, min. 1 x 10/100/1000 Base-T RJ45, 1x RS-232 RJ45 Serial Port nebo 1x USB konektor pro lokální správu
* Access Point vybavený rádiem pro 2,4 GHz a 5 GHz pásmo, podpora standardu 802.11a/b/g/n/ac a Wi-Fi 6 (802.11ax)
* Přenosová rychlost na radiu 2,4 GHz min 574 Mbps, na radiu 5 GHz min 2400 Mbps
* Podpora minimálně 4x4 MU-MIMO, UL/DL OFDMA, TWT, BSS
* Min. 8 inzerovaných SSID (BSSID) per radio
* Podpora mechanismu pro připojení klientů mezi pásmy a bezvýpadkového přechodu klientů mezi jednotlivými AP
* Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x supplicant
* Podpora přímého přístupu na příkazovou řádku AP přes sériovou konzoli a přes IPv4 pomocí SSH
* Možnost 802.3af/at PoE napájení AP z přepínače nebo injektoru
* Spotřeba Access pointu max. 30 W

## Firewall – typ č.1

Za účelem zabezpečení síťové infrastruktury, interní segmentace sítě a zabezpečení síťového perimetru je poptáváno 6 ks zařízení typu Next Generation Firewall (dále jen NGFW) ve formě hardware appliance s podporou výrobce v režimu 24x7x365 s hodinovou odezvou na kritické incidenty a odezvou následující pracovní den pro incidenty nekritické na dobu 7 let, a to s následujícími vlastnostmi.

**Technické požadavky**

* HW o velikosti max. 1 RU
* Podpora režimu vysoké dostupnosti pro dvojici firewallů (active/active i active/passive)
* Správa zařízení pracujících v režimu vysoké dostupnosti musí probíhat skrze jedno konfigurační rozhraní, je požadována automatická synchronizace provozních a stavových informací mezi jednotlivými zařízení v jednom celku vysoké dostupnosti
* Podpora virtualizace uvnitř hw appliance formou vytváření virtuálních kontextů
* Grafické konfigurační rozhraní a příkazový řádek
* Minimální počty požadovaných fyzických rozhraní:
  + 16x GE RJ45
  + 8x GE SFP
  + 4x 10 GE SFP+
  + 1x RJ 45 Management port
  + 1x USB
* Zdvojený (redundantní) zdroj napájení
* Podpora plnohodnotné inspekce síťového provozu v režimech
  + NAT/router
  + L2 transparentní režim (dva a více síťových rozhraní)
  + L2 interface pair (dvě síťové rozhraní)
  + L4 podpora skenování na transportní vrstvě
  + L7 kontrola na úrovni aplikací

**Výkonové parametry**

* Minimální požadovaná propustnost stavového firewallu pro IPv4 i IPv6 provoz 36 Gbps (UDP pakety o velikosti 512 B)
* Zpoždění zařízení (latence – UDP pakety o velikosti 64 byte) max. 3.5μs
* Minimální počet současně navázaných spojení firewallu 3 M
* Minimální počet nových spojení za sekundu 120 000
* Výkon zařízení minimálně 40 Mpps
* Propustnost při zapnutí bezpečnostních a inspekčních funkcí (měřeno na reálném provozu)
  + Propustnost NGFW (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, logování) minimálně 5 Gbps
  + Propustnost ochrany proti hrozbám a škodlivému kódu (kombinace stavového firewall, IPS, rozpoznávání aplikací na L7, ochrana proti škodlivému kódu, logování) minimálně 2.5 Gbps
  + Propustnost ochrany proti hrozbám (IPS, ochrana proti síťovým útokům,
  + logování) minimálně 2.5 Gbps
  + Propustnost funkce rozpoznávání síťových aplikací na L7 min. 6 Gbps o Propustnost IPSEC VPN v konfiguraci AES256/SHA256 min. 30 Gbps o Propustnost funkce SSL inspekce provozu minimálně 3 Gbps
  + Minimálně 10 konfigurovatelných virtuálních kontextů na každém zařízení v rámci základní licence

**Funkční požadavky**

* Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů, správa pomocí konzole pro centrální správu identického výrobce
* Podpora stavového firewallingu pro IPv4 i IPv6, podpora NAT 64/46
* 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
* Podpora lokální databáze a vzdálené databáze (RADIUS, LDAP, TACACS+, SAML, KERBEROS) pro ověřování uživatelů
* Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu
* Funkce QoS, traffic shaping a SD-WAN minimálně v režimu vytvoření overlay a underlay virtuálních síťových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek
* Podpora funkcí VPN brány – IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran) - SSL VPN pro klientský přístup s tunelovacím režimem včetně klienta pro osobní počítače i mobilní platformy, portálový režim pro bezklientský přístup
* 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 síťovými 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 sanitizace dokumentů (odstranění aktivního obsahu) a předení zkoumaných souborů pro analýzu v prostředí typu sandbox
* Funkce kategorizace webových stránek (web filtering na čtyřech NGFW) 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. **Dvě z dodávaných NGFW zařízení je možné dodat bez funkce web filteringu**.
* 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, brány z URL filtrační databáze (např. kategorie bankovnictví, zdravotnictví atd.)
* Certifikace výrobce v security testech společnosti NSS LABS Recommended

## Firewall – typ č.2

Za účelem zajištění zabezpečené šifrované komunikace na radiové převaděče digitální radiové sítě Mototrbo a zabezpečení síťového perimetru je poptáváno zařízení typu Next Generation Firewall (dále jen NGFW) ve formě hardware appliance, a to s následujícími vlastnostmi.

**Technické požadavky**

* HW v „desktopovém“ provedení nebo provedení pro montáž do rack velikosti max. 1 RU
* Grafické konfigurační rozhraní a příkazový řádek
* Úložná kapacita minimálně 16 GB (eMMC, případně SSD)
* Velikost operační paměti minimálně 4 GB
* Napájení zdrojem s 12 V
* Minimální počty požadovaných fyzických rozhraní:
  + 4x 1 GE
  + 1x GE SFP
  + 1x konzolový port pro lokální správu
  + 1x USB

**Výkonové parametry**

* Minimální požadovaná propustnost firewallu 9 Gbps
* Zpoždění zařízení (latence – UDP pakety o velikosti 64 byte) max. 5 μs
* Minimální počet nových spojení za sekundu 40 000
* Minimální požadovaná propustnost IPsec VPN 6 000 Mbps
* Minimální propustnost IPS 2 000 Mbps
* Minimální propustnost NGFW 2 000 Mbps
* Podpora minimálně IPsec VPN 500
* Plná kompatibilita VPN spojení (IPSec + SSL VPN) se stávajícím VPN koncentrátorem (Sophos XGS 2100), kdy musí být zaručeno udržování stabilního a bezproblémového spojení pro přenos datového toku hlasové komunikace radiostanic sítě Mototrbo firmy Motorola.
* Dodaný typ zařízení pro VPN spojení musí být podporován ze strany výrobce stávajícího VPN koncentrátoru. Stávající VPN koncentrátor zajišťuje spojení pro dalších 35 poboček zadavatele a výměna koncentrátorů za jiný typ by tak znamenala nutnost výměny zařízení na všech pobočkách, což by neefektivní, neekonomické a neúčelné.

**Funkční požadavky**

* Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek
* Podpora centrálního managementu
* Podpora statického a dynamického routování (BGP, OSPF)
* Stavový firewall s hloubkovou inspekcí paketů
* Ochrana proti zahlcení, blokování DoS, DDoS a skenování portů
* Autentizace s podporou: Active Directory, eDirectory, RADIUS, LDAP a TACACS+
* Transparentní autentizace s podporou Active Directory
* Možnosti VPN – IPSec, SSL, PPTP, L2TP

## Software pro evidenci výpočetní techniky

Za účelem evidence výpočetní techniky je poptávána aplikace umožňující online, případně off-line, provádět audit hardware a software na počítačích připojených v síťové infrastruktuře. U aplikace jsou požadovány následující vlastnosti:

* možný audit hardware pro všechny operační systémy Windows, které jsou v době prodeje podporovány společností Microsoft a pro OS Linux ekvivalentní verzi Red Hat verze 9.0 a vyšší
* evidenci HW, tzn evidenci naskenovaných technických parametrů počítačů, ale i jejich komponent jako jsou tiskárny apod. Naskenované údaje musí být možné doplnit i manuálně.
* audit software
* správa licencí provozovaného software
* generování předávacích protokolů
* možnost vzdálené skryté instalace klienta na počítačích připojených do domény pomocí za pomocí doménové administrátorského oprávnění, doménových politik nebo vytvořeného msi balíčku.
* možnost manuální instalace klienta na vybrané stanice pomocí ručního instalátoru.
* Instalace aplikačního serveru musí být možná na server s OS Microsoft Windows Server 2019 a vyšší, případně součástí dodávky musí být instance operačního systému podporující běh ve virtualizačním prostředí Hyper-V
* aplikační server musí umožňovat konektivitu s provozovaným databázovým serverem SQL server 2019 a vyšší, případně součástí dodávky musí být vlastní databázový systém
* dodaná licence musí být trvalá a funkční i po ukončení podpory

## Software k řízení síťového provozu

Za účelem centrálního řízení síťového přístupu zařízení, které se připojují do síťové infrastruktury je poptáváno řešení umožňující kontrolu zařízení třetích stran a automatickou reakci na události v sítí. U aplikace jsou požadovány následující vlastnosti:

Klíčové vlastnosti:

* podpora výrobce 24x7x365 s hodinovou odezvou na kritické incidenty a odezvou následující pracovní den pro incidenty nekritické na dobu 7 let,
* skenování síťové infrastruktury pro klasifikaci připojených zařízení,
* dle průběžné analýzy udržuje aktualizovaný seznam všech síťových zařízení.

Požadavky na integraci:

* podpora pro integraci zařízení na základě specifikací koncových zařízení v MIB souborech pro komunikaci SNMP
* podpora pro integraci přepínačů značek HP, 3COM, Aruba, Cisco, Meraki a jiných
* podpora pro integraci přístupových bodů značek Aruba, Cisco, Ubiquiti a jiných
* podpora systémů s OS Microsoft Windows, Linux, Apple Mac OS X, Apple iOS, Android
* podpora autentizačních služeb ACS Cisco, Free Radius, OpenLDAP a Microsoft Active Directory

Požadované funkce:

* 2x virtuální appliance s možností instalace na platformu Hyper-V server verze 2022 a vyšší a Vmware ESX verze 7 a vyšší nebo 2x HW zařízení v HA režimu
* podpora distribuované architektury s centrálním prvkem správy
* autentizační brány musí být nasazené mimo samotný datový tok
* podpora HA v režimu active-passive
* sdílení licencí v HA režimu active-passive
* komunikace se síťovými prvky (drátovými i bezdrátovými) pomocí SNMP a CLI, i u jiných výrobců
* vymáhání definovaných bezpečnostních politik bez nutnosti využití 802.1x nebo MAB
* možnost instalace samostatného NAC řešení bez nutnosti nákupu dalších prvků (např. centrální management). Pokud je další prvek nutný, musí být součástí nabídky na NAC
* autentizační brána poskytuje služby DHCP a DNS pro zařízení, která je třeba registrovat do systému před jejich vpuštěním do produkční sítě
* řešení funguje samo o sobě jako Radius server pro autentizaci i accounting
* správa řešení pomocí SSH CLI a HTTPS
* možnost granulárního nastavení administrátorských oprávnění do úrovně spravovaných síťových zařízení a portů
* autentizace a bezpečnostní kontrola koncového zařízení před jeho připojením do sítě nezávisle na způsobu připojení (LAN, WiFi, VPN)
* profilace připojeného zařízení a klienta buď manuálně vytvořeným pravidlem nebo na základě jeho otisku, který je získán skenem sítě nebo komunikací s externím systémy
* Podpora politik pro automatickou profilaci zařízení, minimálně dle: SNMP, Radius, Syslog, DHCP, API, SSH, Nmap, HTTP/S, IP range, telnet, vyhodnocení TCP/UDP portů, Vendor OUI/MAC, WMI profil
* Periodická kontrola připojeného zařízení, zda stále odpovídá profilu, na základě, kterého bylo vpuštěno do sítě a možnost jeho odpojení v případě, že nesplňuje podmínky původního profilu
* Podporované autentizační protokoly MS-CHAP v2, PAP, EAP-MD5, EAP-PEAP, EAP-TLS, EAP-FAST, EAP-TTLS
* Po úspěšné autentizaci možnost definice parametrů síťového portu či SSID pomocí standardních Radius atributů
* Po úspěšné autentizaci je možné na síťové zařízení instalovat z NAC brány konfiguraci, např. ACL
* Podpora 802.1x
* Podpora MAB autentizace
* Podpora tvorby lokálních účtů a lokální autentizace
* Podpora registrace koncových zařízení v NAC před jejich fyzickým připojením do sítě
* Podpora funkce Radius Proxy
* Možnost integrace se stávající certifikační autoritou (CA)
* Podpora agentů pro operační systémy Windows, MacOS, Linux. Licence pro tyto agenty je součástí dodané licence NAC
* Podpora integrace se stávajícím Active Directory serverem pro autentizaci uživatelů pomocí LDAP
* Podpora CAPTIVE portálu v rámci autentizační brány s plně editovatelným prostředím
* Nejméně 5 různých CAPTIVE portálů z důvodu velikosti prostředí
* V případě zjištění bezpečnostního incidentu je řešení schopné zablokovat konektivitu připojeného zařízení nebo změnit síťový segment na úrovni vrstvy L2
* Podpora integrace s MDM nástroji (např. MS In-Tune či jiné obdobné)
* Podpora integrace s poptávaným firewallem a analytickým řešením nad provozem poptávaného firewallu i NAC
* Uživatel s oprávněním administrátora má možnost ručně registrovat, zablokovat nebo smazat nové zařízení nebo uživatele
* Kontrola pravidel se provádí před povolením přístupu do sítě na základě profilu nebo agenta na koncovém zařízení
* Kontrolu je možné provádět periodicky, pokud je zařízení připojeno do sítě
* Kontrola stavu registrů síťových klientů s Windows
* Kontrola stavu antiviru na stanici
* Kontrola existence konkrétních souborů v lokálním systému
* Ověření domény
* Ověření certifikátu a jeho atributů (vydavatele, expirace, common-name a dalších)
* Ověření verze a úrovně aktualizací na operačním systému
* Možnost sběru informací o nainstalovaných aplikacích na stanici
* Upozornění uživatele v případě nesplnění bezpečnostní kontroly, případně s přesměrováním na CAPTIVE portál
* Možnost odeslání zprávy na koncovou stanici v případě nasazení agenta
* Řešení je možné ovládat i pomocí výrobcem popsaných API, které musí být dostupné v manuálech či dokumentaci na stránkách výrobce
* Dostupnost a možnost tvorby reportů o stavu platformy a připojených zařízení v reálném čase a zpětně alespoň o jeden týden
* Všechny požadované funkce pokrývá jeden typ licence, je možné dodatečně dokoupit další licence
* Licence minimálně pro 700 zařízení, s možností budoucího rozšíření až do počtu 25.000 zařízení
* Dodaná licence musí být trvalá a funkční i po ukončení podpory

## Dodávka licencí

V rámci dodávky hardwarových komponent musí být součástí dodávka všech potřebných licencí, které budou umožňovat provozování požadovaných funkcionalit a rozsahu využití hardware (např. při licencování na port, musí být pokryt požadovaný počet portů apod.). Pokud je nabízena spolu s hardware licence trvalá, která umožňuje provozování funkcionalit na neomezenou domu, musí být dodán tento typ licence. V případě, že dodávka takové licence není možná, bude dodána licence na dobu provozu 7 let.

## Podpora nasazení

Dodavatel poskytne v ceně dodávky za účelem nasazení všech dodaných HW prvků a SW instalační a konfigurační podporu a to na vyžádání Zadavatele v maximálním rozsahu 10 člověkodní, které bude mít možnost zadavatel vyčerpat v průběhu prvních dvou let od data dodání. Do uvedeného času se započítává pouze aktivní práce a konzultace za účasti Zadavatele, případná příprava a řešení mimo součinnost Zadavatele nebude do rozsahu započítána. Instalační a konfigurační podpora bude poskytována pracovníky dodavatele či pracovníky podpory dodavatelů (výrobců) zařízení a software, přičemž tato podpora je zahrnuta v ceně plnění; tím není dotčena povinnost dle čl. VI odst. 1 písm. i) smlouvy.