

Příloha č. 2 – Formulář technických požadavků

VZ Zvýšení kybernetické bezpečnosti Zlínského kraje

Dodávka a implementace bezpečnostních prvků komunikační sítě, ochrany e-mailové komunikace a koncových zařízení včetně zajištění následné podpory

Číslo	Minimální požadované vlastnosti a funkce (požadavky)	Splňuje dodavatel požadavky (Ano/Ne)	Popis naplnění požadavků dodavatelem
0.	Dodávané řešení ani žádná z jeho částí nesmí být v době podání nabídky v režimu End of Sale / End of Support	ANO	dle aktuálně dostupných informací
1.	Modernizace aktivních prvků komunikační sítě		
1.1	Modernizace aktivních prvků společného bezpečnostního perimetru pro sítě LAN KÚZK a 21Net podporující ochranu proti „pokročilým hrozbám“		
1.1.1	NGFW		
1.1.1.1	HW platforma	ANO	Budou dodány HW boxy
1.1.1.2	řízení bezpečného přístupu mezi vnější a vnitřní sítí	ANO	Konfigurací pravidel dle výstupu prováděcího projektu
1.1.1.3	segmentaci zejména použitím demilitarizovaných zón	ANO	Konfigurací pravidel dle výstupu prováděcího projektu
1.1.1.4	zajištění bezpečného vzdáleného přístupu pro uživatele (SSL VNP)	ANO	Konfigurací pravidel dle výstupu prováděcího projektu
1.1.1.5	zajištění blokování přenášených dat, které neodpovídají požadavkům	ANO	Konfigurací pravidel dle výstupu prováděcího projektu
1.1.1.6	podpora WAN load balancing	ANO	Funkcionalita SD-WAN, viz. "Datový list - FortiOS"
1.1.1.7	IPSec VPN – propojení lokalit formou LAN-to-LAN	ANO	viz. "Datový list - FortiOS"
1.1.1.8	podpora NGFW/UTM (AV, IPS, application control, WebFiltering)	ANO	viz. "Datový list - FortiOS"
1.1.1.9	možnost centrálního sběru logů s následnou analýzou	ANO	viz. "Datový list - FortiOS"
1.1.1.10	podpora Syslog pro zasílání logů	ANO	viz. "Datový list - FortiOS"
1.1.1.11	zabezpečený management (GUI / CLI) - SSH, HTTPS přístup	ANO	viz. "Datový list - FortiOS"
1.1.1.12	podpora IPv6	ANO	viz. "Datový list - FortiOS"
1.1.1.13	podpora záložního připojení do internetu	ANO	viz. "Datový list - FortiOS"
1.1.1.14	podpora dynamických směrovacích protokolů RIP, BGP, OSPF	ANO	viz. "Datový list - FortiOS"
1.1.1.15	podpora HA nasazení v režimech Active/Passive a Active/Active	ANO	viz. "Datový list - FortiOS"

1.1.1 .16	podpora min. 20 virtuálních instancí	ANO	viz. "Datový list - Fortigate 1500D"
1.1.1 .17	duální napájecí zdroje	ANO	viz. "Datový list - Fortigate 1500D"
1.1.1 .18	integrace s technologií SandBoxu (bod 1.1.2)	ANO	viz. "Datový list - FortiOS"
1.1.1 .19	lokální úložiště: 240 GB	ANO	viz. "Datový list - Fortigate 1500D"
1.1.1 .20	porty: 8x 10GB SFP+, 16x GE SFP, 16x GE RJ45	ANO	viz. "Datový list - Fortigate 1500D"
1.1.1 .21	min. propustnost FW pro 512 byte UDP paket: 60 Gbps	ANO	viz. "Datový list - Fortigate 1500D"
1.1.1 .22	počet současných připojení: 12 Mil	ANO	viz. "Datový list - Fortigate 1500D"
1.1.1 .23	nové session/sec: 300 000	ANO	viz. "Datový list - Fortigate 1500D"
1.1.1 .24	propustnost IPSEC VPN: 40 Gbps	ANO	viz. "Datový list - Fortigate 1500D"
1.1.1 .25	Propustnost SSL inspekce: 10 Gbps	ANO	viz. "Datový list - Fortigate 1500D"
1.1.1 .26	propustnost application control: 15 Gbps	ANO	viz. "Datový list - Fortigate 1500D"
1.1.1 .27	propustnost při současně zapnutých funkcích FW, IPS, APP Control a Malware protection = threat protection: 5 Gbps	ANO	viz. "Datový list - Fortigate 1500D"
1.1.2	SandBox		
1.1.2 .1	HW platforma nebo vApp/VM do prostředí TC KÚZK	ANO	Bude dodán HW box
1.1.2 .2	webové uživatelské rozhraní a příkazová řádka	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .3	možnost vytvořit více účtů správců	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .4	zálohování a obnova nastavení	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .5	upozorňování na odhalené škodlivé soubory e- mailem	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .6	možnost reportingu	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .7	centralizovaná stránka pro vyhledávání umožňující nastavit vlastní podmínky vyhledávání	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .8	automatické aktualizace signatur	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .9	automatické kontroly a stahování nových obrazů virtuálního stroje	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .10	monitorování stavu virtuálního stroje	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .11	ověřování správců pomocí serveru Radius nebo LDAP/AD	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .12	podpora statického směrování	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .13	vstup souborů od integrovaných zařízení (NGFW a MailGW)	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .14	možnost vytvořit pro zkoumaný soubor simulované uzavřené síťové prostředí	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .15	podpora klastrování pro vysokou dostupnost	ANO	viz. "Datový list - FortiSandbox"

1.1.2 .16	dynamické aktualizace databáze hrozeb a periodické předávání dynamické databáze registrovaným entitám	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .17	databáze kontrolních součtů souborů a škodlivých URL	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .18	vzdálený záznam událostí na syslog server	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .19	možnost nastavení podporovaných typů souborů u virtuálních strojů	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .20	detekce síťových hrozeb v režimu odposlechu	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .21	identifikace aktivity botnetu a síťových útoků, návštěvy škodlivých URL	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .22	plánovatelné prohledávání síťových úložišť sdílených přes SMB/NFS a karanténa podezřelých souborů	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .23	kontrola URL adres vložených v dokumentech	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .24	widgety pro monitorování v reálném čase (zobrazení podle zdroje a časového období)	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .25	podrobný prohlížeč událostí: dynamická tabulka s detaily o akcích, názvy škodlivého softwaru, hodnocením, typem, zdrojem, destinací, časem detekce a cestou ke stažení	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .26	záznam událostí — grafické uživatelské rozhraní, stažení protokolu ve formátu RAW	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .27	generování reportů o škodlivých souborech: podrobné zprávy o charakteristice a chování souboru – modifikace souboru, související procesy, zásahy do registrů, chování v síti, snímek virtuálního stroje, chronologický přehled chování	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .28	další analýza: stáhnutelné soubory — vzorek souboru, protokoly událostí v sandboxu, PCAP Capture a indikátory ve formátu STIX	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .29	stažitelné zachycené balíčky, originální soubory, tracer logy a screenshoty	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .30	aktivní část řešení vybavena grafickým komunikačním rozhraním v podobě HTTPS aplikace	ANO	viz. "FortiSandbox-3.0.1-Administration-Guide"
1.1.2 .31	Počet podporovaných VM v ceně / maximálně: 4/50	ANO	V ceně řešení je zahrnuta podpora pro 4 VM. Požadované maximální hodnoty lze dosáhnout clustrováním dalších HW boxů - viz. "FortiSandbox-3.0.1-Administration-Guide"
1.1.2 .32	Požadované licencování OS v ceně řešení: 4x Win10	ANO	V ceně řešení je zahrnuta licence 8x Win10
1.1.2 .33	Požadované licencování MS Office v ceně řešení: 4x MS Office	ANO	V ceně řešení je zahrnuta licence 4x MS Office
1.1.2 .34	Kapacita VM sandboxu (souborů/h): 160	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .35	Antivirová kontrola (souborů/h): 6000	ANO	viz. "Datový list - FortiSandbox"
1.1.2 .36	Podporované OS VM: Windows 7, Windows 10, macOS, Android	ANO	viz. "Datový list - FortiSandbox"

1.1.2.37	podporované soubory: .7z, .ace, .apk, .arj, .bat, .bz2, .cab, .cmd, .dll, .doc, .docm, .docx, .dot, .dotm, .dotx, .exe, .gz, .htm, html, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEblink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip	ANO	viz. "Datový list - FortiSandbox"
1.1.2.38	podporované protokoly v integrovaném nasazení: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM a jejich SSL kryptované verze	ANO	viz. "Datový list - FortiSandbox"
1.1.2.39	Pro chod VApp/VM v prostředí TCK KÚZK bude možnost vyhrazení HW prostředků s následující charakteristikou: počet podporovaných vCPU: 8 počet virtuálních NIC 6 velikost úložiště virtuálního stroje: 1 TB velikost operační paměti virtuálního stroje: 16 GB	ANO	Požadavky na VM v prostředí TCK KÚZK pravděpodobně nebudeme využívat, protože se jedná o dodávku HW nodu. Nicméně, až na základě Prováděcího projektu bude stanoveno, zda nabízené zdroje nebudeme opravdu využívat.
1.1.3	Požadovaná implementace a integrace NGFW a SandBox		
1.1.3.1	integrace do provozovaného SIEM řešení	ANO	Konfigurací dle výstupu Prováděcího projektu
1.1.3.2	vzájemná integrace NGFW a Sandboxu	ANO	Konfigurací dle výstupu Prováděcího projektu
1.1.3.3	integrace s technologií MailGW (bod 2)	ANO	Konfigurací dle výstupu Prováděcího projektu
1.1.3.4	migrace FW pravidel ze současného řešení a jejich profilaxe	ANO	Konfigurací dle výstupu Prováděcího projektu
1.1.3.5	instalace a konfigurace dle Prováděcího projektu včetně návrhu řešení	ANO	Instalací a konfigurací dle Prováděcího projektu včetně návrhu řešení
1.1.3.6	kvalifikované seznámení obsluhy v rozsahu min. 2 MD	ANO	Dle Plánu kvalifikovaného seznámení uživatelů a administrátorů s dodaným dílem, který je požadován jako součást Prováděcího projektu
1.2	Modernizace aktivních prvků sítě LAN KÚZK pro možnost „adaptivního řízení“ přístupu do komunikační infrastruktury		
1.2.1	Přístupový přepínač – 48p		
1.2.1.1	základní L3 přepínač	ANO	Statický i dynamický routing, viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1.2	zabezpečený management (GUI / CLI)-SSH, HTTPS přístup	ANO	Všechny jmenované způsoby viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1.3	podpora linkové agregace (LACP/statická)	ANO	Všechny jmenované způsoby viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1.4	možnost diagnostiky a troubleshooting	ANO	GUI, CLI, RestAPI, Mirroring, OpenFlow, SNMP, Syslog export ... viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1.5	provedení do RACK -1U	ANO	Velikost 1RU viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf

1.2.1 .6	podpora VLAN	ANO	IEEE 802.1Q (4,094 VLAN IDs), 2048 současně, viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1 .7	Podpora dynamických VLAN	ANO	IEEE 802.1x a GVRP/MVRP viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1 .8	Podpora ověřování 801.X	ANO	Široké možnosti IEEE 802.1x viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1 .9	statické routování, RIP	ANO	Staticky, RIP, OSPF vč. IPv6 verzí viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1 .10	podpora IPv6	ANO	IPv6 Ready Certified viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1 .11	ACL pro přístup k prvku, definice ACL na úrovni VLAN	ANO	Managemetn VLAN, ACL i RADIUS/Tacacs+ viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf resp. KB - https://community.arubanetworks.com/t5/Wired-Intelligent-Edge-Campus/ArubaOS-Switch-How-to-Configure-a-Management-VLAN/ta-p/421280
1.2.1 .12	48x 10/100/1000 Mbit RJ45 POE+ port	ANO	48x RJ45 10/100/1000Mbps PoE+ a 4x SFP+ 1/10Gbps viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1 .13	4x SFP+ 1/10GB port	ANO	48x RJ45 10/100/1000Mbps PoE+ a 4x SFP+ 1/10Gbps viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1 .14	switching kapacita 170 Gbps	ANO	176Gbps switching viz Performance v DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1 .15	propustnost 100 Mpps	ANO	112Mpps throughput viz Performance v DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1 .16	MAC tabulka min. 32 000 záznamů	ANO	32 768 položek v MAC table size Performance v DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1 .17	Routing tabulka IPv4/IPv6 – 10000/5000 záznamů	ANO	10000 záznamů IPv4 při použití RIP protokolu viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1 .18	napájení PoE+ (30W / port), celkově PoE kapacita 370W	ANO	IEEE 802.3at, 370W PoE+ a 30W na port viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1 .19	možnost stohování switchů přes min. 2x 10 Gbps port	ANO	Virtuální VSF stoh (až 8 přepínačů ve stohu) viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf

1.2.1 .20	režimy portu: access, trunk a hybrid	ANO	IEEE 802.1Q (4,094 VLAN IDs), 2048 současně, viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf VoIP vlan a její přiřazení (od strany 48) - https://support.hpe.com/hpsc/doc/public/display?docId=a00038722en_us
1.2.1 .21	DHCP snooping, ARP protection, port security, loopback protection	ANO	ARP / DHCP Protection, Port Security viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf Loop Protection (strana 528) v CLI REF - http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c04793912-4.pdf
1.2.1 .22	integrace s centrální správou aktivních prvků (bod 1.2.6)	ANO	Nativně podporovaný device. AirWave viz Management v tab. tech. Spec. v DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1 .23	tzv. zero touch provisioning	ANO	Viz ZTP v DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.1 .24	integrace s technologií policíy enforceru (bod 4)	ANO	Široké možnosti IEEE 802.1x a další benefity s Aruba ClearPass viz DS - https://www.arubanetworks.com/assets/ds/DS_2930FSwitchSeries.pdf
1.2.2	Agregační přepínač		
1.2.2 .1	modulární L3 přepínač	ANO	Statický i dynamický routing, viz DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .2	zabezpečený management (GUI / CLI) - SSH, HTTPS přístup	ANO	Všechny jmenované způsoby viz DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .3	možnost N+1 redundance napájení AC240V	ANO	Ano viz PowerSupplies v tab. Specification a dále DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .4	možnost redundance logických management karet (modulů)	ANO	Viz Redundant Management v DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .5	6× 40Gb QSFP+ port	ANO	Viz I/O ports and slots v tab. Specification v DC - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .6	24× 1/10Gb SFP+ port	ANO	Viz I/O ports and slots v tab. Specification v DC - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .7	12× 1GB SFP	ANO	Viz I/O ports and slots v tab. Specification v DC - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .8	24× 10/100/1000 Base-T POE+	ANO	Viz I/O ports and slots v tab. Specification v DC - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf

1.2.2 .9	2 volné sloty pro osazení budoucích linkových karet	ANO	Viz předložená nabídka osazení chassis a popis 12ti slotové verze viz Specification v DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .10	podpora linkové agregace (LACP/statická)	ANO	Všechny jmenované způsoby viz DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .11	podpora virtuálního chassi – až 4 prvky	ANO	Virtuální VSF stoh (momentálně s limitem dvou memberů v případě chassis) viz MCG - http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00038741en_us-1.pdf , v souladu s odpovědí "Vysvětlení zadávací dokumentace č. 5" (dotaz č.1)
1.2.2 .12	možnost diagnostiky a troubleshooting	ANO	GUI, CLI, RestAPI, Mirroring, OpenFlow, SNMP, Syslog export ... viz DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .13	provedení do RACK	ANO	Mounting and Enclosure v tab. Specification viz DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .14	podpora VLAN	ANO	IEEE 802.1Q (4,094 VLAN současně), viz DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .15	Podpora dynamických VLAN	ANO	IEEE 802.1x a GVRP/MVRP viz DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .16	Podpora ověřování 801.X,statické routování, RIP, OSPF	ANO	Vše uvedené a rovněž i BGP viz DS - Layer 3 v DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .17	podpora IPv6	ANO	IPv6 Ready Certified viz DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .18	ACL pro přístup k prvku, definice ACL na úrovni VLAN	ANO	Managementn VLAN, ACL i RADIUS/Tacacs+ viz DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf resp. KB - https://community.arubanetworks.com/t5/Wired-Intelligent-Edge-Campus/ArubaOS-Switch-How-to-Configure-a-Management-VLAN/ta-p/421280
1.2.2 .19	switching kapacita 1200 Gbps	ANO	1920Gbps switching viz Performance v DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .20	propustnost 1100 Mpps	ANO	1142Mpps throughput viz Performance v DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .21	MAC tabulka min. 64 000 záznamů	ANO	64000 záznamů viz DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .22	Routing tabulka IPv4/IPv6 – 10000/5000 záznamů	ANO	10000 / 5000 záznamů v rout. tabulce viz DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf

1.2.2 .23	DHCP snooping, ARP protection, port security, loopback protection	ANO	ARP / DHCP Protection, Port Security viz DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf Loop Protection (strana 528) v CLI REF - http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c04793912-4.pdf
1.2.2 .24	integrace s centrálním správou aktivních prvků (bod 1.2.6)	ANO	Nativně podporovaný device. AirWave viz Management v tab. tech. Spec. v DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.2 .25	integrace s technologií policíy enforceru (bod 4)	ANO	Široké možnosti IEEE 802.1x a další benefity s Aruba ClearPass viz DS - https://www.arubanetworks.com/assets/ds/DS_5400Rzl2SwitchSeries.pdf
1.2.3	CORE přepínač		
1.2.3 .1	modulární Advanced L3 přepínač	ANO	2RU Modulární forma viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .2	zabezpečený management (GUI / CLI) - SSH, HTTPS přístup	ANO	Všechny jmenované způsoby viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .3	N+1 redundance napájení AC240V	ANO	Redundance 2+2, lze osadit až 4 zdroje do 2RU. Redundantní zdroje a ventilátory viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .4	20x 40Gb QSFP+ port	ANO	Viz IO ports and slots v tab. Specification v DC - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .5	24x 1/10Gb SFP+ port	ANO	Viz IO ports and slots v tab. Specification v DC - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .6	24x 1/10GBase-T	ANO	Viz IO ports and slots v tab. Specification v DC - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .7	podpora linkové agregace (LACP/statická)	ANO	Obě uvedené formy viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .8	podpora virtuálního chassi – min 4 prvky	ANO	Ano až 10 viz IRF v DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .9	možnost diagnostiky a troubleshooting	ANO	GUI, CLI, RestAPI, Mirroring, OpenFlow, SNMP, Syslog export, sFlow ... viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .10	provedení do RACK	ANO	2RU Modulární forma viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .11	podpora VLAN	ANO	IEEE 802.1Q (4,094 VLAN současně na portu), viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf

1.2.3 .12	Podpora dynamických VLAN	ANO	IEEE 802.1x a VxLAN s OVSDB viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .13	Podpora ověřování 801.X	ANO	IEEE 802.1x viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .14	podpora VXLAN, VTEP a OVSDB	ANO	Vše uvedené viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .15	DCB protokol	ANO	Viz DCB protocols v DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .16	role-based access control (RBAC)	ANO	Viz Remote configuration and management v DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .17	podpora IPv6	ANO	Viz IPv6 v tab. Standards and Protocols viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .18	statické routování, RIP, OSPFv2/v3, BGP/BGP+, Policy routing	ANO	Vše uvedené viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .19	ACL pro přístup k prvku, definice ACL na úrovni VLAN	ANO	Viz Management security v DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .20	switching kapacita 3,2 Tbps	ANO	3,2Tbps switching viz Performance v DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .21	propustnost 2790 Mpps	ANO	2796Mpps throughput viz Performance v DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .22	MAC tabulka min. 130 000 záznamů	ANO	136000 záznamů viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .23	Routing tabulka IPv4/IPv6 – 128000/64000 záznamů	ANO	12800 / 64000 záznamů v rout. tabulce viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.2.3 .24	DHCP snooping, ARP protection, port security, loopback protection	ANO	DHCP Snooping, Port Security viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf ARP Snooping / Protection (strana 693) v SCR - https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c05349565 LBD viz např. https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c03529362
1.2.3 .25	integrace s centrální správou aktivních prvků (bod 1.2.6)	ANO	Skrze SNMP jako tzv. Generic SNMP device viz APM User Guide např. strana 122: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.4	WIFI AP		

1.2.4 .1	současné vysílání dualband (2,4 / 5 GHz)	ANO	Dual-radio (5G .11AC Wave2 / 2,4G .11N) viz DS - https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.4 .2	podpora AC Wave2 - napájení přes PoE	ANO	Wave2 s 802.3at bez omezení, viz DFS - https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.4 .3	podpora RADIUS	ANO	Viz Aruba 8.x User Guide (od strany 236): https://www.arubanetworks.com/techdocs/ArubaOS_83_Web_Help/Content/PDFs/ArubaOS%208.3.0.x%20User%20Guide.pdf
1.2.4 .4	podpora min. 6 SSID na jednom rádiu	ANO	Až 16 ESSID per radio viz DS - https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.4 .5	podpora 802.11 a/b/g/n/ac wave2	ANO	Dual-radio (5G .11AC Wave2 / 2,4G .11N) viz DS - https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.4 .6	podpora MIMO 3x3:3	ANO	3x3:3 v případě 5GHz a 2x2:3 v případě 2,5Ghz radia, DS- https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.4 .7	podpora 802.3 af/at	ANO	IEEE 802.3af/802.3at (.3at bez omezení) viz DFS - https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.4 .8	zabezpečený management	ANO	Viz Aruba 8.x User Guide (od strany 811): https://www.arubanetworks.com/techdocs/ArubaOS_83_Web_Help/Content/PDFs/ArubaOS%208.3.0.x%20User%20Guide.pdf
1.2.4 .9	decentralizovaný management	ANO	Možné módy - Instant cluster / RAP / stand-alone - viz, https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf a např. https://www.arubanetworks.com/techdocs/Instant_40_Mobile/Advanced/Content/UG_files/IAP_management/ConvertingIAPtoStandalone.htm
1.2.4 .10	AP pro enterprise použití	ANO	Až 1,3Gbps, základní enterprise model AP, viz DS - https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.4 .11	integrovaná anténa	ANO	V případě nabízeného IAP-305 ano, viz DS - https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.4 .12	správa prvků z jednoho místa	ANO	Ideálně za pomoci management nástroje AirWave (např. od strany 13)- http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.4 .13	oddělení sítí pro jednotlivé typy uživatelů	ANO	Až 16 oddělených sítí (SSID) s individuálním nastavením, také dle autentizace. DS - https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf

1.2.4 .14	nastavení bezpečnosti samostatně pro každou síť	ANO	Až 16 oddělených sítí (SSID) s individuálním nastavením, také dle autentizace. DS - https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.4 .15	podpora zabezpečené Guest sítě	ANO	Přístup hosta a bezpečnost takové sítě s Aruba Instant: https://www.arubanetworks.com/assets/so/SO_ArubaInstantWiFi.pdf nebo také (od strany 118) - https://www.arubanetworks.com/techdocs/Instant_83_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf Případně s Aruba ClearPass (od strany 397): https://www.arubanetworks.com/techdocs/Instant_83_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf
1.2.4 .16	integrace s centrální správou aktivních prvků (bod 1.2.6)	ANO	Nativně podporované zařízení. Viz např. - https://www.arubanetworks.com/techdocs/Instant_83_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf
1.2.4 .17	integrace s technologií políciy enforceru (bod 4)	ANO	IEEE 802.1x metody, Captive portál, MAC auth ... a jiné (od strany 144) - https://www.arubanetworks.com/techdocs/Instant_83_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf
1.2.5	Virtuální WLC		
1.2.5 .1	virtualizovaný kontroler	ANO	Aruba Instant AP Cluster viz DS - https://www.arubanetworks.com/assets/so/SO_ArubaInstantWiFi.pdf
1.2.5 .2	možnost běhu i na HW vlastních AP	ANO	Aruba Instant AP Cluster viz DS - https://www.arubanetworks.com/assets/so/SO_ArubaInstantWiFi.pdf https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.5 .3	podpora mechanismu izolace klientů	ANO	Více způsobů možných vč. filtrace na úrovni fw. Základní nastavení ale dostačuje požadavku, viz: https://www.arubanetworks.com/techdocs/InstantWenger_Mobile/Advanced/Content/Instant%20User%20Guide%20-%20volumes/Deny_Inter_User_Bridging.htm
1.2.5 .4	centralizovaná architektura správy WiFi	ANO	Aruba Instant AP Cluster viz DS - https://www.arubanetworks.com/assets/so/SO_ArubaInstantWiFi.pdf
1.2.5 .5	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	ANO	Aruba Instant AP Cluster viz DS - https://www.arubanetworks.com/assets/so/SO_ArubaInstantWiFi.pdf https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.5 .6	Podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius (např. LDAP, MS AD ...)	ANO	IEEE 802.1x metody, Captive portál, MAC auth ... a jiné (od strany 144) - https://www.arubanetworks.com/techdocs/Instant_83_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf

			Instant_83_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf
1.2.5.7	ACL pro filtrování provozu	ANO	Politiky firewall a content filtrace (od strany 176): https://www.arubanetworks.com/techdocs/Instant_83_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf
1.2.5.8	Rychlá instalace i rozšíření sítě, škálovatelnost	ANO	Aruba Instant AP Cluster viz DS - https://www.arubanetworks.com/assets/so/SO_ArubaInstantWiFi.pdf
1.2.5.9	RF optimalizace sítě	ANO	Viz RF Management v DS - https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.5.10	Automatický QoS pro hlas a video	ANO	WMM (od strany 282) - https://www.arubanetworks.com/techdocs/Instant_83_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf ,ale také celá řada dalších mechanismů vč. šifrovaných přenosů hlasu a videa (UC) https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.5.11	Vysoká dostupnost	ANO	Aruba Instant AP Cluster viz DS - https://www.arubanetworks.com/assets/so/SO_ArubaInstantWiFi.pdf https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.5.12	Integrovaný Firewall, integrované wireless IPS/IDS	ANO	Všechny uvedené, viz: https://www.arubanetworks.com/assets/so/SO_ArubaInstantWiFi.pdf https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf
1.2.6	Centrální správa aktivních prvků LAN KÚZK		
1.2.6.1	Správa autonomních AP, "tenkých" AP, fyzických i virtuálních WiFi controlérů a přepínačů.	ANO	Všechny Aruba prvky, wireless především. Viz DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf Také viz stana 15 tabulka 1: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6.2	Licence pro správu všech dodávaných přepínačů a bezdrátových prvků, možnost flexibilního rozšiřování až do 2500 zařízení.	ANO	S VM v Enterprise módu až teoreticky 4000. Viz DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf
1.2.6.3	Software bude dodán ve formě VApp/VM bez nutnosti pořizovat další licence např. pro OS nebo databáze.	ANO	Nabízen jako VM appliance vč. všech potřebných licencí ke správě nabízených zařízení, další licence nevyžaduje. Veškeré součásti již integrované ve VM appliance. Licencuje na zařízení, viz DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf

1.2.6 .4	Manuální a automatické discovery síťových zařízení pomocí SNMP, HTTP a CDP skenování.	ANO	Všechny uvedené (od strany 118), viz: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .5	Monitorovací nebo plný-managed režim pro nově objevená zařízení jako ochrana před nechtěným přepsáním konfigurace.	ANO	Monitoring vs. Managed mod správy od strany 185. Oprava / přepis konfigurace viz tab. strana 127. http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .6	RBAC pro jednotlivé síťové operátory na úrovni síťových zařízení a jejich funkcí. Možnost plného oddělení tak aby se v rámci jednoho systému dalo spravovat více samostatných entit s vlastními procesy.	ANO	RBAC viz Easy to Use Web Interface v DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf Případně Administrative Roles (od strany 16 resp. 36) viz: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .7	Webové uživatelské rozhraní s podporou HTTPS.	ANO	Viz Easy to Use Web Interface v DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf Add SSL certificate viz strana 372 tab. 177, bod 9-3: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .8	Možnost přizpůsobení prostředí ovládací obrazovky (webový dashboard), zvláště pro každého síťového operátora.	ANO	Viz Customizing the Dashboard (strana 264): http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .9	Vyhledávání koncových uživatelů na základě MAC adresy, IP adresy, uživatelského jména a LAN hostname.	ANO	Viz Troubleshooting and Diagnostics v DS: https://www.arubanetworks.com/assets/ds/DS_AW.pdf Dále pak viz Search Methods (strana 21): http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .10	Real-time monitoring každého uživatele v síti včetně charakteristik jako jsou: kvalita RF signálu, utilizace pásma (in/out), autentizační status a čas, historie roamingu, délka trvání připojení, typ klientského zařízení, asociace s SSID, objem a seznam používaných L7 aplikací a navštívených webových kategorií.	ANO	Viz Real Time Monitoring and Visibility v DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf Dále pak viz kapitola About Homepage v: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .11	Real-time monitoring všech připojených a řízených fyzických a virtuálních zařízení a zasílání alarmů při změnách stavu.	ANO	Viz Real Time Monitoring and Visibility v DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf Dále pak viz kapitola Using Topology v (od strany 174) a Types of Triggers respektive (strana 246): http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .12	Podpora sběru flow z každého připojeného zařízení.	ANO	Aplikační flow pomocí technologie AppRF viz : http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf

1.2.6 .13	Podpora alarmování s možností nastavitelných prahů pro jednotlivé události. Podporované události: odchylka od baseline konfigurace, RF metrika, nově objevené zařízení, Radius autentizace, Rogue AP, nadměrné využití AP (bandwidth), počet připojených klientů, nadměrná využití klientem (bandwidth), Up/Down zařízení, Up/Down Radio, IDS událost.	ANO	Viz Real Time Monitoring and Visibility v DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf Dále pak viz kapitola Using Topology v (od strany 174) a Types of Triggers respektive (strana 246): http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .14	Konfigurace formu politik aplikovatelných na všechna zařízení, jejich skupinu nebo jednotlivé zařízení.	ANO	Viz Configuration Management v DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf , případně viz Device Groups (strana 71) v: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .15	Možnost tvorby konfiguračních šablon, jak nových tak z běžících zařízení jako jsou AP nebo kontrolery.	ANO	Viz Configuration Management v DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf , případně viz Groups Templates (od strany 200) v: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .16	Podpora konfiguračních změn a upgrade firmwaru pomocí jednorázových nebo opakujících se pracovních úloh (scheduled-job).	ANO	Viz Configuration Management v DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf Dále pak pod-kapitolou začínající "Using the System > ..." od strany 257: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .17	Kontrola provedených konfiguračních změn, v případě nesouladu definice a runtime stavu konfigurační rollback.	ANO	Viz Configuration Management v DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf Dále viz Configuration Audit - kapitola AP/Devices > Audit (strana 127) a Configuration Compliance (obecně Verifying / Mismatched statut zařízení) a dále pak Configuration Change Jobs: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .18	Archivace konfigurací.	ANO	Viz Configuration Management v DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf
1.2.6 .19	Audit konfigurace, porovnání rozdílů proti přednastaveným politikám individuálně pro jednotlivá a hromadně proti skupině zařízení.	ANO	Viz Configuration Management v DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf Dále viz Configuration Audit - kapitola AP/Devices > Audit (strana 127) a Configuration Compliance (obecně Verifying / Mismatched statut zařízení) a dále pak Configuration Change Jobs. Porovnání konfigurace pak viz Configuring and Managing Devices (strana 185): http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf

1.2.6 .20	Konfigurační management: zálohy a obnova konfigurace, srovnávání rozdílů, auditování podle přednastavených i vlastních pravidel.	ANO	Viz Configuration Management v DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf Dále viz Configuration Audit - kapitola AP/Devices > Audit (strana 127) a Configuration Compliance (obecně Verifying / Mismatched statut zařízení) a dále pak Configuration Change Jobs. Porovnání konfigurace pak viz Configuring and Managing Devices (strana 185). Porovnání skupin viz Comparing Device Groups (strana 109): http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .21	Možnost funkčního rozšíření o monitorování stability a odezvy ostatních síťových služeb pro jednotlivé klienty jako je průměrný čas odpovědi na DNS dotaz nebo průměrný čas zpracování RADIUS autentizace.	ANO	Clarity Synthetic schopnosti viz Connectivity Analytics v DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf a https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Command/Core_Download/Default.aspx?EntryId=28938
1.2.6 .22	Vytváření reportů v PDF formátů reportujících různé přehledové statistiky o využití sítě a jejím stavu. Automatizované pravidelné zasílání reportů mailem.	ANO	Viz kapitola 10 Creating, Running, and sending Reports (od strany 294): http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .23	Vizualizace umístění prvků sítě ve fyzických mapách. Zobrazení bezdrátových klientů na mapě a jejich signálu a využívaných L7 aplikací.	ANO	VisualRF a AppRF popsané v DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf Blíže pak kapitola 11 Using VisualRF (od strany 330) v: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .24	Možnost monitorování wireless IDS událostí z více samostatných systémů současně.	ANO	RAPIDS viz DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf Spolupracuje s dalšími systémy, nejen Aruba WIPS, prvky LAN, ale spolupracuje i se systémy 3. výrobců viz kapitola 8, Using RAPIDS and Rogue Classification od strany 220: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .25	Podpora systému pro automatizované bezzásahové zprovoznění připojeného zařízení.	ANO	Například Aruba Zero-touch-provisioning viz (strana 78): https://www.arubanetworks.com/assets/ds/DS_AW.pdf
1.2.6 .26	Monitoring a detekce síťových anomálií jako je např. nadměrné a neobvyklé navýšení objemu provozu a upozorňování na tyto stavy pomocí alarmů.	ANO	Monitoring každého uživatele vč. anomálií s AppRF, detailní statistika provozu, grafická a textová. Trendy a anomálie viz DS - https://www.arubanetworks.com/assets/ds/DS_AW.pdf Dále také viz Monitoring Basis (od strany 131) http://h20628.www2.hp.com/km-

			ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.2.6 .27	Pro chod VApp/VM v prostředí TCK KÚZK bude možnost vyhrazení HW prostředků s následující charakteristikou: počet podporovaných vCPU: 4 počet virtuálních NIC: 6 velikost úložiště virtuálního stroje: 500 GB velikost operační paměti virtuálního stroje: 16 GB	ANO	Celkový počet podporovaných vždy závisí na přidělených sys. prostředcích (a výkonu v IO) a počtu dalšího obsahu v AirWave - FloorPlans, Clients, RogueAPs Viz SizingGuide - https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Command/Core_Download/Default.aspx?EntryId=28949
1.2.7	Cílový stav topologie a příslušenství		
1.2.7 .1	Součástí dodávky je vybudování nových optických rozvodů v sídle Objednatele mezi serverovnou (2. patro) a jednotlivými patrovými rozvodnami (9., 10., 11., 12., 13., 14. a 15. patro) umístěnými horizontálně nad sebou. Optické trasy budou nataženy singlemódovým optickým kabelem 9/125 μm s minimálně 12 vlákny. Ukončení jednotlivých tras bude provedeno na obou stranách v optických vanách a ukončeno SC/PC nebo SC/APC konektory. Útlum jednotlivých optických vláken bude proměřen přímou nebo nepřímou metodou a ke každému vláknu bude vyhotoven měřicí protokol. Montáž a instalace bude probíhat dle norem ČSN50173 a ČSN50174 – je připuštěna možnost nabídnutí jiného rovnocenného řešení.	ANO	dle zadání a Vysvětlení zadávací dokumentace č. 8
1.2.7 .2	Všechny dodávané a implementované prvky musí být vybaveny komunikačními transceivery, kabely a DAC kabely tak, aby bylo možné nasazené prostředí plně propojit dle cílového schématu (kapitola 1.2.7, Příloha č. 1 - Podrobné vymezení díla).	ANO	dle zadání
1.2.8	Požadovaná implementace a integrace:		
1.2.8 .1	integrace do provozovaného SIEM řešení	ANO	integrace do provozovaného SIEM řešení
1.2.8 .2	vzájemná integrace s technologií Policy Enforceru (bod 4)	ANO	vzájemná integrace s technologií Policy Enforceru (bod 4)
1.2.8 .3	kvalifikované seznámení obsluhy v rozsahu min. 2 MD	ANO	kvalifikované seznámení obsluhy v rozsahu min. 2 MD
1.3	Modernizace aktivních prvků sítě 21Net podporující kryptaci provozu na L2 vrstvě ISO/OSI modelu		
1.3.1	CORE router		
1.3.1 .1	modulární Advanced L3 přepínač	ANO	2RU Modulární forma viz DS - https://h20195.www2.hp.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf

1.3.1 .2	zabezpečený management (GUI / CLI) - SSH, HTTPS přístup	ANO	Všechny jmenované způsoby viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .3	N+1 redundance napájení AC240V	ANO	Redundance 2+2, lze osadit až 4 zdroje do 2RU. Redundantní zdroje a ventilátory viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .4	4x 40Gb QSFP+ port	ANO	Viz IO ports and slots v tab. Specification v DC - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .5	20x 1/10Gb SFP+ port s podporou MACsec	ANO	Viz IO ports and slots v tab. Specification v DC - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .6	24x 1/10GBase-T	ANO	Viz IO ports and slots v tab. Specification v DC - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .7	podpora linkové agregace (LACP/statická)	ANO	Obě uvedené formy viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .8	podpora virtuálního chassi – min 4 prvky	ANO	Ano až 10 viz IRF v DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .9	možnost diagnostiky a troubleshooting	ANO	GUI, CLI, RestAPI, Mirroring, OpenFlow, SNMP, Syslog export, sFlow ... viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .10	provedení do RACK	ANO	2RU Modulární forma viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .11	podpora VLAN	ANO	IEEE 802.1Q (4,094 VLAN současně na portu), viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .12	podpora VXLAN, VTEP a OVSDDB	ANO	Vše uvedené viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .13	DCB protokol	ANO	Viz DCB protocols v DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .14	role-based access control (RBAC)	ANO	Viz Remote configuration and management v DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .15	podpora IPv6	ANO	Viz IPv6 v tab. Standards and Protocols viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .16	statické routování, RIP, OSPFv2/v3, BGP/BGP+, Policy routing	ANO	Vše uvedené viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf

1.3.1 .17	podpora MPLS a VPLS řešení VPN, VRF	ANO	MPLS a RF (VPN Instance) viz Conf.Guide: https://support.hpe.com/hpsc/doc/public/display?docId=c05162597 VPLS viz ReleaseNotes od strany 392: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00038185en_us-4.pdf
1.3.1 .18	ACL pro přístup k prvku	ANO	Viz Management security v DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .19	switching kapacita 3,2 Tbps	ANO	3,2Tbps switching viz Performance v DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .20	propustnost 2790 Mpps	ANO	2796Mpps throughput viz Performance v DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .21	MAC tabulka min. 130 000 záznamů	ANO	136000 záznamů viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .22	Routing tabulka IPv4/IPv6 – 128000/64000 záznamů	ANO	12800 / 64000 záznamů v rout. tabulce viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.1 .23	DHCP snooping, ARP protection	ANO	DHCP Snooping, Port Security viz DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf ARP Snooping / Protection (strana 693) v SCR - https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c05349565 LBD viz např. https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c03529362
1.3.1 .24	integrace s centrální správou aktivních prvků (bod 1.2.6)	ANO	Skrze SNMP jako tzv. Generic SNMP device viz APM User Guide např. strana 122: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.3.2	PE MPLS přepínač 21NET		
1.3.2 .1	Advanced L3 přepínač	ANO	Viz L3 Series a L3 Routing v DS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2 .2	zabezpečený management (GUI / CLI) - SSH, HTTPS přístup	ANO	Všechny jmenované viz DS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2 .3	N+1 redundance napájení AC240V	ANO	Redundance v úrovni pouze 1+1, ale dostatečná vzhledem k odpovědi č. 2 ve Vysvětlení ZD č. 7. DS viz DualRedundant PS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf

1.3.2.4	2x 1/10Gb SFP+ port s podporou MACsec - uplink	ANO	MACsec za pomoci vloženého modulu JH157A viz Parts list k 5510: https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c05215958
1.3.2.5	4x 1/10Gb SFP+ port	ANO	Viz I/O ports and slots v tab. Specification v DC - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2.6	16x 1GB SFP porty	ANO	Viz I/O ports and slots v tab. Specification v DC - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2.7	8x 1GB Dual SFP/ RJ45 porty	ANO	Viz I/O ports and slots v tab. Specification v DC - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2.8	podpora linkové agregace (LACP/statická)	ANO	Všechny jmenované způsoby viz DS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2.9	možnost diagnostiky a troubleshooting	ANO	GUI, CLI, RestAPI, Mirroring, OpenFlow, SNMP, Syslog export ... sFlow viz DS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2.10	podpora VLAN	ANO	IEEE 802.1Q (4,094 VLAN současně), viz DS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2.11	statické routování, RIP, OSPFv2/v3, BGP/BGP+	ANO	Vše uvedené, protokoly v sekci Layer 3 Routing v DS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2.12	podpora MPLS a VPLS řešení VPN	ANO	Vše uvedené, protokoly v sekci Layer 3 Routing v DS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2.13	podpora IPv6	ANO	Viz IPv6 v tab. Standards and Protocols viz DS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2.14	ACL pro přístup k prvku	ANO	Viz Security v DS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2.15	switching kapacita 280 Gbps	ANO	288Gbps switching viz Performance v DS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf

1.3.2 .16	propustnost 210 Mpps	ANO	214Mpps throughput viz Performance v DS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2 .17	MAC tabulka min. 32 000 záznamů	ANO	32768 záznamů viz DS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2 .18	Routing tabulka IPv4/IPv6 – 32000/16000 záznamů	ANO	32768 / 16384 záznamů v rout. tabulce viz DS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2 .19	možnost virtuálního chassi switchů přes min. 2x 10 Gbps	ANO	Ano až 9 viz IRF v DS - https://h20195.www2.hpe.com/v2/GetPDF.aspx/4AA6-5303ENW.pdf
1.3.2 .20	DHCP snooping, ARP protection	ANO	DHCP Snooping a Dynamic ARP protection viz DS - https://h50146.www5.hpe.com/products/networking/datasheet/HPE_FlexNetwork_5510_HI_Switch_Series.pdf
1.3.2 .21	integrace s centrální správou aktivních prvků (bod 1.2.6)	ANO	Skrze SNMP jako tzv. Generic SNMP device viz APM User Guide např. strana 122: http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-a00028488en_us-2.pdf
1.3.3	Firewally uzlových bodů 21NET		
1.3.3 .1	HW platforma	ANO	Budou dodány HW boxy
1.3.3 .2	řízení bezpečného přístupu mezi vnější a vnitřní sítí	ANO	Konfigurací pravidel dle výstupu prováděcího projektu
1.3.3 .3	segmentaci zejména použitím demilitarizovaných zón	ANO	Konfigurací pravidel dle výstupu prováděcího projektu
1.3.3 .4	zajištění bezpečného vzdáleného přístupu pro uživatele (SSL VNP)	ANO	Konfigurací pravidel dle výstupu prováděcího projektu
1.3.3 .5	zajištění blokování přenášených dat, které neodpovídají požadavkům	ANO	Konfigurací pravidel dle výstupu prováděcího projektu
1.3.3 .6	IPSec VPN – propojení lokalit formou LAN-to-LAN	ANO	viz. "Datový list - FortiOS"
1.3.3 .7	podpora NGFW/UTM (AV, IPS, application control, WebFiltering)	ANO	viz. "Datový list - FortiOS"
1.3.3 .8	možnost centrálního sběru logů s následnou analýzou	ANO	viz. "Datový list - FortiOS"
1.3.3 .9	podpora Syslog pro zasílání logů	ANO	viz. "Datový list - FortiOS"
1.3.3 .10	zabezpečený management (GUI / CLI) - SSH, HTTPS přístup	ANO	viz. "Datový list - FortiOS"
1.3.3 .11	podpora IPv6	ANO	viz. "Datový list - FortiOS"
1.3.3 .12	podpora záložního připojení do internetu	ANO	viz. "Datový list - FortiOS"
1.3.3 .13	min 6x 1GB port Base-T	ANO	viz. "Datový list - FortiGate_60E_Series"
1.3.3 .14	min. propustnost FW pro 512 byte UDP paket – 3Gbps	ANO	viz. "Datový list - FortiGate_60E_Series"

1.3.3 .15	min. počet současných připojení – 1,3 Milionů	ANO	viz. "Datový list - FortiGate_60E_Series"
1.3.3 .16	min. počet nových session/sec – 30.000	ANO	viz. "Datový list - FortiGate_60E_Series"
1.3.3 .17	min. propustnost IPSEC VPN – 2 Gbps	ANO	viz. "Datový list - FortiGate_60E_Series"
1.3.3 .18	min. propustnost při současně zapnutých funkcích FW, IPS, APP Control a Malware protection = threat protection = 200 Mbps	ANO	viz. "Datový list - FortiGate_60E_Series"
1.3.4	Cílový stav topologie a příslušenství		
1.3.4 .1	Všechny dodávané a implementované prvky musí být vybaveny komunikačními transceivery, kabely a DAC kabely tak, aby bylo možné nasazené prostředí plně propojit dle cílového schématu (kapitola 1.3.4, Příloha č. 1 - Podrobné vymezení díla).	ANO	Všechny dodávané a implementované prvky v rámci nabízeného řešení, jsou vybaveny komunikačními transceivery, kabely a DAC kabely tak, aby bylo možné nasazené prostředí plně propojit dle cílového schématu (kapitola 1.3.4, Příloha č. 1 - Podrobné vymezení díla).
1.3.5	Požadovaná implementace a integrace		
1.3.5 .1	Integrace do provozovaného SIEM řešení.	ANO	Konfigurací dle výstupu Prováděcího projektu
1.3.5 .2	Vzájemná integrace s technologií Policy Enforceru (bod 4).	ANO	Konfigurací dle výstupu Prováděcího projektu
1.3.5 .3	Kvalifikované seznámení obsluhy v rozsahu min. 1 MD.	ANO	Dle Plánu kvalifikovaného seznámení uživatelů a administrátorů s dodaným dílem, který je požadován jako součást Prováděcího projektu
2.	Nasazení mailové brány (GW) pro zajištění podpory ochrany příchozí i odchozí mailové komunikace KU proti pokročilým hrozbám		
2.1	2.1 MailGW – základní funkce a vlastnosti		
2.1.1	Implementace jako vApp/VM do prostředí TC KÚZK nebo součástí HW NGFW (bod 1.1.1).	ANO	Implementace vApp do virtualizačního prostředí TC KÚZK
2.1.2	Dodaná licence umožní provoz dvou MailGW vApp/VM instancí za účelem rozložení SMTP zátěže a failoveru.	ANO	Nabízené řešení obsahuje licenčně dvě vApp mailové brány
2.1.3	Kontrola příchozí i odchozí emailové komunikace s nastavením separátních akcí pro oba směry zahrnující: - spam, - vir, - malware (adware, grayware, spyware, fishing atd.), - content filtering, - integrace se SandBoxem (bod 1.1.2).	ANO	Konfigurací dle výstupu Prováděcího projektu
2.1.4	Aktivní část řešení pro uživatele a administrátory je přístupná přes grafické komunikační rozhraní v podobě HTTPS aplikace.	ANO	viz. "FortiMail-6.0.1.-Administration-Guide"
2.1.5	Možnost více e-mailových domén.	ANO	viz. "Datový list - FortiMail"
2.1.6	Podpora adresních prostorů IPv4 a IPv6.	ANO	viz. "Datový list - FortiMail"

2.1.7	Podpora ověřování SMTP adres přes: - LDAPS nebo MS AD; - RADIUS; - volitelně POP3 a IMAP.	ANO	viz. "Datový list - FortiMail"
2.1.8	Směrování a kontrola e-mailu pomocí LDAP.	ANO	viz. "Datový list - FortiMail"
2.1.9	Řízení fronty zpráv.	ANO	viz. "Datový list - FortiMail"
2.1.10	Plně kompatibilní podle RFC pro e-mail a MS Exchange server.	ANO	viz. "Datový list - FortiMail"
2.1.11	Možnost vytvoření administrátorských účtů s definováním administrátorských rolí.	ANO	viz. "Datový list - FortiMail"
2.1.12	Vestavěná funkce pro komplexní reporting (message queue size, system resources, health monitoring, incidenty, atd.).	ANO	viz. "Datový list - FortiMail"
2.1.13	Centralizovaná karanténa pro rozsáhlé implementace, zahrnující minimálně: - Možnost nastavení časové retence zpráv v karanténě nebo po dosažení velikosti obsahu karanténní složky s automatickým promazáváním starých zpráv. - Automatická emailová notifikace uživatelům při zachycení emailové zprávy do karantény. - Možnost přístupu do karantény jednotlivým uživatelům po přihlášení přes SSO nebo unikátní HTTPS odkaz. - Možnost jednoduchých operací nad zachycenými zprávami v uživatelské karanténě (náhled, smazání, uvolnění).	ANO	viz. "FortiMail-6.0.1.-Administration-Guide"
2.1.14	Možnost nahrání vlastního SSL certifikátu za účelem bezpečného HTTPS přístupu do Administrátorské nebo uživatelské konzole.	ANO	viz. "Datový list - FortiMail"
2.1.15	Podpora SNMP s využitím standardních a privátních MIB se zasíláním trapů při dosažení hraničních úrovní.	ANO	viz. "Datový list - FortiMail"
2.1.16	Podpora lokálního nebo externího ukládacího serveru včetně zařízení iSCSI.	ANO	viz. "Datový list - FortiMail"
2.1.17	Podpora pro externí Syslog.	ANO	viz. "Datový list - FortiMail"
2.1.18	Možnost komplexního vyhledávání v historii emailové komunikace minimálně na základě následujících parametrů: Odesílatel, Příjemce, Předmět, Čas.	ANO	viz. "FortiMail-6.0.1.-Administration-Guide"
2.2	Ochrana proti spamu		
2.2.1	Ochrana proti spamovým epidemiím v reálném čase.	ANO	viz. "Datový list - FortiMail"
2.2.2	Identifikátory URI zdrojových e-mailových adres spamu a phishingu.	ANO	viz. "Datový list - FortiMail"
2.2.3	Možnost využití nástroje pro filtrování URL.	ANO	viz. "Datový list - FortiMail"
2.2.4	Dočasné blokování (greylisting) IPv4 a IPv6 adres a e-mailových účtů.	ANO	viz. "Datový list - FortiMail"
2.2.5	Reputace lokálních odesílatelů (podle IPv4, IPv6 a ID koncového bodu).	ANO	viz. "Datový list - FortiMail"
2.2.6	Hlubková inspekce hlaviček e-mailových zpráv, kde na základě specifické hodnoty hlavičky provedení akce, a to minimálně: - zadržení emailu v karanténě; - smazání emailů.	ANO	viz. "Datový list - FortiMail"

2.2.7	Integrace s externími seznamy identifikátorů spamu (URI) a reálnými seznamy nežádoucích entit (SURBL/RBL).	ANO	viz. "Datový list - FortiMail"
2.2.8	Detekce newsletterů/marketing emailů.	ANO	viz. "Datový list - FortiMail"
2.2.9	Administrátorem definovatelné seznamy nežádoucích a povolených entit: - globální – IPv4 a IPv6 adresy; - doménové – všechny adresy z dané domény; - uživatel / adresa – konkrétní adresa z dané domény.	ANO	viz. "FortiMail-6.0.1.-Administration-Guide"
2.2.10	Podpora podnikových standardů pro identitu odesílatele: - validační systém Sender Policy Framework (SPF); - elektronický podpis hlaviček Domain Keys Identified Mail (DKIM); - validace pomocí Domain-Based Message Authentication (DMARC).	ANO	viz. "Datový list - FortiMail"
2.2.11	Práce se spam e-maily v rámci centralizované karantény.	ANO	viz. "Datový list - FortiMail"
2.2.12	Flexibilní profily akcí a upozornění.	ANO	viz. "Datový list - FortiMail"
2.3	Minimální výkonnostní a systémové požadavky řešení		
2.3.1	Výkon (zpráva/h) bez řazení do fronty, zprávy o velikosti 100 KB Směrování e-mailu: 3000 Antispam: 2400 Antispam + Antivirus: 2000	ANO	viz. "Datový list - FortiMail"
2.3.2	Konfigurované domény: 5	ANO	viz. "Datový list - FortiMail"
2.3.3	Pravidla podle příjemců (na doménu / na systém) – příchozí nebo odchozí: 60 / 300	ANO	viz. "Datový list - FortiMail"
2.3.4	Antispam, antivirus, ověřování a profily obsahu (na doménu / na systém: 50 / 60	ANO	viz. "Datový list - FortiMail"
2.3.5	Pro chod VApp/VM v prostředí TCK KÚZK bude možnost vyhrazení HW prostředků s následující charakteristikou: počet podporovaných vCPU: 2 počet virtuálních NIC: 2 velikost úložiště virtuálního stroje: 500 GB velikost operační paměti virtuálního stroje: 6 GB	ANO	Nabídnuté vyhrazené prostředky TC KÚZK využijeme v rámci našeho nabízeného řešení. Jejich přesnou dimenzaci určí až Prováděcí projekt.
2.4	Požadovaná implementace a integrace		
2.4.1	Integrace s technologií SandBoxu (bod 1.1.2).	ANO	Konfigurací dle výstupu Prováděcího projektu
2.4.2	Integrace do provozovaného SIEM řešení.	ANO	Konfigurací dle výstupu Prováděcího projektu
2.4.3	Kvalifikované seznámení obsluhy v rozsahu min. 0,5 MD.	ANO	Dle Plánu kvalifikovaného seznámení uživatelů a administrátorů s dodaným dílem, který je požadován jako součást Prováděcího projektu
3.	Modernizace SW ochrany "operačních systémů klientských a serverových zařízení" pro zajištění podpory ochrany proti pokročilým hrozbám		

3.1	SW ochrana – základní funkce a vlastnosti		
3.1.1	Požadované množstevní pokrytí: - OS MS Windows Serverů (2008,2012,2016) – 120 ks; - OS NonWindows Serverů (linux, unix atd.) – 30 ks; - OS PC a notebooků (MS Win7, 10) – 493 ks; - OS Mobilních platforem (Android, iOS...) – 250 ks.	ANO	bude dosaženo odpovídajícím počtem licencí
3.1.2	Centrální konzole pro správu AV řešení na stanicích a serverech.	ANO	Instalace Kaspersky Security Centra viz https://help.kaspersky.com/KSC/SP3/en-US/5022.htm
3.1.3	Centrální konzole pro správu AV řešení na mobilních zařízeních (android, iOS...).	ANO	je součástí Kaspersky Security Centra
3.1.4	Zabezpečení koncových stanic a serverů		
3.1.4.1	Pokročilá ochrana stanic a serverů: - Intrusion Prevention na úrovni stanice; - ochrana před síťovými hrozbami – ochrana prohlížeče, ochrana před přístupem na škodlivé destinace, botnet ochrana a ochrana před vzdáleným napadnutím; - rootkit ochrana; - detekce a blokace podezřelého chování (heuristika) i neznámých verzí škodlivého kódu (zero hour/zero day) a ransomware.	ANO	bude splněno pomocí modulů Host Intrusion Prevention, Web Threat Protection, Network Attack Blocker, Behavior Detection ,Rootkit Scan viz https://help.kaspersky.com/KESWin/11/en-US/127968.htm
3.1.4.2	Zakázání spuštění aplikací minimálně pomocí následujících parametrů: - file path; - názvu aplikace nebo aplikačního souboru.	ANO	bude splněno pomocí Application Startup Control https://help.kaspersky.com/KESWin/11/en-US/130540.htm , Application Launch Control https://docs.s.kaspersky-labs.com/english/ks4ws_admin_guide_en.pdf str 31, tab. 3
3.1.4.3	Kontrola a blokace přístupu k periferiím: - zamezení používání USB flash disků mimo Objednatelem centrálně povolené výjimky; - zamezení používání CD-DVD mimo Objednatelem centrálně povolené výjimky; - zamezení používání neschválené třídy zařízení nebo konkrétního zařízení, např. rozeznávání Class i Device ID.	ANO	řešeno pomocí Device Control https://help.kaspersky.com/KESWin/11/en-US/34890.htm https://docs.s.kaspersky-labs.com/english/ks4ws_admin_guide_en.pdf str 31, tab. 3
3.1.4.4	Kontrola a blokace přístupu na web - Mmožnost vytvoření centrálních blacklistů webových stránek a serverů.	ANO	splněno prostřednictvím modulu Web Control https://help.kaspersky.com/KESWin/11/en-US/128048.htm a Traffic Security https://docs.s.kaspersky-labs.com/english/ks4ws_admin_guide_en.pdf str 31, tab. 3
3.1.4.5	Karanténa: - možnost obnovy souboru do originální lokality; - automatické mazání souborů v karanténě starších než zadaná doba stáří.	ANO	základní funkce Kaspersky Security Centra https://help.kaspersky.com/KESWin/11/en-US/128132.htm
3.1.4.6	Plánované skenování, možnost definování spuštění naplánovaného testu v časovém intervalu.	ANO	pomocí naplánovaných úloh

3.1.4.7	Modul Firewallu pro koncové stanice: - Možnost vytváření Firewallových pravidel na základě připojeného média (WiFi, kabel) nebo přiřazené adresy (subnet). - Možnost vypnutí Windows firewallu.	ANO	splněno pomocí Firewall modulu https://help.kaspersky.com/KESWin/11/en-US/43497.htm
3.1.4.8	Funkcionalita „tiché“ vzdálené instalace na koncové stanice včetně bezobslužné konfigurace.	ANO	základní funkcionalita Kaspersky Security Centra https://help.kaspersky.com/KSC/SP3/en-US/6374.htm
3.1.5	Zabezpečení mobilních zařízení:		
3.1.5.1	Podporované platformy: - Android Lollipop 5.1 a vyšší; - iOS 10 a vyšší.	ANO	Kompatibilita zaručena dle https://help.kaspersky.com/KESMob/10SP4/en-US/102017.htm
3.1.5.2	Anti-Theft funkce: - Remote-Lock; - Remote-Wipe; - lokace; - ochrana programu heslem před změnou nastavení Anti-Theft a odinstalováním.	ANO	splněno pomocí základních funkcí řešení https://help.kaspersky.com/KESMob/10SP4/en-US/89902.htm
3.1.5.3	Detekce nejnovějších hrozeb v reálném čase.	ANO	splněno pomocí real-time protection a cloudové ochrany KSN http://ksn.kaspersky.com
3.1.5.4	Aplikace nesmí výrazně ovlivnit životnost baterie, nezpomalí systém a negeneruje moc velký síťový provoz.	ANO	dosaženo by design a možností plánování update tasků
3.1.6	Automatická a efektivní aktualizace definic na koncových zařízeních.	ANO	dosaženo by design, možnost optimalizace vytížení sítě dle časových oken, možnost více distribučních bodů
3.1.7	Implementace centrální části jako vApp/VM do prostředí TC KÚZK.	ANO	Centrální část lze instalovat na VM, popř. provést jako deployment hotového vhd
3.1.8	Pro chod VApp/VM v prostředí TCK KÚZK bude možnost vyhrazení HW prostředků s následující charakteristikou: - počet podporovaných vCPU: 2 - počet virtuálních NIC: 2 - velikost úložiště virtuálního stroje: 300 GB - velikost operační paměti virtuálního stroje: 8 GB - velikost databáze na sdíleném MS SQL 2014/2016 řešení KÚZK: 10 GB	ANO	zadané HW prostředky vyhovují HW požadavkům pro instalaci centrální části https://help.kaspersky.com/KSC/SP3/en-US/96255.htm
3.2	Požadovaná implementace a integrace		
3.2.1	Integrace do MS AD KÚZK.	ANO	Integrace s AD je přímo součástí instalační procedury
3.2.2	Integrace do provozovaného SIEMU KÚZK.	ANO	Integrace do SIEMu je podporována přímo v centrální správě https://help.kaspersky.com/KSC/SP3/en-US/151331.htm
3.2.3	Integrace do řešení Adaptivního řízení přístupu (bod 4).	ANO	bude dosaženo dle zadání zákazníka
3.2.4	Instalace a konfigurace řídicí konzole, serverů a centrálních komponent navrhovaného řešení dle Prováděcího projektu včetně návrhu řešení.	ANO	bude splněno certifikovaným pracovníkem Dodavatele
3.2.5	Zpracování podrobného plánu nasazení nového AV do celého prostředí KÚZK (viz množství pokrytí) včetně komplexního nastavení funkčnosti v KÚZK.	ANO	bude splněno certifikovaným pracovníkem Dodavatele

3.2.6	V rámci možností přichystání automatizované odinstalace stávajícího antivirového řešení z klientských stanic a serverů.	ANO	bude splněno pomocí funkce centrální správy https://help.kaspersky.com/KSC/SP3/en-US/92468_1.htm , popř. pracovníkem dodavatele
3.2.7	Automatizovaná instalace navrhovaného řešení na 2 zařízení každého jmenovaného OS: - MS Windows 7 a Windows 10 Enterprise CZ; - MS Windows Server 2012 R2 a Windows Server 2016; - Android, iOS; - V případě dodání stejného produktu nebude požadována reinstalace ale hloubková revize stávajících politik a současného nasazení, úpravy v návaznosti na Adaptivní řízení přístupu (bod 4).	ANO	bude splněno certifikovaným pracovníkem Dodavatele
3.2.8	Implementace metodik a pracovních postupů.	ANO	bude splněno certifikovaným pracovníkem Dodavatele
3.2.9	Kvalifikované seznámení obsluhy v rozsahu min. 0,5 MD.	ANO	bude splněno certifikovaným pracovníkem Dodavatele
3.2.10	V případě dodání stejného produktu používaného Objednatelem (bližší popis může být poskytnut na vyžádání): - nebude požadována reinstalace, - nebude požadována integrace do MS AD a SIEM KÚZK, - nebude požadováno zpracování plánu nasazení, - nebude požadována implementace metodik a pracovních postupů, - nebude požadováno kvalifikované seznámení obsluhy, - bude požadována hloubková revize stávajících politik a současného nasazení, - budou požadovány úpravy v návaznosti na Adaptivní řízení přístupu (kapitola 4).	ANO	dodáváme jiný produkt
4.	Zavedení dynamického, adaptivního řízení přístupu uživatelů a zařízení ke komunikačnímu systému lokální počítačové sítě LAN KÚZK.		
4.1	Security Enforcer – základní funkce a vlastnosti		
4.1.1	On premise řešení pro externí captive portál pro hosty a jejich rozšířenou autentizaci a pro BYOD.	ANO	HW nebo virtual appliance Viz https://www.arubanetworks.com/assets/ds/DS_ClearPass_PolicyManager.pdf strana 3
4.1.2	Implementace jako vApp/VM do prostředí TC KÚZK.	ANO	Virtual Appliance https://www.arubanetworks.com/assets/ds/DS_ClearPass_PolicyManager.pdf strana 3
4.1.3	802.1X autentizace pro WiFi, Ethernet LAN sítě a VPN.	ANO	802.1X https://www.arubanetworks.com/assets/ds/DS_ClearPass_PolicyManager.pdf strana 3
4.1.4	Podpora minimálně pro 1500 autentizovaných zařízení (pomocí 802.1X) s možností navýšení počtu.	ANO	1500 autentizovaných zařízení viz rozpočet a https://www.arubanetworks.com/assets/ds/DS_ClearPass_PolicyManager.pdf strana 5

	Podpora klastrování pro vysokou dostupnost pro všechny funkcionality řešení.	ANO	viz https://www.arubanetworks.com/assets/ds/DS_ClearPass_PolicyManager.pdf strana 1
4.1.5	Podpora následujících metod autentizace: PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace.	ANO	viz https://www.arubanetworks.com/assets/ds/DS_ClearPass_PolicyManager.pdf strana 3
4.1.6	Podpora TACACS+ autentizace správců síťových zařízení.	ANO	viz https://www.arubanetworks.com/assets/ds/DS_ClearPass_PolicyManager.pdf strana 3
4.1.7	Podpora dalších možností autentizace a autorizace: LDAP, MS AD, Token, MAC auth, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta).	ANO	viz https://www.arubanetworks.com/assets/ds/DS_ClearPass_PolicyManager.pdf strana 1
4.1.8	Možnost provozovat více graficky i obsahově unikátních portálů v rámci jedné instalace.	ANO	viz https://www.arubanetworks.com/assets/ds/DS_ClearPass_PolicyManager.pdf strana 1
4.1.9	Redakční systém pro plnou grafickou a obsahovou úpravu jednotlivých captive portálů: - Úprava barev, fontů, pozadí a loga. - Úprava registračních formulářů – přidávání a odebírání polí pro vstupní data formuláře včetně validace vkládaného obsahu. - Možnost vkládání animací a videí. - Vytváření specifických stránek pro různé typy zařízení a operačních systémů (např. pro efektivní navedení do specifického app store).	ANO	Viz http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c05323976-1.pdf strana 183
4.1.10	Samoobslužný Captive portal pro řízení přístupu hostů: - Registrace a přihlášení s nutností zadání a ověření telefonického čísla (SMS). - Přístup zdarma pouze s akceptací podmínek užití. - Tarify lze omezit časově, z hlediska rychlosti připojení či objemu přenesených dat. - Vynucení odpojení zařízení ihned po naplnění jakéhokoliv z limitů. - Podpora autentizace lokálními účty v rámci portálu. - Podpora autentizace pomocí sociálních sítí – Google, Google Plus, Facebook, Facebook WIFI, Twitter, LinkedIn, Microsoft. - Perzistence autentizace/registrace skrze MAC caching a zobrazení už jen uvítacích stránek s osobním oslovením hosta při dalších návštěvách. - Vytváření účtů samoobslužnou registrací. - Průměrný počet ověřených unikátních hostů/pracovní den = 1000.	ANO	Viz http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c05323976-1.pdf strana 222
4.1.12	Sběr dodatečných informací o připojených zařízeních ("profiling") jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě.	ANO	viz https://www.arubanetworks.com/assets/ds/DS_ClearPass_PolicyManager.pdf strana 3

4.1.1 3	Samoobslužný BYOD portal pro Onboarding koncových zařízení: - Přihlášení s nutností zadání AD jména hesla + následná registrace zařízení. - Portál umožňuje vydávat certifikáty, funguje jako certifikační autorita a jednoduchý způsob importu certifikátů do zařízení. - Automatické profilování zařízení. - Celkový počet unikátních onboardovaných zařízení = 1000.	ANO	viz http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c05323976-1.pdf strana 69
4.1.1 4	Podpora ochrany koncových zařízení formou posture assessments a health checks.	ANO	viz https://www.arubanetworks.com/assets/ds/DS_ClearPass_PolicyManager.pdf strana 2
4.1.1 5	Podpora software (NAC agenta) pro MS Windows 7 a vyšší, Mac OS X 10.7 a vyšší, RHEL 4 a vyšší, Ubuntu 12.x a vyšší.	ANO	viz https://www.arubanetworks.com/assets/ds/DS_ClearPass_OnGuard.pdf strana 1
4.1.1 6	Kontrola stavu koncového zařízení na přítomnost aktuálního antiviru.	ANO	viz https://www.arubanetworks.com/assets/ds/DS_ClearPass_OnGuard.pdf strana 1
4.1.1 7	NAC formou permanentního nebo dočasného SW agenta.	ANO	viz https://www.arubanetworks.com/assets/ds/DS_ClearPass_OnGuard.pdf strana 1
4.1.1 8	NAC podporuje v návaznosti na autentizační proces kontrolu systémových procesů, aplikací, klíčů registru, použití USB zařízení, přítomnost anti-viru, firewallu.	ANO	viz https://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/Content/CPPM_UserGuide/Posture/CPWindowsUnivSystemHealthVal.htm#WinUnivSysHVpage
4.1.1 9	Pro chod VApp/VM v prostředí TCK KÚZK bude možnost vyhrazení HW prostředků s následující charakteristikou: - počet podporovaných vCPU: 4 - počet virtuálních NIC: 2 - velikost úložiště virtuálního stroje: 300 GB - velikost operační paměti virtuálního stroje: 24 GB - velikost databáze na sdíleném MS SQL 2014/2016 řešení KÚZK: 10 GB	ANO	dle zadání
4.2	Požadovaná implementace a integrace		
4.2.1	Integrace do MS Active Directory KÚZK.	ANO	integrace bude provedena
4.2.2	Integrace do provozovaného SIEM KÚZK.	ANO	integrace bude provedena
4.2.3	Integrace do řešení KS LAN KÚZK (bod 1).	ANO	integrace bude provedena
4.2.4	Kvalifikované seznámení obsluhy v rozsahu min. 1 MD.	ANO	školení 1MD
5.	Požadované služby		
5.1	Služby v rámci dodávky		
5.1.1	Projektové řízení dodávky řešení.	ANO	projektovým managerem
5.1.2	Zpracování návrhu řešení implementace jednotlivých částí – Prováděcí projekt včetně návrhu řešení specifikovaný v Příloze č. 3 Povinná struktura Prováděcího projektu včetně návrhu řešení.	ANO	dle zadání
5.1.3	Dodávka, implementace, instalace, zapojení a konfigurace všech částí dle Prováděcího projektu včetně návrhu řešení.	ANO	dle zadání a prováděcího projektu
5.1.4	Vytvoření a předání Objednateli zálohy konfigurace.	ANO	zálohy konfigurace provedeme dle prováděcího projektu

5.1.5	Ověření funkčnosti dodaného řešení a jeho částí.	ANO	provedeme dle prováděcího projektu
5.1.6	Dodávka dokumentace dodaného vybavení a jeho částí.	ANO	provedeme dle prováděcího projektu
5.1.7	Kvalifikované seznámení uživatelů a administrátorů – seznámení s funkcionalitami, obsluhou dodávaného řešení a jeho budoucím provozem.	ANO	dle zadání
5.1.8	Provedení zkušebního provozu.	ANO	viz fáze 3
5.2	Podpora provozu		
5.2.1	Poskytnutí podpory provozu díla min. 66 měsíců.	ANO	66 měsíců
5.2.2	Požadavek na servisní zásah může být Objednatelem uplatněn: - systémem helpdesk na adrese upřesněné Zhotovitelem (Zhotovitel je povinen zpřístupnit svůj helpdesk Objednateli nejpozději v průběhu fáze 2.) - e-mailem na adrese upřesněné Zhotovitelem, pokud není možno použít helpdesk, Zhotovitel požadavek do helpdesku dodatečně doplní - telefonem na čísle upřesněné Zhotovitelem, pokud není možno použít helpdesk, Zhotovitel požadavek do helpdesku dodatečně doplní	ANO	dle zadání
5.2.3	Systém helpdesk musí zajistit: - jednoduché a pohodlné vkládání požadavků uživatelem podle jeho oprávnění - seznam všech hlášených požadavků s historií a aktuálním stavem řešení a řešitelem - e-mailové notifikace při změně stavu řešení požadavku - možnost nastavení priorit řešení - přístup k aplikaci přes webový prohlížeč 24 hodin denně – bez nákladů na software pro Objednatele	ANO	dle zadání
5.2.4	Smluvní podpora díla zahrnuje především následující:		
5.2.4 .1	Odstranění nedostatků implementace zjištěných ve fázi 3 uvedené ve smlouvě o dílo.	ANO	dle zadání a smlouvy
5.2.4 .2	Odstraňování závad HW: Režim odstraňování závad 8x5 NBD pro: NGFW, Přístupový přepínač 48p, Agregáčn ^í přepínač, CORE přepínač, WIFI AP, CORE Router Režim odstraňování závad 24x7 ND pro: Firewall uzlových bodů 21NET, PE MPLS přepínač 21NET Režim odstraňování závad 8x5 NBD ostatní HW Režim odstraňování závad 8x5 NBD znamená: - začátek řešení nejpozději následující pracovní den; - oprava nebo výměna HW nejpozději do 5 pracovních dnů v místě instalace; - garantovaná záruka 8x5 NBD od výrobce. Režim odstraňování závad 24x7 ND znamená: - oprava nebo výměna HW nejpozději	ANO	dle zadání a smlouvy

	<p>následující den v místě instalace; - garantovaná záruka 24x7 ND od výrobce. Režim odstraňování závad 8x5 NBD ostatní HW znamená: - začátek řešení nejpozději následující pracovní den; - oprava nebo výměna HW nejpozději do 7 pracovních dnů v místě instalace.</p> <p>Součástí opravy nebo výměny HW ve všech výše uvedených režimech nejsou činnosti popsané v bodu 5.2.6.</p>		
5.2.4 .3	Řešení závad SW v místě instalace v souladu s SLA dle čl. III, odst. 2 této přílohy.	ANO	dle zadání a smlouvy
5.2.4 .4	Podpora a subscriptions pro NGFW/UTM (AV, IPS, application control, WebFiltering) s možností prodloužení přímo u výrobce HW po skončení podpory provozu díla.	ANO	u výrobce dostupné
5.2.4 .5	Přístup k update a upgrade firmware u HW a update a upgrade u SW.	ANO	zajištěno
5.2.4 .6	Přístup k technické podpoře výrobce dodaného HW a SW.	ANO	technická podpora zajištěna
5.2.4 .7	Provoz helpdesk systému sloužícího pro evidenci veškerých požadavků na podporu a reporting řešení závad a požadavků za fakturační období.	ANO	zajištěno

5.2.5	<p>Specifikace požadovaných služeb (SLA), které je zhotovitel povinen zajistit: Závady a požadavky jsou klasifikovány dle jejich závažnosti a provozních podmínek na tři kategorie důležitosti:</p> <p>Vysoká</p> <ul style="list-style-type: none"> - závady vylučující užívání systému nebo jeho důležité a ucelené části (tj. problémy zabraňující provozu systému), provoz systému je zastaven. - požadavky vysoké priority řešení, zejména ohrožující provoz nebo bezpečnost díla či jeho částí - potvrzení o přijetí závad a požadavků do 1 hodiny - max. doba do vyřešení závad a požadavků od nahlášení do 1 pracovního dne* <p>Střední</p> <ul style="list-style-type: none"> - závady způsobující problémy při užívání a provozování systému nebo jeho části, ale umožňující provoz systému. Provoz systému je omezen, ale činnosti mohou pokračovat určitou dobu náhradním způsobem. - požadavky střední priority řešení - potvrzení o přijetí závad a požadavků do 1 hodiny - max. doba do vyřešení závad a požadavků od nahlášení do 3 pracovních dnů* <p>Nízká</p> <ul style="list-style-type: none"> - provoz systému je závadou ovlivněn, ale může pokračovat jiným způsobem, např. organizačními opatřeními. - ostatní požadavky - potvrzení o přijetí závad a požadavků do 1 hodiny - max. doba do vyřešení závad a požadavků od nahlášení do 5 pracovních dnů* <p>Řešení závad a požadavků probíhá v režimu 8 x 5 tj. v pracovní dny od 8:00 do 16:00. *pracovním dnem se rozumí doba od 8.00 do 16.00 hodin v pracovní dny pondělí až pátek (mimo víkendy a svátky platné v České republice), přičemž platí, že max. doba vyřešení závad a požadavků se počítá od hodiny nahlášení závady či požadavku.</p>	ANO	dle zadání a smlouvy
5.2.6	<p>Od začátku fáze 4 - podpora díla po dobu prvních 6 měsíců jsou poskytovány v souladu s SLA dle bodu 5.2.5 ještě navíc následující služby:</p>		
5.2.6.1	<p>správa, monitoring a proaktivní podpora díla; - proaktivní podporou se rozumí řešení závad ihned po zjištění bez nutnosti nahlášení Objednatelem; - maximální doba do vyřešení závad a požadavků od nahlášení se může prodloužit o čas potřebný pro uplatnění záruky dle režimu v bodu 5.2.4.2</p>	ANO	dle zadání a smlouvy

5.2.6 .2	změna konfigurace dodaného HW a SW;	ANO	Případné změny konfigurace budou prováděny v míře definované prováděcím projektem
5.2.6 .3	instalace upgrade a update;	ANO	dle zadání a smlouvy
5.2.6 .4	konzultace.	ANO	dle zadání a smlouvy
5.2.6 .5	Předpokládaný počet požadavků spadající pod body 5.2.6.2, 5.2.6.3 a 5.2.6.4 je 20 za měsíc.	ANO	viz. zadávací dokumentace a Vysvětlení zadávací dokumentace č. 8, 20 požadavků odpovídá 30-ti hodinám odborných seniorských prací za měsíc
5.3	Dokumentace		
5.3.1	V rámci plnění bude dodána zhotovitelem kompletní dokumentace řešení (dokumentace může být jedním dokumentem, nicméně musí obsahovat všechny relevantní informace) obsahující minimálně:	ANO	dle zadání
5.3.2	Podrobná systémová a bezpečnostní dokumentace (administrátorská dokumentace) v českém jazyce: - popis skutečného provedení řešení min. ve struktuře dle Prováděcího projektu včetně návrhu řešení; - princip aktualizace; - seznam licencí.	ANO	dle zadání
5.3.3	Kompletní provozní dokumentace ke všem částem v českém nebo anglickém jazyce.	ANO	dle zadání